Configurar comunicação segura entre o Finesse e o servidor CTI

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Informações de Apoio Configurar **CCE CTI Server Secure** Configuração segura do Finesse Gerar certificado do agente PG (servidor CTI) Obter o certificado CSR assinado por uma CA Importar os certificados CA assinados do CCE PG Gerar certificado Finesse Assinar o certificado Finesse por uma AC Importar o aplicativo Finesse e os certificados assinados raiz Verificar Troubleshoot

Introduction

Este documento descreve como implementar certificados assinados pela autoridade de certificação (CA) entre o Cisco Finesse e o servidor de integração de telefonia por computador (CTI) na solução Cisco Contact Center Enterprise (CCE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CCE versão 12.0(1)
- Finesse versão 12.0(1)
- Servidor CTI

Componentes Utilizados

As informações neste documento são baseadas nestas versões 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

No CCE versão 11.5, a Cisco iniciou o suporte da versão 1.2 do Transport Layer Security (TLS), que permite que as mensagens Session Initiation Protocol (SIP) e Real-time Transport Protocol (RTP) sejam transportadas com segurança via TLS 1.2. Do CCE 12.0 e como parte da proteção dos dados em movimento, a Cisco começou o suporte do TLS 1.2 na maioria dos fluxos de chamadas da central de contatos: Voz de entrada e saída, multicanal e dip de banco de dados externo. O foco deste documento é a voz de entrada, especialmente a comunicação entre o Finesse e o CTI Server.

O servidor CTI suporta estes modos de conexões:

- Conexão somente segura: Permite a conexão segura entre o servidor CTI e os clientes CTI (Finesse, dialer, CTIOS e ctitest).
- Conexão segura e não segura (modo misto): Permite conexão segura, bem como não segura entre o servidor CTI e os clientes CTI. Este é o modo de conexão padrão. Esse modo será configurado quando você atualizar versões anteriores para o CCE 12.0(1).

Note: O modo somente não seguro não é suportado.

Configurar

CCE CTI Server Secure

Etapa 1. Na Estação de trabalho administrativa (AW) do PCCE, abra a pasta **Unified CCE Tools** e clique duas vezes em **Configuração do gateway periférico**.



Etapa 2. Selecione CG3A e clique em Editar.

Cisco Unified ICM/Contact Cer	nter Enterprise Components Setup
ICM Instances Add Edit Edit Delete To set up Administration Data Server (Di Interface Controller (NIC), WebView or N Web Setup tool. To set up Administration Client (Client AV and Setup tool. The Instance cc cannot be deleted bec Web Setup or Administration Client Setu to remove those components before deleted Setup.	Instance Components Add PG1A PG2A PG3A RoutesA Belete Add Edt Delete Category RoutesA Delete V), use the Administration Client Installer ause it has components set up by the p tool. You must use the applicable tool eting the instance in Peripheral Gateway
	Help Exit Setup

Etapa 3. Nas propriedades do servidor CTI, clique em **Avançar**. Na pergunta sobre a interrupção da configuração do serviço **CG3A**, selecione **Sim**.

Etapa 4. Nas **Propriedades dos componentes do servidor CTI**, selecione **Ativar modo somente seguro.** Observe a **Porta de Conexão Segura (46030)**, pois você precisa configurar a mesma porta no Finesse no próximo exercício. Clique em 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: A comunicação segura padrão é 42030, entretanto, o laboratório usado para este documento é 40630. O número da porta faz parte de uma fórmula que inclui o ID do sistema ICM. Quando o ID do sistema é 1 (CG1a), o número da porta padrão, em geral, é 42030. Como a id do sistema no laboratório é 3 (CG3a), o número da porta padrão é 46030.

Etapa 5. Em CTI Network Interface Properties, clique em Next. Verifique as Informações de configuração e clique em Avançar.

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:ljicm	=
Configuration: PG node is pccealin1p CTI Gateway is simplexed DMP address is 3	~
<	>
Texts all field and	
sing caronield	Cancel

Etapa 6. Clique em **Concluir** como mostrado na imagem.

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

Passo 7. Clique em **Exit Setup (Sair da configuração**) e aguarde até que a janela de configuração seja fechada, como mostrado na imagem.

ICM Instances		Instance Compone	nts
cc	Add	AW CG24	Add
		LoggerA	
	Edit	PG1A PG2A	Edit
	Duble	PG3A	Datas
	Delete	PiouteiA	Delete
fo 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

Etapa 8. Na área de trabalho PCCEAllin1, clique duas vezes em Unified CCE Service Control.

