CCEソリューションでのCA署名付き証明書の実装

内容

はじめに

このドキュメントでは、Cisco Contact Center Enterprise(CCE)ソリューションで認証局(CA)署名付き証明書を実装する方法について説明します。

著者：Cisco TACエンジニア、Anuj Bhatia、Robert Rogier、Ramiro Amaya

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Unified Contact Center Enterprise(UCCE)リリース12.5(1)
- Package Contact Center Enterpriseリリース12.5(1)
- Customer Voice Portal(CVP)リリース12.5(1)
- Cisco Virtualized Voice Browser(VVB)
- Cisco CVP Operations and Administration Console(OAMP)
- Cisco Unified Intelligence Center（CUIC）
- Cisco Unified Communications Manager（CUCM）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- Finesss 12.5（2015年12月）
- CUIC 12.5
- Windows 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド

証明書は、クライアントとサーバ間の認証で通信が安全であることを保証するために使用されます。

ユーザはCAから証明書を購入するか、自己署名証明書を使用できます。

自己署名証明書（名前が示すように）は、認証局によって署名されるのではなく、IDが証明される同じエンティティによって署名されます。自己署名証明書は、CA証明書ほど安全とは見なされませんが、多くのアプリケーションでデフォルトで使用されます。

Package Contact Center Enterprise(PCCE)ソリューションバージョン12.xでは、ソリューションのすべてのコンポーネントが、プリンシパルAdmin Workstation(AW)サーバでホストされるSingle Pane of Glass(SPOG)によって制御されます。

PCCE 12.5(1)バージョンのSecurity Management Compliance(SRC)により、SPOGとソリューション内の他のコンポーネント間のすべての通信は、セキュアHTTPプロトコルを介して行われます。UCCE 12.5では、コンポーネント間の通信もセキュアHTTPプロトコルを介して行われます。

このドキュメントでは、セキュアなHTTP通信のためにCCEソリューションでCA署名付き証明書を実装するために必要な手順について詳しく説明します。その他のUCCEセキュリティの考慮事

項については、『UCCEセキュリティガイドライン』を参照してください。セキュアHTTPとは異なる、その他のCVPのセキュア通信については、『CVP Configuration Guide: CVP Security Guidelines』のセキュリティガイドラインを参照してください。

