

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:

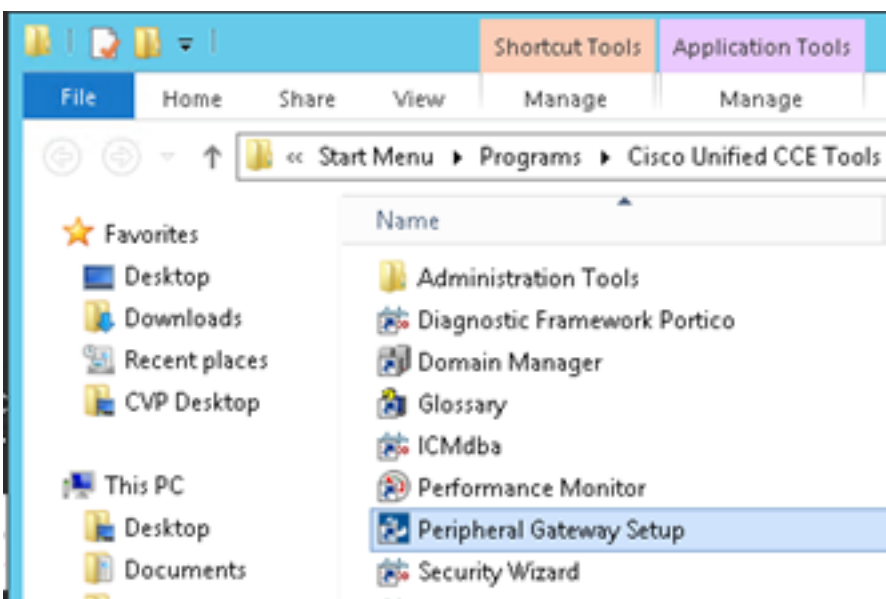
- **Conexão somente segura:** Permite a conexão segura entre o servidor CTI e os clientes CTI (Finesse, dialer, CTIOS e ctitest).
- **Conexão segura e não segura (modo misto):** Permite conexão segura, bem como não segura entre o servidor CTI e os clientes CTI. Este é o modo de conexão padrão. Esse modo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

Note: O modo somente não seguro não é suportado.

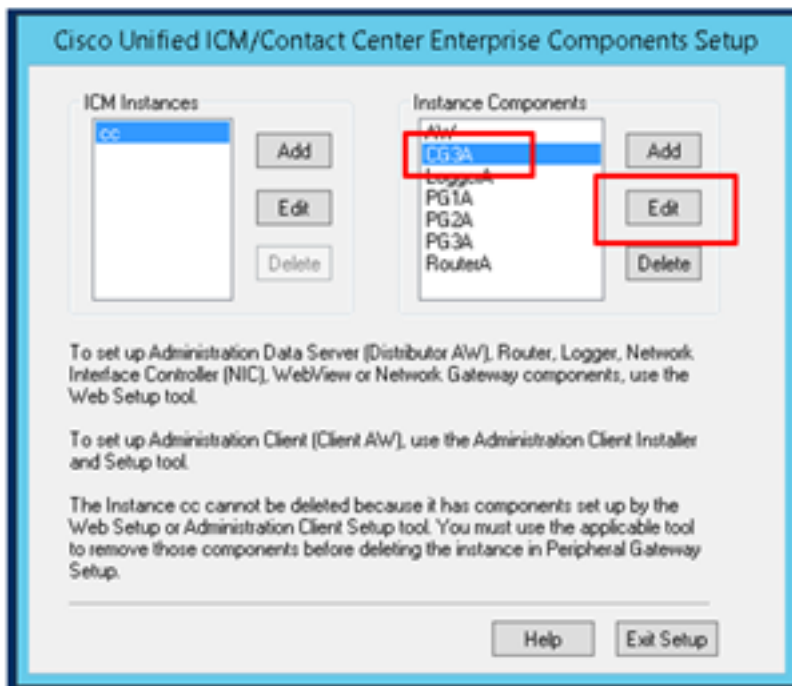
Configurar

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**.

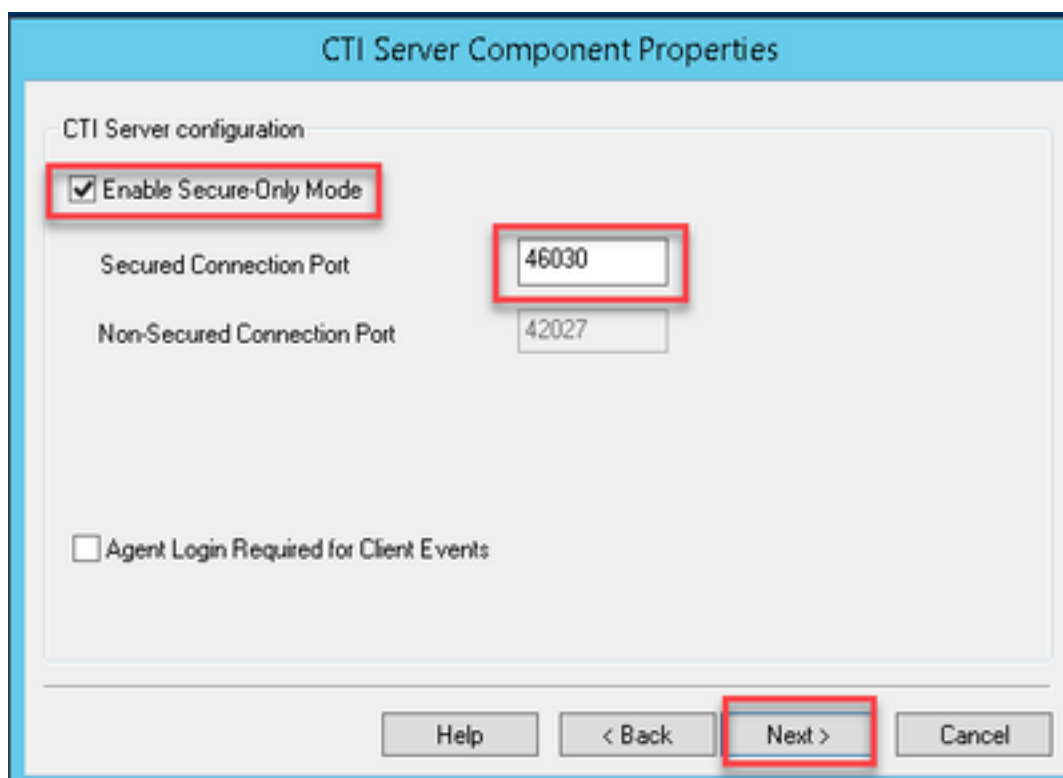


Etapa 2. Selecione **CG3A** e clique em **Editar**.