Etapa 9. Selecione Cisco ICM cc CG3A e clique em Iniciar.

Configuração segura do Finesse

Etapa 1. Abra um navegador da Web e navegue até Finesse Administration.

Etapa 2. Role para baixo até a seção **Configurações do servidor CTI do Contact Center Enterprise** como mostrado na imagem.

Contact Center Ent	erprise CTI Server Se	ttings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget re se CTI Server Settings	quire 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	t		

Etapa 3. Altere a porta lateral A para a porta de comunicação segura configurada no CG3A no exercício anterior: **46030.** Marque **Ativar criptografia SSL** e clique em **Salvar**.

Contact Center Ent	erprise CTI Server Se	ettings	
Note: Any changes made to Contact Center Enterpris	o the settings on this gadget in se CTI Server Settings	equire 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		

Observação: para testar a conexão, é necessário reiniciar o Finesse Tomcat Service primeiro ou reiniciar o servidor Finesse.

Etapa 4. Saia da página Finesse Administration.

Etapa 5. Abra uma sessão SSH com o Finesse.

Etapa 6. Na sessão FINESSEA SSH, execute o comando:

reinicialização do sistema de utils

Digite yes quando solicitado se deseja reiniciar o sistema.

```
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...
```

Gerar certificado do agente PG (servidor CTI)

O CiscoCertUtils é uma nova ferramenta lançada no CCE versão 12. Use esta ferramenta para gerenciar todos os certificados CCE para voz de entrada. Neste documento, você usa estes

CiscoCertUtils para gerar os Gateways Periféricos (PGs) Certificate Signing Requests (CSRs).

Etapa 1. Execute este comando para gerar um certificado CSR: CiscoCertUtil /generateCSR



Forneça as informações solicitadas, por exemplo:

Nome do país: US

Nome do Estado ou Província: MA

Nome da localidade: BXB

Nome da empresa: Cisco

Unidade organizacional: CX

Nome comum: PCCEAllin1.cc.lab

E-mail: jdoe@cc.lab

Uma senha secreta: Treinar1ng!

Nome opcional da empresa: Cisco

O certificado e a chave do host são armazenados em C:\icm\ssl\certs e C:\icm\ssl\keys.

Etapa 2. Navegue até a pasta C:\icm\ssl\certs e verifique se o arquivo host.csr foi gerado.

Obtenha o certificado CSR Assinado por uma CA

Depois que os certificados CSR são gerados, eles precisam ser assinados por uma CA de terceiros. Neste exercício, o Microsoft CA instalado no Controlador de Domínio é usado como CA de terceiros.

Certifique-se de que o modelo de certificado utilizado pela AC inclui a autenticação de cliente e servidor, como mostrado na imagem quando a AC da Microsoft é utilizada.

Properties of New Template	ons	
Subject Name Server Issuance Requirements Compatibility General Request Handling Cuptography 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 P	
Basic Constraints	An application policy defi used.	Add Application Policy
Key Usage	Application pglicies: 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 Certificate Request Agent Elent 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

Etapa 1. Abra um navegador da Web e navegue até a CA.

Etapa 2. Nos Serviços de Certificados do Microsoft Ative Diretory, selecione Solicitar um certificado.

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

Etapa 3. Selecione a opção de solicitação de certificado avançado.

Micr	osoft Activ	e Directory Co	ertifical X	+				
$\leftarrow \rightarrow$	С°Ш		i 🔒	https://dc.c	c.lab/certsrv/en	-us/certr	qus.asp	
CUCM	🛅 CUIC	🛅 Finesse	🛅 Remote E	xpert Mobile	🛅 MediaSense	CVP	🛅 CCE	
Microsoft	Active Dir	ectory Certifi	cate Services	- cc-DC-0	CA			
Request	a Certif	icate						
Select th	e certific Certificat	ate type: e						
Or cubm	it an ad	ancod co	dificate rea	un et				

Etapa 4. Na **solicitação de certificado avançado,** copie e cole o conteúdo do certificado do PG Agent CSR na caixa **Solicitação salva**.

Etapa 5. Selecione o modelo **do Servidor Web** com autenticação de cliente e servidor. No laboratório, o modelo CC Web Server foi criado com autenticação de cliente e servidor.

To submit a sav Saved Request	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):	3Lhn1D3GsLbIYivb7lbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnH J75nKDoyAh7C+F0u9tmg261 rArT900dxJem END CERTIFICATE RH <	fqH1509jMcZ3uZrciC SkUAZqin/56HjuGb4h c38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd CQUESTsna	<
Certificate Templ	ate:		
Ľ	CC Web Server	~	_
Additional Attribu	ites:		
Attributes:			_

Etapa 6. Clique em Enviar.

