

# Implementar certificados CA assinados em uma solução CCE

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Background](#)

[Procedimento](#)

[Servidores baseados em Windows CCE](#)

[1. Gerar CSR](#)

[2. Obter os Certificados Assinados pela CA](#)

[3. Carregar os Certificados Assinados pela CA](#)

[4. Associar o Certificado Assinado pela CA ao IIS](#)

[5. Vincular o Certificado Assinado pela CA ao Pórtico de Diagnóstico](#)

[6. Importe o Certificado Raiz e Intermediário para o Armazenamento de Chaves Java](#)

[Solução CVP](#)

[1. Gerar Certificados com FQDN](#)

[2. Gerar o CSR](#)

[3. Obter os Certificados Assinados pela CA](#)

[4. Importar os Certificados Assinados pela CA](#)

[Servidores VOS](#)

[1. Gerar Certificado CSR](#)

[2. Obter os Certificados Assinados pela CA](#)

[3. Carregar o Aplicativo e Certificados Raiz](#)

[Verificar](#)

[Troubleshooting](#)

[Informações relacionadas](#)

---

## Introdução

Este documento descreve como implementar certificados assinados de Autoridade de certificação (CA) na solução Cisco Contact Center Enterprise (CCE).

Contribuição de Anuj Bhatia, Robert Rogier e Ramiro Amaya, engenheiros do Cisco TAC.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Unified Contact Center Enterprise (UCCE) versão 12.5(1)
- Package Contact Center Enterprise Versão 12.5(1)
- Customer Voice Portal (CVP) versão 12.5 (1)
- Cisco Virtualized Voice Browser (VVB)
- Console de operações e administração (OAMP) do Cisco CVP
  
- Cisco Unified Intelligence Center (CUIC)
  
- Cisco Unified Communication Manager (CUCM)

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VB 12.5
- Finesss 12,5
- CUIC 12.5
- Windows 2016

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Background

Os certificados são usados para garantir que a comunicação seja segura com a autenticação entre clientes e servidores.

Os usuários podem comprar certificados de uma CA ou usar certificados autoassinados.

Os certificados autoassinados (como o nome indica) são assinados pela mesma entidade cuja identidade eles certificam, ao contrário de serem assinados por uma autoridade de certificação. Os certificados autoassinados não são considerados tão seguros quanto os certificados de CA, mas são usados por padrão em muitos aplicativos.

Na versão 12.x da solução Package Contact Center Enterprise (PCCE), todos os componentes da solução são controlados pelo Single Pane of Glass (SPOG), que está hospedado no servidor principal da Admin Workstation (AW).

Devido à Conformidade de Gerenciamento de Segurança (SRC - Security Management Compliance) na versão PCCE 12.5(1), toda a comunicação entre o SPOG e outros componentes na solução é feita através do protocolo HTTP seguro. Na UCCE 12.5, a comunicação entre componentes também é feita através do protocolo HTTP seguro.

Este documento explica em detalhes as etapas necessárias para implementar certificados

assinados CA em uma solução CCE para comunicação HTTP segura. Para quaisquer outras considerações de segurança do UCCE, consulte [Diretrizes de segurança do UCCE](#). Para qualquer comunicação segura CVP adicional diferente do HTTP seguro, consulte as diretrizes de segurança no guia de configuração do CVP: [Diretrizes de segurança do CVP](#).

## Procedimento

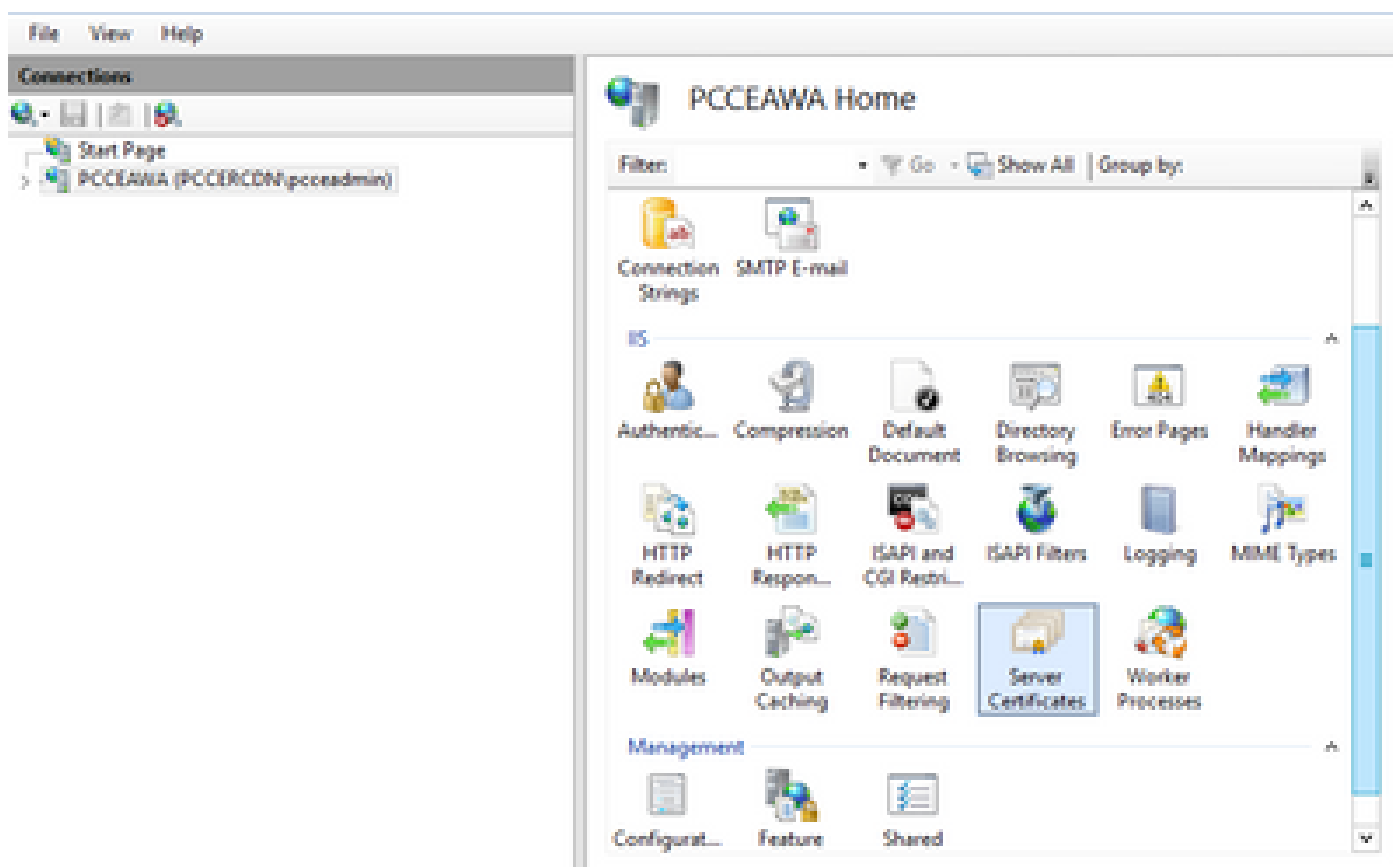
### Servidores baseados em Windows CCE

#### 1. Gerar CSR

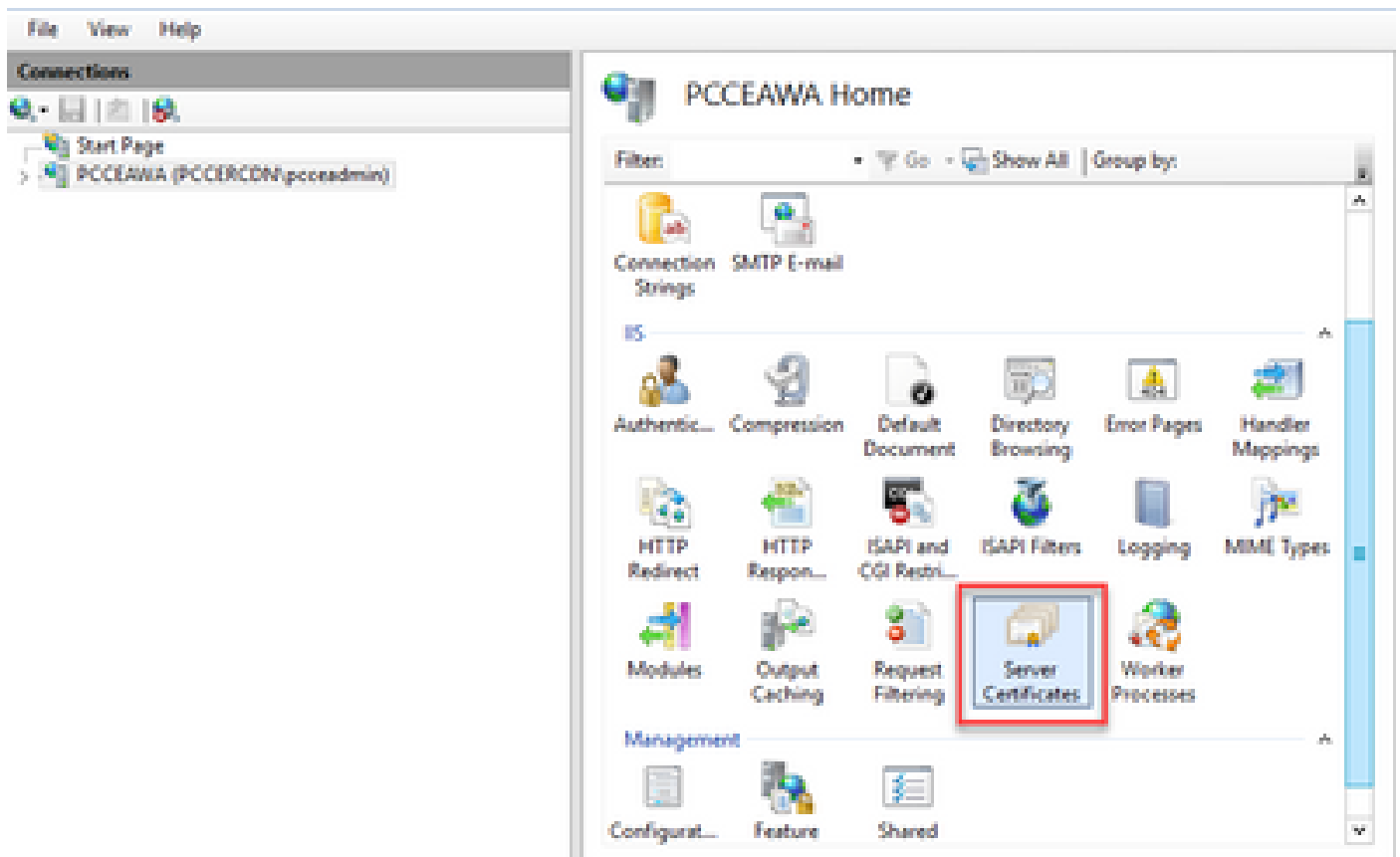
Este procedimento explica como gerar uma CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado) a partir do Gerenciador dos Serviços de Informações da Internet (IIS).

Etapa 1. Faça logon no Windows e escolha Painel de Controle > Ferramentas Administrativas > Gerenciador dos Serviços de Informações da Internet (IIS).

