在CCE解决方案中实施CA签名证书

目录

简介

本文档介绍如何在Cisco Contact Center Enterprise(CCE)解决方案中实施证书颁发机构(CA)签名证书。

作者：Anuj Bhatia、Robert Rogier和Ramiro Amaya，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 统一联络中心企业版(UCCE)版本12.5(1)
- 套装联络中心企业版12.5(1)

- 客户语音门户(CVP)版本12.5(1)
- 思科虚拟化语音浏览器(VVB)
- 思科CVP操作和管理控制台(OAMP)
- 思科统一情报中心(CUIC)
- Cisco Unified Communications Manager (CUCM)

使用的组件

本文档中的信息基于以下软件版本：

- PCCE 12.5(1)
- CVP 12.5(1)
- 思科VVB 12.5
- Finess 12.5
- CUIC 12.5
- Windows 2016

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

证书用于确保客户端和服务器之间的身份验证通信安全。

用户可以从CA购买证书，也可以使用自签名证书。

自签名证书（顾名思义）由身份经过其认证的同一实体签名，而不是由证书颁发机构签名。自签名证书并不像CA证书那样安全，但是在许多应用程序中默认使用自签名证书。

在Package Contact Center Enterprise(PCCE)解决方案版本12.x中，该解决方案的所有组件均由单一平台(SPOG)控制，该平台托管在主要管理工作站(AW)服务器中。

由于PCCE 12.5(1)版本中的安全管理合规性(SRC),SPOG和解决方案中的其他组件之间的所有通信都通过安全的HTTP协议完成。在UCCE 12.5中，组件之间的通信也通过安全HTTP协议完成。

本文档详细介绍在CCE解决方案中实施CA签名证书以实现安全HTTP通信所需的步骤。有关任何其他UCCE安全注意事项，请参阅UCCE安全指南。有关不同于安全HTTP的其他CVP安全通信，请参阅CVP配置指南：CVP安全指南中的安全指南。

步骤

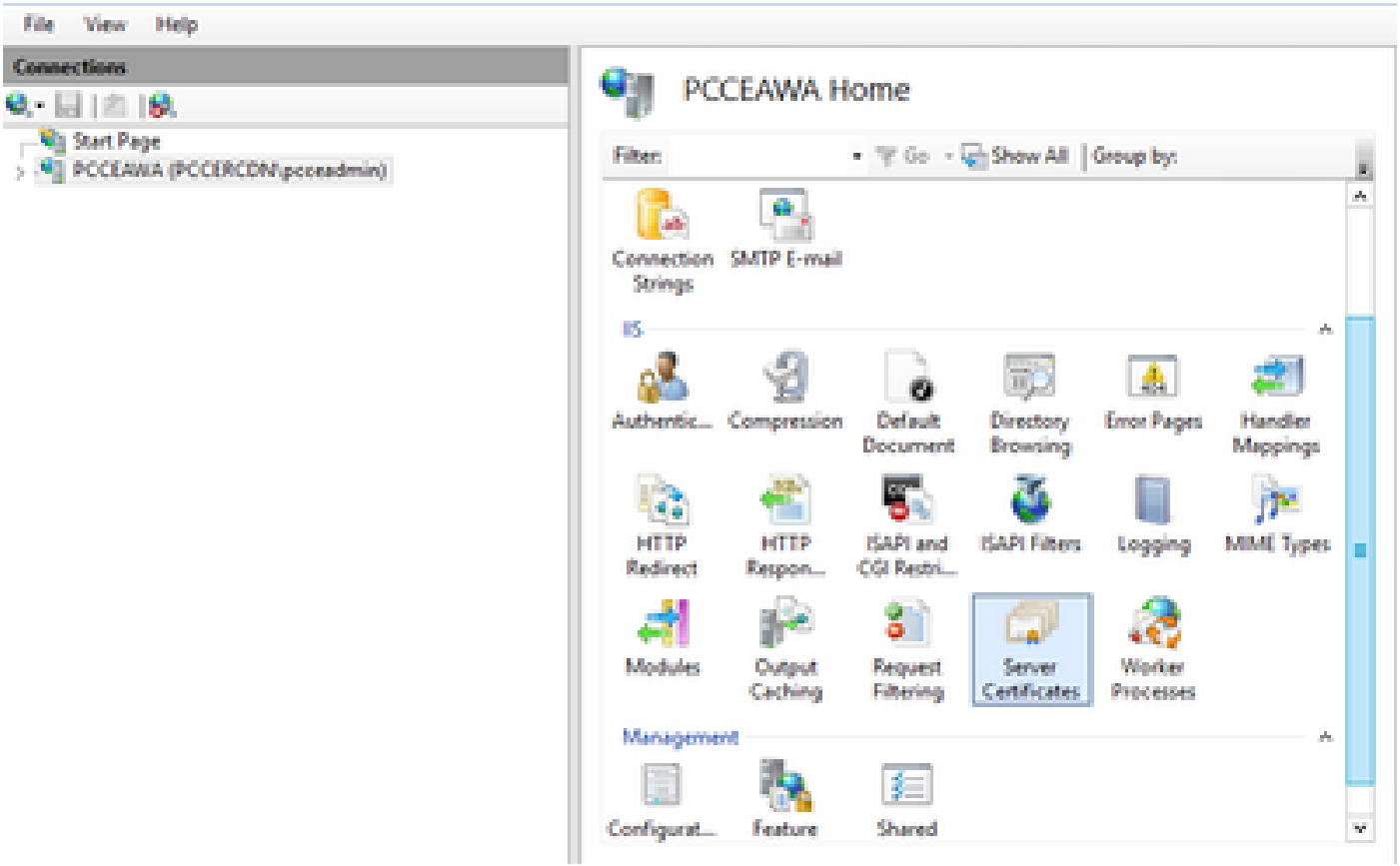
基于CCE Windows的服务器

1.生成CSR

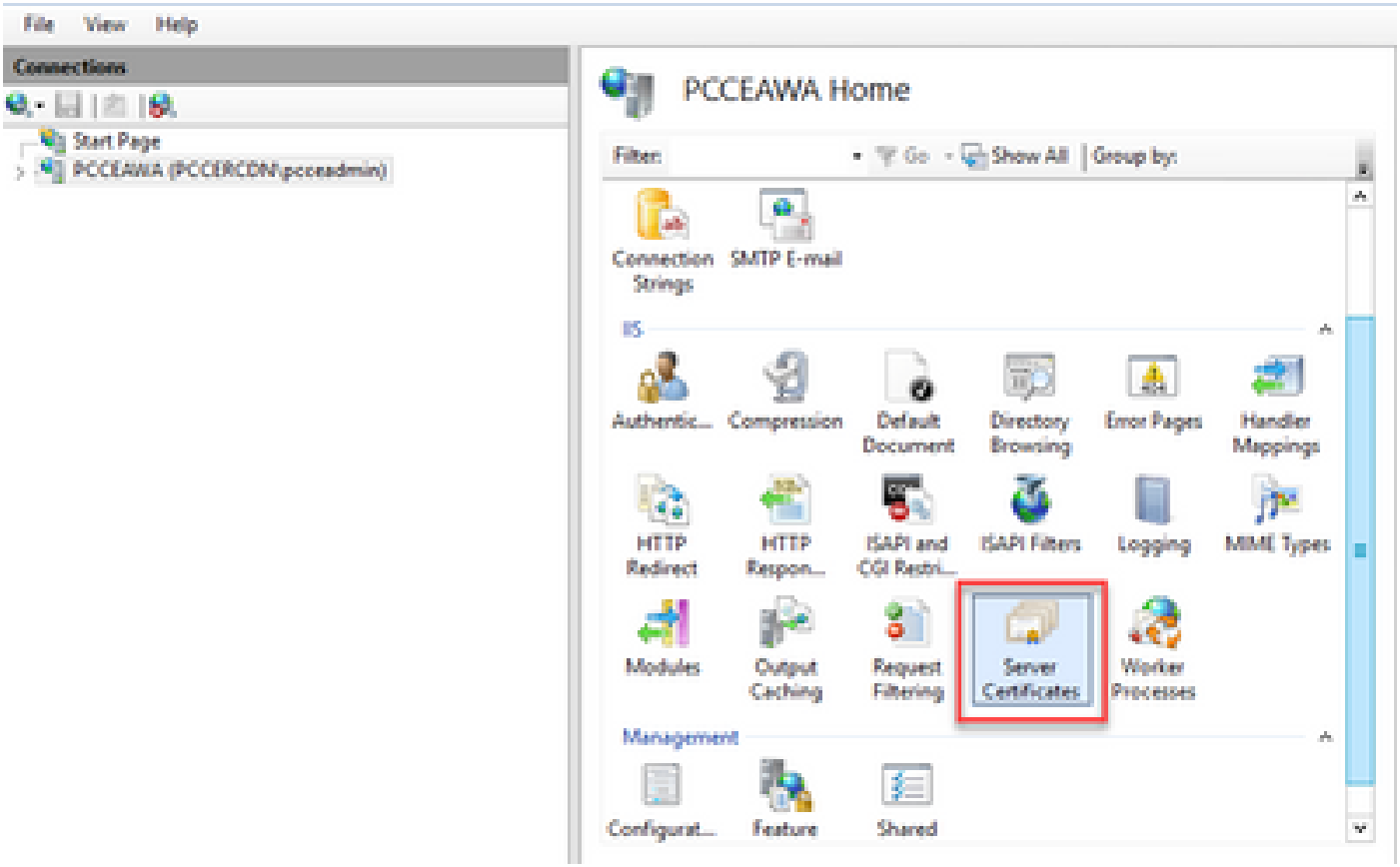
此过程说明如何从Internet信息服务(IIS)管理器生成证书签名请求(CSR)。

步骤1:登录到Windows，然后选择控制面板>管理工具> Internet信息服务(IIS)管理器。

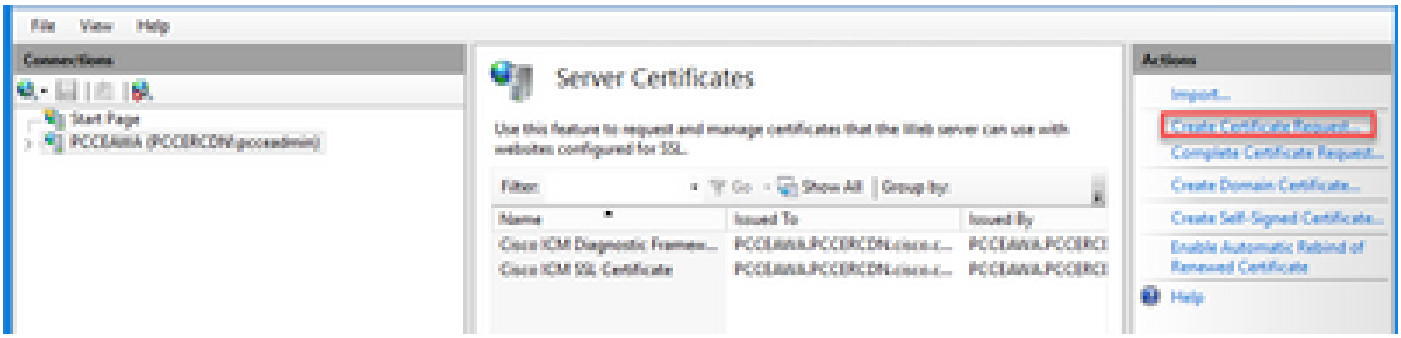
步骤 2在Connections窗格中，点击服务器名称。系统将显示Server Home窗格。