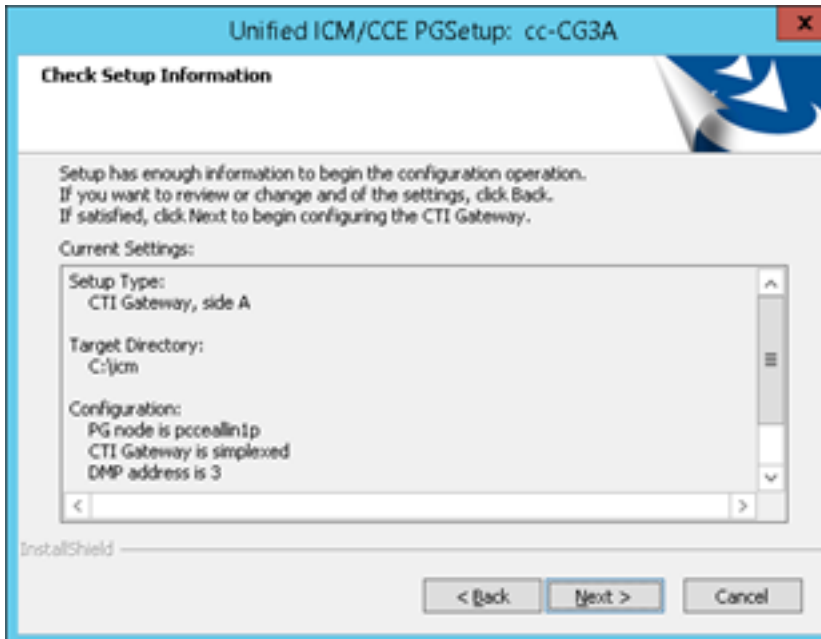
Etapa 3. Nas propriedades do servidor CTI, clique em **Avançar**. Na pergunta sobre a interrupção da configuração do serviço **CG3A**, selecione **Sim**.

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.

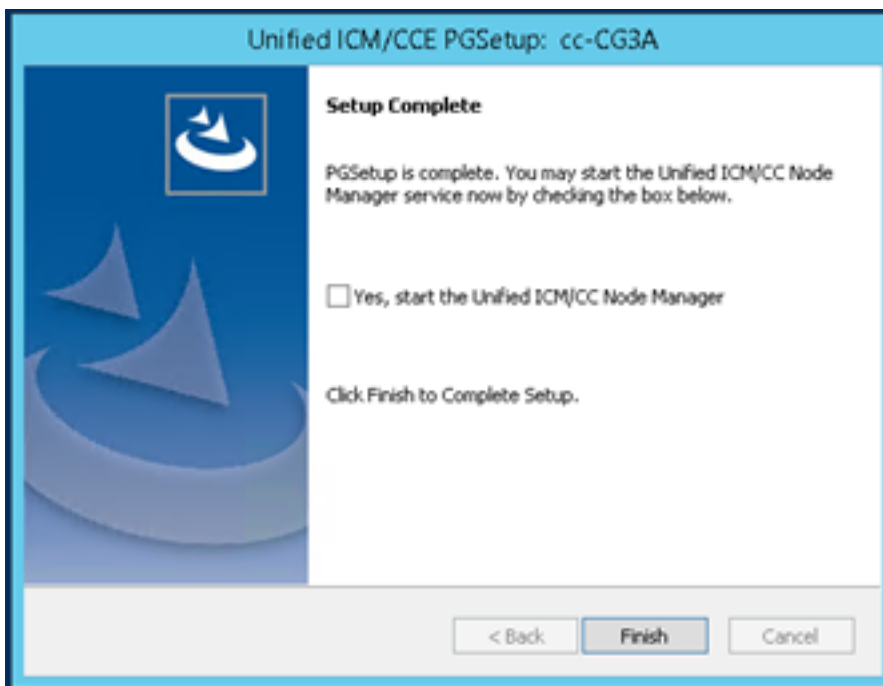


Note: A comunicação segura padrão é 42030, entretanto, o laboratório usado para este documento é 40630. O número da porta faz parte de uma fórmula que inclui o ID do sistema ICM. Quando o ID do sistema é 1 (CG1a), o número da porta padrão, em geral, é 42030. Como a id do sistema no laboratório é 3 (CG3a), o número da porta padrão é 46030.

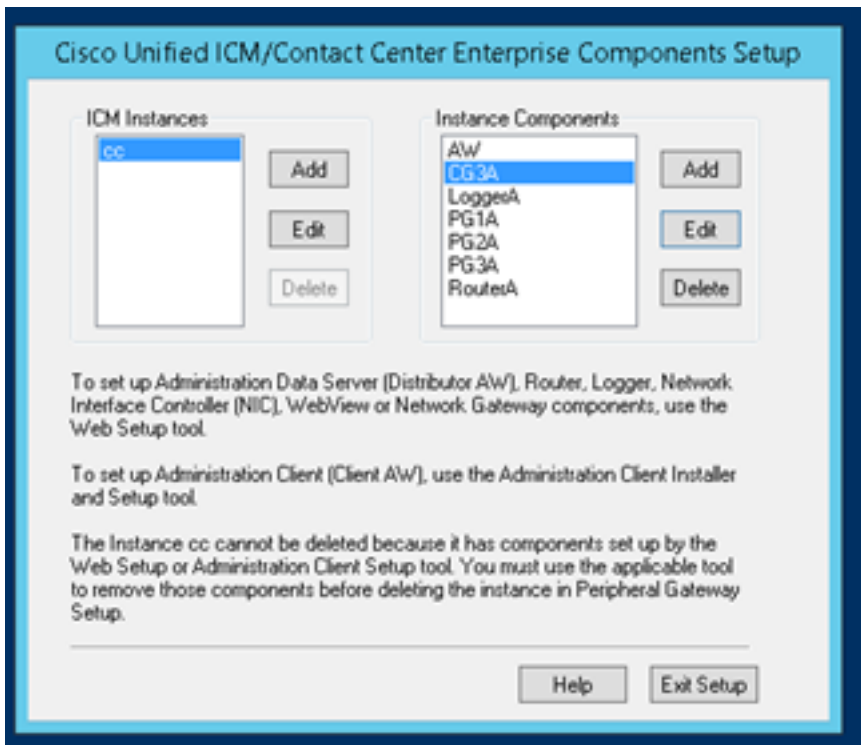
Etapa 5. Em **CTI Network Interface Properties**, clique em **Next**. Verifique as **Informações de configuração** e clique em **Avançar**.