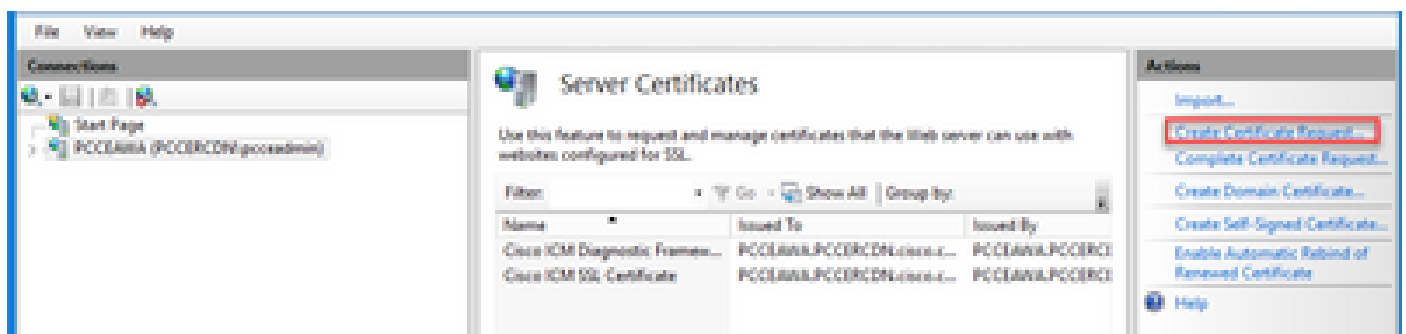
Etapa 2. No painel Conexões, clique no nome do servidor. O painel Início do servidor é exibido.



Etapa 3. Na área do IIS, clique duas vezes em Certificados do Servidor.



Etapa 4. No painel Ações, clique em Criar solicitação de certificado.



Etapa 5. Na caixa de diálogo Solicitar Certificado, faça o seguinte:

Especifique as informações necessárias nos campos exibidos e clique em Avançar.

Request Certificate

**Distinguished Name Properties**

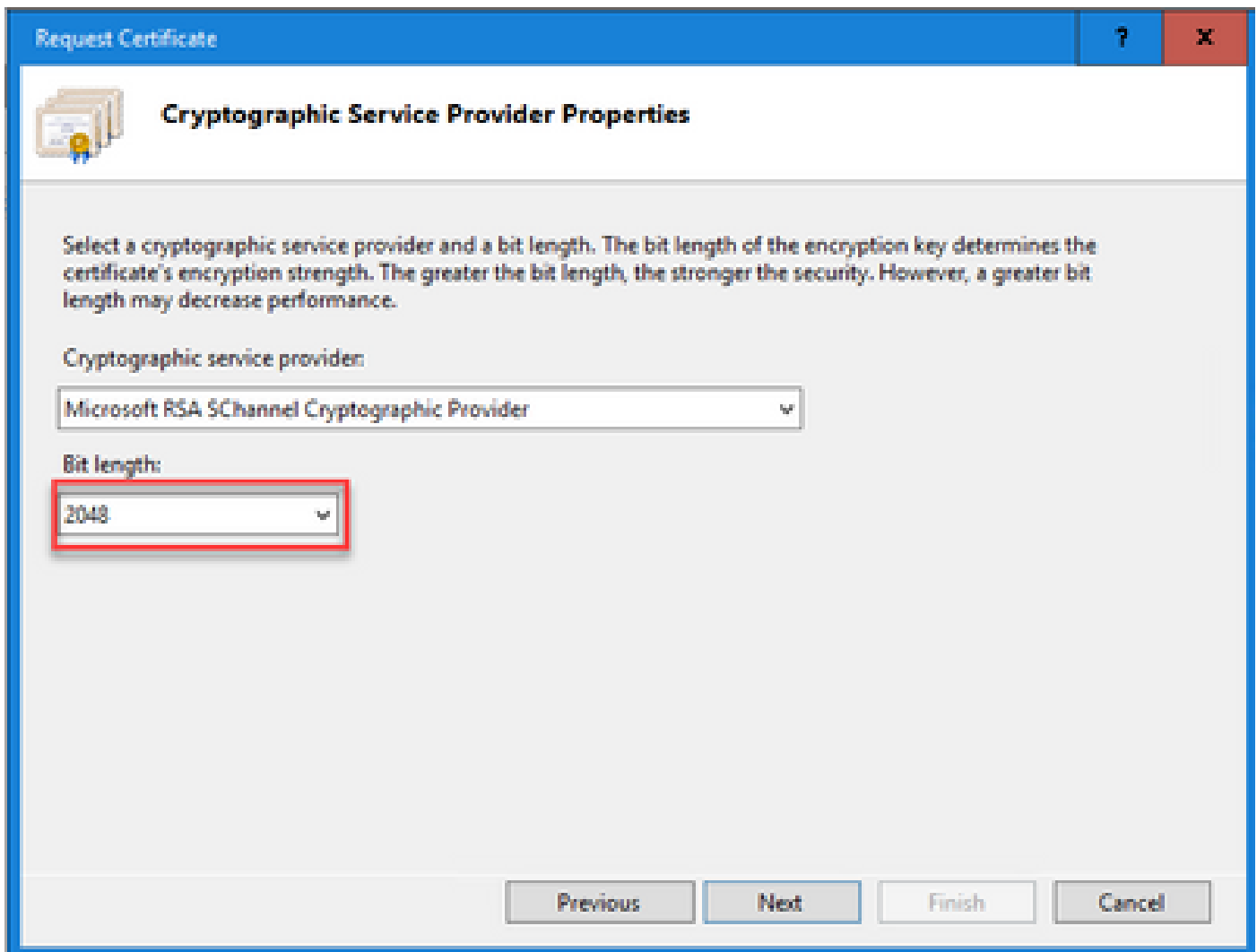
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="pccerwa.pccercdn.cisco.com"/>
Organization:	<input type="text" value="Cisco"/>
Organizational unit:	<input type="text" value="CX"/>
City/locality:	<input type="text" value="RCDN"/>
State/province:	<input type="text" value="TX"/>
Country/region:	<input type="text" value="US"/>

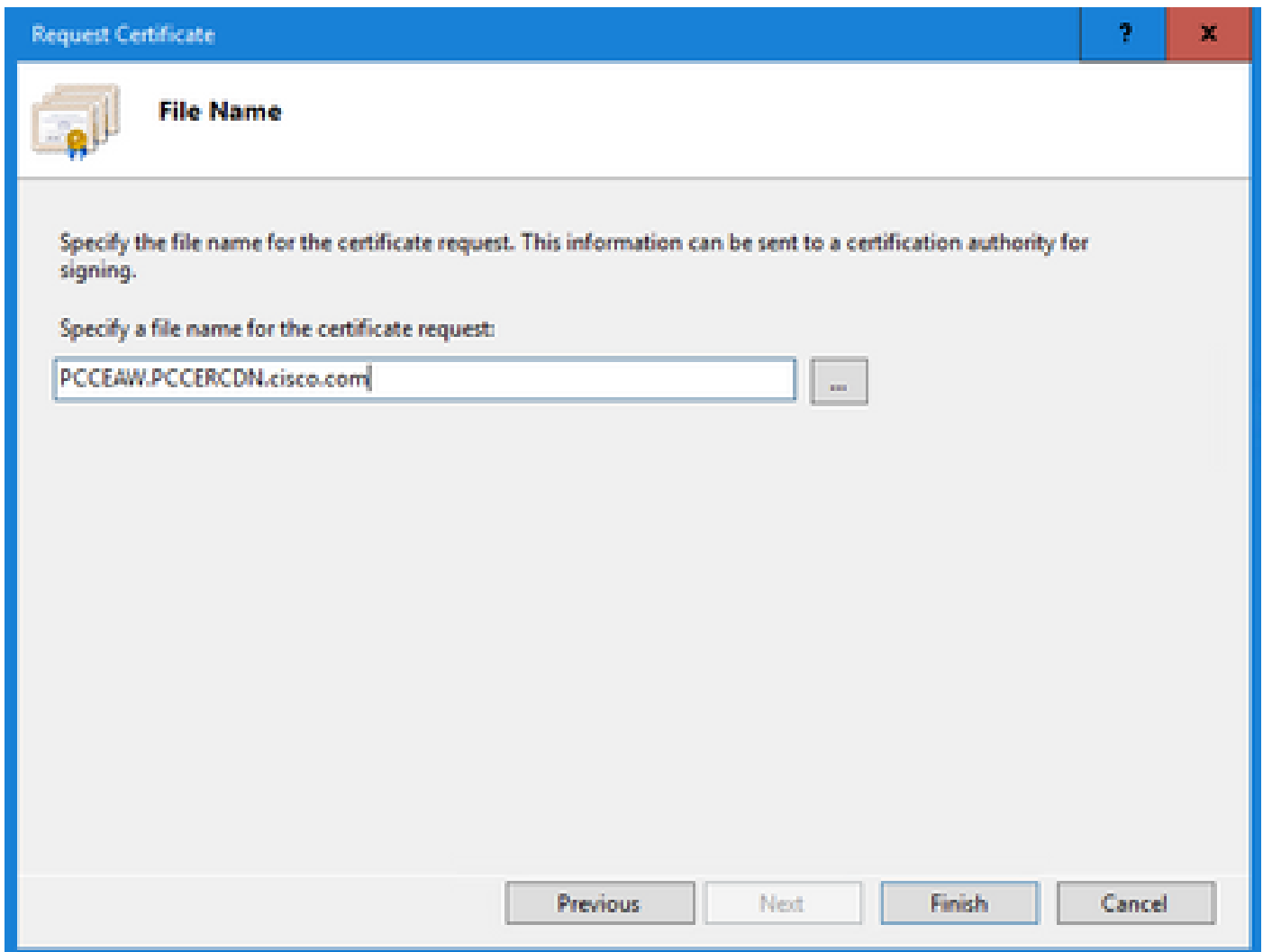
Previous Next Finish Cancel

Na lista suspensa Provedor de serviços de criptografia, deixe a configuração padrão.

Na lista suspensa Tamanho do bit, selecione 2048.




Etapa 6. Especifique um nome de arquivo para a solicitação de certificado e clique em Concluir.



## 2. Obter os Certificados Assinados pela CA

Etapa 1. Assinar o certificado em uma CA.

---

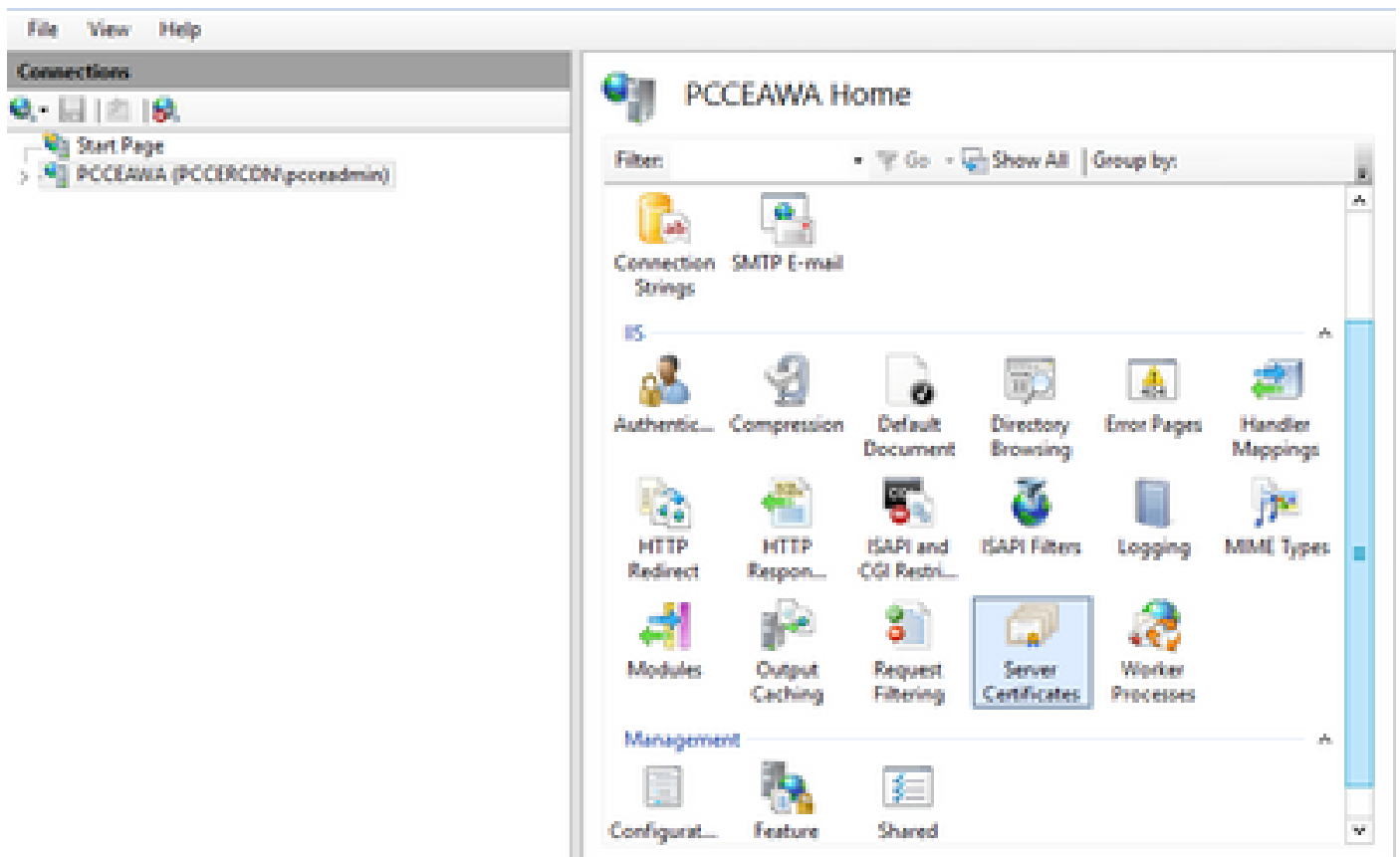
 Observação: certifique-se de que o modelo de certificado usado pela autoridade de certificação inclua autenticação de cliente e servidor.

