# Configuración de la comunicación segura entre Finesse y el servidor CTI

## Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Configurar Servidor CCE CTI seguro Configuración segura de Finesse Generar certificado PG de agente (servidor CTI) Obtenga el certificado CSR firmado por una CA Importar certificados firmados por CA de CCE PGs Generar certificado Finesse Firmar certificado Finesse por una CA Importar la aplicación Finesse y los certificados firmados raíz Verificación Troubleshoot

## Introducción

Este documento describe cómo implementar certificados firmados por la Autoridad de Certificación (CA) entre Cisco Finesse y Computer Telephony Integration (CTI) Server en la solución Cisco Contact Center Enterprise (CCE).

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CCE versión 12.0(1)
- Versión 12.0(1) de Finesse
- CTI Server

### **Componentes Utilizados**

La información que contiene este documento se basa en estas versiones de software:

• 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

En la versión 11.5 de CCE, Cisco inició la compatibilidad con la versión 1.2 de seguridad de la capa de transporte (TLS), que permite que los mensajes de protocolo de inicio de sesión (SIP) y protocolo de transporte en tiempo real (RTP) se transporten de forma segura a través de TLS 1.2. Desde CCE 12.0 y como parte de la protección de los datos en movimiento, Cisco comenzó a admitir TLS 1.2 en la mayoría de los flujos de llamadas del centro de contacto: Voz entrante y saliente, multicanal y base de datos externa. El objetivo de este documento es la voz entrante, especialmente la comunicación entre Finesse y el servidor CTI.

El servidor CTI admite estos modos de conexión:

- Conexión Sólo Segura: Permite la conexión segura entre el servidor CTI y los clientes CTI (Finesse, dialer, CTIOS y ctitest).
- Conexión segura y no segura (modo mixto): Permite la seguridad, así como la conexión no segura entre el servidor CTI y los clientes CTI. Éste es el modo de conexión predeterminado. Este modo se configurará cuando actualice versiones anteriores a CCE 12.0(1).

Nota: No se admite el modo de sólo seguridad.

## Configurar

### Servidor CCE CTI seguro

Paso 1. En la estación de trabajo administrativa PCCE (AW), abra la carpeta **Herramientas de Unified CCE** y haga doble clic en **Configuración de gateway periférico**.



Paso 2. Seleccione CG3A y haga clic en Editar.

Cisco Unified ICM/Contact Ce	nter Enterprise Components Setup
ICM Instances Add Edit Delete To set up Administration Data Server (D Interface Controller (NIC), WebView or N Web Setup tool. To set up Administration Client (Client A) and Setup tool. The Instance cc cannot be deleted bec Web Setup or Administration Client (Setu to remove those components before del Setup.	Instance Components Add PG1A PG2A PG3A RoutesA PG3A, RoutesA PG3A, RoutesA PG3A, RoutesA PG3A, RoutesA PG3A, RoutesA Delete Delete W], use the Administration Client Installer cause it has components set up by the up tool. You must use the applicable tool leting the instance in Peripheral Gateway
	Help Exit Setup

Paso 3. En las propiedades del servidor CTI, haga clic en **Next**. En la pregunta sobre la configuración que detiene el servicio **CG3A**, seleccione **Yes**.

Paso 4. En **CTI Server Components Properties**, seleccione **Enable Secured-only mode**. Observe el **Puerto de conexión seguro (46030)**, ya que debe configurar el mismo puerto en Finesse en el ejercicio siguiente. Haga clic en Next (Siguiente).

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 comunicación segura predeterminada es 42030; sin embargo, el laboratorio utilizado para este documento es 40630. El número de puerto es parte de una fórmula que incluye el ID del sistema ICM. Cuando el ID del sistema es 1 (CG1a), el número de puerto predeterminado, en general, es 42030. Dado que la ID del sistema en el laboratorio es 3 (CG3a), el número de puerto predeterminado es 46030.

Paso 5. En **CTI Network Interface Properties**, haga clic en **Next**. Compruebe la **información de configuración** y haga clic en **Siguiente**.

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

Paso 6. Haga clic en **Finalizar** como se muestra en la imagen.

Unifie	ed ICM/CCE PGSetup: cc-CG3A
J.	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

Paso 7. Haga clic en **Salir de la configuración** y espere hasta que la ventana de configuración se cierre como se muestra en la imagen.