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



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



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.

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 Enterprise CTI Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Contact Center Enterprise CTI Server Settings

A Side Host/IP Address*	<input type="text" value="10.10.10.10"/>	B Side Host/IP Address	<input type="text"/>
A Side Port*	<input type="text" value="46030"/>	B Side Port	<input type="text"/>
Peripheral ID*	<input type="text" value="5000"/>		

Enable SSL encryption

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**

```
C:\Users\Administrator.CC>
C:\Users\Administrator.CC>CiscoCertUtil /generateCSR

Key already exists at C:\icm\ssl\keys\host.key. It will be used to generate the
CSR.

SSL config path = C:\icm\ssl\cfg\openssl.cfg
SYSTEM command is C:\icm\ssl\bin\openssl.exe req -new -key C:\icm\ssl\keys\host.
key -out C:\icm\ssl\certs\host.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
```

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

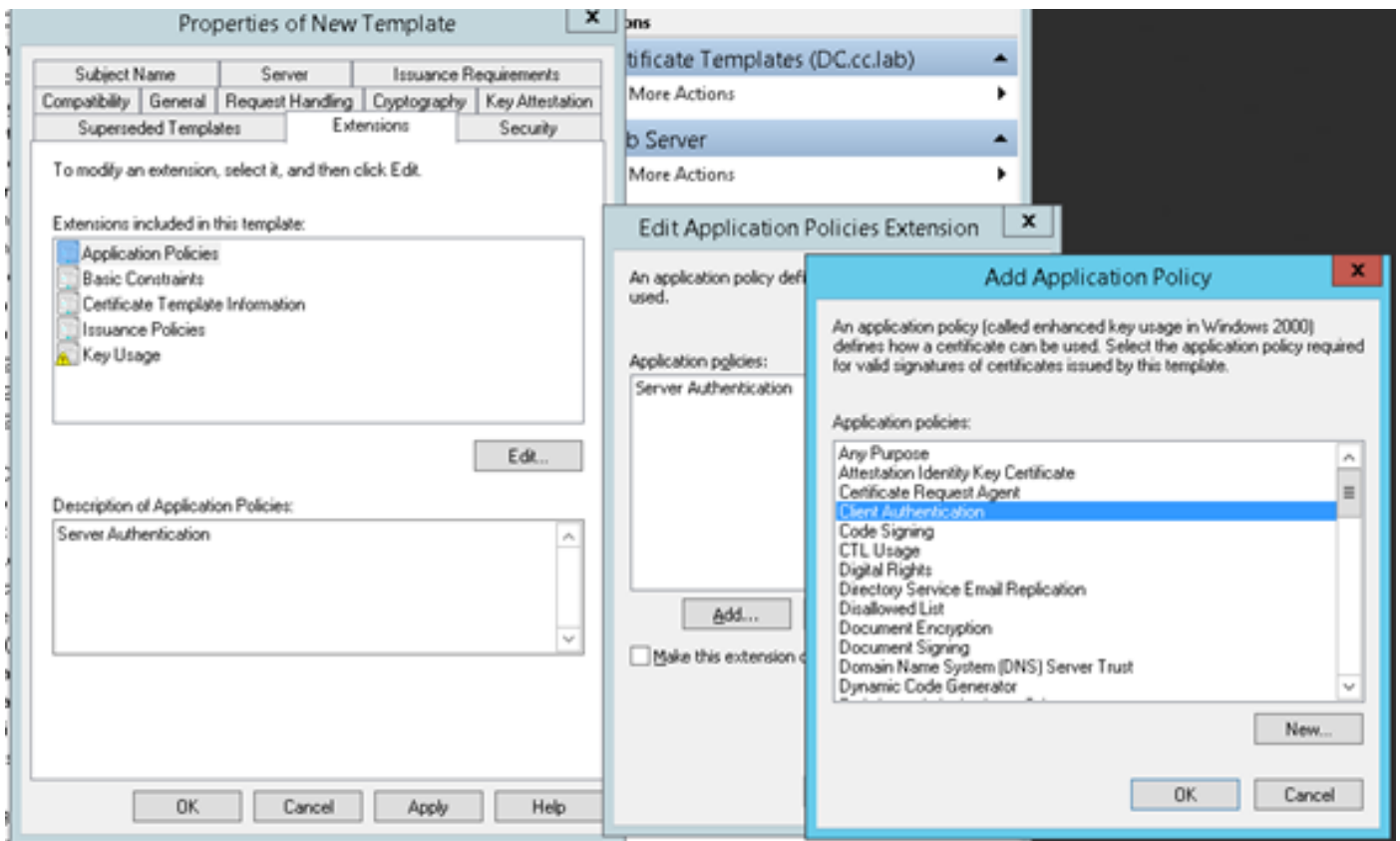
O certificado e a chave do host são armazenados em **C:\icm\ssl\certs** e **C:\icm\ssl\keys**.