---

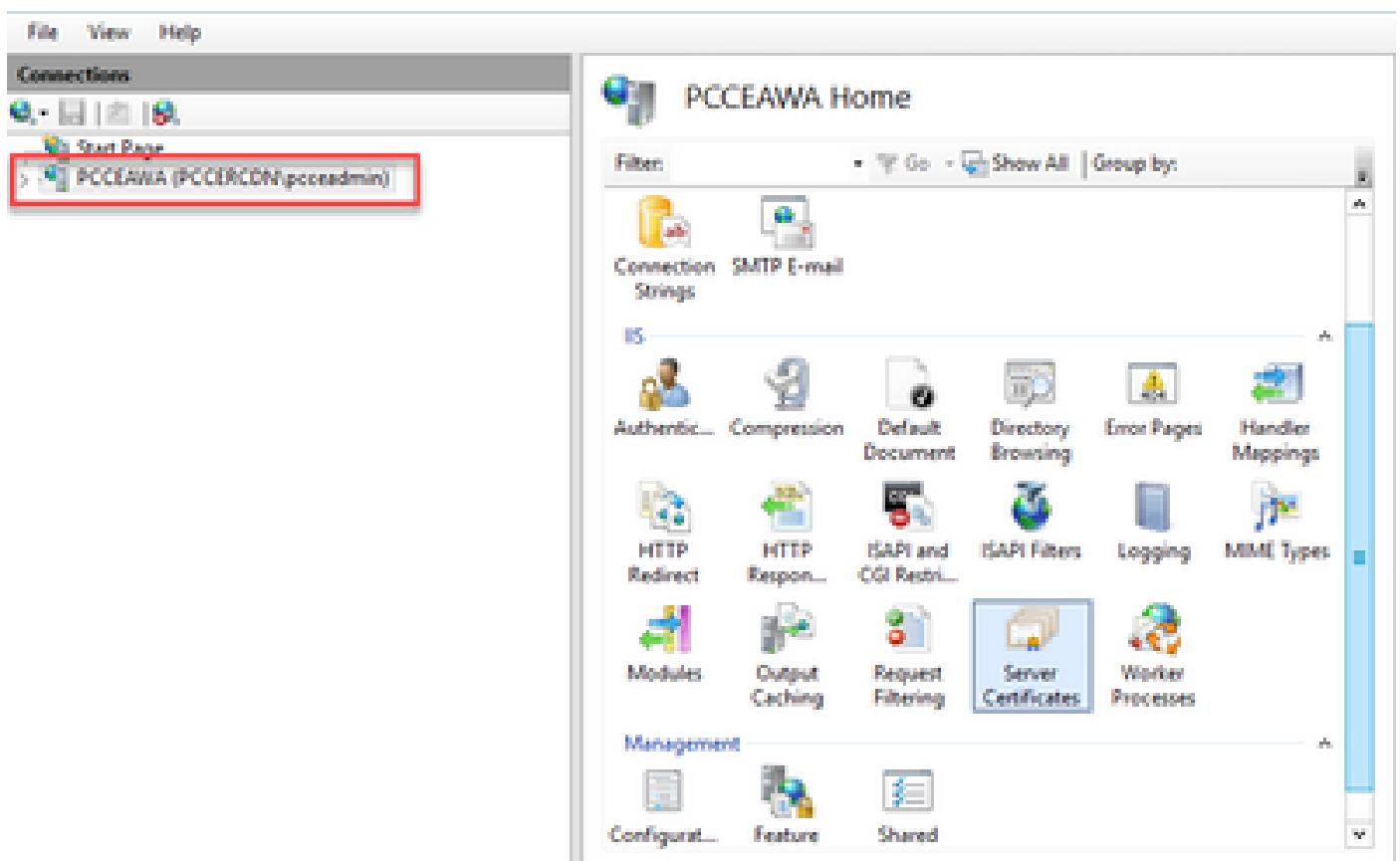
Etapa 2. Obtenha os certificados CA assinados de sua autoridade de certificação (raiz, aplicativo e intermediário, se houver ).

## 3. Carregar os Certificados Assinados pela CA

Etapa 1. Faça login no Windows e escolha Painel de Controle > Ferramentas Administrativas > Gerenciador dos Serviços de Informações da Internet (IIS).

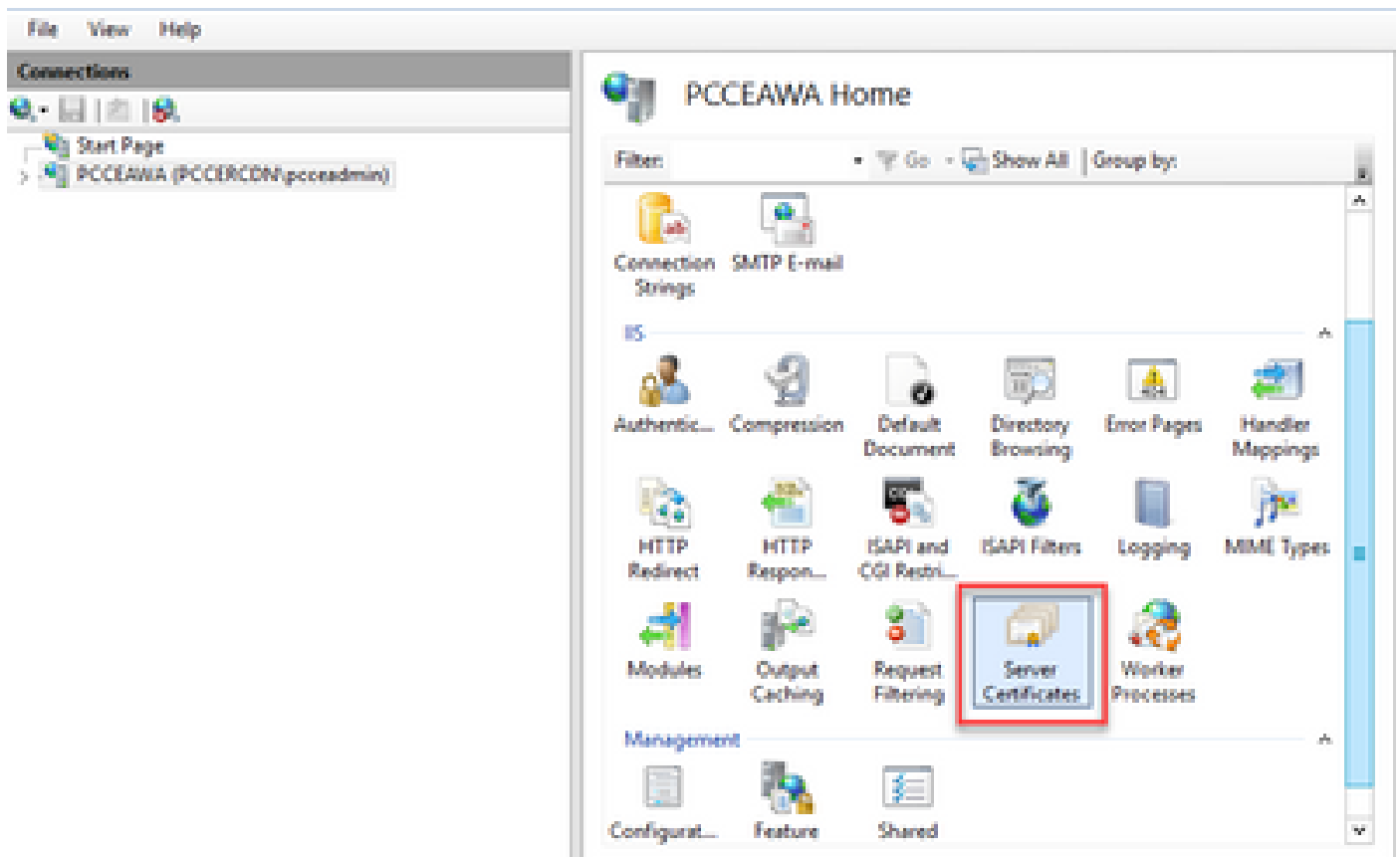


Etapa 2. No painel Conexões, clique no nome do servidor.

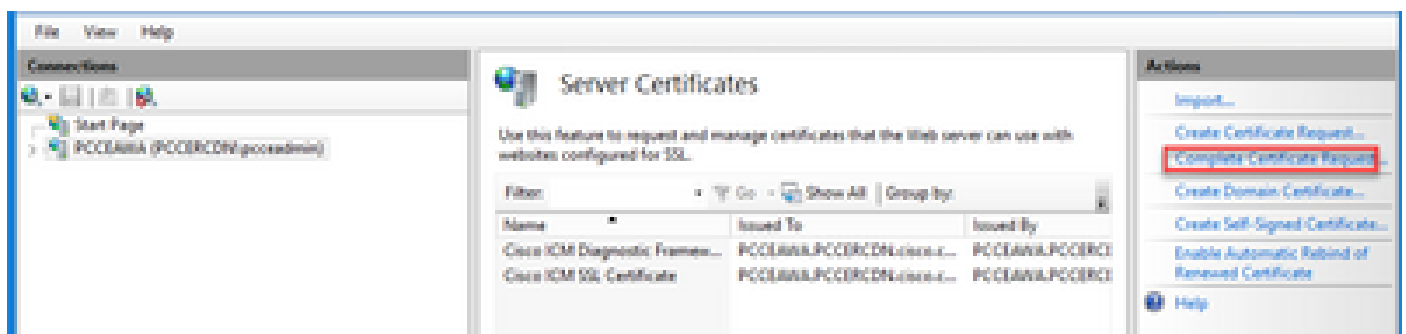


Etapa 3. Na área do IIS, clique duas vezes em Certificados do Servidor.






Etapa 4. No painel Ações, clique em Concluir solicitação de certificado.