ICM Instances	Instance Compor	ents
ce /	Add CG3A	Add
	LoggesA PG1A	
	dit PG2A	Edit
	elete PG3A	Delete
To set up Administration D+ nterface Controller (NIC), V //eb Setup tool.	ka Server (Distributor AW), Router /ebView or Network Gateway con	, Logger, Network aponents, use the
To set up Administration Da Interface Controller (NIIC), V Web Setup tool. To set up Administration Cli and Setup tool.	ita Server (Distributor AW), Router /ebView or Network Gateway con ent (Client AW), use the Administra	, Logger, Network aponents, use the ation Client Installer
To set up Administration D4 Interface Controller (NIC), V Web Setup tool. To set up Administration Cli and Setup tool. The Instance cc cannot be Web Setup or Administration o remove those component	Aa Server (Distributor AW), Router /ebView or Network Gateway con ent (Client AW), use the Administra deleted because it has compone in Client Setup tool, You must use it before deleting the instruce in I	Logger, Network apponents, use the stion Client Installer Ints set up by the the applicable tool Perioheral Gateway
To set up Administration De nterface Controller (NIC), V Web Setup tool. To set up Administration Cli and Setup tool. The Instance cc cannot be Web Setup or Administratio o remove those componen Setup.	Ita Server (Distributor AW), Router VebView or Network Gateway con ent (Client AW), use the Administra deleted because it has compone in Client Setup tool. You must use its before deleting the instance in f	, Logger, Network aponents, use the ation Client Installer Ints set up by the the applicable tool Peripheral Gateway

Paso 8. En el escritorio PCCEAllin1, haga doble clic en Unified CCE service Control.

Paso 9. Seleccione Cisco ICM cc CG3A y haga clic en Inicio.

#### Configuración segura de Finesse

Paso 1. Abra un navegador web y navegue hasta Administración de Finesse.

Paso 2. Desplácese hacia abajo hasta la sección **Configuración del servidor CTI de Contact Center Enterprise** como se muestra en la imagen.

Contact Center Ent	erprise CTI Server S	lettings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget se CTI Server Settings	require a restart of Cisco Finesse Tomcat to t	ake 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 Reve	rt 🗌		

Paso 3. Cambie el puerto lateral A para el puerto de comunicación segura configurado en CG3A en el ejercicio anterior: **46030.** Marque **Enable SSL encryption** y haga clic en **Save**.

Contact Center Ent	erprise CTI Server S	Settings	
Note: Any changes made to Contact Center Enterpris	o the settings on this gadget se CTI Server Settings	t require 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**: Para probar la conexión, primero debe reiniciar el servicio Finesse Tomcat o reiniciar el servidor Finesse.

Paso 4. Cierre sesión en la página Administración de Finesse.

Paso 5. Abra una sesión SSH con Finesse.

Paso 6. En la sesión FINESSEA SSH, ejecute el comando:

#### utils system restart

Ingrese **yes** cuando se le pregunte si desea reiniciar el sistema.

```
<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...
```

#### Generar certificado PG de agente (servidor CTI)

CiscoCertUtils es una nueva herramienta lanzada en la versión 12 de CCE. Utilice esta herramienta para administrar todos los certificados CCE de voz entrante. En este documento,

usted utiliza estas CiscoCertUtils para generar las solicitudes de firma de certificados (CSR) de puertas de enlace periféricas (Gateways periféricos).

Paso 1. Ejecute este comando para generar un certificado CSR: CiscoUtil /generateCSR



Proporcione la información solicitada, por ejemplo:

Nombre del país: US

Nombre de estado o provincia: MA

Nombre de localidad: BXB

Nombre de la organización: Cisco

Unidad organizativa: CX

Nombre común: PCCEAllin1.cc.lab

Correo electrónico: jdoe@cc.lab

Una contraseña de desafío: Train1ng!

Nombre de la empresa opcional: Cisco

El certificado y la clave del host se almacenan en C:\icm\ssl\certs y C:\icm\ssl\keys.

Paso 2. Navegue hasta la carpeta C:\icm\ssl\certs y asegúrese de que el archivo host.csr se ha generado.

### Obtener el certificado CSR Firmado por una CA

Una vez generados los certificados CSR, deben estar firmados por una CA de terceros. En este ejercicio, la CA de Microsoft instalada en el controlador de dominio se utiliza como la CA de terceros.

Asegúrese de que la plantilla de certificado utilizada por la CA incluya la autenticación de cliente y servidor como se muestra en la imagen cuando se utiliza Microsoft CA.

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 Edk.           Extensions included in this template:	tificate Templates More Actions b Server More Actions	(DC.cc.lab)
Application Policies	An application policy def	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. Application policies:
Edk Description of Application Policies:		Any Purpose Attestation Identity Key Certificate Certificate Request Agent Elect Authentication
Server Authentication	Add	Code Signing CTL Usage Digital Right: Directory Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel Apply Help		OK Cancel

Paso 1. Abra un explorador web y navegue hasta la CA.

Paso 2. En Microsoft Active Directory Certificate Services, seleccione Solicitar un certificado.