手順

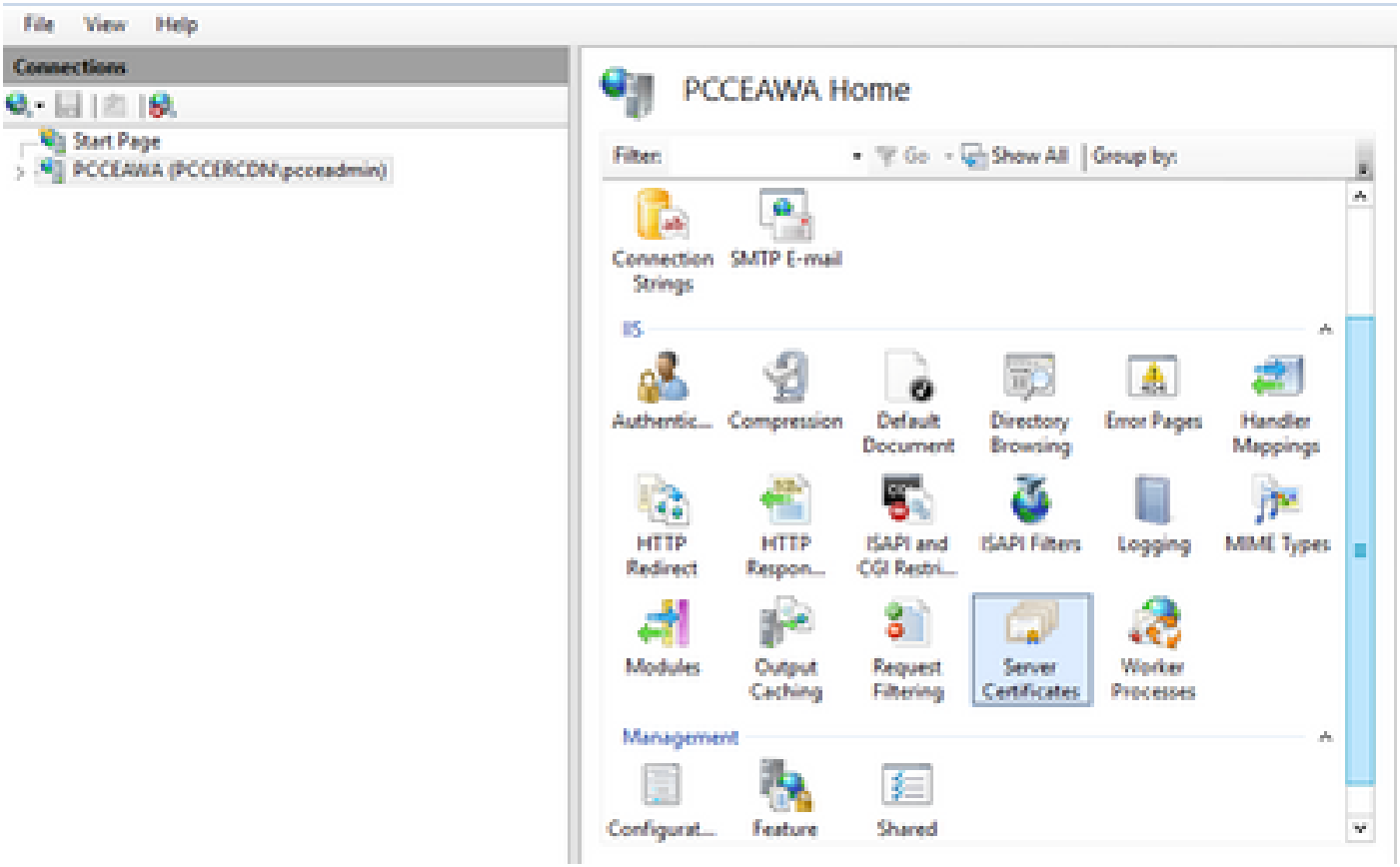
CCE Windowsベースのサーバ

1. CSRの生成

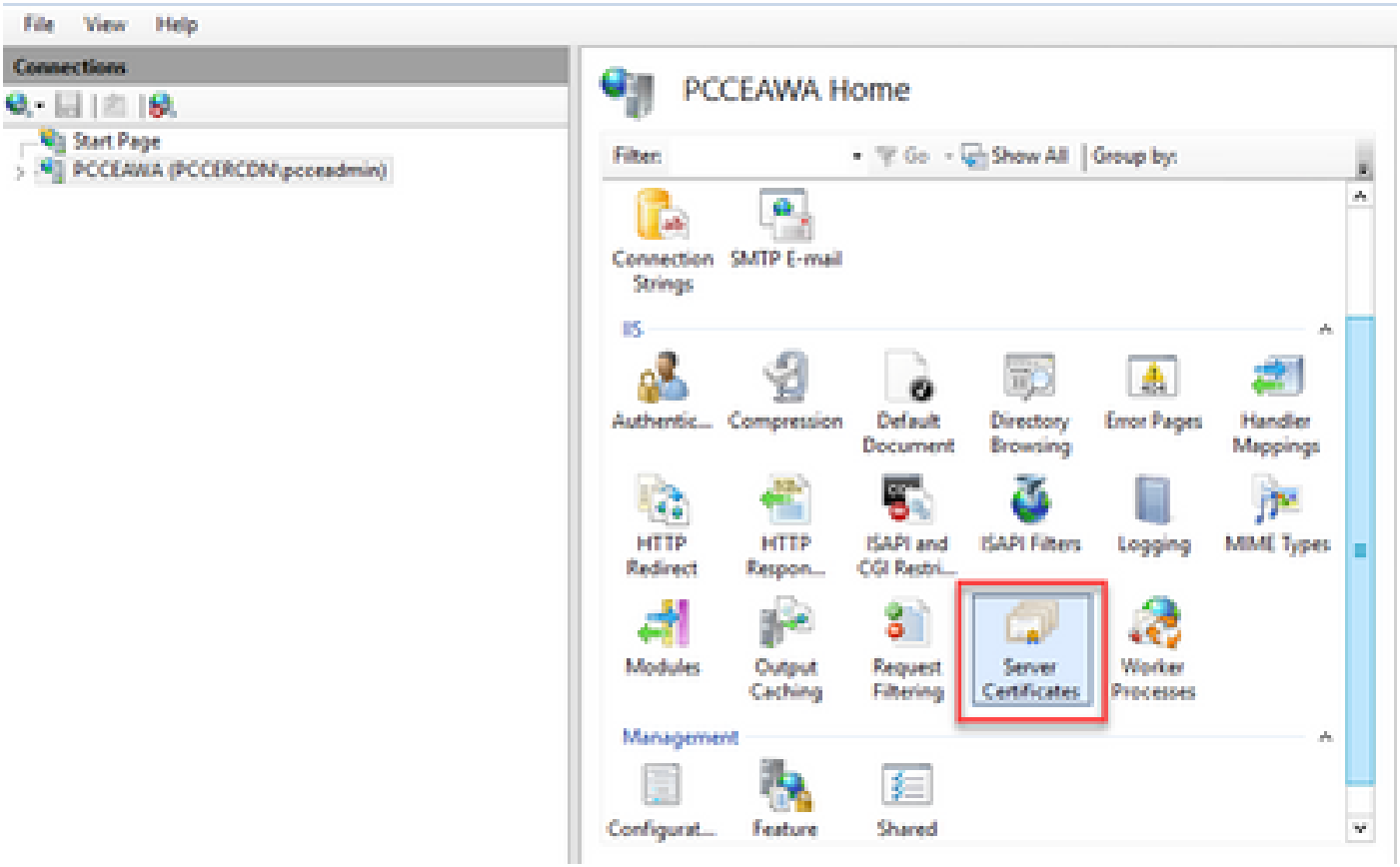
この手順では、インターネットインフォメーションサービス(IIS)マネージャから証明書署名要求(CSR)を生成する方法について説明します。