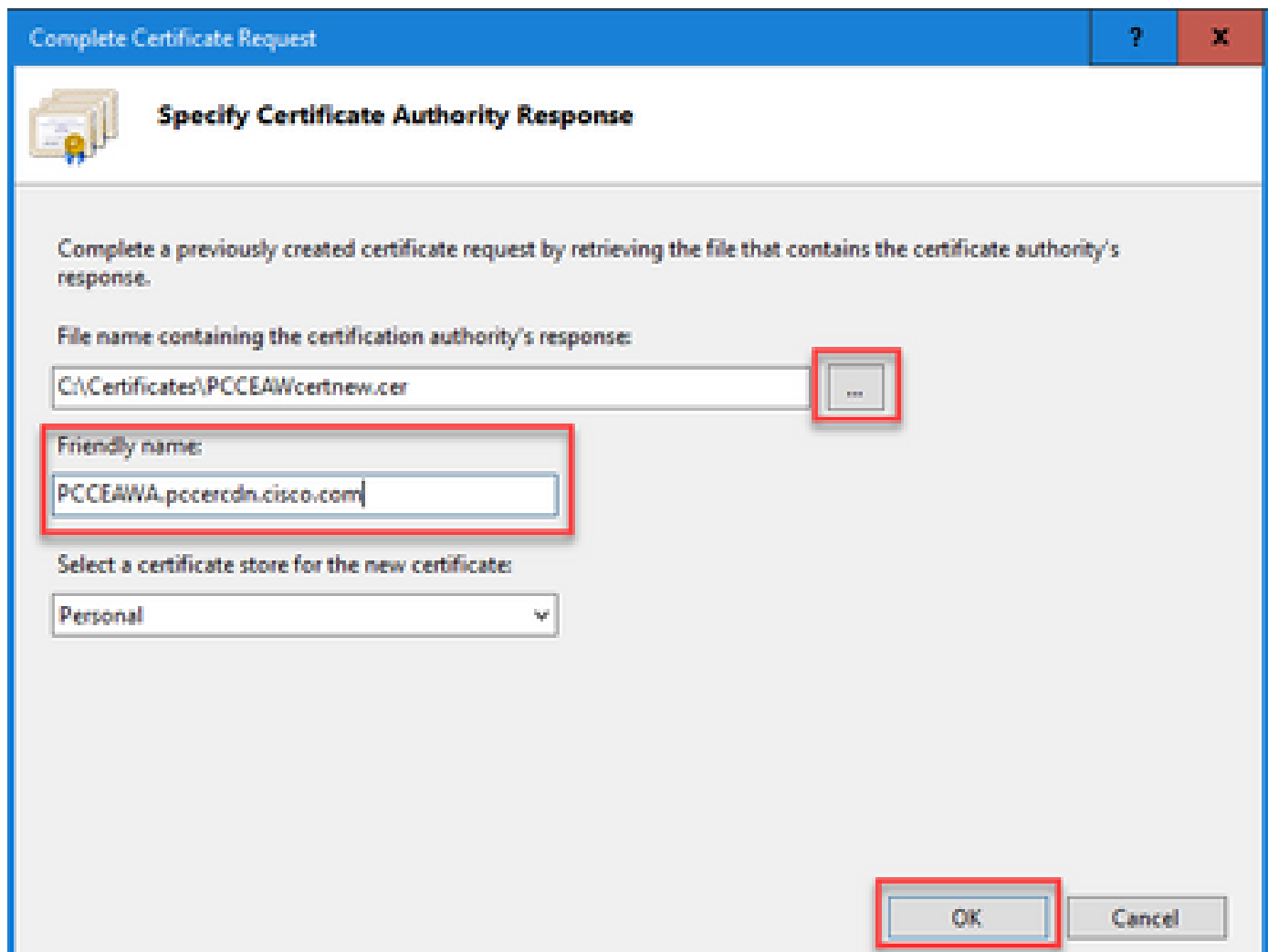
Etapa 5. Na caixa de diálogo Concluir Solicitação de Certificado, preencha estes campos:

No campo Nome do arquivo que contém a resposta da autoridade de certificação, clique no botão ...

Navegue até o local onde o certificado de aplicativo assinado está armazenado e clique em Abrir.

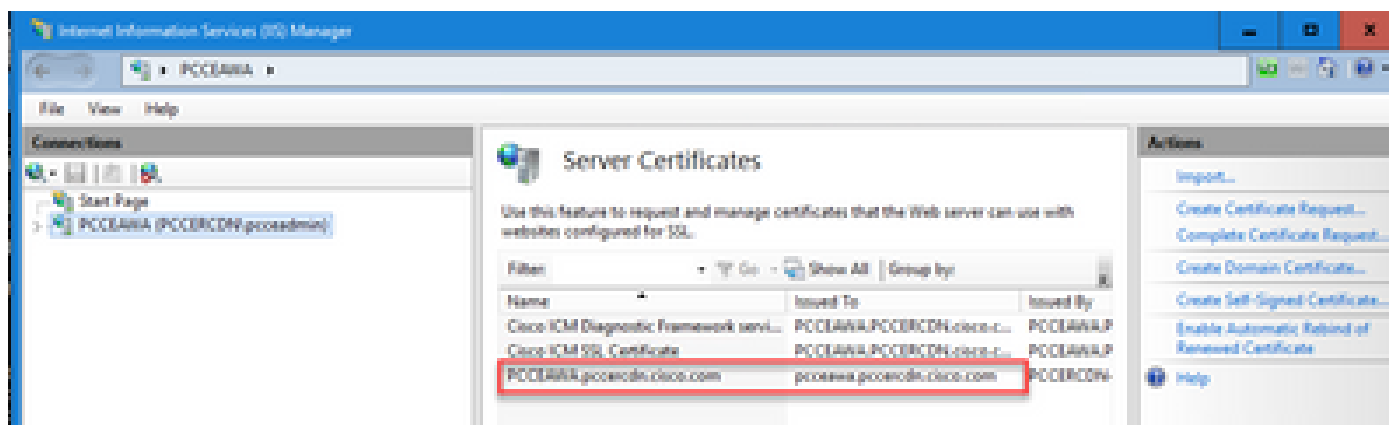
 Observação: se esta for uma implementação de CA de 2 camadas e o certificado raiz ainda não estiver no repositório de certificados do servidor, a raiz precisará ser carregada no Windows Store antes de você importar o certificado assinado. Consulte este documento se precisar carregar a CA raiz na Windows Store <https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate>.

No campo Nome amigável, insira o FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) do servidor ou qualquer nome significativo para você. Certifique-se de que a lista suspensa Selecionar um repositório de certificados para o novo certificado permaneça como Pessoal.



Etapa 6. Clique em OK para carregar o certificado.

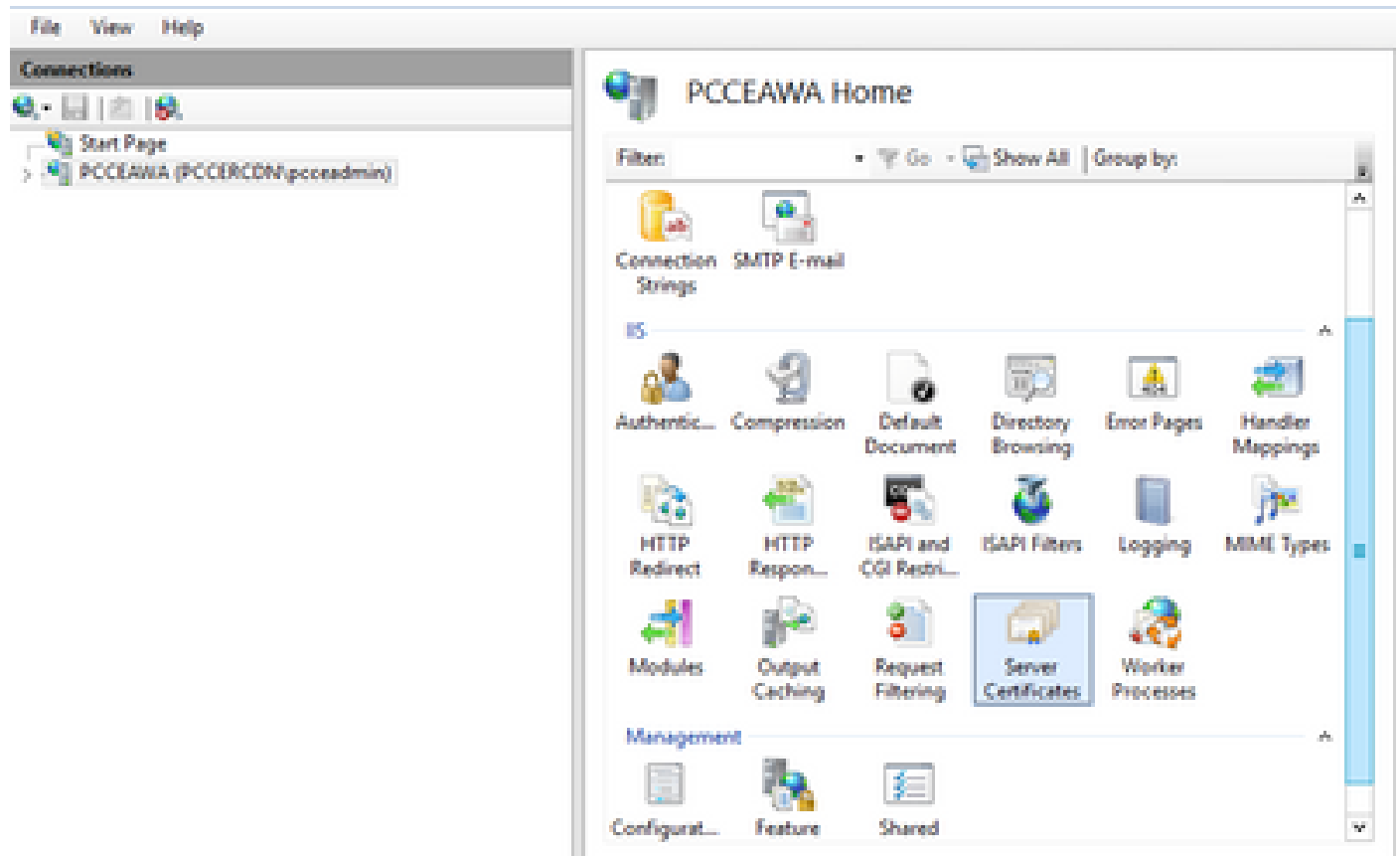
Se o carregamento do certificado for bem-sucedido, o certificado será exibido no painel Certificados do Servidor.



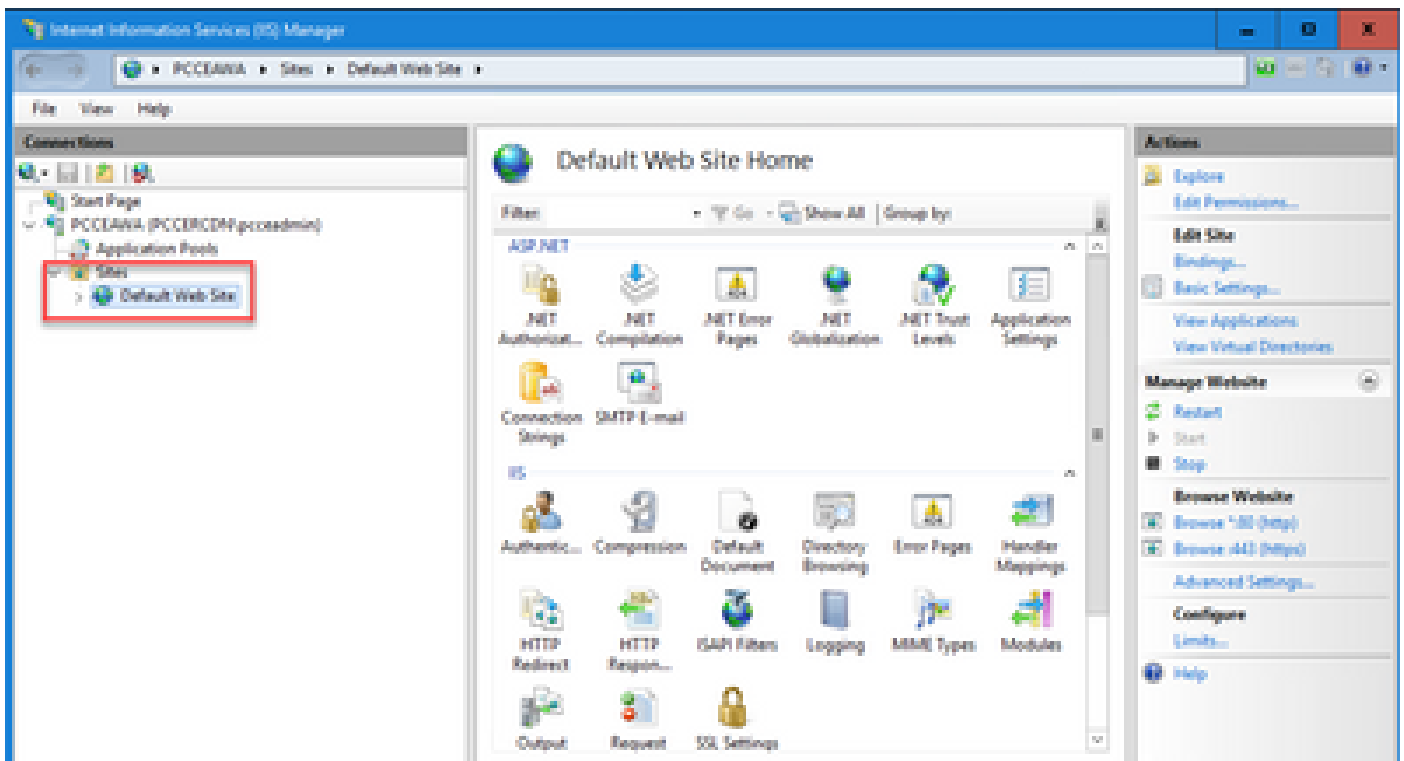
#### 4. Associar o Certificado Assinado pela CA ao IIS

Este procedimento explica como vincular um certificado assinado pela CA no Gerenciador do IIS.