_ O X
🗲 💿 🖉 https://dc.ec.lab/certsiv/en-us/ 🖉 🖌 🔒 🖉 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

Paso 3. Seleccione la opción 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:					_

Paso 4. En la **solicitud de certificado avanzada,** copie y pegue el contenido del certificado CSR del agente PG en el **cuadro Solicitud guardada**.

Paso 5. Seleccione la plantilla **Web Server** con autenticación de cliente y servidor. En el laboratorio, la plantilla de servidor Web CC se creó con autenticación de cliente y servidor.

To submit a sav Saved Reques	ved request to the CA, par t box.	Copy and paste the of the expected CS	contents R file
Saved Request:			_
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7lbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnH J75nKDoyAh7C+F0u9tmg26 rArT90OdxJem END CERTIFICATE R <	fqH1509jMcZ3uZrciC 5kUAZqin/56HjuGb4h k38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	<ul> <li>•</li> </ul>
Certificate Temp	ate:		
	CC Web Server	~	-
Additional Attribu	ites:		
Attributes:			-

Paso 6. Haga clic en Enviar.

Paso 7. Seleccione **Base 64 codificada** y haga clic en **Descargar certificado** como se muestra en la imagen.

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.	-	-	-	a
	-		1.1	
	v	~	-11	L.
м	1		<i>.</i> .	
	_			

Download certificate Download certificate chain

Paso 8. Guarde el archivo y haga clic en Aceptar. El archivo se guarda en la carpeta Descargas.

Paso 9. Cambie el nombre del archivo a host.cer (opcional).

Paso 10. También debe generar un certificado raíz. Vuelva a la página de certificados de CA y, a continuación, seleccione **Descargar un certificado de CA, cadena de certificados o CRL**. Solo tiene que realizar este paso una vez, ya que el certificado raíz será el mismo para todos los servidores (PG Agent y Finesse).

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>

Paso 11. Haga clic en Base 64 y seleccione Descargar certificado CA.

Microsoft Active Directory Certificate Senices - 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

Paso 12. Haga clic en Guardar archivo y seleccione **Aceptar**. El archivo se guardará en la ubicación predeterminada, **Descargas**.

### Importar certificados firmados por CA de CCE PGs

Paso 1. En el PG Agent navegue hasta **C:\icm\ssl\certs** y pegue aquí la raíz y los archivos firmados por el PG Agent.

Paso 2. Cambie el nombre del certificado host.pem en c:\icm\ssl\certs como selfhost.pem.

Paso 3. Cambie el nombre host.cer a host.pem en la carpeta c:\icm\ssl\certs .

Paso 4. Instale el certificado raíz. En el símbolo del sistema, ejecute este comando: CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



Paso 5. Instale el certificado firmado de la aplicación ejecutando el mismo comando: CiscoCertUtil /install C:\icm\ssl\certs\host.pem



Paso 6. Cicle el PG. Abra el control de servicio de Unified CCE y active el PG de Cisco ICM Agent.

### Generar certificado Finesse

Paso 1. Abra el navegador web y navegue hasta Finesse OS Admin.

Paso 2. Inicie sesión con las credenciales de administración del sistema operativo y navegue hasta **Seguridad > Administración de certificados** como se muestra en la imagen.



Paso 3. Haga clic en Generar CSR como se muestra en la imagen.



Paso 4. En la **Solicitud de firma de certificado**, utilice los valores predeterminados y haga clic en **Generar.** 

enerate Certificate S	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**	tomat v
Distribution*	FINESSEA.cc.lab
Common Name*	FINESSEA.cc.lab
Subject Alternate Nar	mes (SANs)
Parent Domain	cc.iab
Key Type**	RSA
Key Length*	2048 🗸
Hash Algorithm*	SHA256 V
Generate Close	
i . indicates require	ed item.
is RSA.	cate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it

Paso 5. Cierre la ventana Generar solicitud de firma de certificado y seleccione Descargar 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	

Paso 6. En Certificate Purpose, seleccione tomcat y haga clic en Download CSR.

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

Paso 7. Seleccione Guardar archivo y haga clic en Aceptar como se muestra en la imagen.

Opening tomcat.csr		х
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	matically for files like this from now on-	
_ bo this gotor	nationly for thesine and north for one	
	OK Cancel	

Paso 8. Cierre la ventana **Descargar solicitud de firma de certificado**. El certificado se guarda en la ubicación predeterminada **(This PC > Downloads)**.

Paso 9. Abra el Explorador de Windows y desplácese a esa carpeta. Haga clic con el botón derecho del ratón en este certificado y cámbiele el nombre: **finessetomcat.csr** 

### Firmar certificado Finesse por una CA

En esta sección, se utiliza la misma CA de Microsoft utilizada en el paso anterior que la CA de terceros.