Passo 7. Selecione **Base 64 codificada** e clique em **Download Certificate** conforme mostrado na imagem.

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

Certificate Issued

The certificate you requested was issued to you.

○DER encoded or ●Base 64 encoded

	-	-		
N,	a	2	ch,	
D.	-	C	~	
н.			τ.,	-

Download certificate Download certificate chain

Etapa 8. Salve o arquivo e clique em OK. O arquivo é salvo na pasta Downloads.

Etapa 9. Renomeie o arquivo para host.cer (opcional).

Etapa 10. Você também precisa gerar um certificado raiz. Volte para a página de certificado CA e selecione **Transferir um certificado CA, cadeia de certificados ou CRL**. Você só precisa fazer essa etapa uma vez, já que o certificado raiz será o mesmo para todos os servidores (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> View the status of a pending certificate request <u>Download a CA certificate, certificate chain, or CRL</u>

Etapa 11. Clique em Base 64 e selecione Baixar certificado 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 (cc-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

Etapa 12. Clique em Salvar arquivo e selecione **OK**. O arquivo será salvo no local padrão, **Downloads**.

Importar os certificados CA assinados do CCE PG

Etapa 1. No PG Agent, navegue até C:\icm\ssl\certs e cole os arquivos raiz e os arquivos assinados pelo PG Agent aqui.

Etapa 2. Renomeie o certificado host.pem em c:\icm\ssl\certs como selfhost.pem.

Etapa 3. Renomeie host.cer para host.pem na pasta c:\icm\ssl\certs .

Etapa 4. Instale o certificado raiz. No prompt de comando, emita este comando: CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



Etapa 5. Instale o certificado assinado do aplicativo executando o mesmo comando: CiscoCertUtil /install C:\icm\ssl\certs\host.pem



Etapa 6. Desligue o PG. Abra o Unified CCE Service Control e desligue e desligue o Cisco ICM Agent PG.

Gerar certificado Finesse

Etapa 1. Abra o navegador da Web e navegue até Finesse OS Admin.

Etapa 2. Faça login com as credenciais do OS Admin e navegue para **Segurança > Gerenciamento de certificado** como mostrado na imagem.



Etapa 3. Clique em Gerar CSR como mostrado na imagem.



Etapa 4. Em Gerar solicitação de assinatura de certificado, use os valores padrão e clique em Gerar.

enerate Certificate S	gning Request		_
Status		teres and the second states when the states	
warning: Generator	g a new CSR for a specific certificate	type will overwrite the existing CSR for that	type
Generate Certificate	Signing Request		
Certificate Purpose**	tomcat	¥	
Distribution*	FINESSEA.cc.lab	~	
Common Name*	FINESSEA.cc.lab		
Subject Alternate Na	mes (SANs)		
Parent Domain	cc.lab		
Key Type**	RSA		
Key Length	2048	~	
Hash Algorithm*	SHA256	~	
Generate Close			
0			
I *- indicates requir	ed item.		
When the Certif	icate Purpose ending with '-ECDSA' is	selected, the certificate/key type is Elliptic (Curve (EC). Otherwise, it

Etapa 5. Feche a janela Generate Certificate Signing Request e selecione Download 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	

Etapa 6. No Certificate Purpose, selecione tomcat e clique em 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 Download CSR Close ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
< >

Passo 7. Selecione Salvar arquivo e clique em OK conforme mostrado na imagem.

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

Etapa 8. Feche a janela **Download Certificate Signing Request**. O certificado é salvo no local padrão **(Este PC > Downloads)**.

Etapa 9. Abra o Windows Explorer e navegue até essa pasta. Clique com o botão direito do mouse neste certificado e renomeie-o: **finessetomcat.csr**

Assinar o certificado Finesse por uma AC

Nesta seção, o mesmo Microsoft CA usado na etapa anterior é usado como CA de terceiros.

Observação: certifique-se de que o modelo de certificado usado pela CA inclua autenticação de cliente e servidor.

Etapa 1. Abra um navegador da Web e navegue até a CA.

Etapa 2. Nos Serviços de Certificados do Microsoft Ative Diretory, selecione Solicitar um certificado.

_ D X
🗲 🗇 🧭 https://dc.ec.lab/centurv/en-us/ 🔎 = 📾 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

Etapa 3. Selecione a opção **de solicitação de certificado avançado** conforme mostrado na imagem.