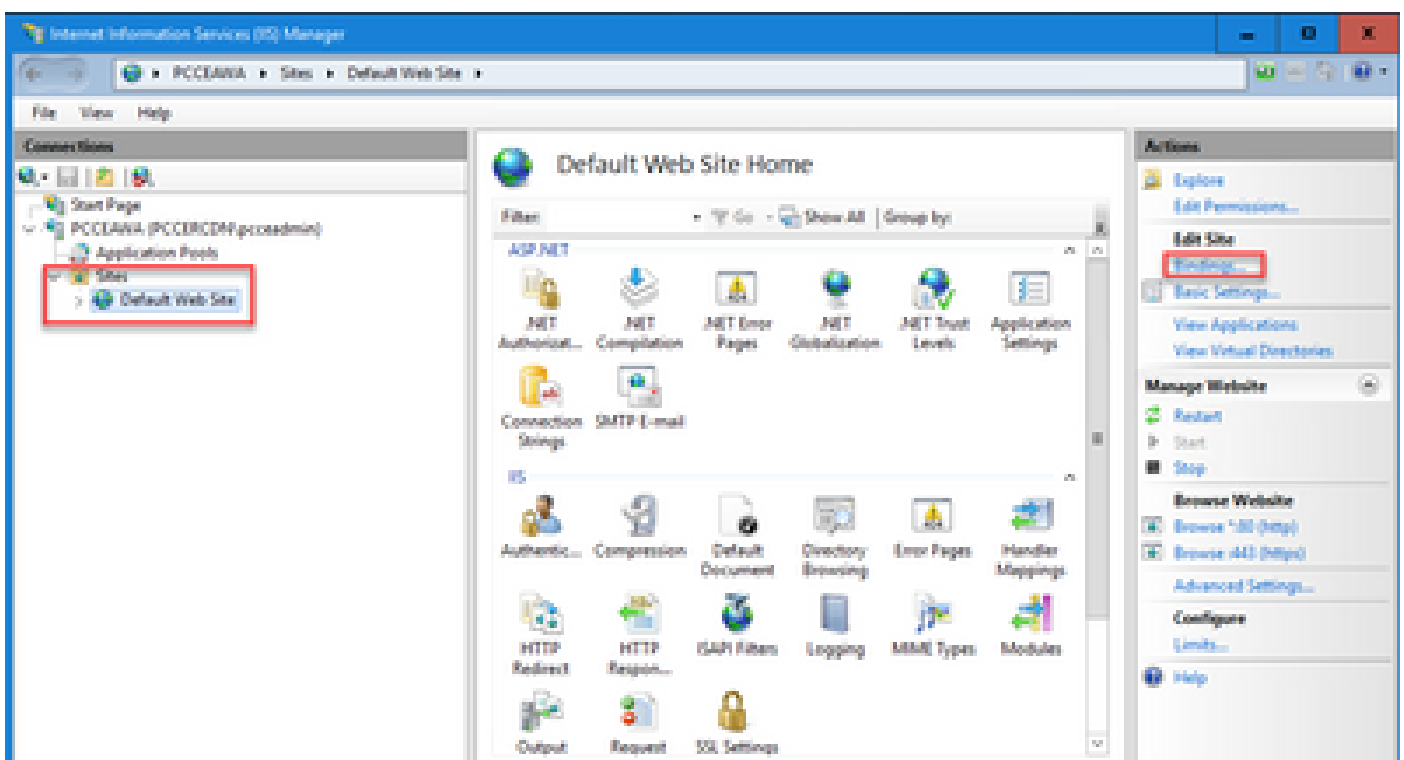
Etapa 1. Faça login no Windows e escolha Painel de Controle > Ferramentas Administrativas > Gerenciador dos Serviços de Informações da Internet (IIS).



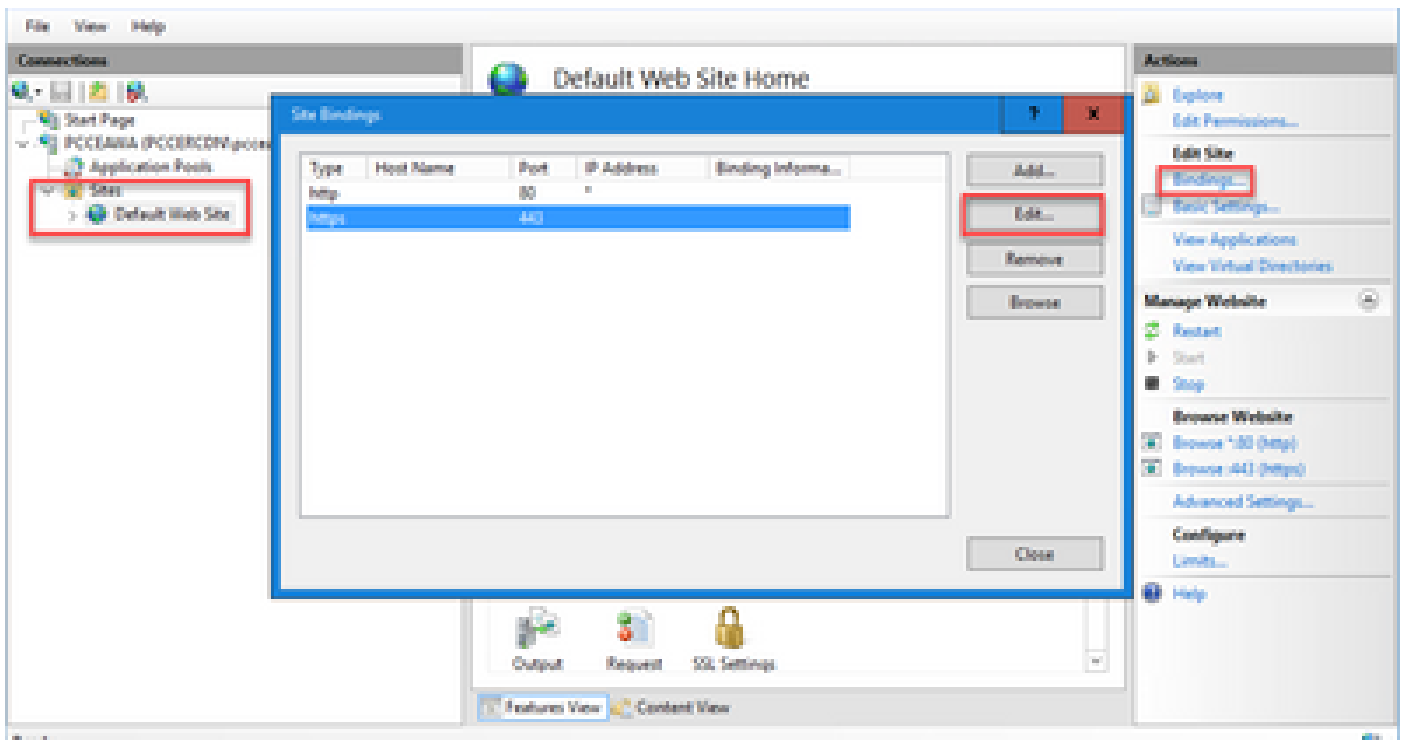
Etapa 2. No painel Conexões, escolha <server\_name> > Sites > Site padrão da Web.



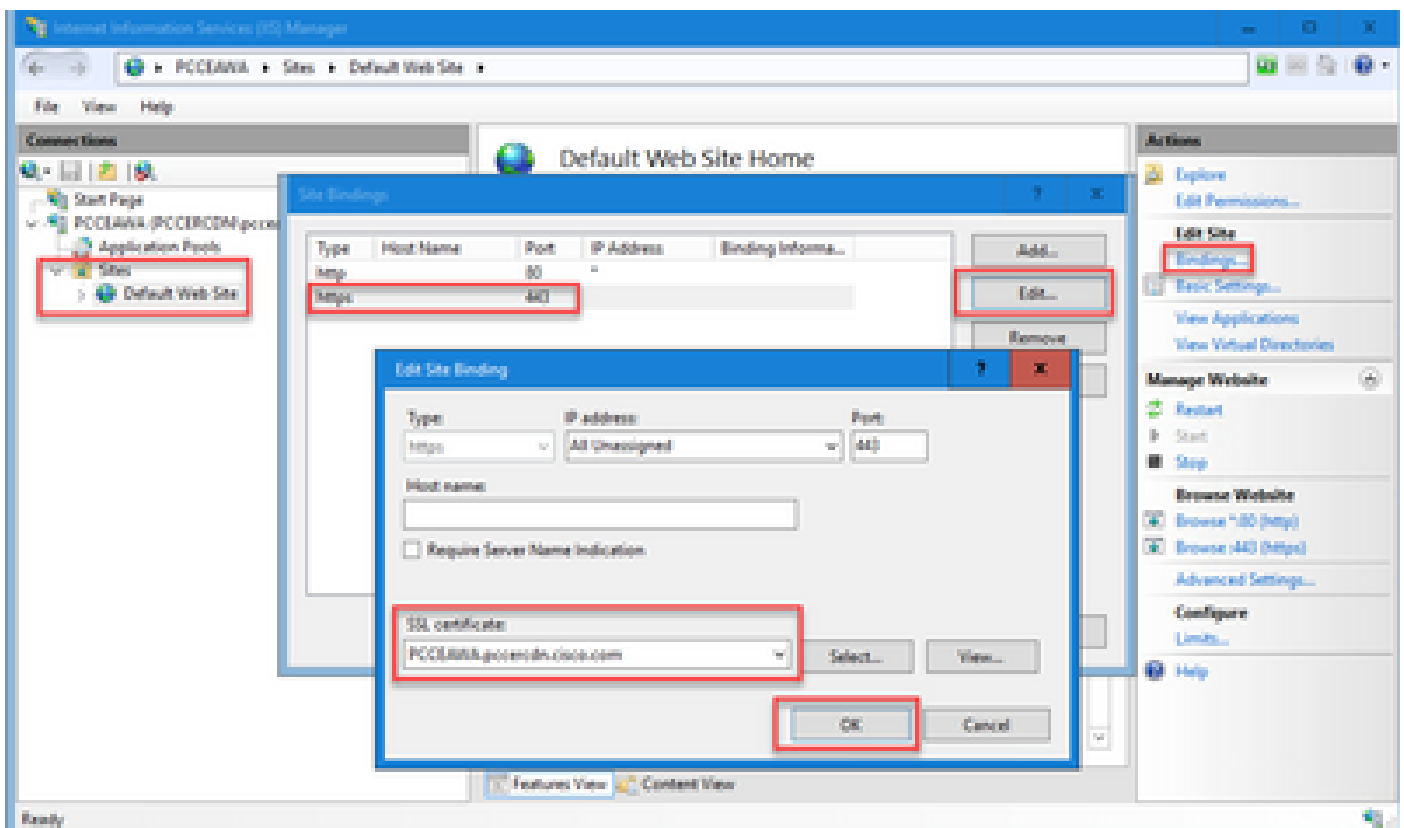
Etapa 3. No painel Ações, clique em Vinculações....