**Nota**: Asegúrese de que la plantilla de certificado utilizada por la CA incluya la autenticación de cliente y servidor.

Paso 1. Abra un explorador web y navegue hasta la CA.

Paso 2. En <b>Microsoft Active</b>	Directory Certificate Services,	seleccione Solicitar un	certificado.
------------------------------------	---------------------------------	-------------------------	--------------

	×
🗲 💿 💋 Mtps://dc.ec.lab/certsiv/en-us/ 🔎 * 🔒 C 🧭 Microsoft Active Directory × 🕦 🏠 🖈	٥
Microsoft Active Directory Certificate Services cc-DC-CA Hoe	-
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.	1
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	
	_

Paso 3. Seleccione la opción advanced certificate request como se muestra en la imagen.



Paso 4. En la **solicitud de certificado avanzada**, copie y pegue el contenido del certificado CSR Finesse en el **cuadro Solicitud guardada**.

Paso 5. Seleccione la plantilla de servidor Web con autenticación de cliente y servidor. En este laboratorio, la plantilla de servidor Web CC se creó con autenticación de cliente y servidor.

Microsoft Active	Directory Certificate Services -	cc-DC-CA				
Submit a Certificate Request or Renewal Request						
To submit a saved request to the CA, par Saved Request box. Copy and paste the of the expected CS			e contents <sup>PK(</sup> SR 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 SkUAZqin/56HjuGb4h k38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	~			
Certificate Temp	late:		_			
L	CC Web Server	$\sim$				
Additional Attribu	utes:		_			
Attributes:		.a				
		Submit >	_			

Paso 6. Haga clic en Enviar.

Paso 7. Seleccione **Base 64 codificada** y haga clic en **Descargar certificado** como se muestra en la imagen.

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

Paso 8. Guarde el archivo y haga clic en Aceptar. El archivo se guarda en la carpeta Descargas.

Paso 9. Cambie el nombre del archivo a finesse.cer.

#### Importar la aplicación Finesse y los certificados firmados raíz

Paso 1. En un proser web, abra la página **Finesse OS Admin** y navegue hasta **Security** > **Certificate Management**.

Paso 2. Haga clic en el botón Cargar certificado/cadena de certificado como se muestra en la imagen.

Generate Self-sign	ed Dipload Certificate/Certificate chain
Certificate List	
Find Certificate List w	here Certificate   begins with

Paso 3. En la ventana emergente, seleccione tomcat-trust para Certificate Purpose.

Paso 4. Haga clic en el botón **Examinar...** y seleccione el archivo de certificado raíz para importar. A continuación, haga clic en el botón **Abrir**.

Paso 5. En la descripción, escriba algo como **tomcatrootcert** y haga clic en el **botón Upload** como se muestra en la imagen.

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

Paso 6. Espere hasta que vea el éxito: Certificado cargado para cerrar la ventana.

Se le solicitará que reinicie el sistema, pero primero continúe cargando el certificado firmado de la aplicación Finesse y, a continuación, podrá reiniciar el sistema.

🛈 🚯 https://finessea.cc.lab:8443/cmplatform/certificateUpload.do		${\times}$	☆	≡
Upload Certificate/Certificate chain				
Dipload 🖳 Close				
Status Success: Certificate Uploaded Restart the node(s) using the CLI command, "utils system restart".				
_ Upload Certificate/Certificate chain				_
Certificate Purpose* tomcat-trust	$\sim$			
Description(friendly name) Upload File BrowseNo file selected.				
Upload Close				
(i) *- indicates required item.				
¢				>

Paso 7. Haga clic en más tiempo en el botón **Cargar certificado/cadena de certificado** para importar el certificado de aplicación Finesse.

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

Paso 8. En la ventana emergente, seleccione tomcat para Finalidad de certificado.

Paso 9. Haga clic en el botón **Examinar...** y seleccione el archivo firmado por Finesse CA, **finesse.cer**. A continuación, haga clic en el botón **Abrir**.

Paso 10. Haga clic en el botón Cargar.

minttps://finessea.cc.lat	b:8443/cmplatform/certificateUpload.do	⊚	☆	Ξ
pload Certificate/Certific	ate chain			
Upload 📑 Close				
Status				
Warning: Uploading a cli Upload Certificate/Certifi	uster-wide certificate will distribute it to all servers	in this cluster		
Warning: Uploading a cl Upload Certificate/Certifi Certificate Purpose*	uster-wide certificate will distribute it to all servers cate chain tomcat	in this cluster		

Paso 11. Espere hasta que vea el éxito: Mensaje de certificado cargado.

Una vez más, se le solicita que reinicie el sistema. Cierre la ventana y continúe reiniciando el sistema.

## Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.