ステップ 1：Windowsにログインし、Control Panel > Administrative Tools > Internet Information Services (IIS) Managerの順に選択します。

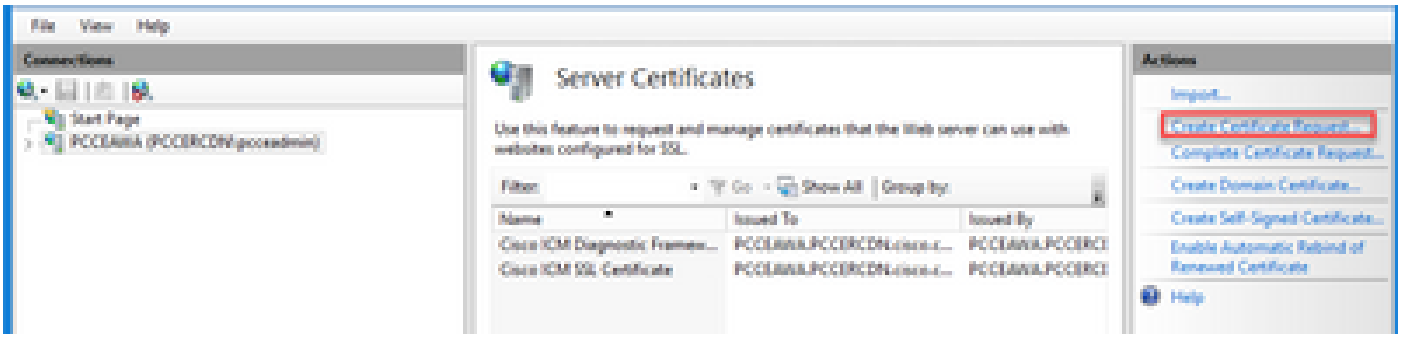
ステップ2.[接続]ウィンドウで、サーバー名をクリックします。サーバのホーム・ペインが表示されます。