第 3 步：在IIS区域中，双击Server Certificates。

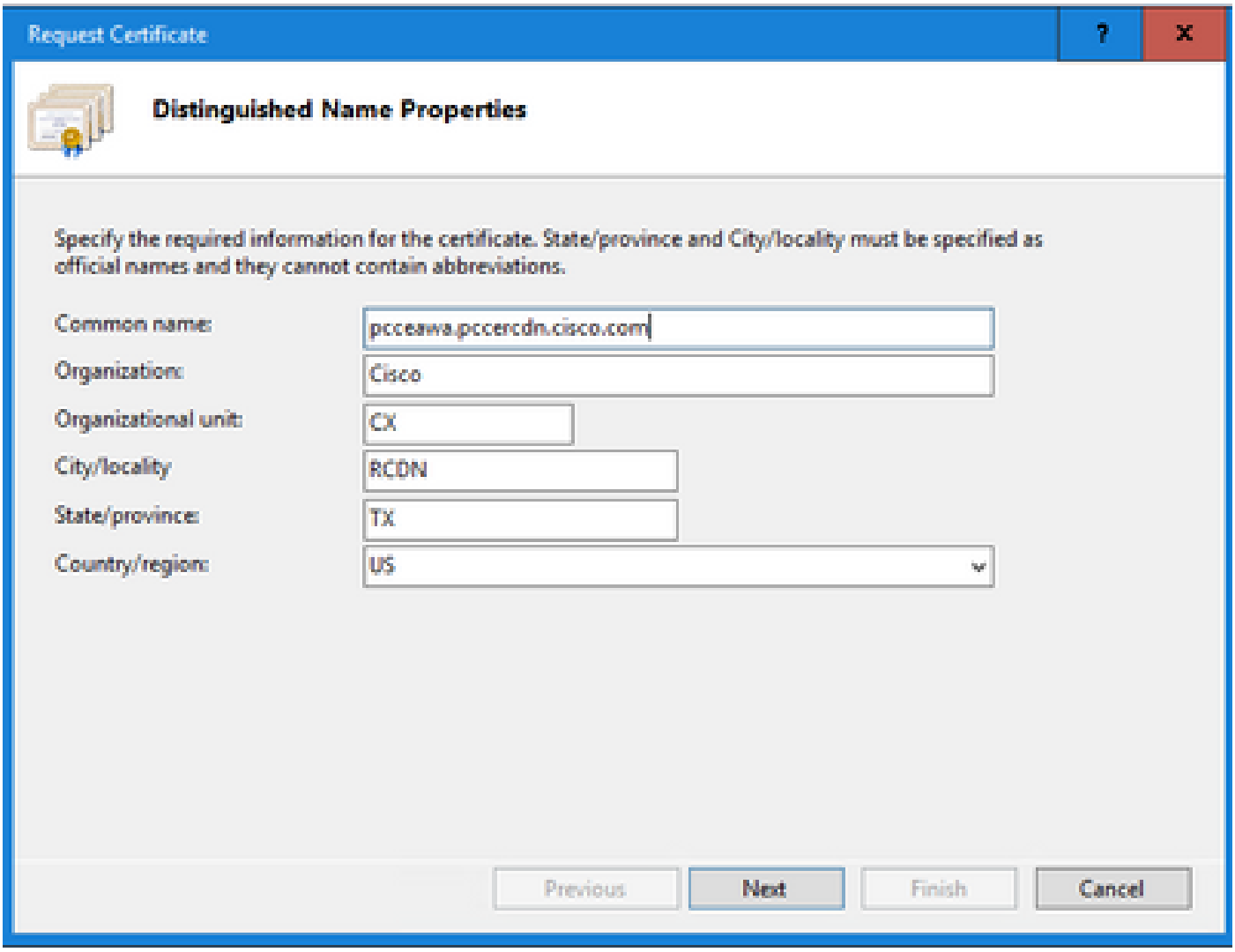


第 4 步：在“操作”窗格中，单击创建证书请求。



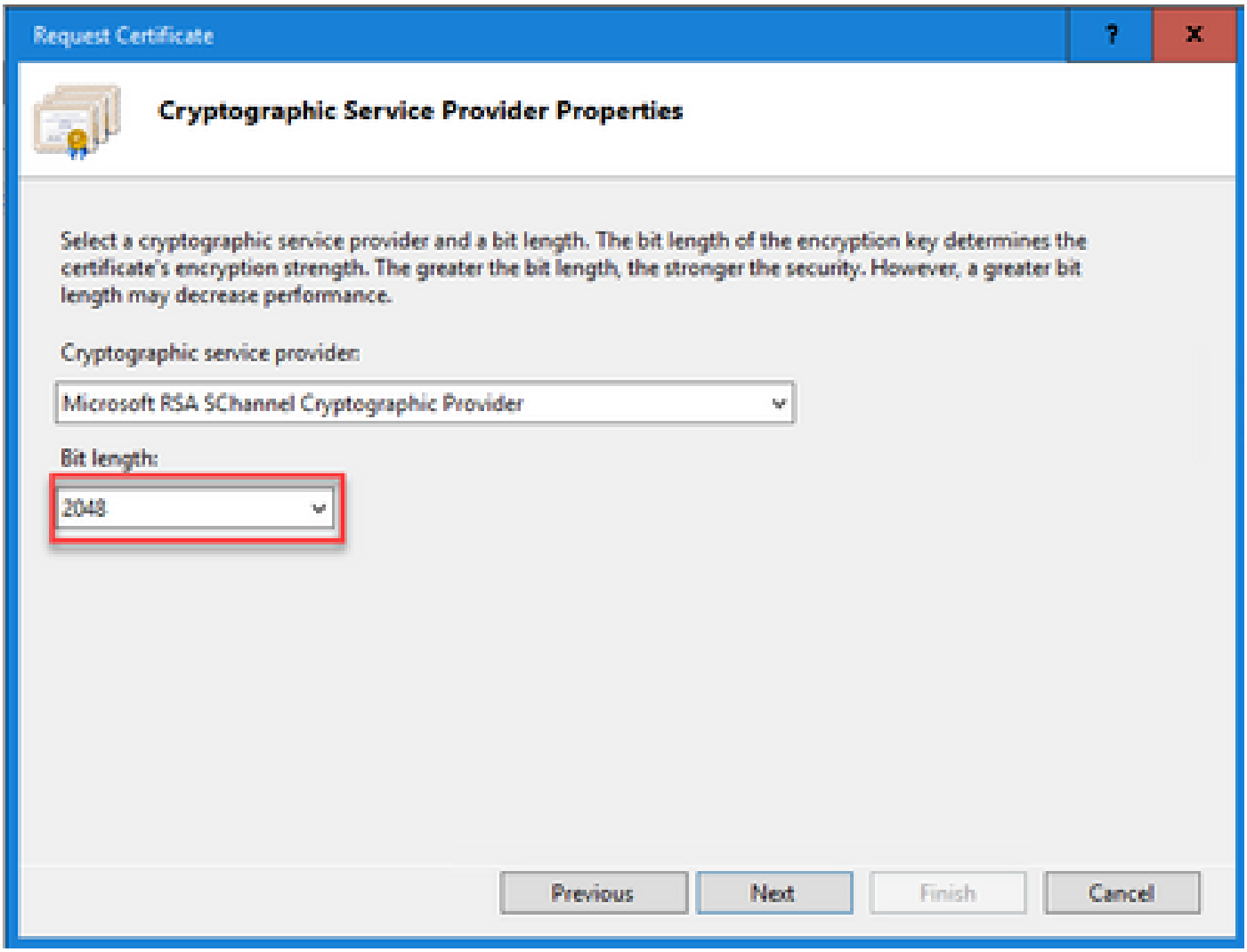
第五步：在Request Certificate对话框中，执行以下操作：

在显示的字段中指定所需信息，然后单击Next。

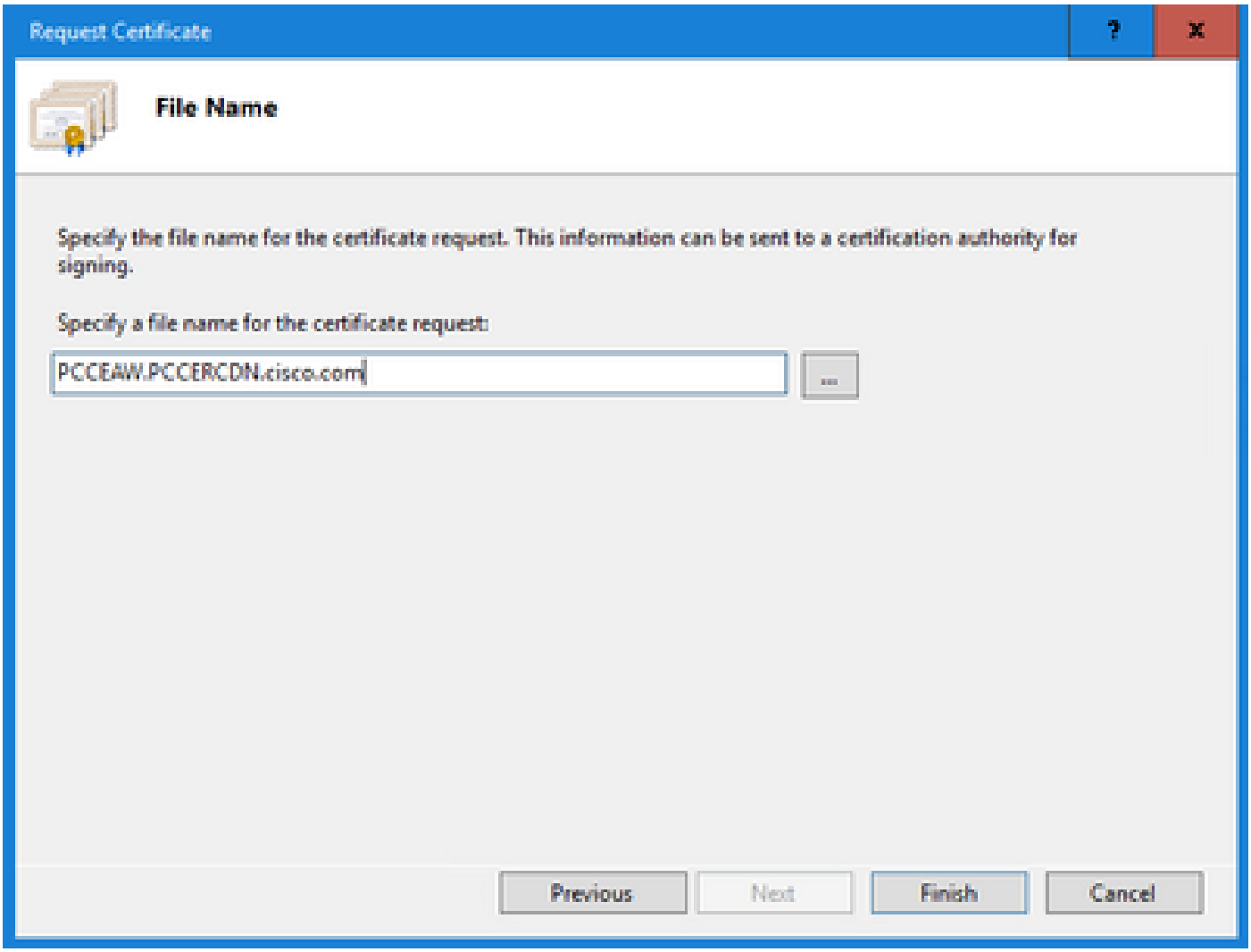


在Cryptographic service provider下拉列表中，保留默认设置。

从Bit length下拉列表中选择2048。



第六步：为证书请求指定文件名，然后单击Finish。



2.获取CA签名证书

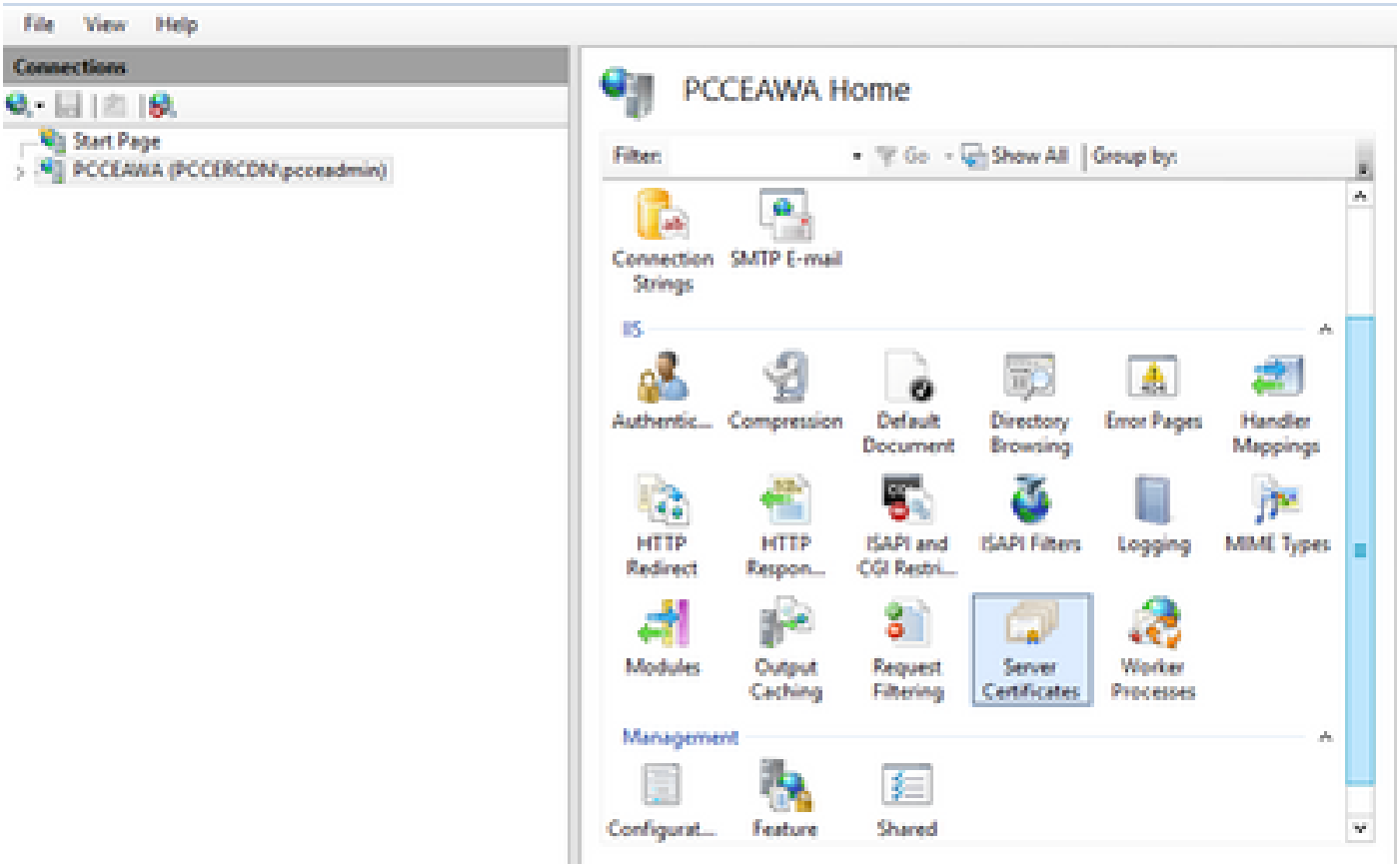
步骤1:在CA上签署证书。

注意：确保CA使用的证书模板包括客户端和服务器身份验证。

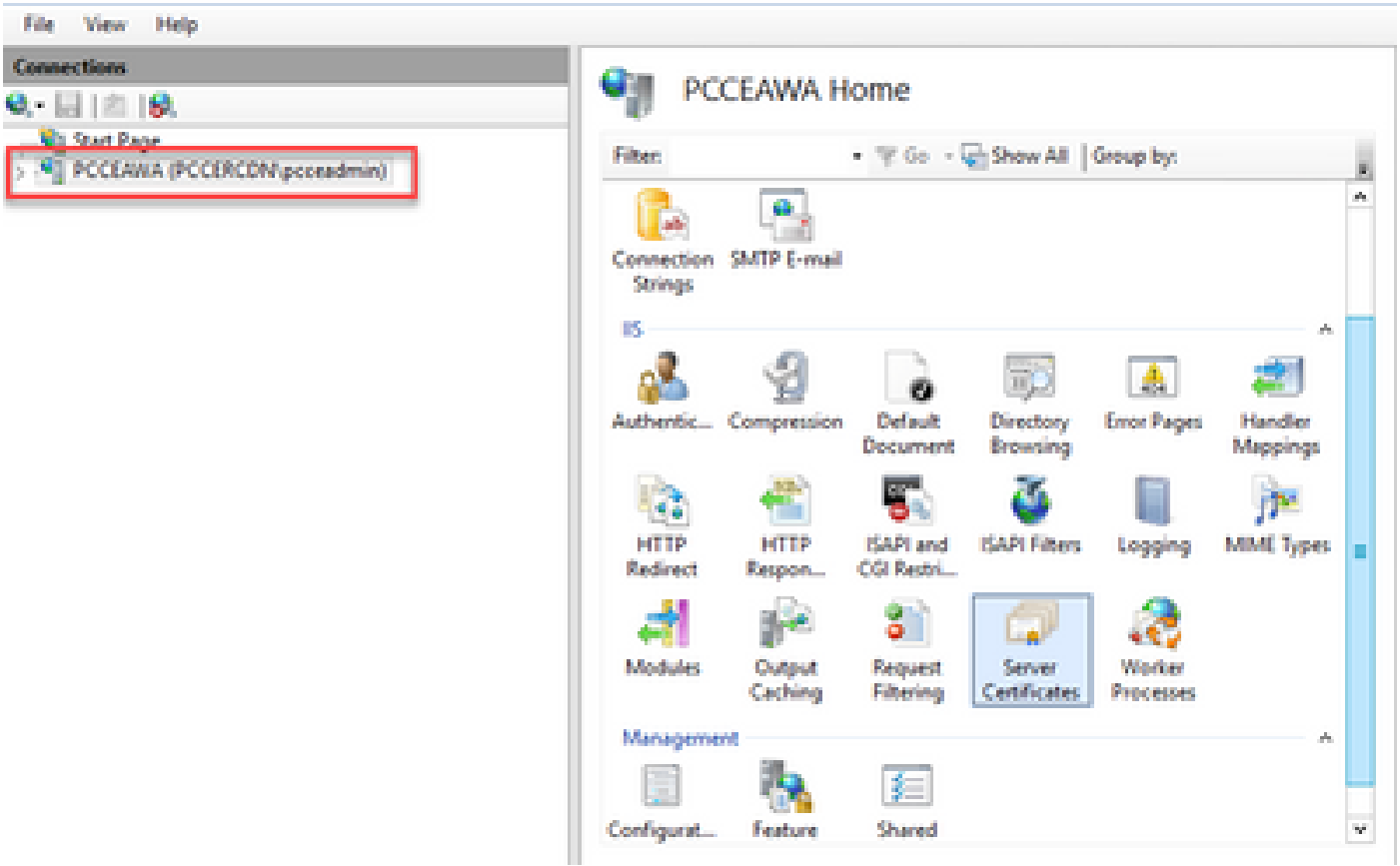
第二步：从证书颁发机构（根、应用和中级，如果有）获取CA签名证书。

3.上传CA签名证书

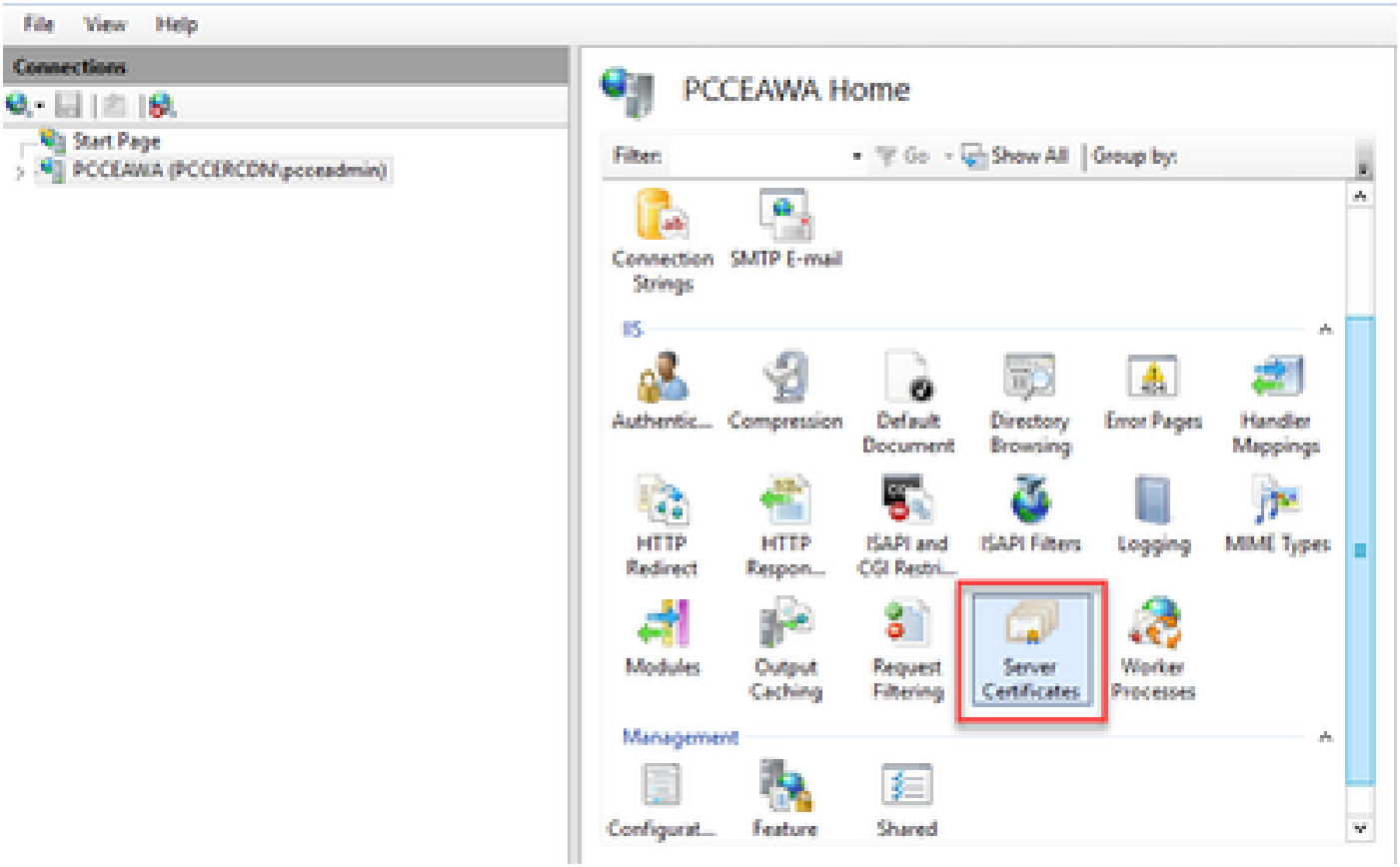