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

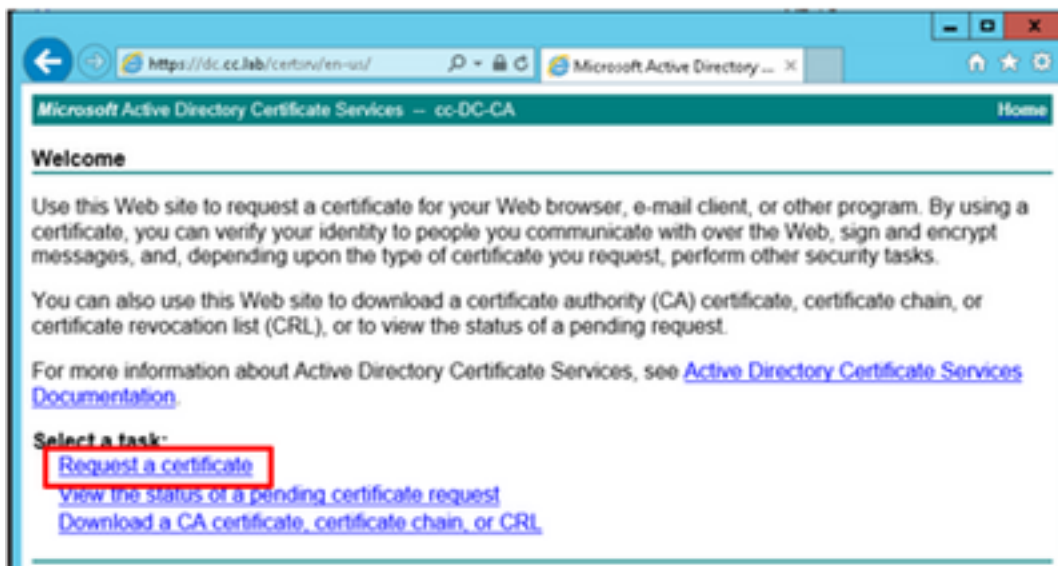
Depois que os certificados CSR são gerados, eles precisam ser assinados por uma CA de terceiros. Neste exercício, o Microsoft CA instalado no Controlador de Domínio é usado como CA de terceiros.

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.

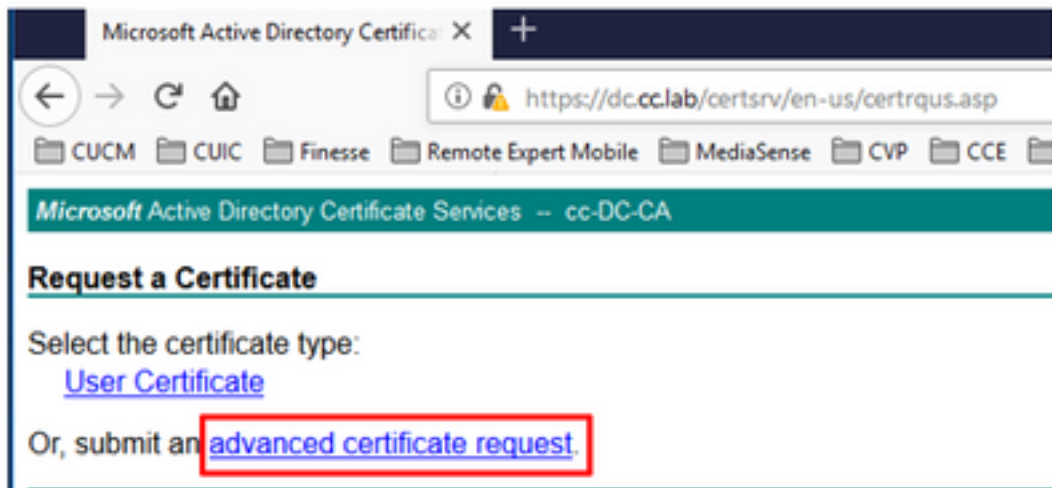


Etapa 1. Abra um navegador da Web e navegue até a CA.

Etapa 2. Nos **Serviços de Certificados do Microsoft Active Directory**, selecione **Solicitar um certificado**.

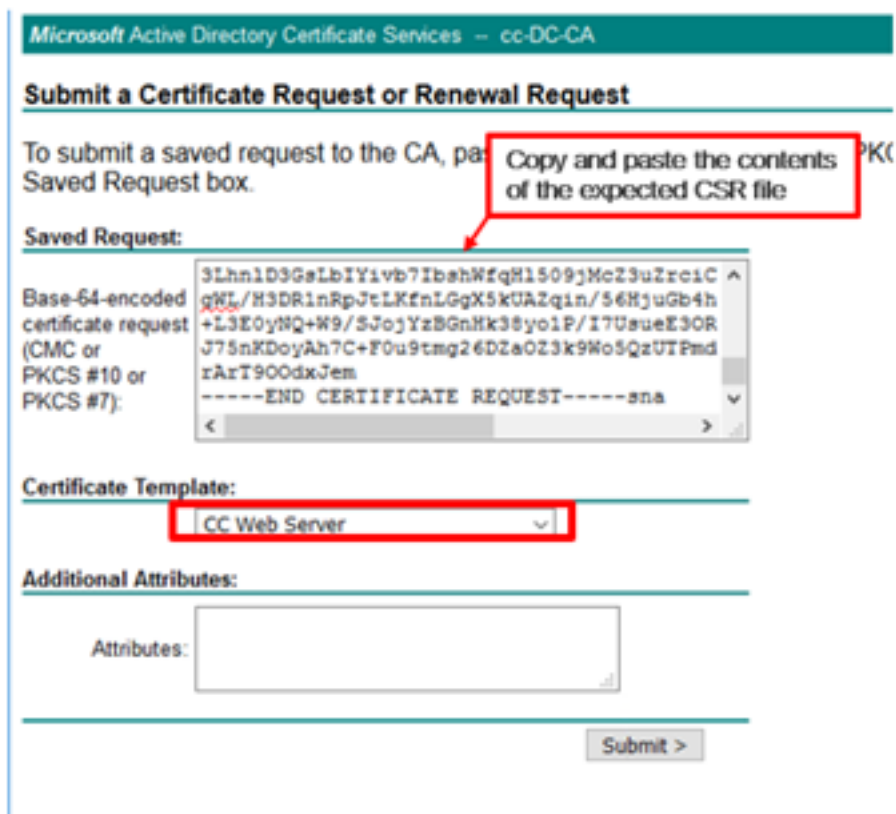


Etapa 3. Selecione a opção de solicitação de certificado avançado.



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.



Etapa 6. Clique em **Enviar**.