Micr	rosoft Activ	e Directory Co	ertifical × +				
\leftrightarrow	C' ŵ		🛈 윩 https://dc.	c.lab/certsrv/en	-us/certr	qus.asp	_
CUCM	🛅 CUIC	🛅 Finesse	🛅 Remote Expert Mobile	🛅 MediaSense	CVP	CCE	Ē
Microsoft Request	Active Dire	ectory Certifi icate	icate Services cc-DC-0	CA			
Select the User (Or. subm	e certific Certificat	ate type: e	tificate request				

Etapa 4. Na **solicitação de certificado avançado,** copie e cole o conteúdo do certificado do Finesse CSR na caixa **Solicitação salva**.

Etapa 5. Selecione o modelo de servidor Web com autenticação de cliente e servidor. Neste laboratório, o modelo do CC Web Server foi criado com autenticação de cliente e servidor.

Saved Reques	ved request to the CA, par 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):	3LhnlD3GsLbIYivb7lbshW gNL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnH J75nKDoyAh7C+F0u9tmg26 rArT900dxJem END CERTIFICATE RI <	fqH1509jMcZ3uZrciC 5kUAZqin/56HjuGb4h k38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	•
ertificate Temp	ato		
	CC Web Server	~	_
Additional Attrib	utes:		
			_

Etapa 6. Clique em Enviar.

Passo 7. Selecione **Base 64 codificada** e clique em **Download certificate** como mostrado na imagem.

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

Etapa 8. Salve o arquivo e clique em OK. O arquivo é salvo na pasta Downloads.

Etapa 9. Renomeie o arquivo para finesse.cer.

Importar o aplicativo Finesse e os certificados assinados raiz

Etapa 1. Em um navegador da Web, abra a página **Finesse OS Admin** e navegue até **Security** > **Certificate Management**.

Etapa 2. Clique no botão **Carregar certificado/cadeia de certificados** conforme mostrado na imagem.

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

Etapa 3. Na janela pop-up, selecione tomcat-trust para fins de certificado.

Etapa 4. Clique no botão **Procurar...** e selecione o arquivo de certificado raiz a ser importado. Em seguida, clique no botão **Abrir**.

Etapa 5. Na descrição, escreva algo como **tomcatrootcert** e clique no botão **Carregar**, como mostrado na imagem.

Upload Certificate/Certific	ate chain
Dipload 🖳 Close	
Status Warning: Uploading a cl	uster-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	em.
c	

Etapa 6. Aguarde até ver o sucesso: Mensagem Certificate Uploaded para fechar a janela.

Você será solicitado a reiniciar o sistema, mas primeiro, continue carregando o certificado assinado do aplicativo Finesse e reinicie o sistema.

🛈 🔏 https://finessea.cc.lab	x8443/cmplatform/certificateUpload.do		⊠ ☆] ≡
Upload Certificate/Certificate/	ate chain			
Dipload 🖳 Close				
Status Success: Certificate Uplo Restart the node(s) using	aded g the CLI command, "utils system restart".			
Upload Certificate/Certific	cate chain			_
Certificate Purpose*	tomcat-trust	~		
Description(friendly name) Upload File	Browse No file selected.			
Upload Close				
(i) *- indicates required ite	m.			
<				>

Passo 7. Clique em mais tempo no botão **Carregar certificado/cadeia de certificados** para importar o certificado do aplicativo Finesse.

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

Etapa 8. Na janela pop-up, selecione tomcat para fins de certificado.

Etapa 9. Clique no botão **Procurar...** e selecione o arquivo assinado da CA Finesse, **finesse.cer**. Em seguida, clique no botão **Abrir**.

Etapa 10. Clique no botão Upload.

🕑 🜇 https://inessea.cc.iac	x8443/cmplatform/certificateUpload.do	🛛	ជ	=
pload Certificate/Certific	ate chain			
Upload 🖳 Close				
Status Warning: Uploading a clu Upload Certificate/Certific	uster-wide certificate will distribute it to all servers	in this cluster		
Status Warning: Uploading a clu Upload Certificate/Certific Certificate Purpose*	uster-wide certificate will distribute it to all servers cate chain	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 cate chain tomcat Self-signed certificate	in this cluster		_

Etapa 11. Aguarde até ver o sucesso: Mensagem de Certificado Carregado.

Novamente, você é solicitado a reiniciar o sistema. Feche a janela e continue a reiniciar o sistema.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.