手順 3：IIS領域で、Server Certificatesをダブルクリックします。

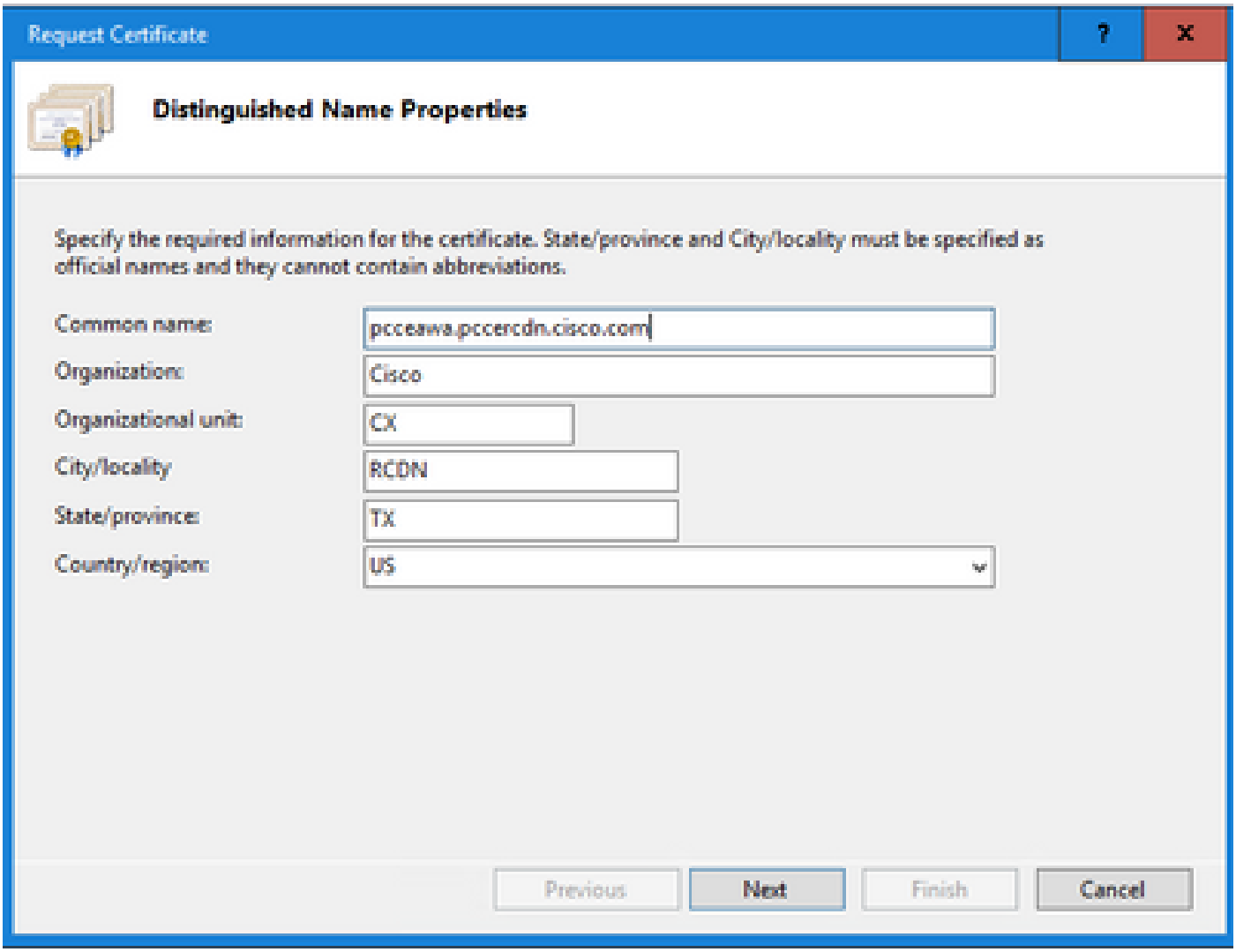


ステップ4.ActionsペインでCreate