Etapa 4. Clique no tipo https com a porta 443 e clique em Editar....

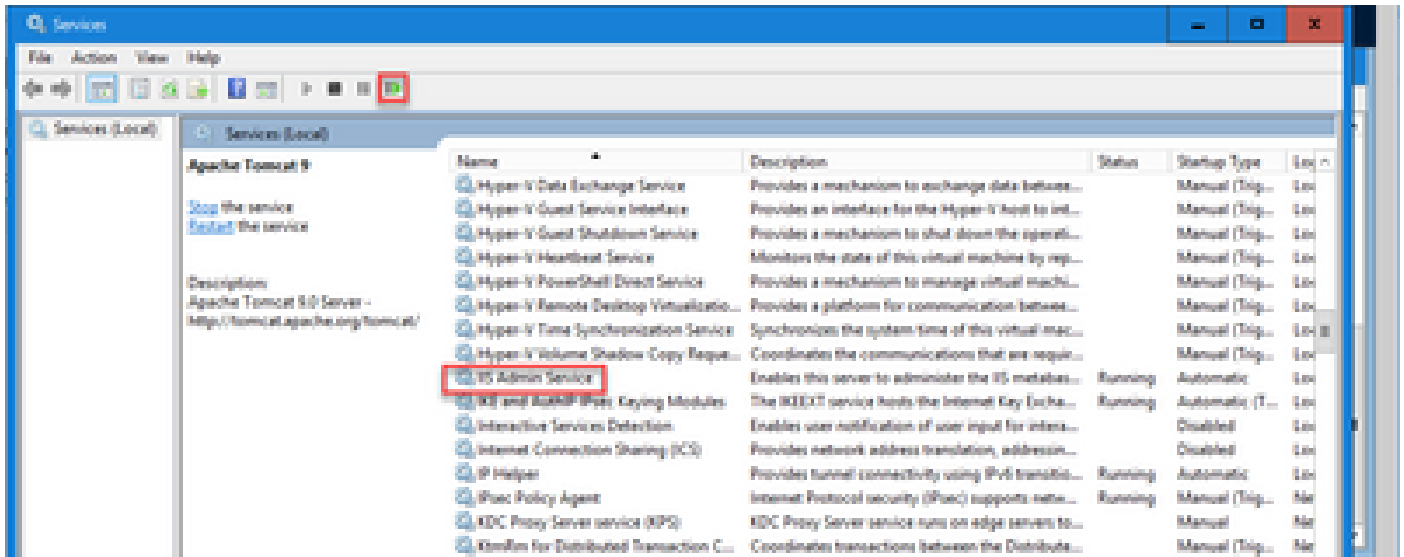


Etapa 5. Na lista suspensa Certificado SSL, selecione o certificado com o mesmo nome amigável fornecido na etapa anterior.



Etapa 6. Click OK.

Passo 7. Navegue até Start > Run > services.msc e reinicie o IIS Admin Service.



Se o IIS for reiniciado com êxito, os avisos de erro de certificado não serão exibidos quando o aplicativo for iniciado.

## 5. Vincular o Certificado Assinado pela CA ao Pórtico de Diagnóstico

Este procedimento explica como vincular um CA Signed Certificate ao Diagnostic Portico.

Etapa 1. Abra o prompt de comando (Executar como administrador).

Etapa 2. Navegue até a pasta inicial do Diagnostic Portico. Execute este comando:

```
cd c:\icm\serviceability\diagnostics\bin
```

Etapa 3. Remova a associação de certificado atual ao Pórtico de Diagnóstico. Execute este comando:

```
DiagFwCertMgr /task:UnbindCert
```

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:UnbindCert
```

```
*****  
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager  
*****
```

```
Executing Task: 'UnbindCert'
```

```
Read port number from service configuration file: '7890'
```

```
ATTEMPTING TO UNBIND CERTIFICATE FROM WINDOWS HTTP SERVICE
```

```
Binding IP Address: '0.0.0.0:7890'
```

```
Attempting to delete the existing binding on 0.0.0.0:7890
```

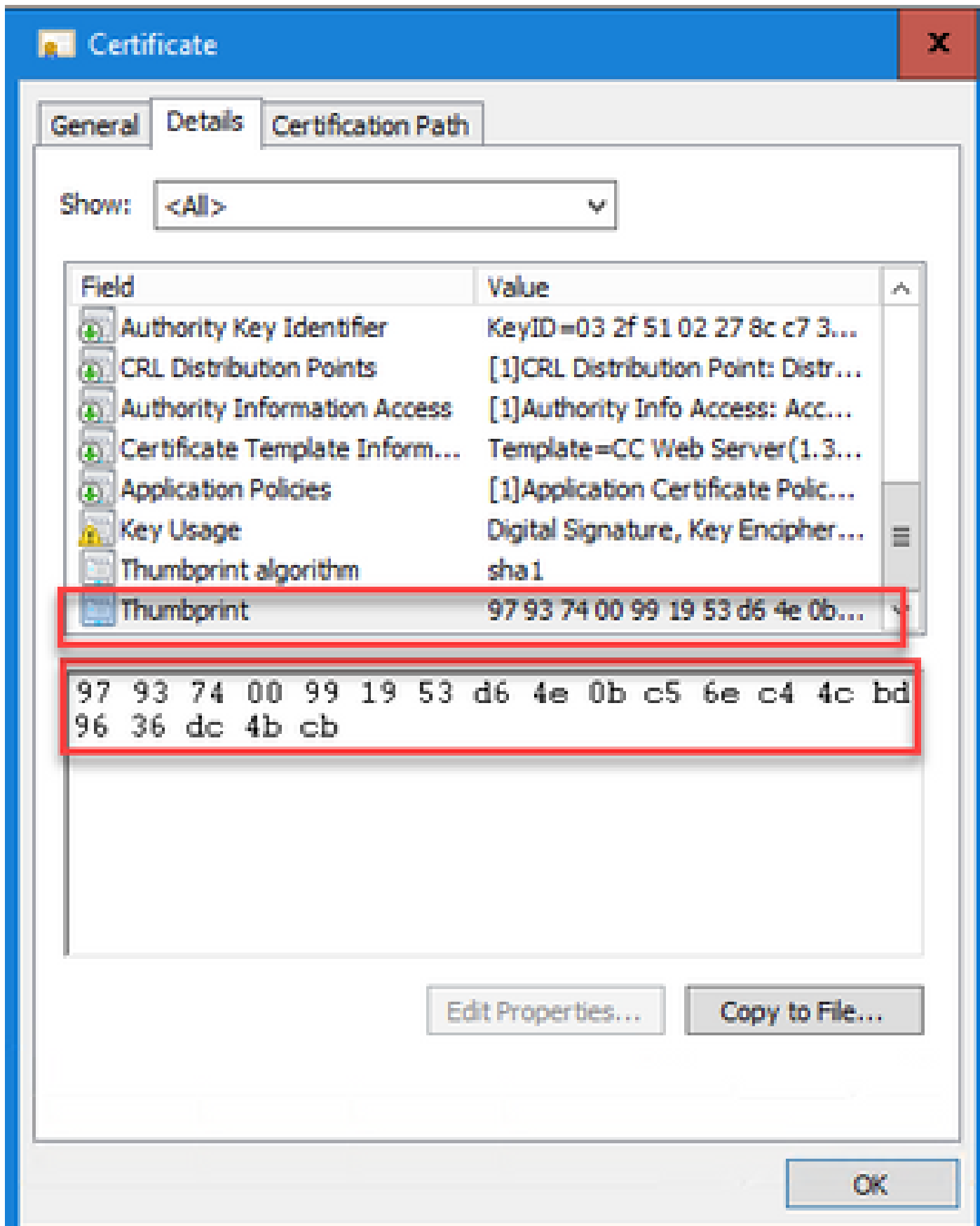
```
Deleted existing binding successfully
```

```
Deleted entry from the service registry
```

```
ALL TASKS FOR UNBINDING THE CERTIFICATE FROM HTTP SERVICE COMPLETED SUCCESSFULLY
```

```
c:\icm\serviceability\diagnostics\bin>_
```

Etapa 4. Abra o certificado assinado e copie o conteúdo de hash (sem espaços) do campo Impressão digital.



Etapa 5. Execute este comando e cole o conteúdo de hash.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```



```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953D64E08C56EC44CB09636DC4BCB0C4Bcb

Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*****

Executing Task: 'BindCertFromStore'
Read port number from service configuration file: '7890'
Certhash Argument Passed: '97937400991953D64E08C56EC44CB09636DC4BCB'
ATTEMPTING TO BIND CERTIFICATE WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Trying to look up certificate: 97937400991953D64E08C56EC44CB09636DC4BCB
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
Certificate bind with HTTP service on 0.0.0.0:7890 completed successfully
Found existing registry key for the service
Hash of certificate used saved in the service registry
ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>
```

Se a associação de certificado for bem-sucedida, será exibida a mensagem A associação de certificado é VÁLIDA.

Etapa 6. Valide se a associação de certificado foi bem-sucedida. Execute este comando:

DiagFwCertMgr /task:ValidateCertBinding

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding

Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*****

Executing Task: 'ValidateCertBinding'
Read port number from service configuration file: '7890'
ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to query HTTP service for SSL certificate binding
Found a certificate binding on 0.0.0.0:7890
Attempting to locate this certificate in the Local Computer certificate store
Trying to look up certificate: 97937400991953D64E08C56EC44CB09636DC4BCB
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
The certificate binding is VALID
Certificate hash stored in service registry matches certificate used by service
ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>
```

 Observação: DiagFwCertMgr usa a porta 7890 por padrão.

Se a associação de certificado for bem-sucedida, será exibida a mensagem A associação de

certificado é VÁLIDA.


Passo 7. Reinicie o serviço Estrutura de Diagnóstico. Execute estes comandos:

```
net stop DiagFwSvc  
net start DiagFwSvc
```

Se o Diagnostic Framework for reiniciado com êxito, os avisos de erro de certificado não serão exibidos quando o aplicativo for iniciado.

6. Importe o Certificado Raiz e Intermediário para o Armazenamento de Chaves Java

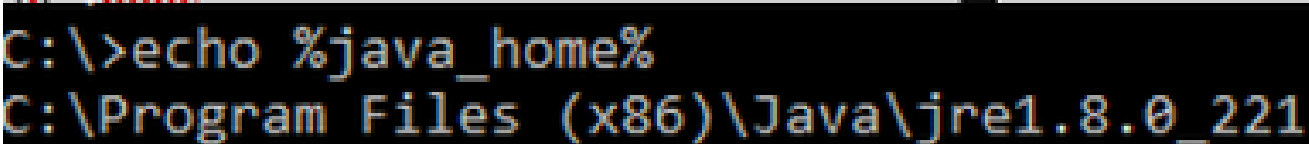
---

 Cuidado: antes de começar, você deve fazer backup do armazenamento de chaves e executar os comandos a partir do java home como um Administrador.