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

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



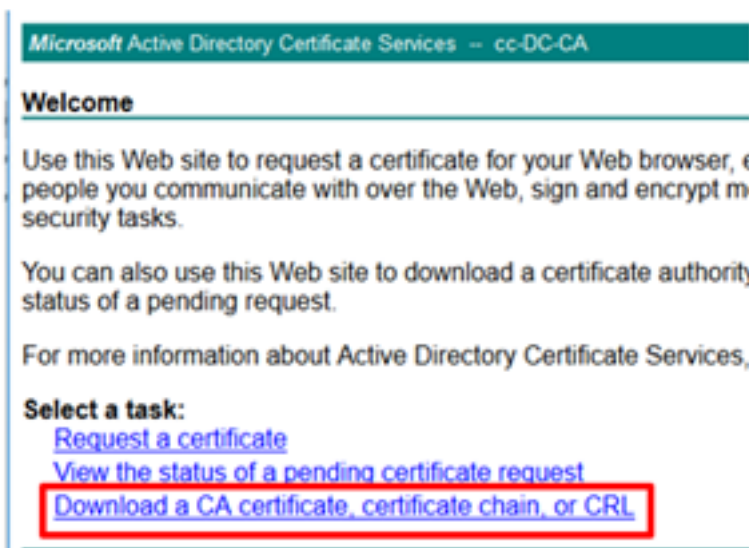
[Download certificate](#)

[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 **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).

A screenshot of the Microsoft Active Directory Certificate Services website. The page has a teal header with the text "Microsoft Active Directory Certificate Services -- cc-DC-CA". Below the header is a "Welcome" section with a horizontal line. The main content area contains three paragraphs of text. The first paragraph explains the website's purpose for requesting certificates. The second paragraph mentions downloading certificate authority information. The third paragraph provides more information about the services. Below the text is a "Select a task:" section with three blue hyperlinks. The third link, "Download a CA certificate, certificate chain, or CRL", is highlighted with a red rectangular box.

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

Welcome

Use this Web site to request a certificate for your Web browser, e people you communicate with over the Web, sign and encrypt m security 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:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Etapa 11. Clique em **Base 64** e selecione **Baixar certificado CA**.



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`

```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\rootAll.cerRoot "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

Exact match:
Element 0:
Serial Number: 480a8f1b836a50b54c66a65f5298faae
Issuer: CN=cc-DC-CA, DC=cc, DC=lab
NotBefore: 2/8/2017 3:43 PM
NotAfter: 2/8/2020 3:53 PM
Subject: CN=cc-DC-CA, DC=cc, DC=lab
CA Version: U0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): ec 49 6e f7 cb 9a c8 3a f5 46 2b ae 4f 1f 1b 15 fd 38 81 5f
Certificate "cc-DC-CA" already in store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

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

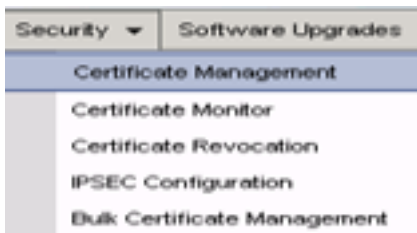
```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\nic\nssl\certs\host.pem
Install String is certutil -enterprise -addstore -f Root C:\nic\nssl\certs\host.p
enRoot "Trusted Root Certification Authorities"
Certificate "PCCALLini.cc.lab" added to store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

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

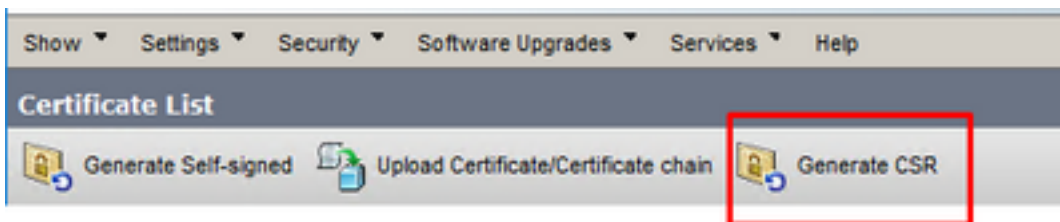
Gerar certificado Finesse

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

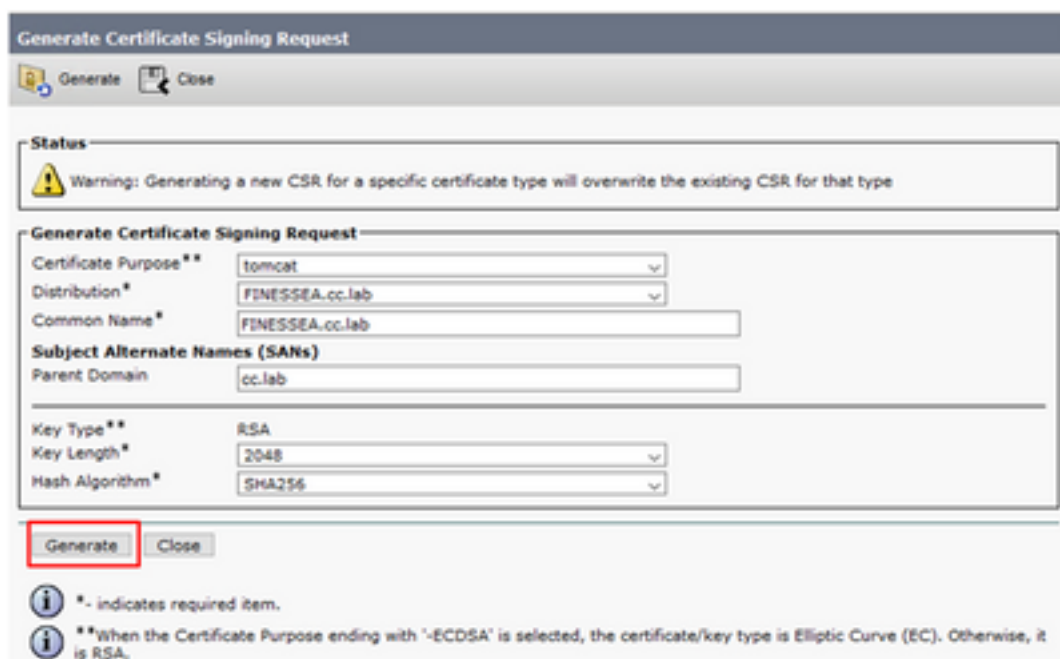
Etapa 2. Faça login com as credenciais do OS Admin e navegue para **Segurança > Gerenciamento de certificado** como mostrado na imagem.