Certificate Requestをクリックします。



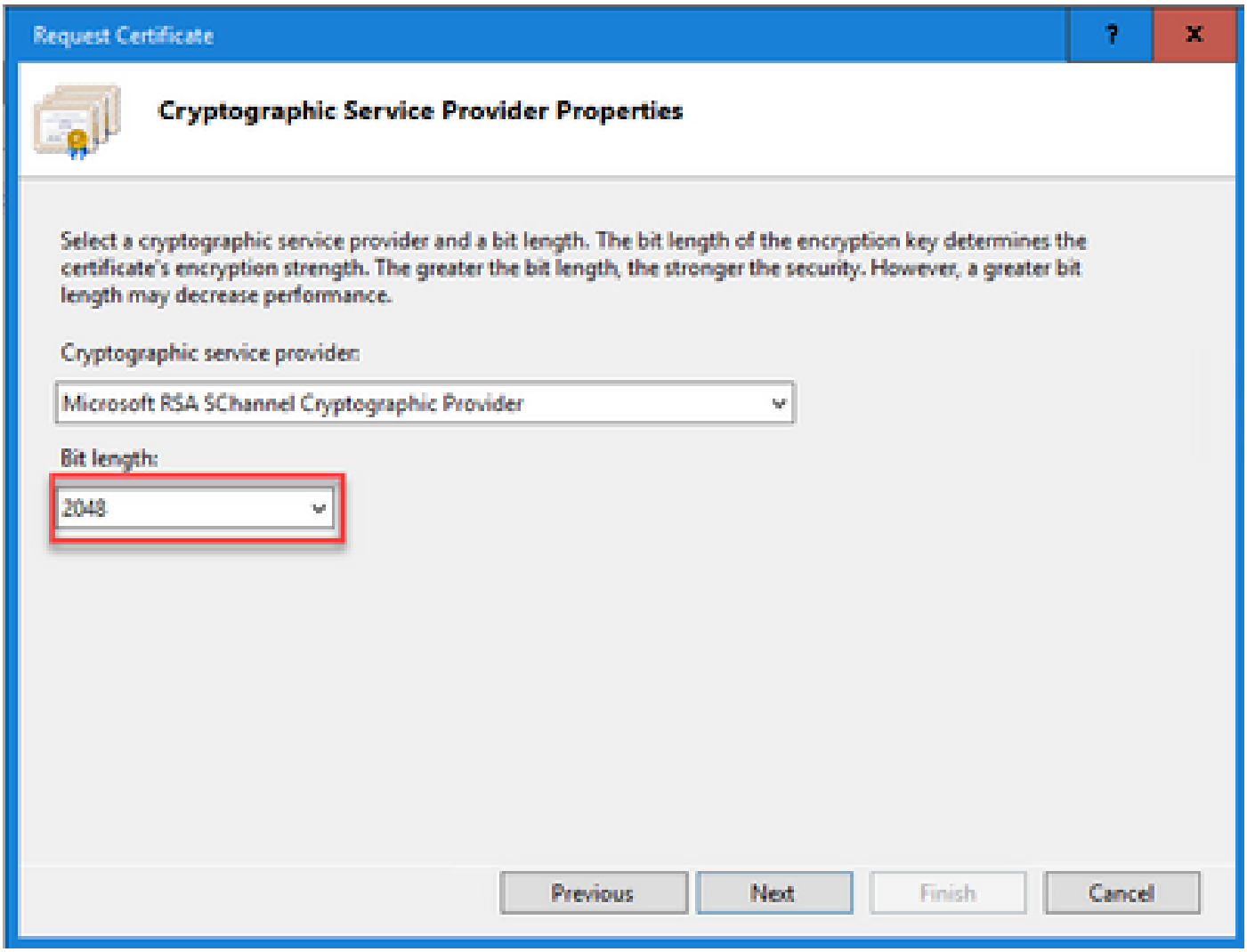
ステップ 5：Request Certificateダイアログボックスで、次の操作を行います。