步骤1:登录到Windows，然后选择控制面板>管理工具> Internet信息服务(IIS)管理器。



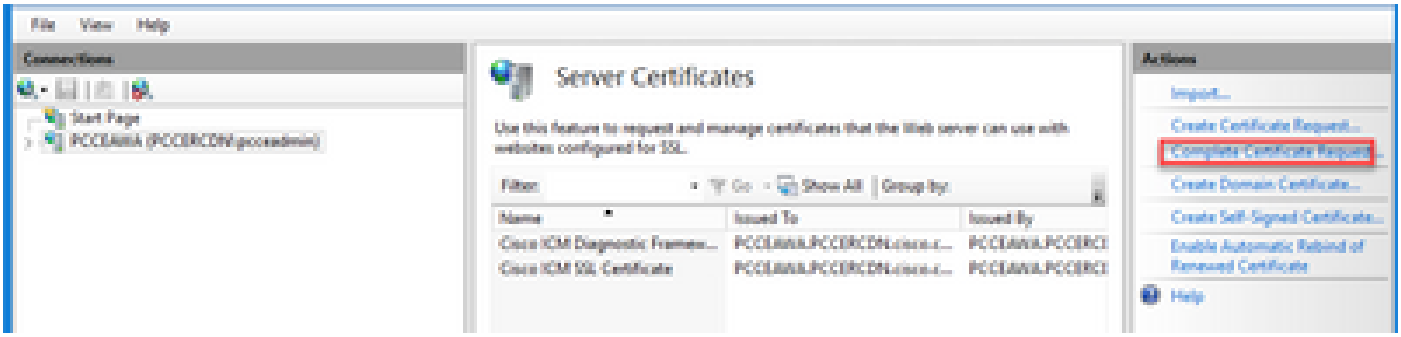
步骤 2在Connections窗格中，点击服务器名称。



第 3 步：在IIS区域中，双击服务器证书。



第 4 步：在Actions窗格中，点击Complete Certificate Request。



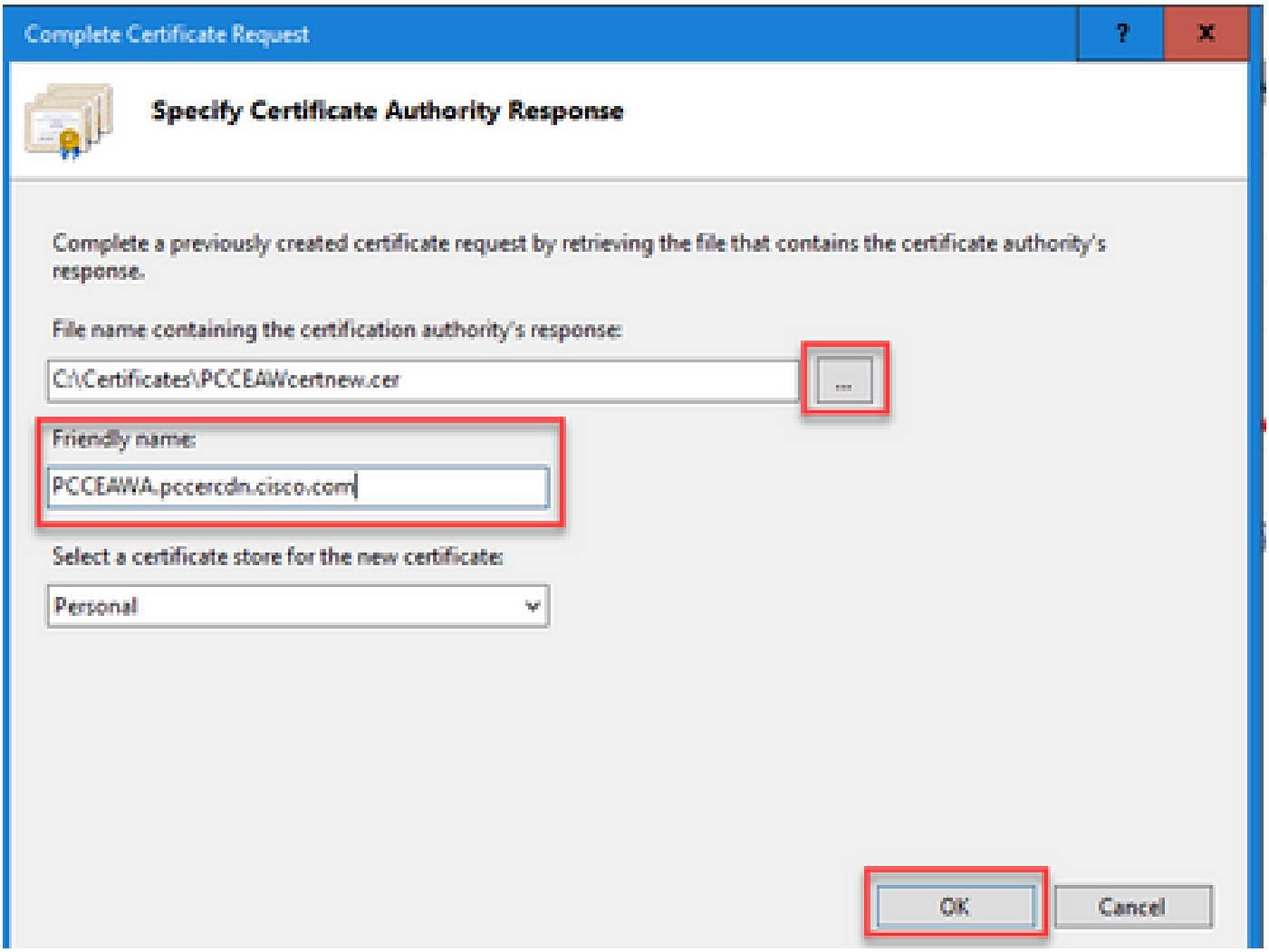
第 5 步：在Complete Certificate Request对话框中，填写以下字段：

在包含证书颁发机构响应字段的文件名中，点击……按钮。

浏览到已签名应用证书的存储位置，然后点击Open。

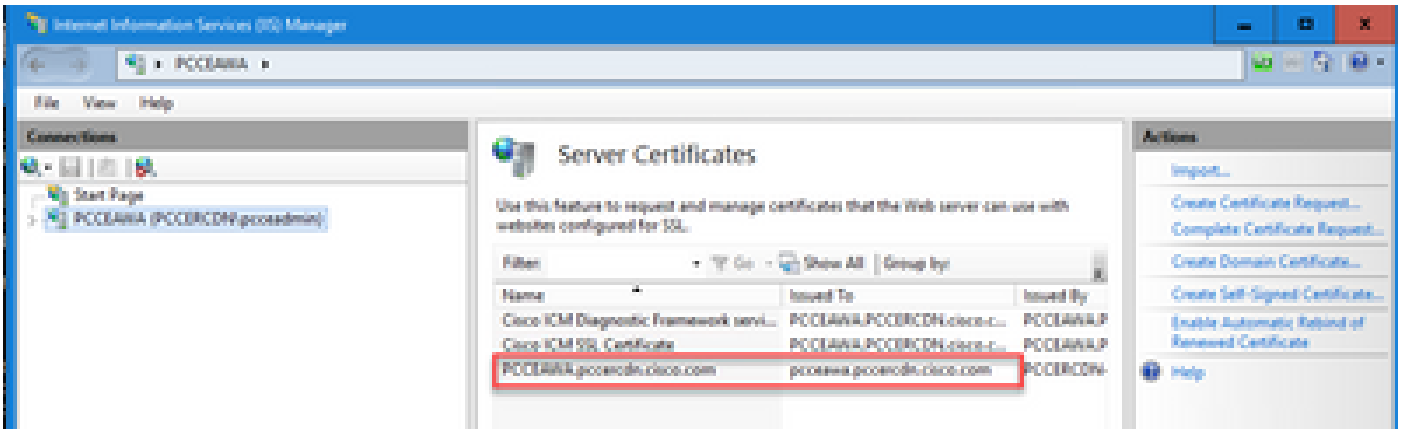
注：如果这是二层CA实施，并且根证书尚未在服务器证书存储中，则需要在导入签名证书之前将根证书上传到Windows存储中。如果需要将根CA上传到Windows应用商店 https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate，请参阅本文档。