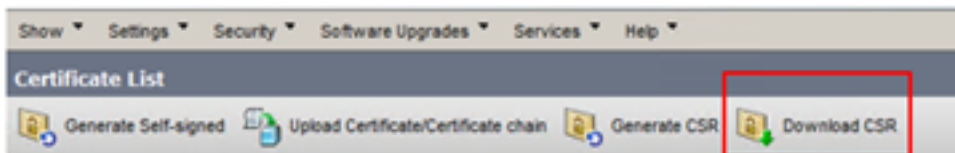
Etapa 3. Clique em **Gerar CSR** como mostrado na imagem.



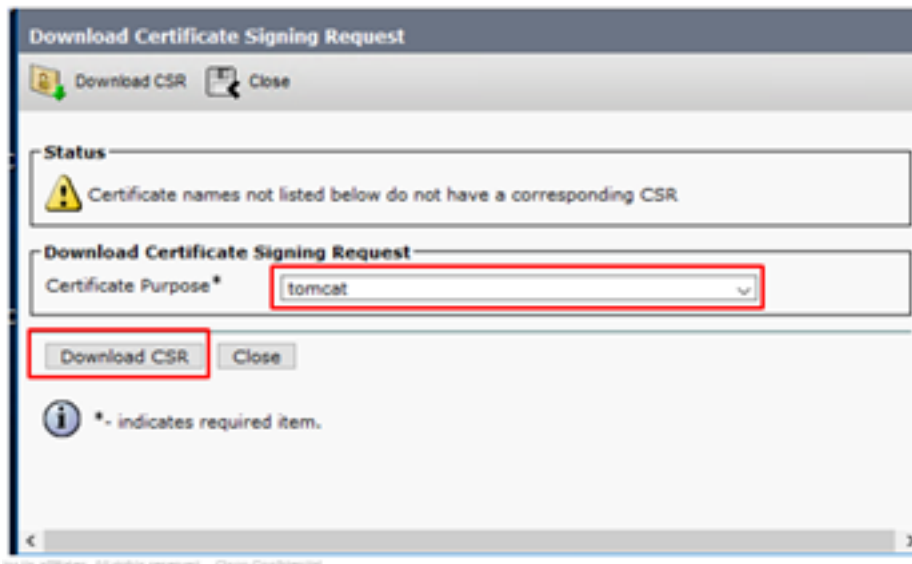
Etapa 4. Em **Gerar solicitação de assinatura de certificado**, use os valores padrão e clique em **Gerar**.



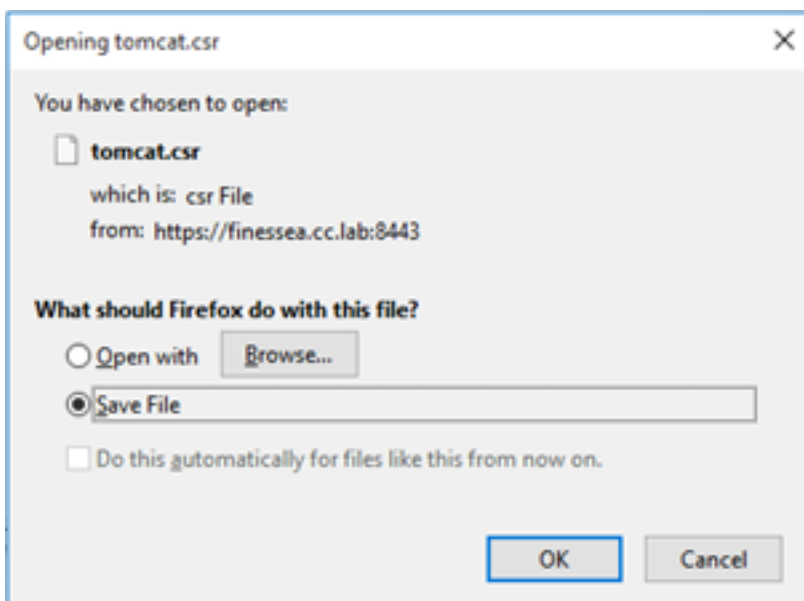
Etapa 5. Feche a janela **Generate Certificate Signing Request** e selecione **Download CSR**.



Etapa 6. No Certificate Purpose, selecione **tomcat** e clique em **Download CSR**.



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



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**

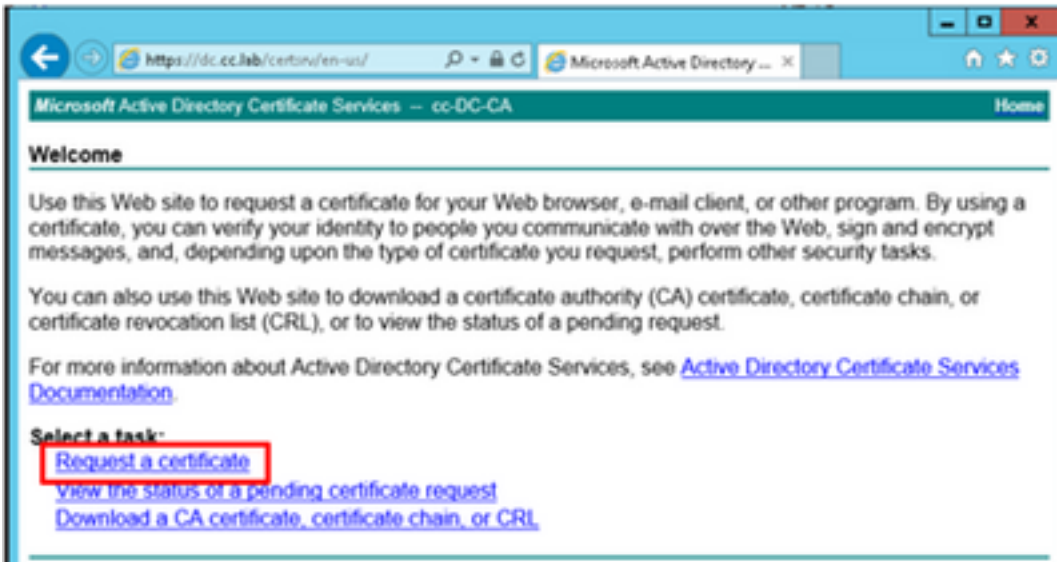
Assinar o certificado Finesse por uma AC