---

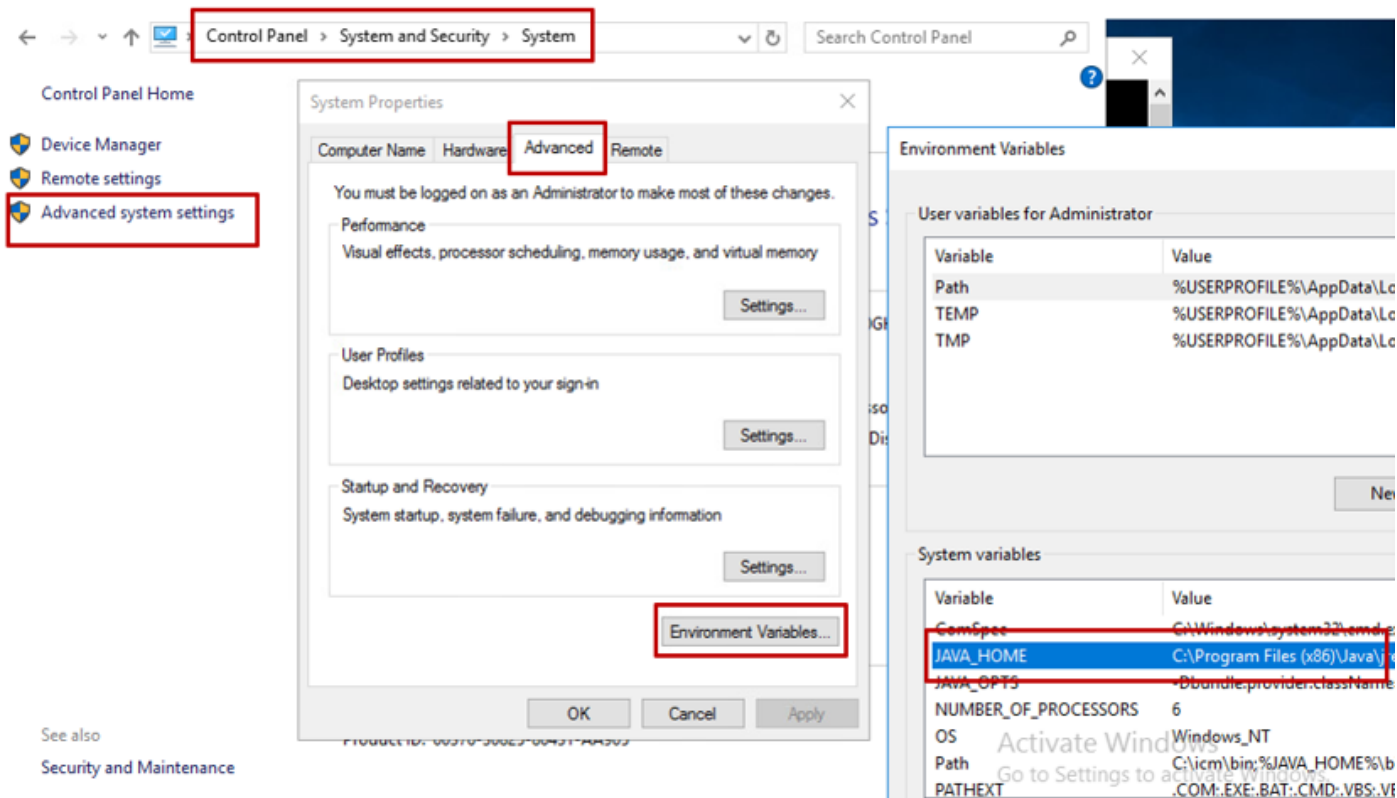
Etapa 1. Conheça o caminho do home do java para garantir onde o keytool do java está hospedado. Há algumas maneiras de encontrar o caminho do início java.


Opção 1: Comando CLI: echo %JAVA\_HOME%



```
C:\>echo %java_home%  
C:\Program Files (x86)\Java\jre1.8.0_221
```

Opção 2: manualmente via configuração de sistema avançada, como mostrado na imagem




 Observação: no UCCE 12.5, o caminho padrão é C:\Program Files (x86)\Java\jre1.8.0\_221\bin. No entanto, se você tiver usado o instalador 12.5(1a) ou tiver o 12.5 ES55 instalado (obrigatório OpenJDK ES), use CCE\_JAVA\_HOME em vez de JAVA\_HOME, pois o caminho do armazenamento de dados foi alterado com OpenJDK. Mais informações sobre a migração do OpenJDK no CCE e no CVP nestes documentos: [Instalar e migrar para o OpenJDK no CCE 2.5\(1\)](#) e [Instalar e migrar para o OpenJDK no CVP 12.5\(1\)](#).

Etapa 2. Faça backup do arquivo cacerts da pasta C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security. Você pode copiá-lo para outro local.

Etapa 3. Abra uma janela de comando como Administrador para executar o comando:

```
keytool.exe -keystore ./cacerts -import -file <path where the Root, or Intermediate certificate are sto
```


 Observação: os certificados específicos necessários dependem da autoridade de certificação que você usa para assinar seus certificados. Em uma autoridade de certificação de dois níveis, que é típica de autoridades de certificação públicas e mais segura do que as internas, você precisa importar os certificados raiz e intermediários. Em uma CA autônoma sem intermediários, que geralmente é vista em um laboratório ou em uma CA interna mais simples, você só precisa importar o certificado raiz.

## Solução CVP


### 1. Gerar Certificados com FQDN

Este procedimento explica como gerar certificados com o FQDN para os serviços Web Service Manager (WSM), Voice XML (VXML), Call Server e Operations Management (OAMP).

---

 Observação: quando você instala o CVP, o nome do certificado inclui apenas o nome do servidor e não o FQDN, portanto, você precisa gerar novamente os certificados.

---

 Cuidado: antes de começar, você deve fazer o seguinte:

1. Obtenha a senha do armazenamento de chaves. Execute o comando: `more %CVP_HOME%\conf\security.properties`. Essa senha é necessária ao executar os comandos `keytool`.
2. Copie a pasta `%CVP_HOME%\conf\security` para outra pasta.
3. Abra uma janela de comando como Administrador para executar os comandos.

---

### Servidores CVP

Etapa 1. Para excluir os servidores CVP, os certificados executam estes comandos:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a  
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a  
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```


Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Para gerar o certificado WSM, execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Digite a senha do armazenamento de chaves quando solicitado.


---

 Observação: por padrão, os certificados são gerados por dois anos. Use `-valid XXXX` para definir a data de expiração quando os certificados forem gerados novamente; caso contrário, os certificados serão válidos por 90 dias e precisarão ser assinados por uma CA antes dessa data. Para a maioria desses certificados, 3 a 5 anos devem ser um tempo de validação razoável.

---

Aqui estão algumas entradas de validade padrão:

Um ano	365
Dois anos	730
Três anos	1095
Quatro anos	1460
Cinco anos	1895
Dez anos	3650

 Cuidado: em 12.5, os certificados devem ser SHA 256, Key Size 2048 e encryption Algorithm RSA, use estes parâmetros para definir estes valores: -keyalg RSA e -keysize 2048. É importante que os comandos keystore do CVP incluam o parâmetro -storetype JCEKS. Se isso não for feito, o certificado, a chave, ou pior, o armazenamento de chaves pode se tornar corrompido.

Especifique o FQDN do servidor na pergunta qual é seu nome e sobrenome?

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore -alias w
m_certificate1 -keysize 2048 -keyalg RSA
Enter keystore password:
what is your first and last name?
[Unknown]: cvp.bona.com
what is the name of your organizational unit?
[Unknown]:
```

Responda a estas outras perguntas:

Qual é o nome da sua unidade organizacional?

[Desconhecido]: <especificar UO>

Qual é o nome da sua empresa?

[Desconhecido]: <especifique o nome da organização>

Qual é o nome da sua cidade ou localidade?

[Desconhecido]: <especifique o nome da cidade/localidade>

Qual é o nome do seu estado ou província?

[Desconhecido]: <especifique o nome do estado/província>

Qual é o código de duas letras do país para essa unidade?

[Desconhecido]: <especifique o código de país com duas letras>

Especifique yes para as duas próximas entradas.

Etapa 3. Execute as mesmas etapas para vxml\_certificate e callserver\_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

## servidor de relatórios CVP

Etapa 1. Para excluir o WSM e os certificados do servidor de relatórios, execute estes comandos:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Para gerar o certificado WSM, execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Digite a senha do armazenamento de chaves quando solicitado.

Especifique o FQDN do servidor para a consulta qual é seu nome e sobrenome? e continue com as mesmas etapas como feito com os servidores CVP.

Etapa 3. Execute as mesmas etapas para callserver\_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

## CVP OAMP (implantação do UCCE)

Como na solução PCCE versão 12.x todos os componentes da solução são controlados pelo SPOG e o OAMP não está instalado, essas etapas são necessárias apenas para uma solução de implantação do UCCE.

Etapa 1. Para excluir os certificados do servidor WSM e OAMP, execute estes comandos:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Para gerar o certificado WSM, execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Digite a senha do armazenamento de chaves quando solicitado.

Especifique o FQDN do servidor para a consulta qual é seu nome e sobrenome? e continue com as mesmas etapas como feito com os servidores CVP.


Etapa 3. Execute as mesmas etapas para oamp\_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Digite a senha do armazenamento de chaves quando solicitado.

## 2. Gerar o CSR

---

 Observação: o navegador compatível com RFC5280 requer que o Nome Alternativo do Assunto (SAN) seja incluído em cada certificado. Isso pode ser feito usando o parâmetro -ext com SAN ao gerar o CSR.

---

### Nome Alternativo do Assunto

O parâmetro -ext permite que um usuário especifique extensões. O exemplo mostrado adiciona um nome alternativo de requerente (SAN) com o nome de domínio totalmente qualificado (FQDN) do servidor, bem como o host local. Campos SAN adicionais podem ser adicionados como valores separados por vírgula.

Os tipos válidos de SAN são:

```
ip:192.168.0.1  
dns:myserver.mydomain.com  
email:name@mydomain.com
```

Por exemplo: `-ext san=dns:mycwp.mydomain.com,dns:localhost`

## Servidores CVP

Etapa 1. Gere a solicitação de certificado para o alias. Execute este comando e salve-o em um arquivo (por exemplo, `wsm_certificate`):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Execute as mesmas etapas para `vxml_certificate` e `callserver_certificate`:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

Digite a senha do armazenamento de chaves quando solicitado.

## servidor de relatórios CVP

Etapa 1. Gere a solicitação de certificado para o alias. Execute este comando e salve-o em um arquivo (por exemplo, `wsmreport_certificate`):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Execute as mesmas etapas para o `callserver_certificate`:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```



Digite a senha do armazenamento de chaves quando solicitado.

## CVP OAMP (implantação do UCCE)

Etapa 1. Gere a solicitação de certificado para o alias. Execute este comando e salve-o em um arquivo (por exemplo, oamp\_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -v  
Ensure to replace "mycvp.mydomain.com" with your OAMP FQDN.  
Enter the keystore password when prompted.
```

Etapa 2. Execute as mesmas etapas para oamp\_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -v
```

Digite a senha do armazenamento de chaves quando solicitado.

## 3. Obter os Certificados Assinados pela CA

Etapa 1. Assine os certificados em uma autoridade de certificação (WSM, Callserver e VXML server para o servidor CVP; WSM e OAMP para o servidor CVP OAMP e WSM e Callserver para o servidor Reporting).

Etapa 2. Baixe os certificados de aplicativo e o certificado raiz da autoridade de certificação.

Etapa 3. Copie o certificado raiz e os certificados assinados pela autoridade de certificação na pasta %CVP\_HOME%\conf\security\ de cada servidor.

## 4. Importar os Certificados Assinados pela CA

Aplique estas etapas a todos os servidores da solução CVP. Somente os certificados para componentes nesse servidor precisam ter o certificado assinado pela autoridade de certificação importado.

Etapa 1. Importe o certificado raiz. Execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.

Se houver um certificado intermediário, execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias intermediate_ca -file
```

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.

Etapa 2. Importe o WSM assinado pela CA para esse certificado de servidor ( CVP, Reporting and OAMP). Execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.

Etapa 3. Nos servidores CVP e nos servidores de relatórios, importe o certificado CA Signed do Callserver. Execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.


Etapa 4. Nos servidores CVP, importe o certificado assinado da autoridade de certificação do servidor VXML. Execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Etapa 5. No servidor CVP OAMP (somente para UCCE), importe o certificado CA Signed do servidor OAMP. Execute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Etapa 6. Reinicialize os servidores.

 Observação: na implantação do UCCE, certifique-se de adicionar os servidores ( Reporting, CVP Server e assim por diante) no CVP OAMP com o FQDN fornecido quando você gerou o CSR.