在“友好名称”字段中，输入服务器的完全限定域名(FQDN)或任何重要名称。确保Select a certificate store for the new certificate下拉列表保留为Personal。



步骤 6 单击OK上传证书。

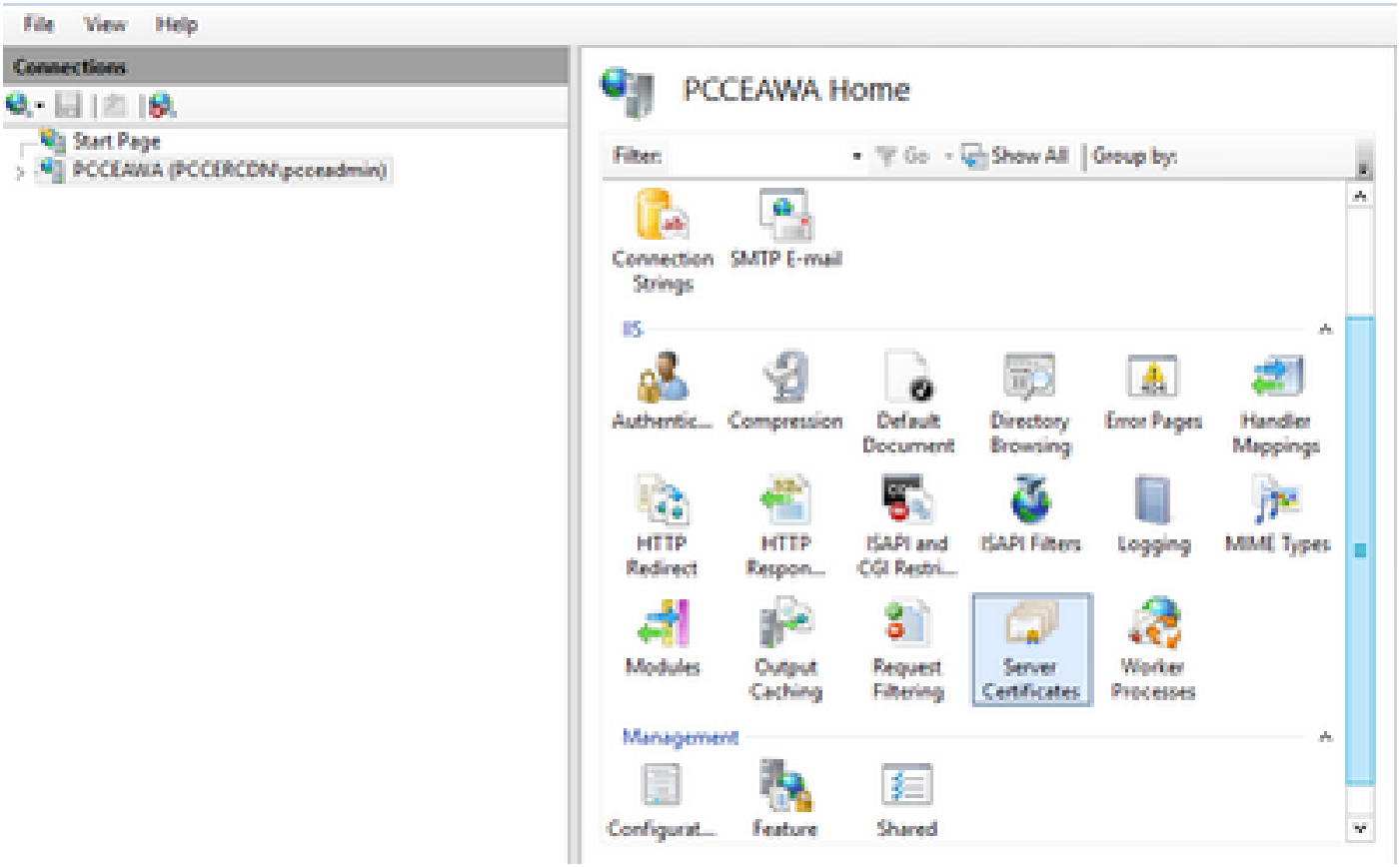
如果证书上传成功，则证书将显示在Server Certificates窗格中。



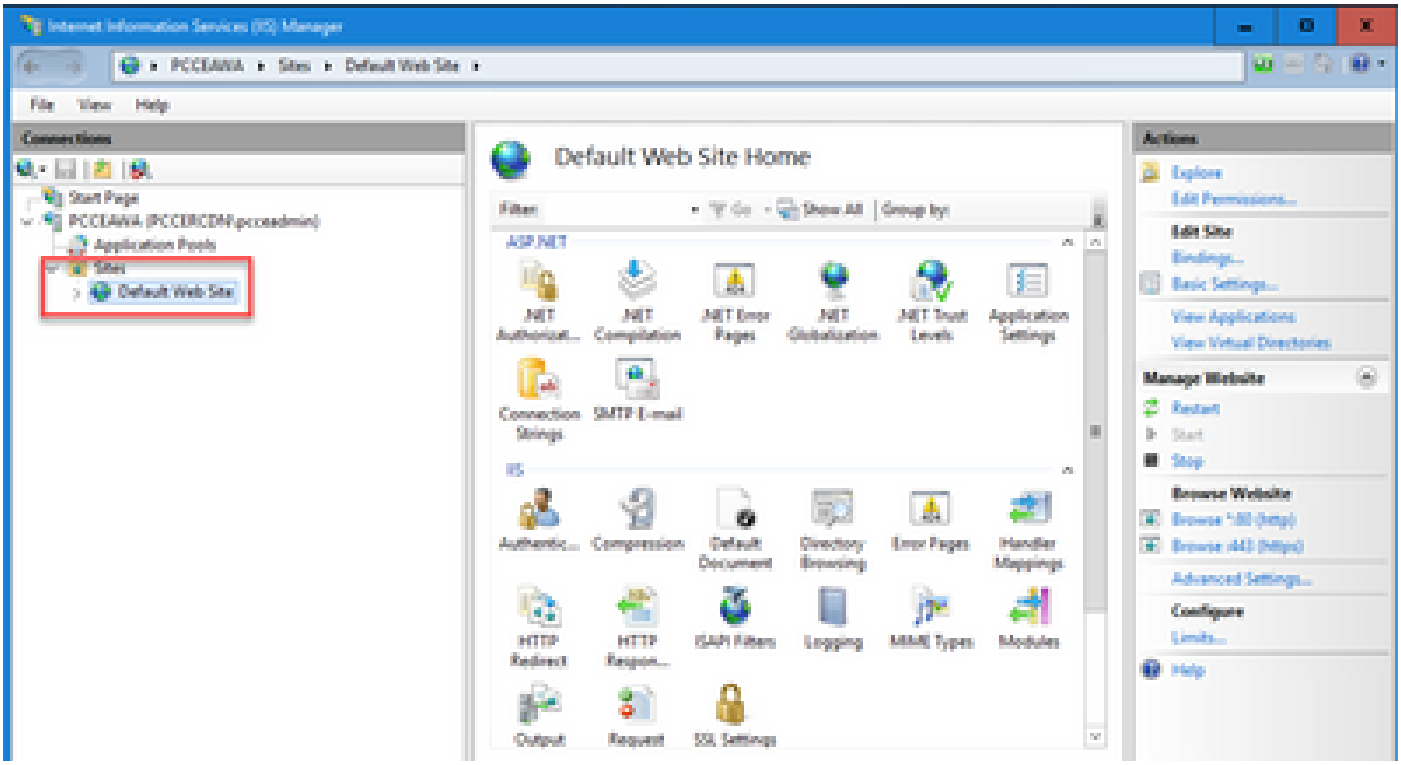
4.将CA签名的证书绑定到IIS

此过程说明如何在IIS管理器中绑定CA签名证书。

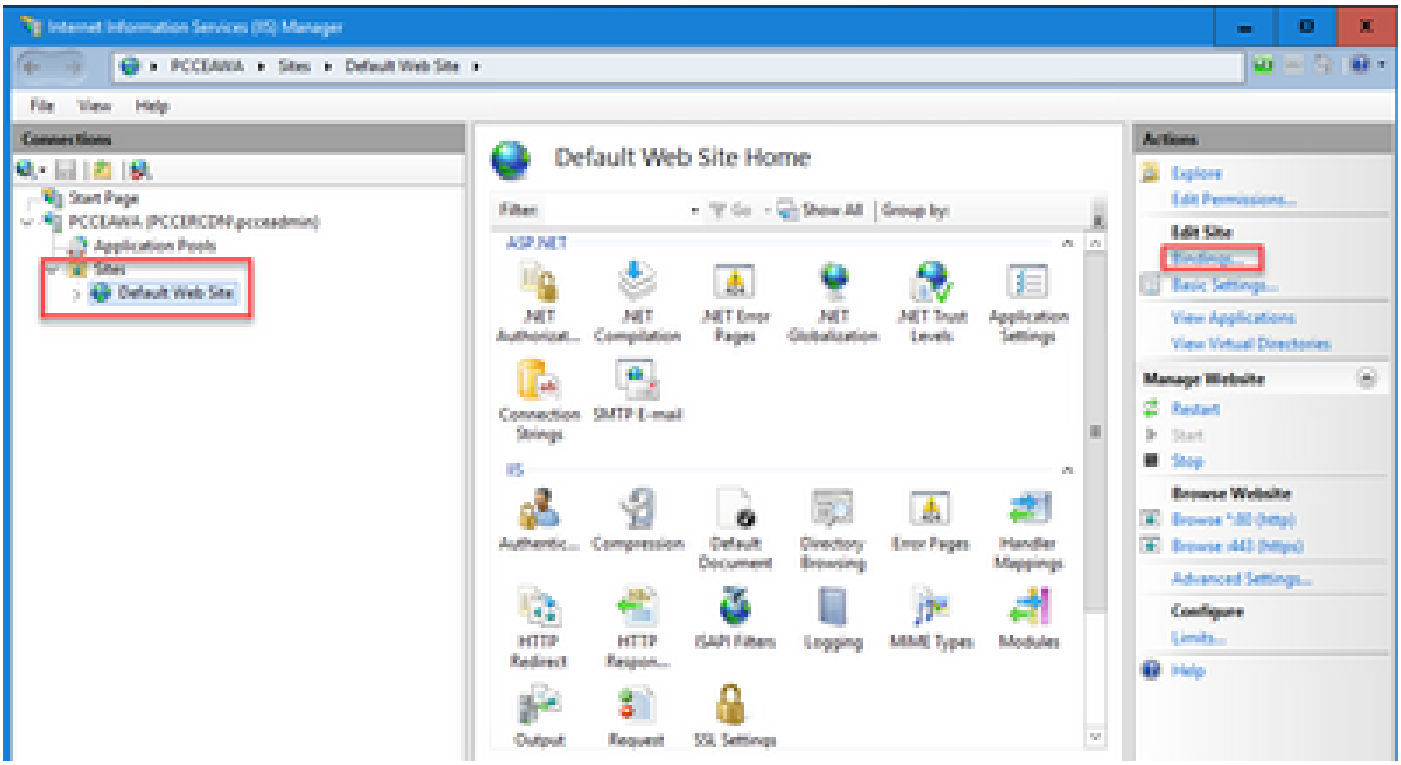
步骤1:登录到Windows，然后选择控制面板>管理工具> Internet信息服务(IIS)管理器。



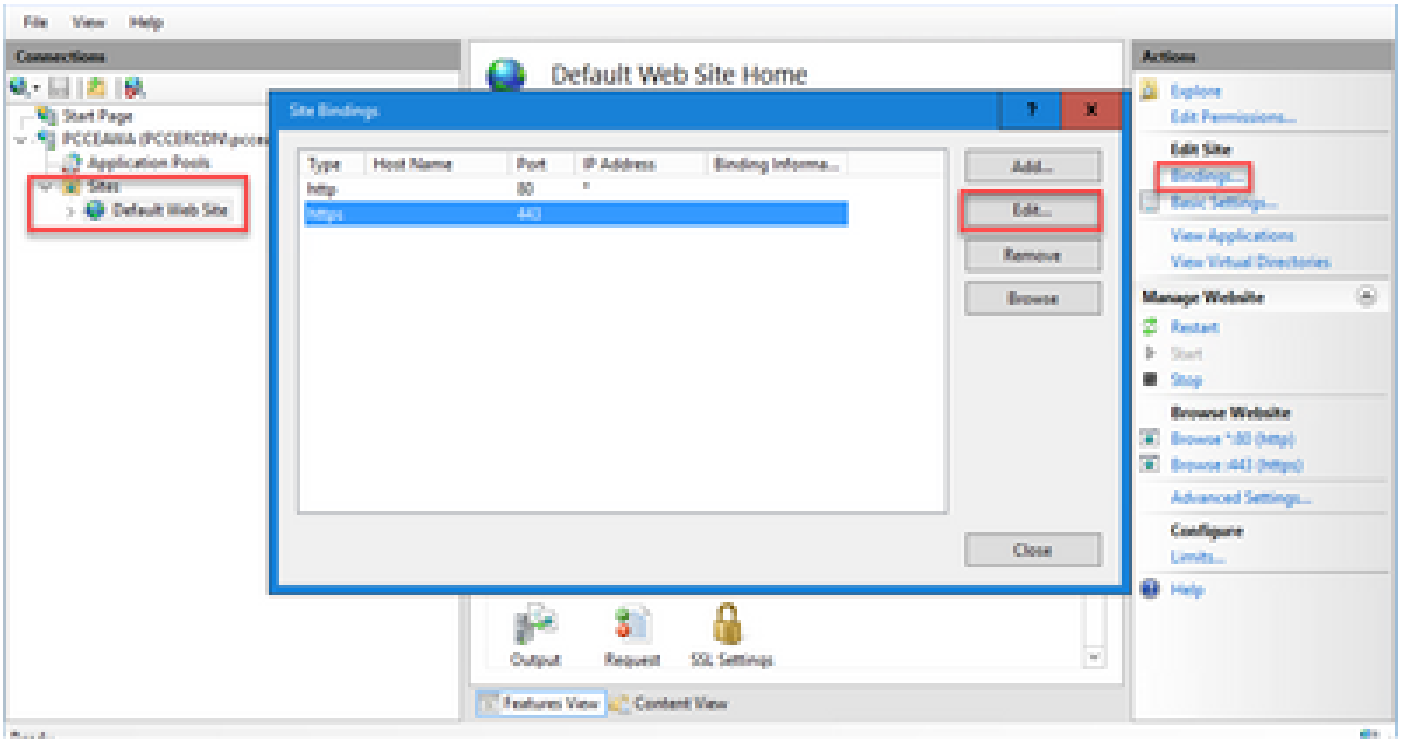
步骤 2在Connections窗格中，选择<server_name> > Sites > Default Web Site。