表示されたフィールドに必要な情報を指定し、Nextをクリックします。

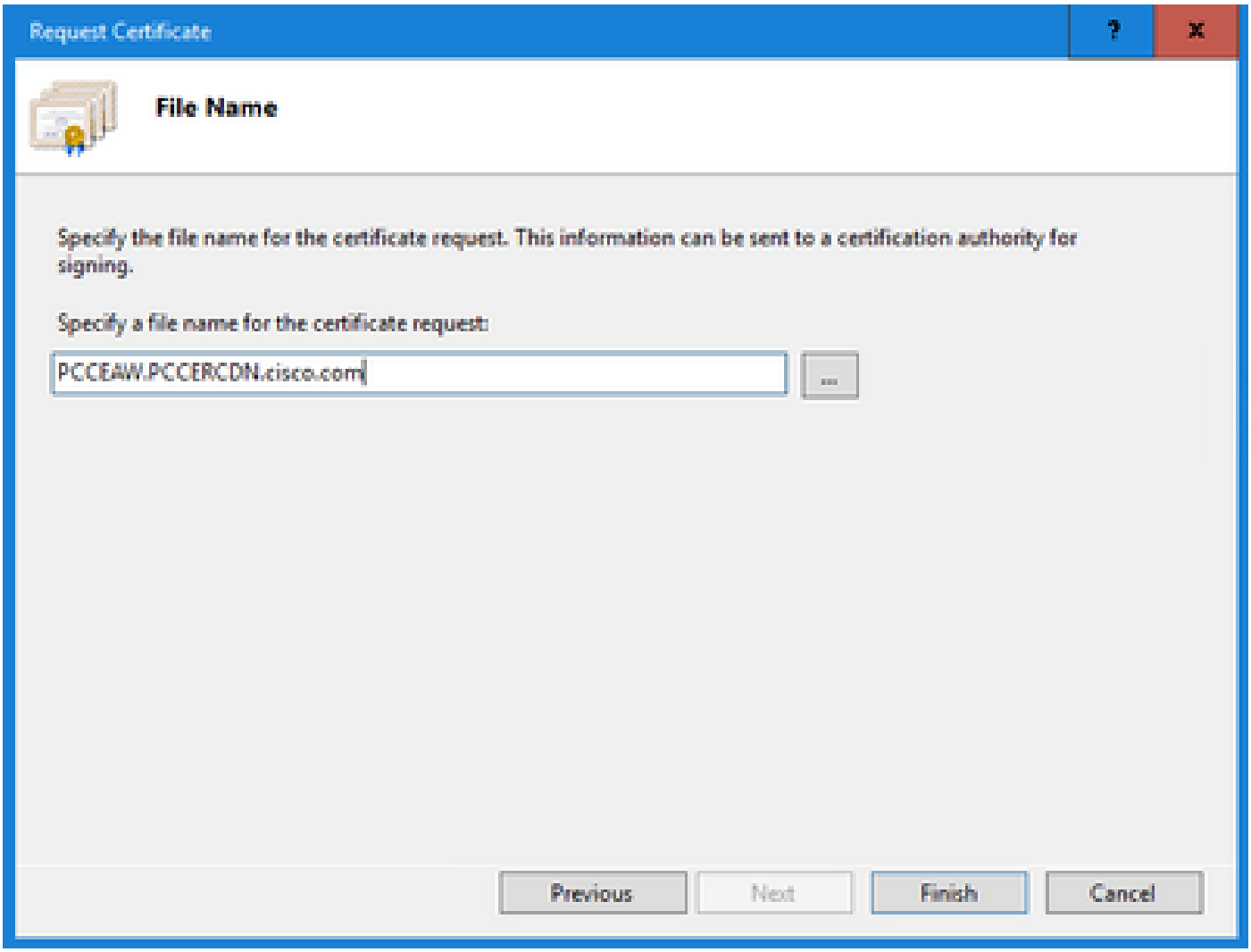


Cryptographic service providerドロップダウンリストで、デフォルト設定を残します。

Bit lengthドロップダウンリストから、2048を選択します。