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

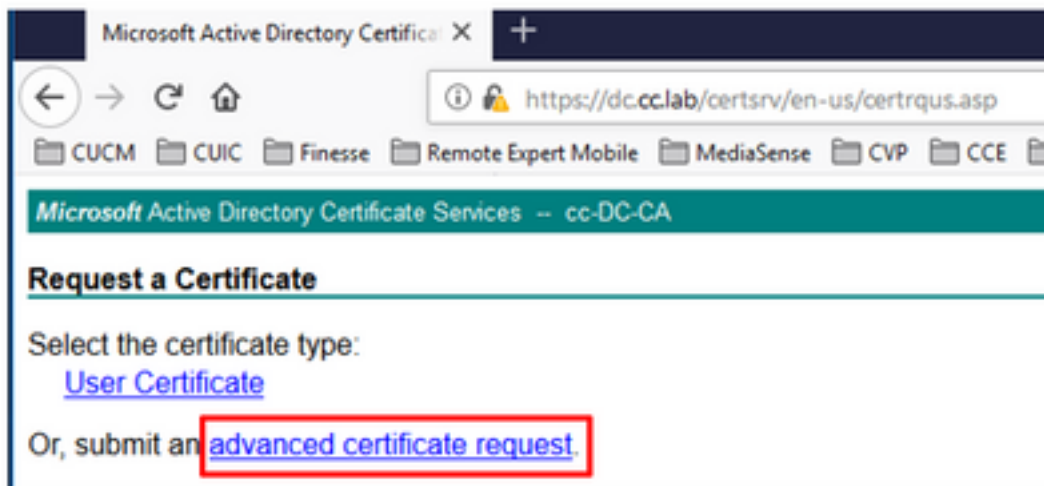
Observação: certifique-se de que o modelo de certificado usado pela CA inclua autenticação de cliente e servidor.

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

Etapa 2. Nos **Serviços de Certificados do Microsoft Active Directory**, selecione **Solicitar um certificado**.



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



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.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste the contents of the Saved Request box. **Copy and paste the contents of the expected CSR file**