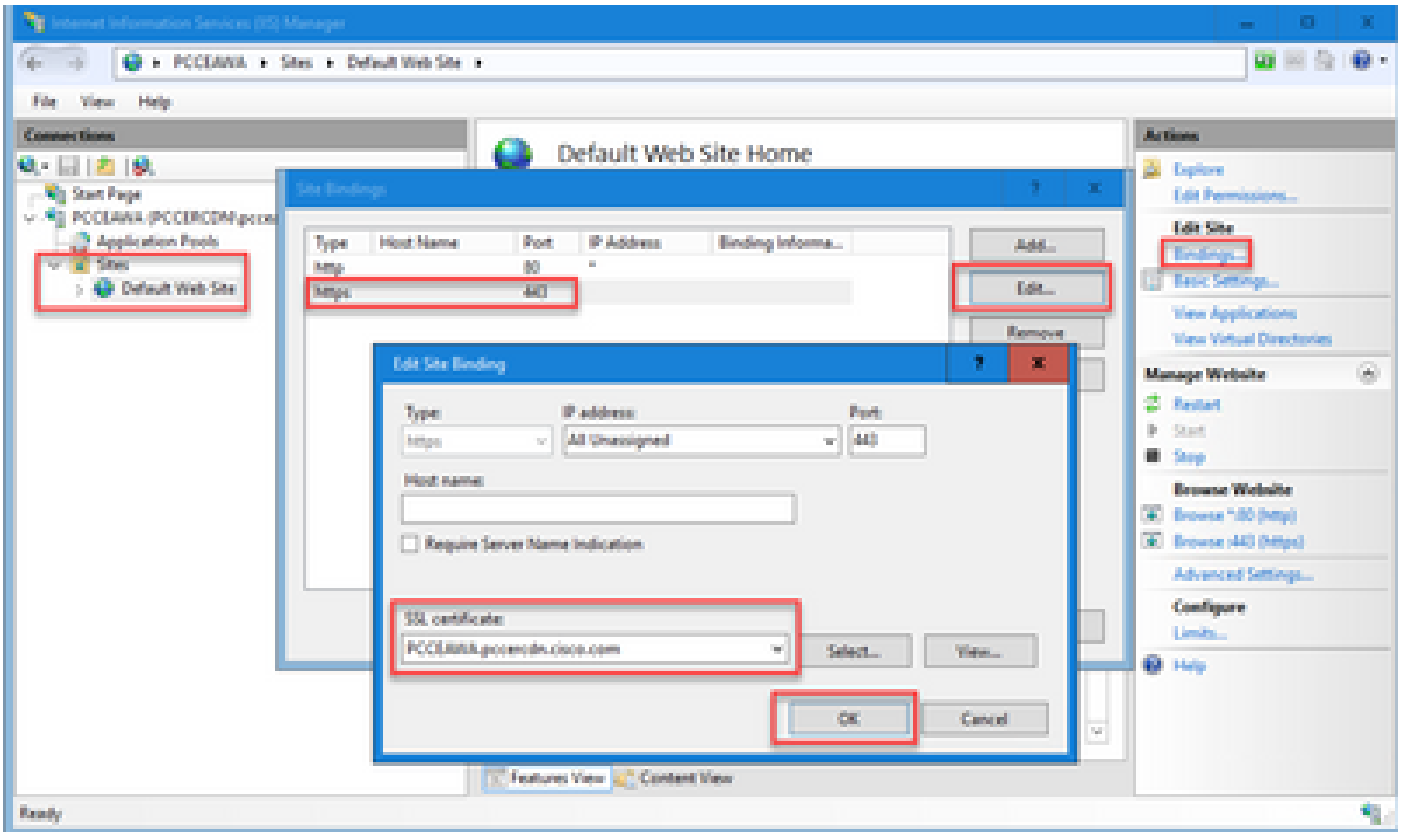
第 3 步：在“操作”窗格中，单击“绑定……”



第 4 步：单击带有端口443的https类型，然后单击Edit...。

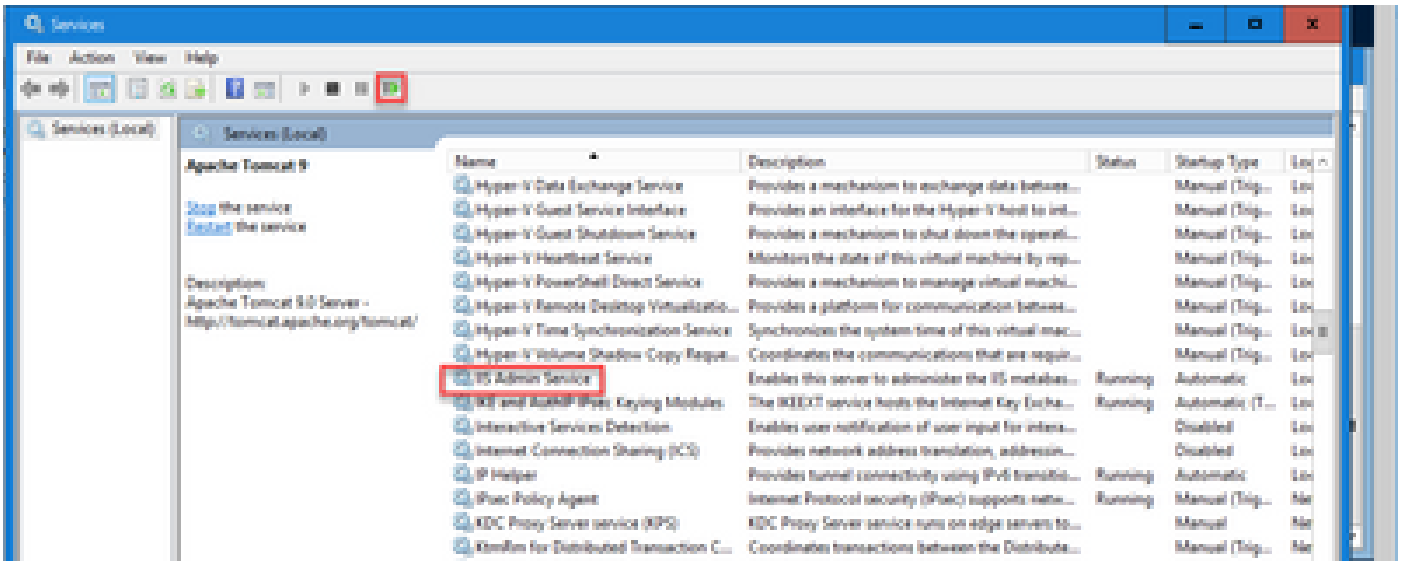


第 5 步：从SSL证书(SSL certificate)下拉列表中，选择与上一步中给定的友好名称相同的证书。



步骤 6 Click OK.

步骤 7.导航到开始>运行> services.msc，然后重新启动IIS管理服务。



如果IIS重新启动成功，则启动应用程序时不会出现证书错误警告。

5.将CA签名的证书绑定到诊断门户

此过程说明如何在Diagnostic Portico中绑定CA签名证书。

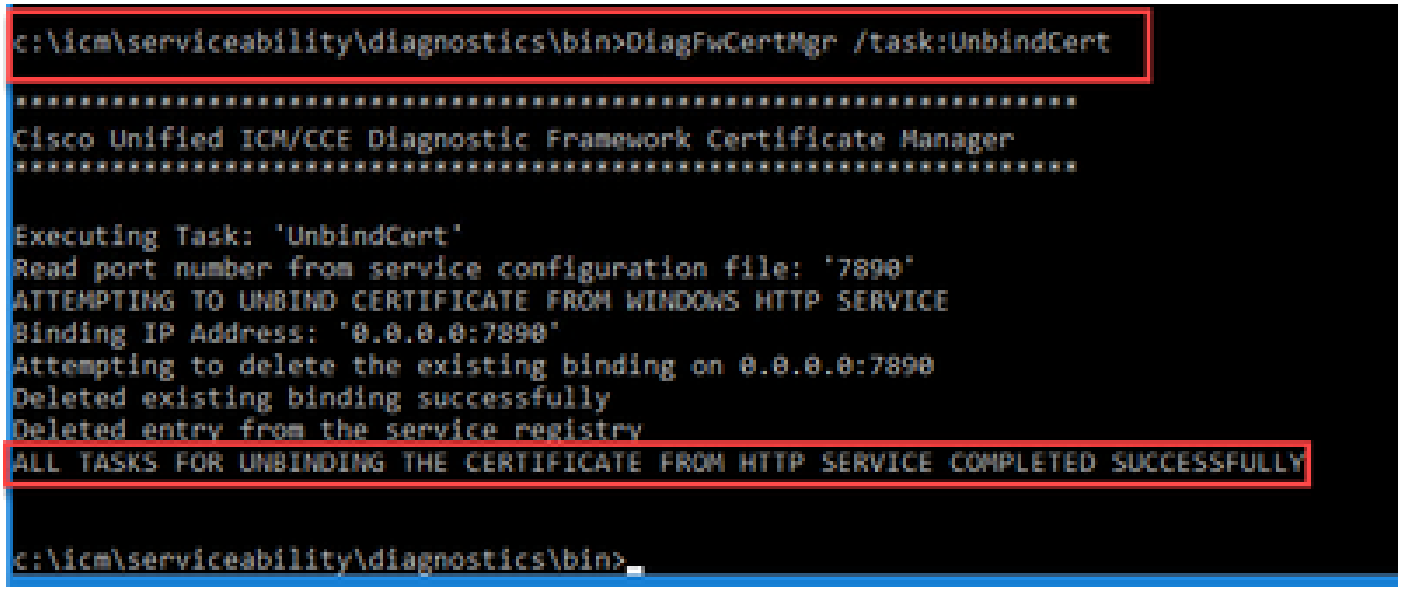
步骤1:打开命令提示符（以管理员身份运行）。

步骤 2导航到Diagnostic Portico主文件夹。运行此指令：

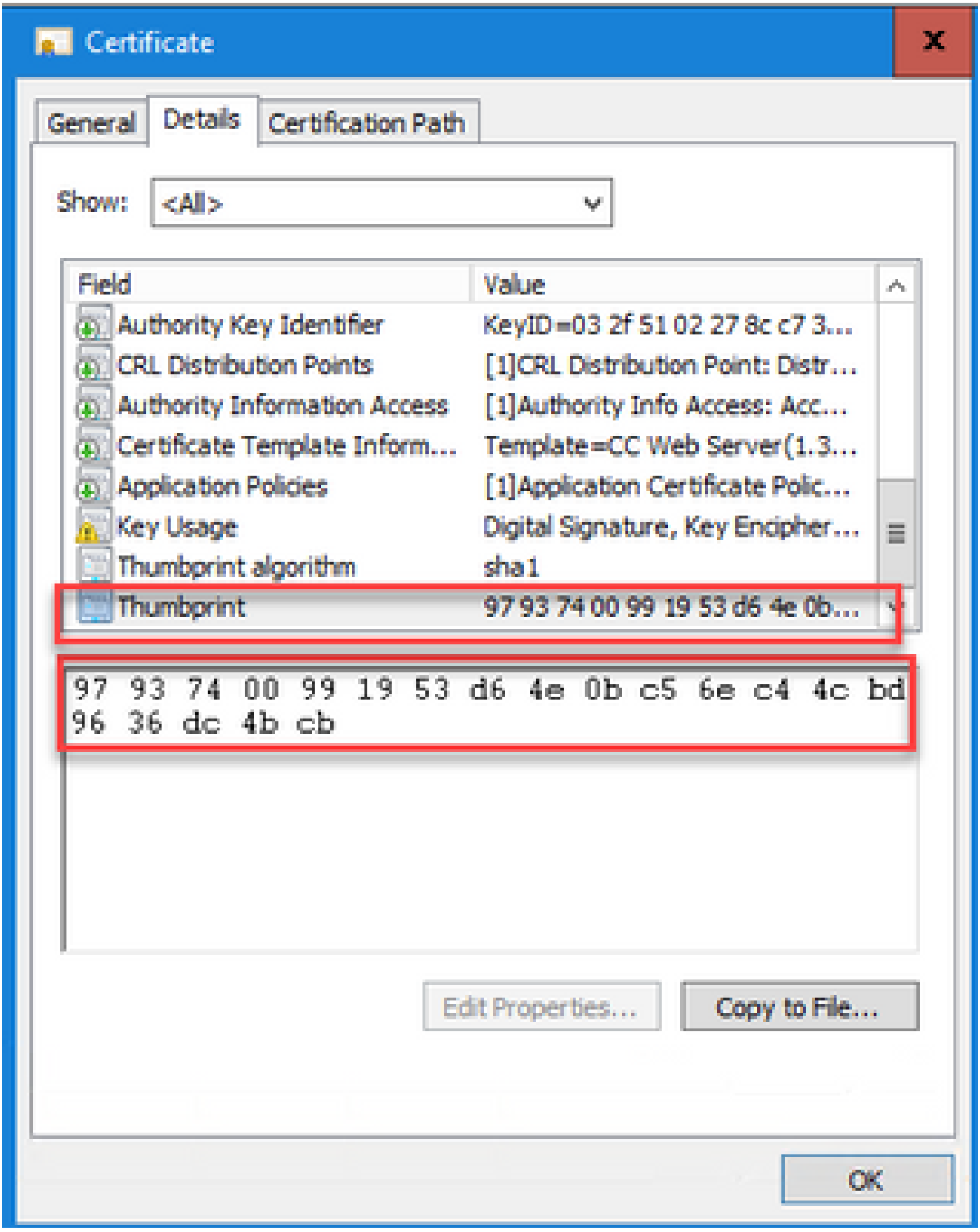
```
cd c:\icm\serviceability\diagnostics\bin
```