## Servidores VOS

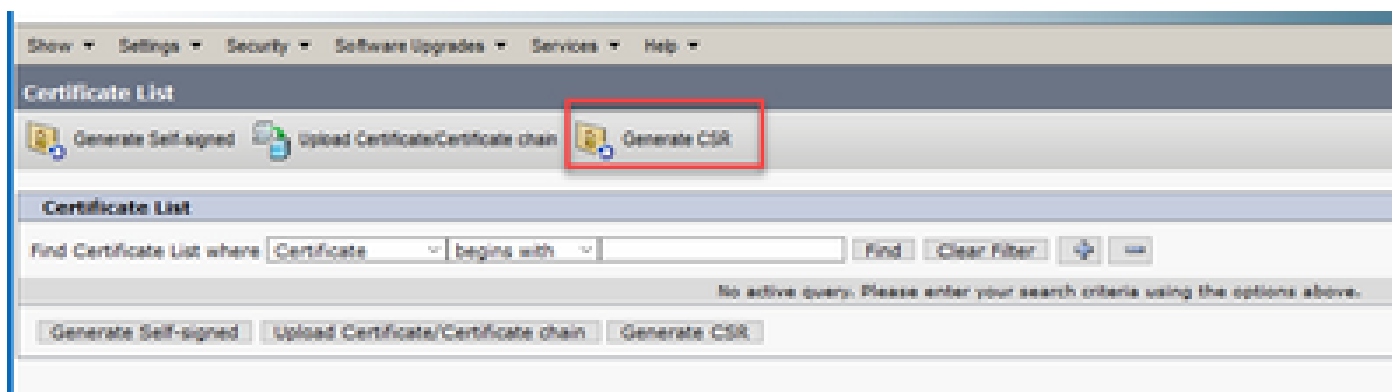
### 1. Gerar Certificado CSR

Este procedimento explica como gerar o certificado Tomcat CSR a partir de plataformas baseadas no Cisco Voice Operating System (VOS). Esse processo se aplica a todos os aplicativos baseados em VOS, como:

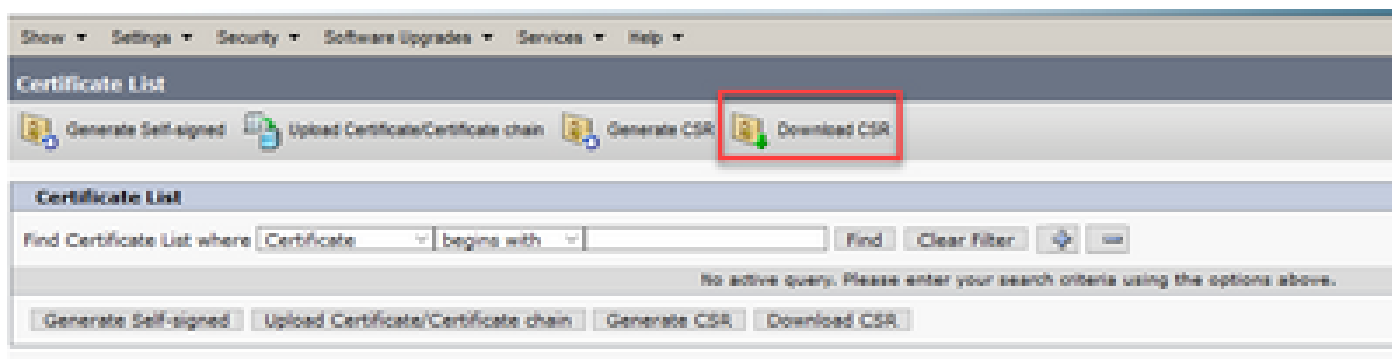
- CUCM
- Finesse
- CUIC \ Live Data (LD) \ Identity Server(IDS)
- Conexão em nuvem
- Cisco VVB

Etapa 1. Navegue para a página de administração do sistema operacional Cisco Unified Communications: <https://FQDN:<8443 ou 443>/cmplatform>.

Etapa 2. Navegue para Segurança > Gerenciamento de certificado e selecione Gerar CSR.



Etapa 3. Depois que o certificado CSR for gerado, feche a janela e selecione Download CSR.



Etapa 4. Certifique-se de que a finalidade do certificado seja tomcat e clique em Download CSR.


Download Certificate Signing Request - Mozilla Firefox

https://10.201.224.234/cmplatform/certificateDownloadNewCsr.do

### Download Certificate Signing Request

Download CSR Close


**Status**

 Certificate names not listed below do not have a corresponding CSR.

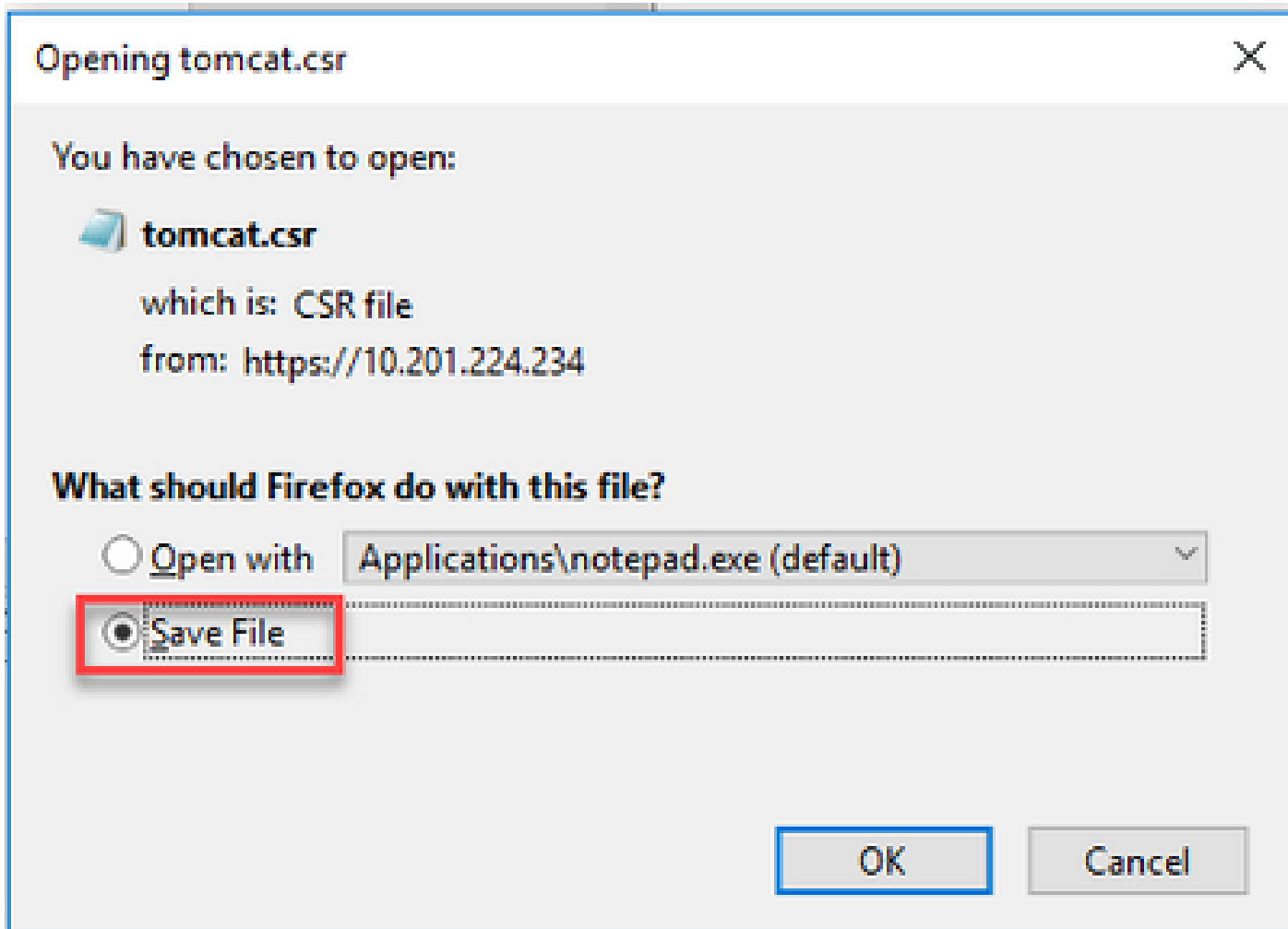
**Download Certificate Signing Request**

Certificate Purpose\* tomcat

Download CSR Close

 \*- indicates required item.

Etapa 5. Clique em Save File. O arquivo é salvo na pasta Download.



## 2. Obter os Certificados Assinados pela CA

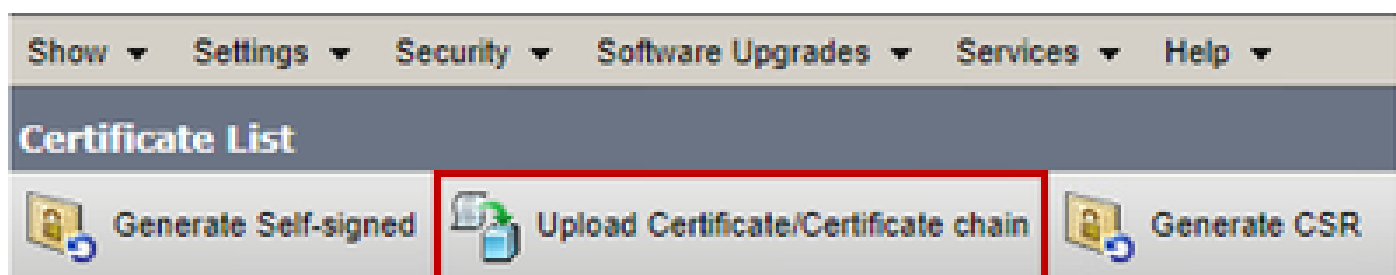
Etapa 1. Assinar o certificado tomcat exportado em uma autoridade de certificação.

Etapa 2. Baixe o aplicativo e a raiz certificada da autoridade de certificação.

## 3. Carregar o Aplicativo e Certificados Raiz

Etapa 1. Navegue para a página de administração do sistema operacional Cisco Unified Communications: <https://FQDN:<8443 ou 443>/cmplatform>.

Etapa 2. Navegue para Segurança > Gerenciamento de Certificado e selecione Carregar Certificado/Cadeia de Certificado.



Etapa 3. Na janela Carregar certificado/cadeia de certificados, selecione tomcat-trust no campo de finalidade do certificado e carregue o certificado raiz.

**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose<sup>®</sup> tomcat-trust

Description(friendly name)

Upload File Choose File No file chosen

Upload Close

Etapa 4. Carregue um certificado intermediário (se houver ) como um tomcat-trust.

Etapa 5. Na janela Upload certificate/Certificate chain, selecione now tomcat no campo Certificate Purpose e carregue o certificado assinado da CA do aplicativo.

### Upload Certificate/Certificate chain

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose <sup>*</sup>	tomcat
Description(friendly name)	Self-signed certificate
Upload File	Browse... No file selected.

Upload Close

**i** <sup>\*</sup> - indicates required item.

Etapa 6. Reinicialize o servidor.

## Verificar

Após reinicializar o servidor, execute estas etapas para verificar a implementação assinada pela CA:

Etapa 1. Abra um navegador da Web e limpe o cache.

Etapa 2. Feche e abra o navegador novamente.

Agora você deve ver o switch de certificado para iniciar o certificado assinado pela CA e a indicação na janela do navegador de que o certificado é autoassinado e, portanto, não confiável, deve desaparecer.

## Troubleshooting

Não há etapas para solucionar problemas da implementação dos certificados CA Signed neste guia.

## Informações Relacionadas

- Guia de configuração do CVP: [Guia de configuração do CVP - Segurança](#)

- Guia de configuração do UCCE: [Guia de configuração do UCCE - Segurança](#)
- Guia de administração do PCCE: [Guia de administração do PCE - Segurança](#)
- Certificados UCCE AutoAssinados: [Exchange Certificados UCCE AutoAssinados](#)
- Certificados com assinatura automática do PCCE: [certificados com assinatura automática do Exchange](#)
- Instalar e migrar para OpenJDK no CCE 12.5(1): [migração do CCE OpenJDK](#)
- Instalar e migrar para OpenJDK no CVP 12.5(1): [migração do CVP OpenJDK](#)

[Suporte Técnico e Documentação - Cisco Systems](#)



## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.