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
3Lhn1D3GgEbIYivb7IbqhWfqH1509jMcZ3uZrciC  
gKtL/H3DR1nRpJcLKfnLGgX5kUAZqin/56HjuGb4h  
+L3E0yNQ+W9/SJoJYzBGnHk38yo1P/I7UaueE3OR  
J75nKDoyAh7C+F0u9tmq26DZa0Z3k9No5QzUTPmd  
rArT900dxJem  
-----END CERTIFICATE REQUEST-----sna
```

Certificate Template:

Additional Attributes:

Attributes:

Submit >

Etapa 6. Clique em **Enviar**.

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

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

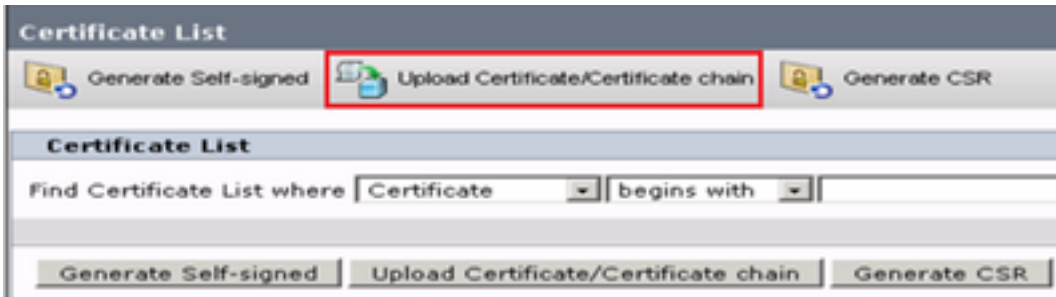
Etapa 8. Salve o arquivo e clique em **OK**. O arquivo é salvo na pasta **Downloads**.

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**.

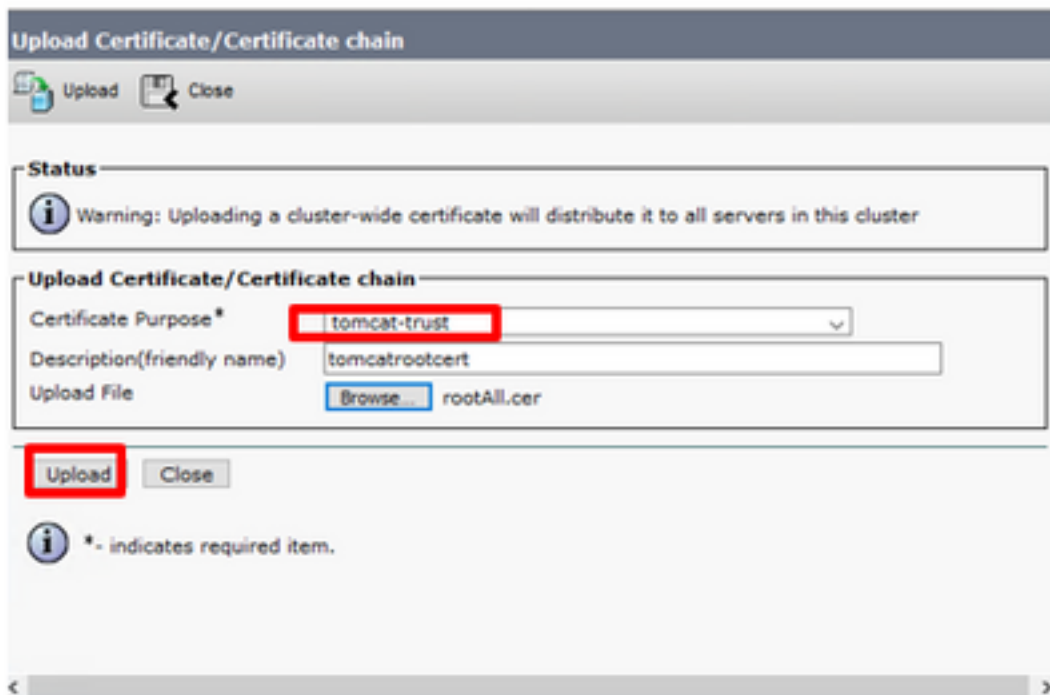
Etapa 2. Clique no botão **Carregar certificado/cadeia de certificados** conforme mostrado na imagem.



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

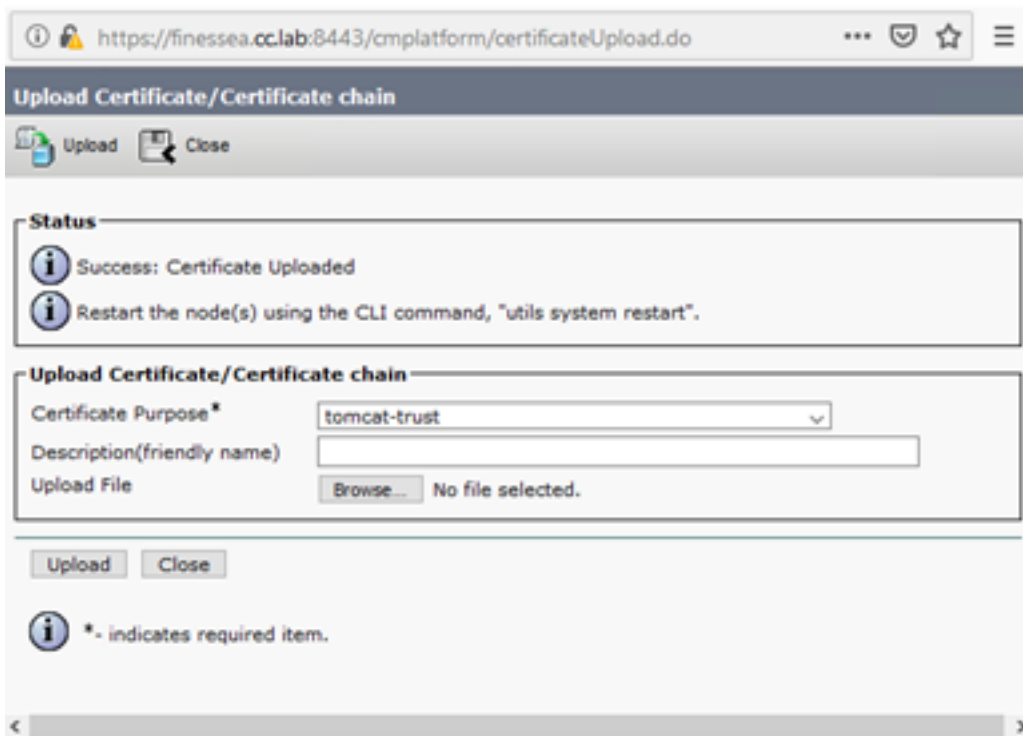
Etapa 4. Clique no botão **Procurar...** e selecione o arquivo de certificado raiz a ser importado. Em seguida, clique no botão **Abrir**.

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

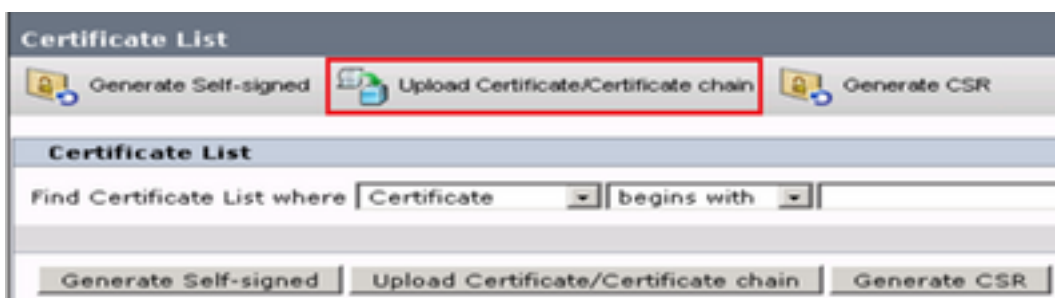


Etapa 6. Aguarde até ver o **sucesso: Mensagem Certificate Uploaded** para fechar a janela.

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



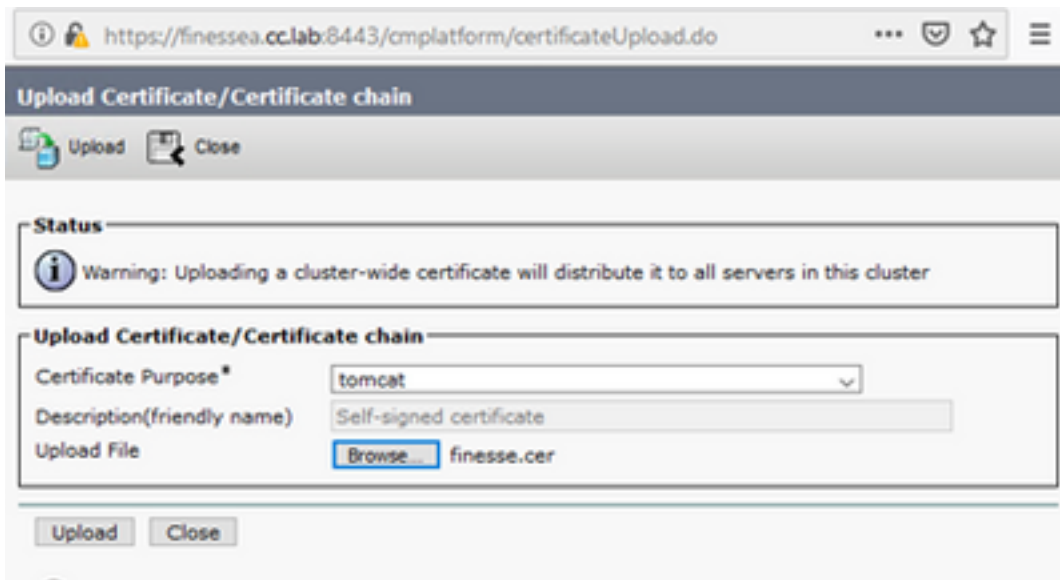
Passo 7. Clique em mais tempo no botão **Carregar certificado/cadeia de certificados** para importar o certificado do aplicativo Finesse.



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**.



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.