第 3 步：删除当前绑定到Diagnostic Portico的证书。运行此指令：

```
DiagFwCertMgr /task:UnbindCert
```

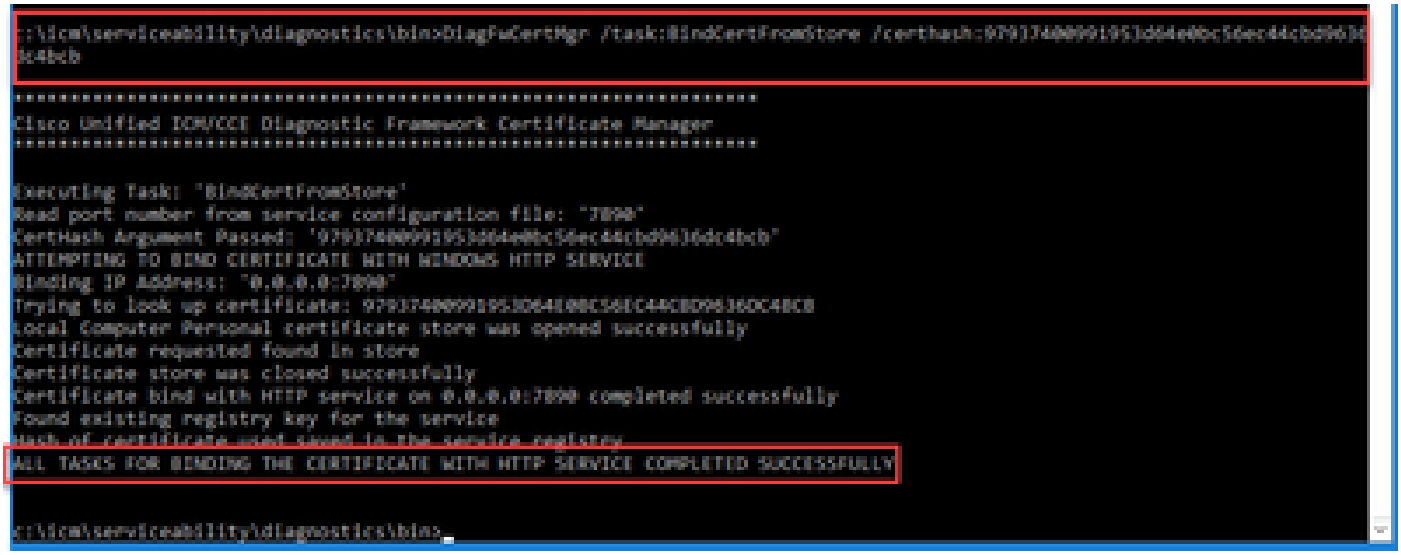


第 4 步：打开签名证书并复制Thumbprint字段的哈希内容（不含空格）。



第五步：运行此命令并粘贴哈希内容。

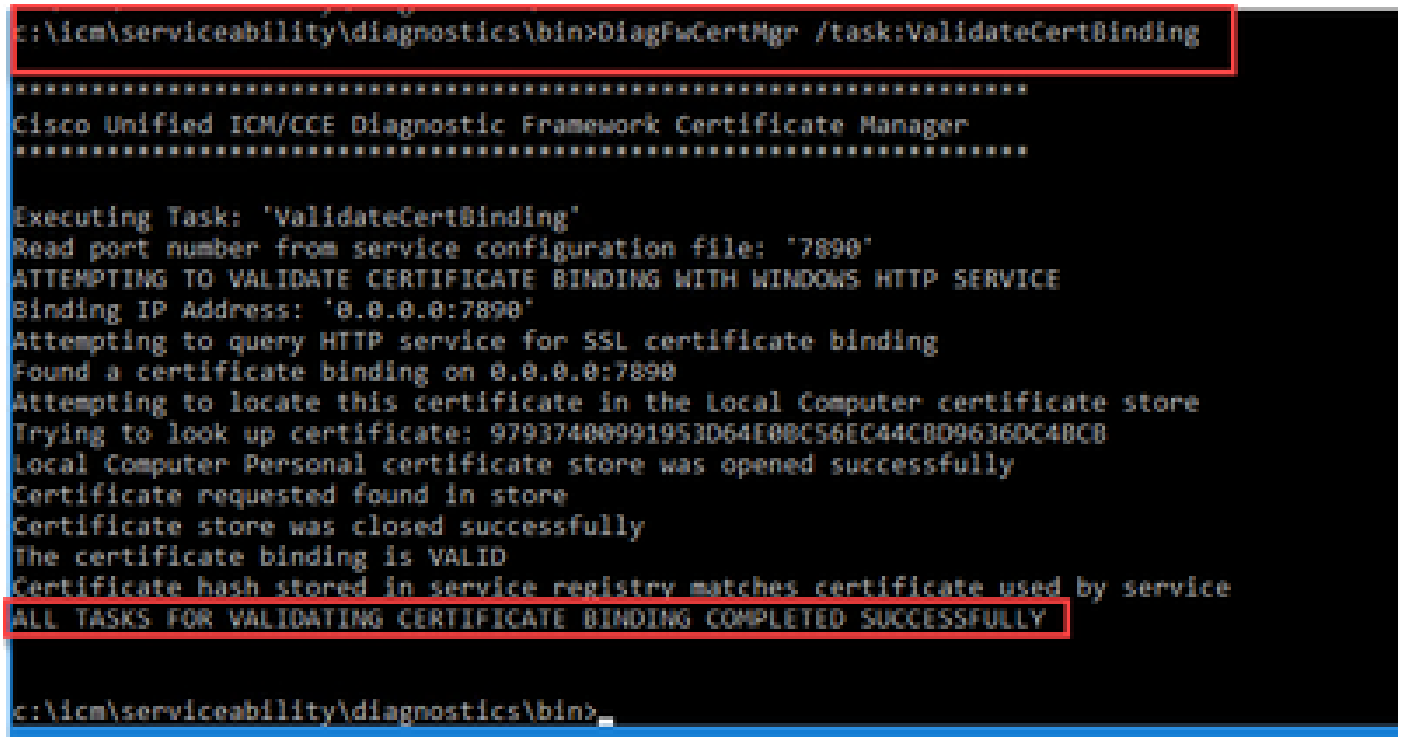
```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```



如果证书绑定成功，则会显示证书绑定为VALID消息。

第六步：验证证书绑定是否成功。运行此指令：

```
DiagFwCertMgr /task:ValidateCertBinding
```



注意：默认情况下，DiagFwCertMgr使用端口7890。

如果证书绑定成功，则会显示证书绑定为VALID消息。

步骤 7.重新启动诊断框架服务。运行以下命令：

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

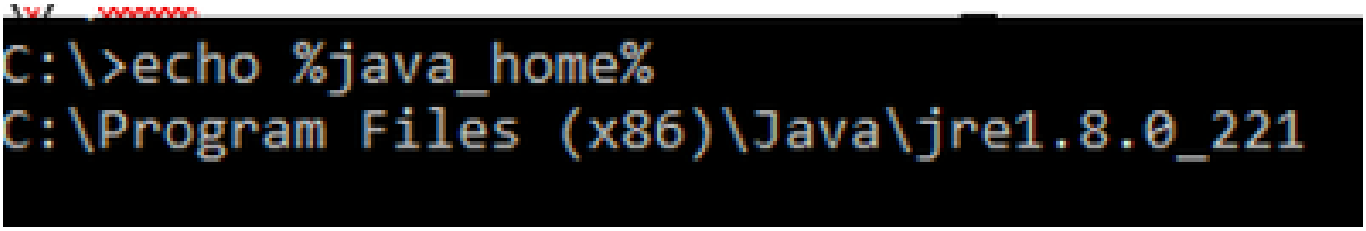
如果诊断框架成功重新启动，则启动应用程序时不会显示证书错误警告。

6.将根证书和中间证书导入Java密钥库

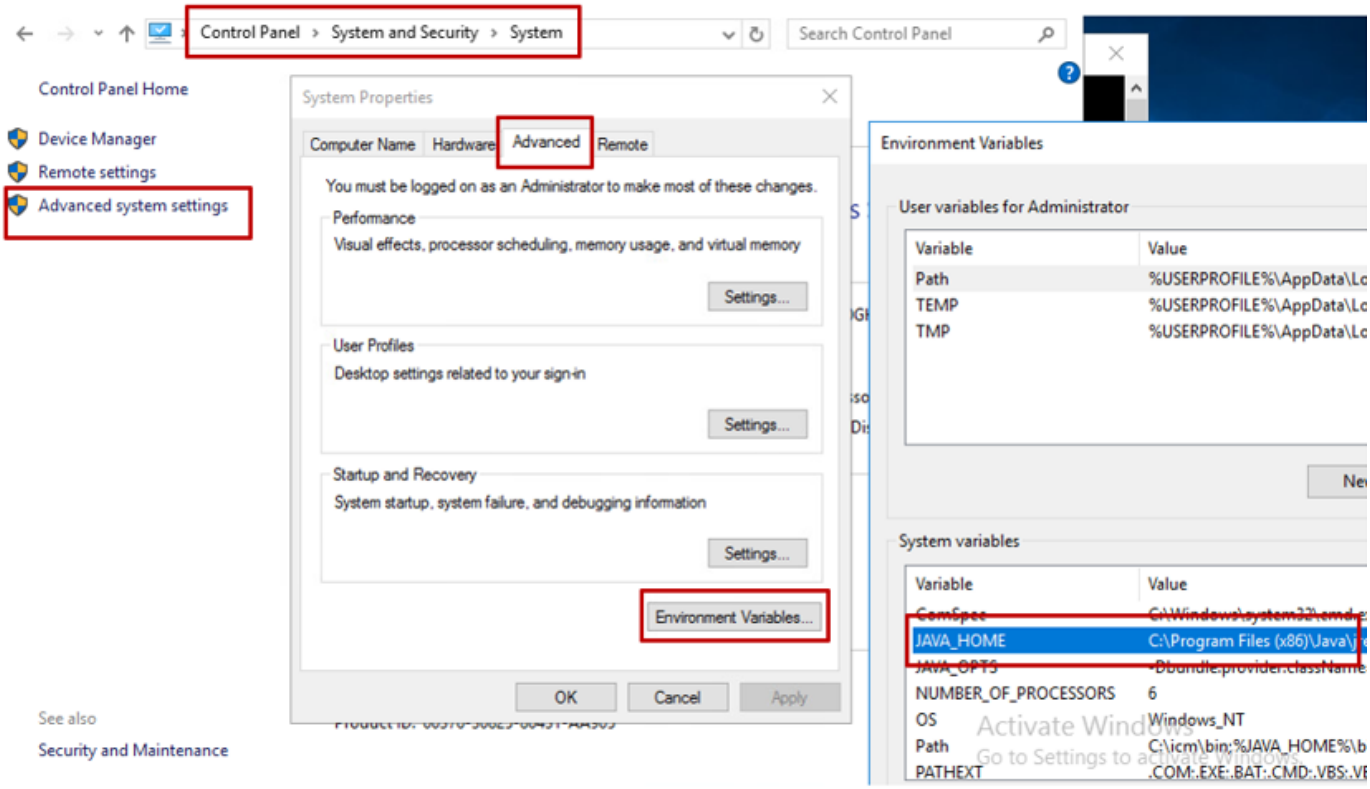
⚠ 注意：在开始之前，您必须备份密钥库并以管理员身份从Java主目录运行命令。

步骤1.了解Java主路径以确保承载Java密钥工具的位置。可通过几种方法查找java home路径。

选项1: CLI命令：echo %JAVA_HOME%



选项2：通过高级系统设置手动设置，如图所示



注：在UCCE 12.5上，默认路径为C:\Program Files(x86)\Java\jre1.8.0_221\bin。但是，如果您已使用12.5(1a)安装程序或安装了12.5 ES55（必备OpenJDK ES），则使用CCE_JAVA_HOME而非JAVA_HOME，因为数据存储路径已随OpenJDK更改。有关在CCE和CVP中进行OpenJDK迁移的详细信息，请参阅以下文档：在CCE 2.5(1)中安装和迁移到OpenJDK和在CVP 12.5(1)中安装和迁移到OpenJDK。

第二步：从文件夹C:\Program Files(x86)\Java\jre1.8.0_221\lib\security备份cacerts文件。 您可以将其复制到其他位置。

第三步：以管理员身份打开命令窗口以运行命令：

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

注：所需的特定证书取决于您用于签署证书的CA。在双层CA中（这是公共CA的典型形式，比内部CA更安全），您需要导入根证书和中间证书。在没有中间体的独立CA中（通常在实验室或更简单的内部CA中可见），您只需要导入根证书。

CVP解决方案

1.使用FQDN生成证书

此过程说明如何使用FQDN为Web服务管理器(WSM)、语音XML(VXML)、呼叫服务器和操作管理(OAMP)服务生成证书。

注意：安装CVP时，证书名称仅包含服务器的名称，而不包含FQDN，因此，您需要重新生成证书。

注意：开始之前，必须执行以下操作：
1.获取密钥库密码。运行命令：more %CVP_HOME%\conf\security.properties。运行keytool命令时需要此密码。
2.将%CVP_HOME%\conf\security文件夹复制到另一个文件夹。
3.以“管理员”身份打开命令窗口以运行命令。

CVP服务器

步骤1:要删除CVP服务器证书，请运行以下命令：

```
%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
```

出现提示时，输入密钥库密码。

第二步：要生成WSM证书，请运行以下命令：

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

出现提示时，输入密钥库密码。

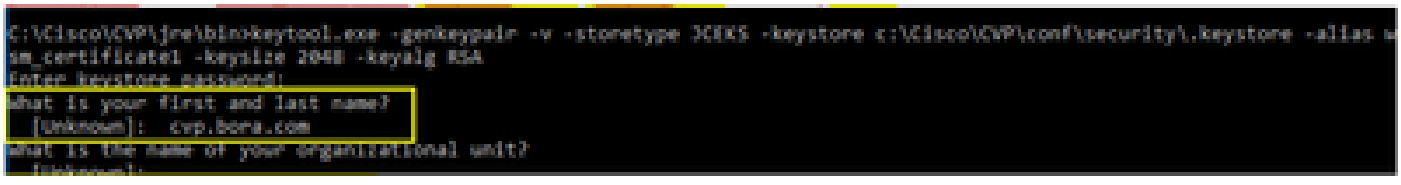
注：默认情况下，证书生成时间为两年。使用 — validity XXXX设置重新生成证书时的到期日期，否则证书有效期为90天，并且需要在此时间之前由CA签名。对于大多数此类证书，3-5年必须是合理的验证时间。

以下是一些标准有效性输入：

一年	365
两年	730
三年	1095
四年	1460
五年	1895
十年	3650

注意：在12.5证书中，必须是SHA 256、密钥大小2048和加密算法RSA，请使用以下参数设置以下值：-keyalg RSA和 — keysize 2048。CVP密钥库命令必须包括 — storetype JCEKS参数。如果不这样做，证书、密钥或更糟的密钥库可能会损坏。

在问题中指定服务器的FQDN，您的名字和姓是什么？



完成以下其他问题：

您的组织单位名称是什么？

[未知]:<指定OU>

贵公司的名称是什么？

[未知]:<指定组织的名称>

您的城市或地区名称是什么？

[未知]:<指定城市/地区的名称>

您所在省/自治区/直辖市的名称是什么？

[未知]:<指定州/省的名称>

此设备的国家代码是多少（两个字母）？

[未知]:<指定两个字母的国家/地区代码>

为接下来的两个输入指定yes。

第三步：对vxml_certificate和callserver_certificate执行相同的步骤：

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

CVP报告服务器

步骤1:要删除WSM和报告服务器证书，请运行以下命令：

```
%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
```

出现提示时，输入密钥库密码。

第二步：要生成WSM证书，请运行以下命令：

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

出现提示时，输入密钥库密码。

指定用于查询的服务器FQDN您的姓和名是什么？并继续执行与CVP服务器相同的步骤。

第三步：对callserver_certificate执行相同的步骤：

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

CVP OAMP（UCCE部署）

由于在PCCE解决方案版本12.x中，该解决方案的所有组件都由SPOG控制，并且未安装OAMP，因此仅对于UCCE部署解决方案而言，才需要这些步骤。

步骤1:要删除WSM和OAMP服务器证书，请运行以下命令：

```
%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
```

出现提示时，输入密钥库密码。

第二步：要生成WSM证书，请运行以下命令：

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

出现提示时，输入密钥库密码。

指定用于查询的服务器FQDN您的姓和名是什么？并继续执行与CVP服务器相同的步骤。

第三步：对oamp_certificate执行相同的步骤：

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

出现提示时，输入密钥库密码。

2.生成CSR

注意：符合RFC5280标准的浏览器要求每个证书中都包含主题备用名称(SAN)。在生成

CSR时，可以在SAN中使用 — ext参数完成此操作。

主题备用名称

-ext参数允许用户使用特定分机。显示的示例添加了主题备用名称(SAN)，该名称带有服务器的完全限定域名(FQDN)以及本地主机。其他SAN字段可作为逗号分隔值添加。

有效的SAN类型包括：

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

例如：-ext san=dns:mycvp.mydomain.com,dns:localhost

CVP服务器

步骤1:生成别名的证书请求。运行此命令并将其保存到文件（例如，wsm_certificate）：

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

出现提示时，输入密钥库密码。

第二步：对vxml_certificate和callserver_certificate执行相同的步骤：

```
%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 -
```

出现提示时，输入密钥库密码。

CVP报告服务器

步骤1:生成别名的证书请求。运行此命令并将其保存到文件（例如，wsmreport_certificate）：

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

出现提示时，输入密钥库密码。

第二步：对callserver_certificate执行相同的步骤：

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

出现提示时，输入密钥库密码。

CVP OAMP（UCCE部署）

步骤1:生成别名的证书请求。运行此命令并将其保存到文件（例如，oamp_certificate）：

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

第二步：对oamp_certificate执行相同的步骤：

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

出现提示时，输入密钥库密码。

3.获取CA签名证书

步骤1:在CA上签署证书（CVP服务器的WSM、Callserver和VXML服务器；CVP OAMP服务器的WSM和OAMP以及报告服务器的WSM和Callserver）。

第二步：从CA机构下载应用证书和根证书。

第三步：将根证书和CA签名证书复制到每台服务器的%CVP_HOME%\conf\security\文件夹中。

4.导入CA签名证书

将这些步骤应用于CVP解决方案的所有服务器。 仅需要导入该服务器上组件的证书CA签名证书。

步骤1:导入根证书。运行此指令：

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

出现提示时，输入密钥库密码。在Trust this certificate提示符下，键入Yes。

如果存在中间证书，请运行以下命令：

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

出现提示时，输入密钥库密码。在Trust this certificate提示符下，键入Yes。

第二步：导入该服务器证书的CA签名WSM（CVP、Reporting和OAMP）。运行此指令：

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

出现提示时，输入密钥库密码。在Trust this certificate提示符下，键入Yes。

第三步：在CVP服务器和报告服务器中导入Callserver CA签名证书。运行此指令：

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

出现提示时，输入密钥库密码。在Trust this certificate提示符下，键入Yes。

第四步：在CVP服务器中导入VXML服务器CA签名证书。运行此指令：

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

第五步：在CVP OAMP服务器（仅适用于UCCE）中导入OAMP服务器CA签名证书。运行此指令：

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

第六步：重新启动服务器。

注意：在UCCE部署中，确保使用生成CSR时提供的FQDN在CVP OAMP中添加服务器（报告、CVP服务器等）。

VOS服务器

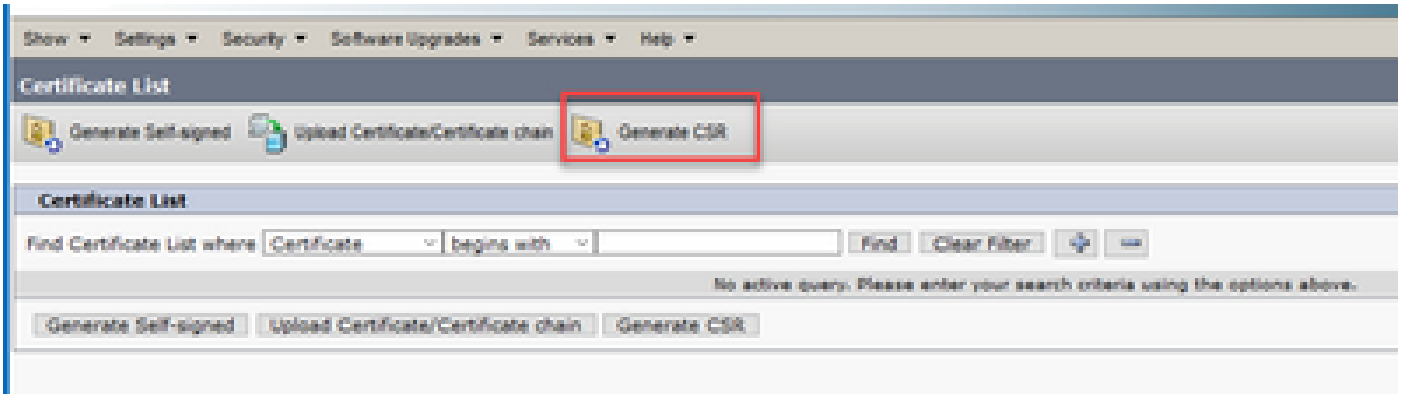
1.生成CSR证书

此程序说明如何从基于思科语音操作系统(VOS)的平台生成Tomcat CSR证书。此过程适用于所有基于VOS的应用，例如：

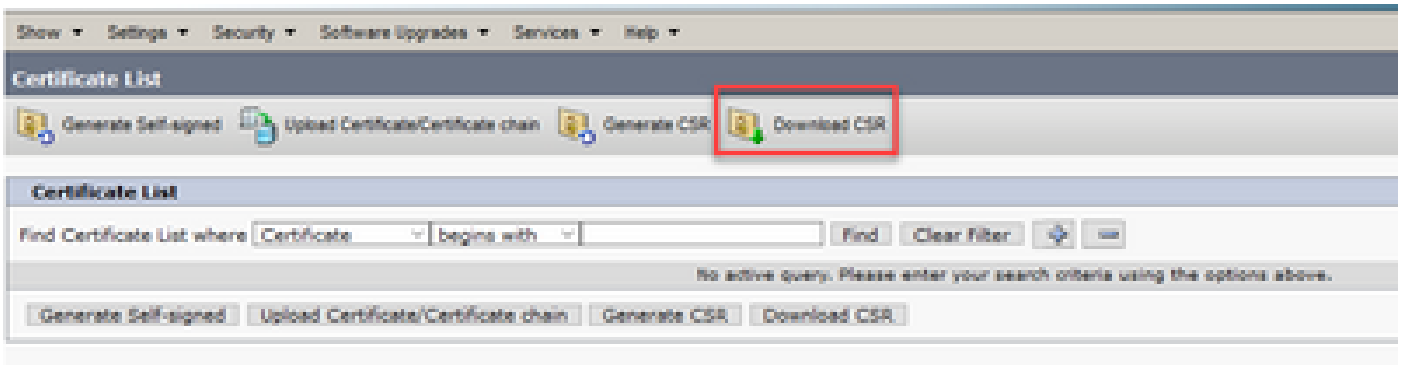
- CUCM
- Finesse
- CUIC \实时数据(LD)\身份服务器(IDS)
- 云连接
- 思科VVB

步骤1:导航至Cisco Unified Communications Operating System Administration页面：https://FQDN:<8443或443>/cmplatform。

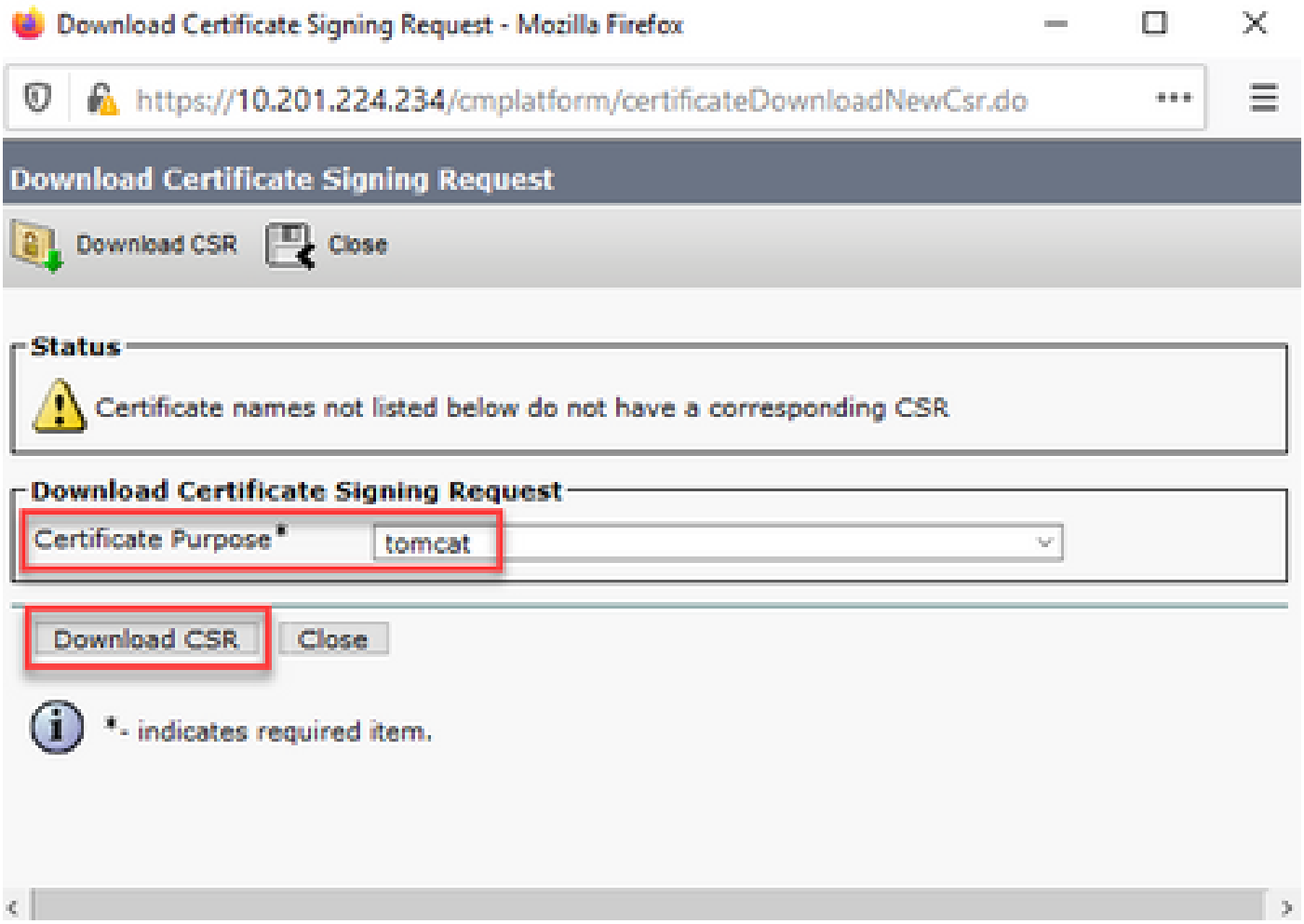
第二步：导航到安全>证书管理，然后选择生成CSR。



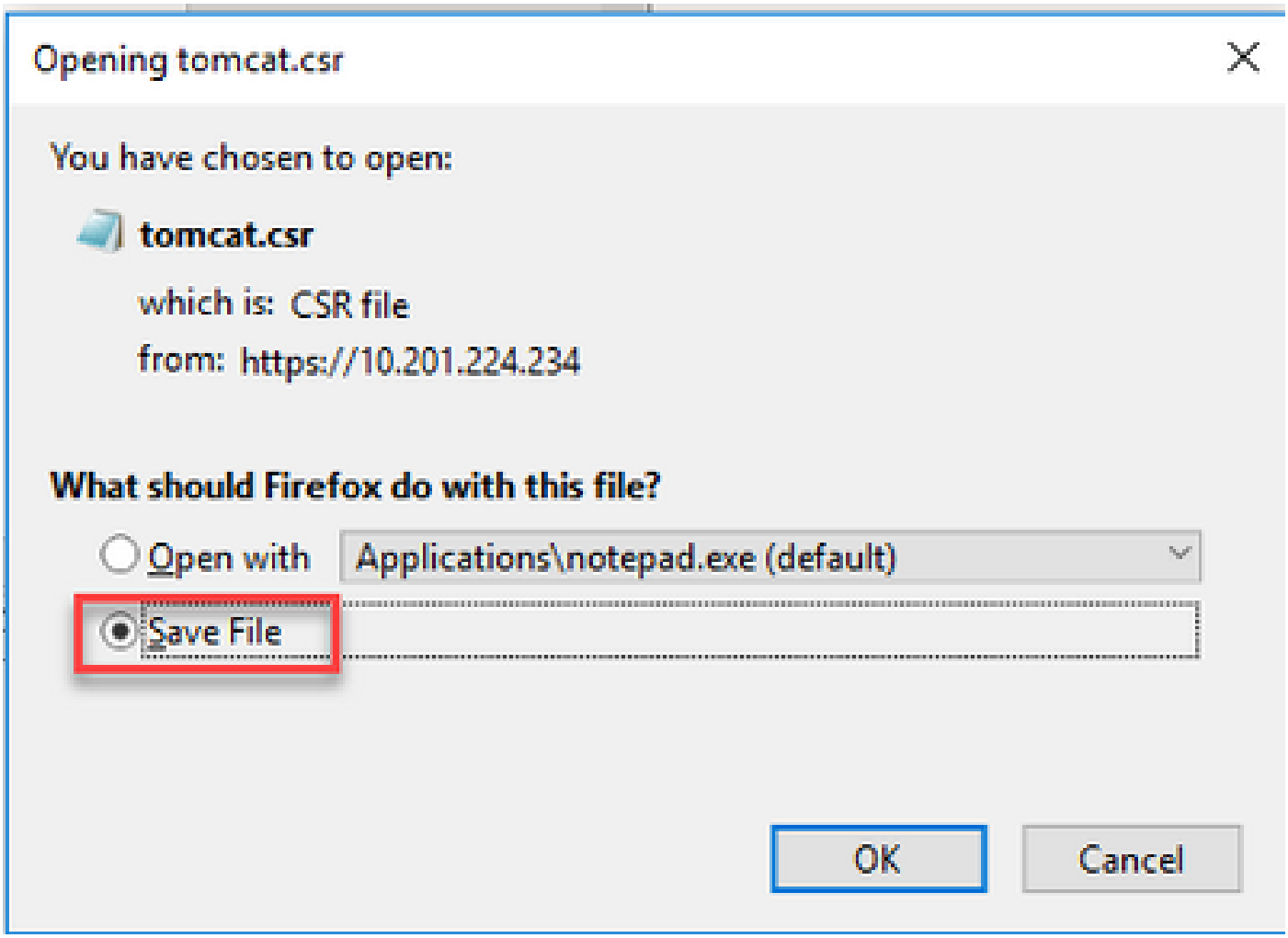
第三步：生成CSR证书后，关闭窗口并选择下载CSR。



第四步：确保证书目的为tomcat，然后单击Download CSR。



第五步：单击Save File。文件保存在Download文件夹中。



2.获取CA签名证书

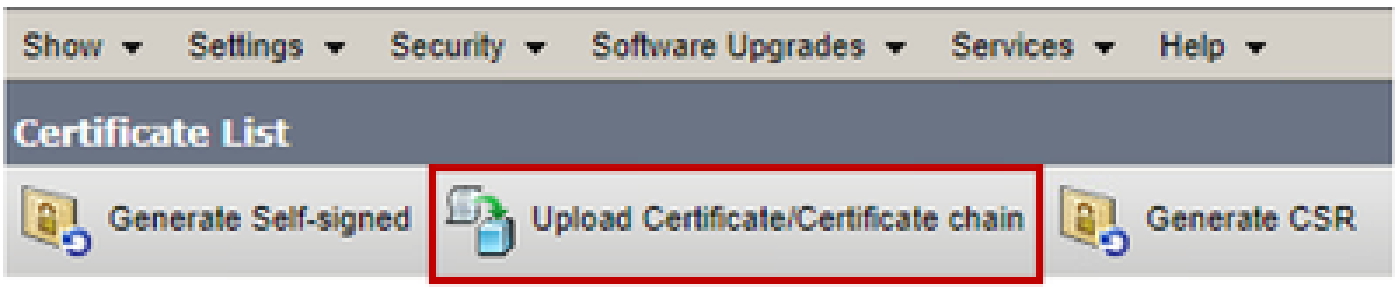
步骤1:在CA上导出的tomcat证书上签名。

第二步：下载应用和从CA机构认证的根证书。

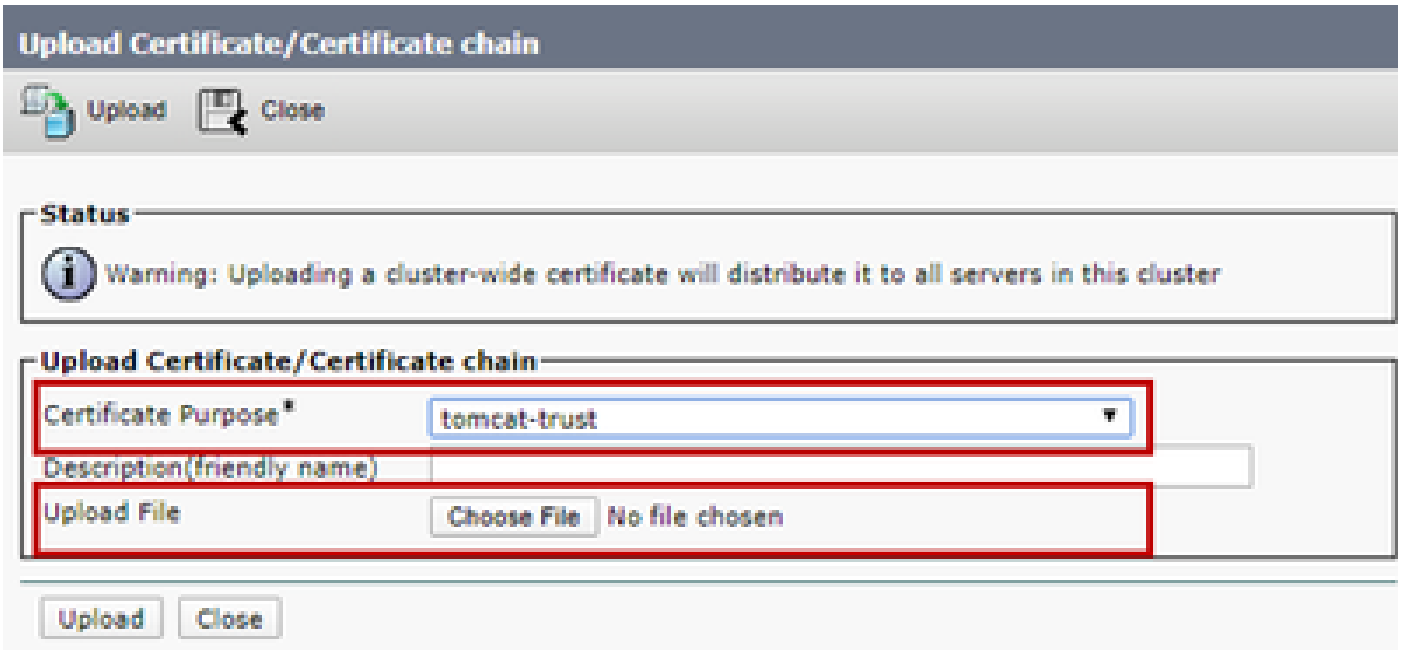
3.上传应用和根证书

步骤1:导航至Cisco Unified Communications Operating System Administration页面：https://FQDN:<8443或443>/cmplatform。

第二步：导航到安全>证书管理，然后选择上传证书/证书链。

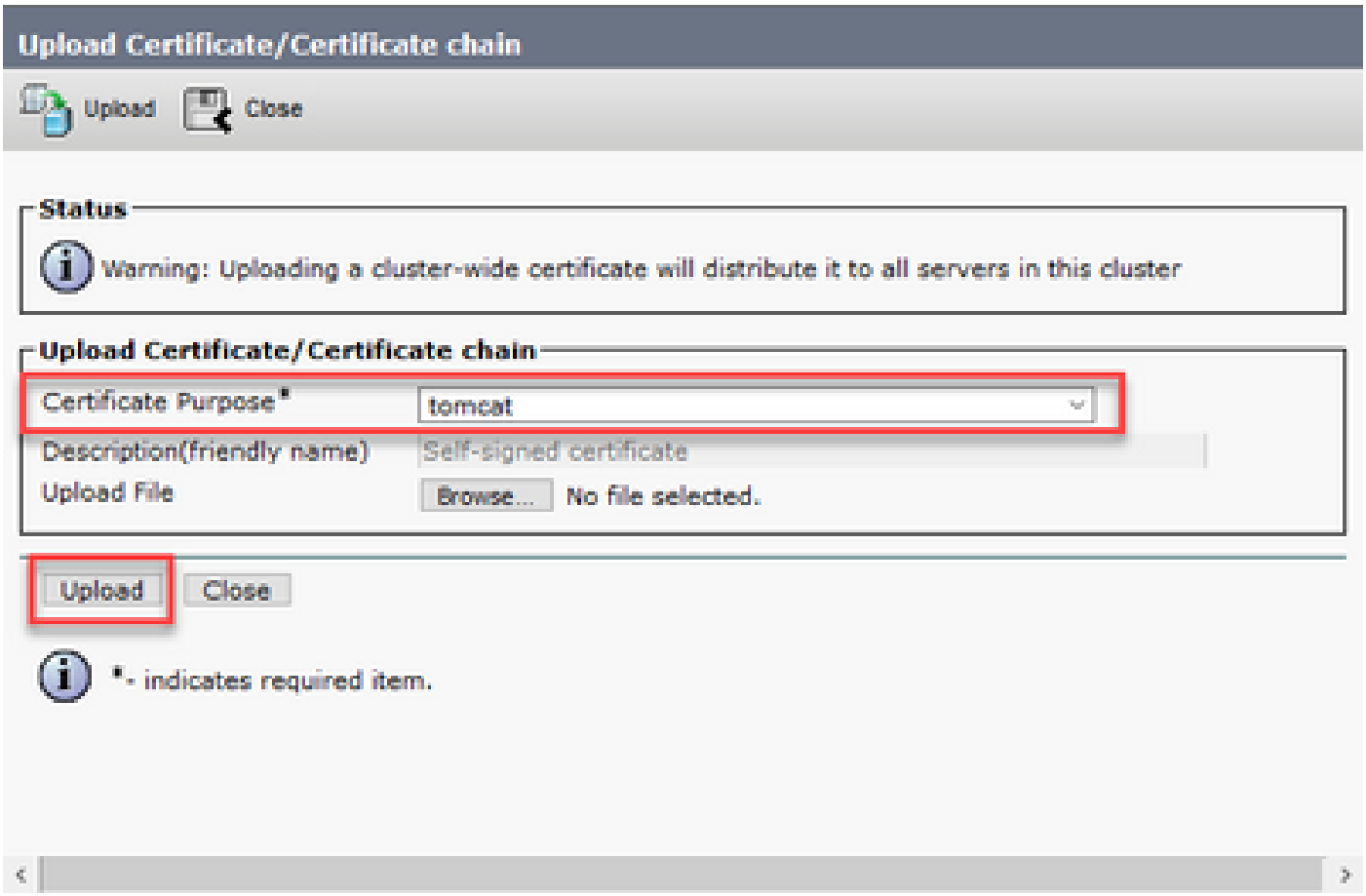


第三步：在Upload certificate/Certificate chain窗口中，选择tomcat-trust in certificate purpose字段并上传根证书。



第四步：将中间证书（如果有）作为tomcat-trust上传。

第五步：在Upload certificate/Certificate chain（上传证书/证书链）窗口中，选择Certificate Purpose（证书用途）字段中的now tomcat，然后上传应用CA签名的证书。



第六步：重新启动服务器。

验证

重新启动服务器后，请执行以下步骤以验证CA签名的实现：

步骤1:打开Web浏览器并清除缓存。

第二步：关闭，然后再次打开浏览器。

现在，您必须看到证书开关以开始CA签名的证书，并且浏览器窗口中指示证书是自签名的，因此不受信任，必须离开。

故障排除

本指南中没有用于排除CA签名证书实施故障的步骤。

相关信息

- CVP配置指南：CVP配置指南 — 安全
- UCCE配置指南：UCCE配置指南 — 安全
- PCCE管理指南：PCE管理指南 — 安全
- UCCE自签名证书：Exchange UCCE自签名证书

- PCCE自签名证书：Exchange PCCE自签名证书
- 在CCE 12.5(1)中安装和迁移到OpenJDK:CCE OpenJDK迁移
- 在CVP 12.5(1)中安装和迁移到OpenJDK:CVP OpenJDK迁移

技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。