手順 6：証明書要求のファイル名を指定して、Finishをクリックします。



2. CA署名付き証明書の取得

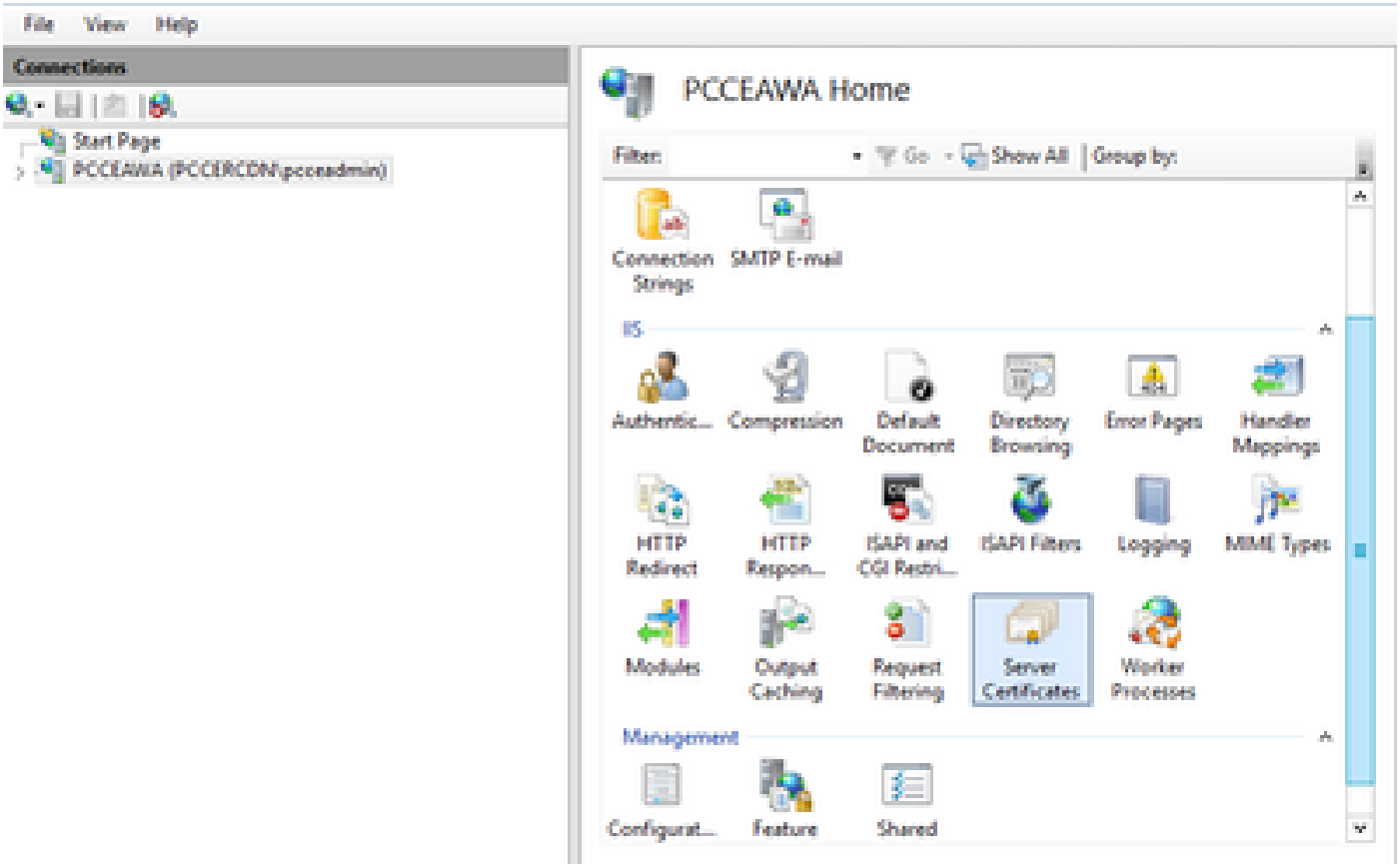
ステップ 1：CAで証明書に署名します。

注:CAが使用する証明書テンプレートにクライアント認証とサーバ認証が含まれていることを確認してください。

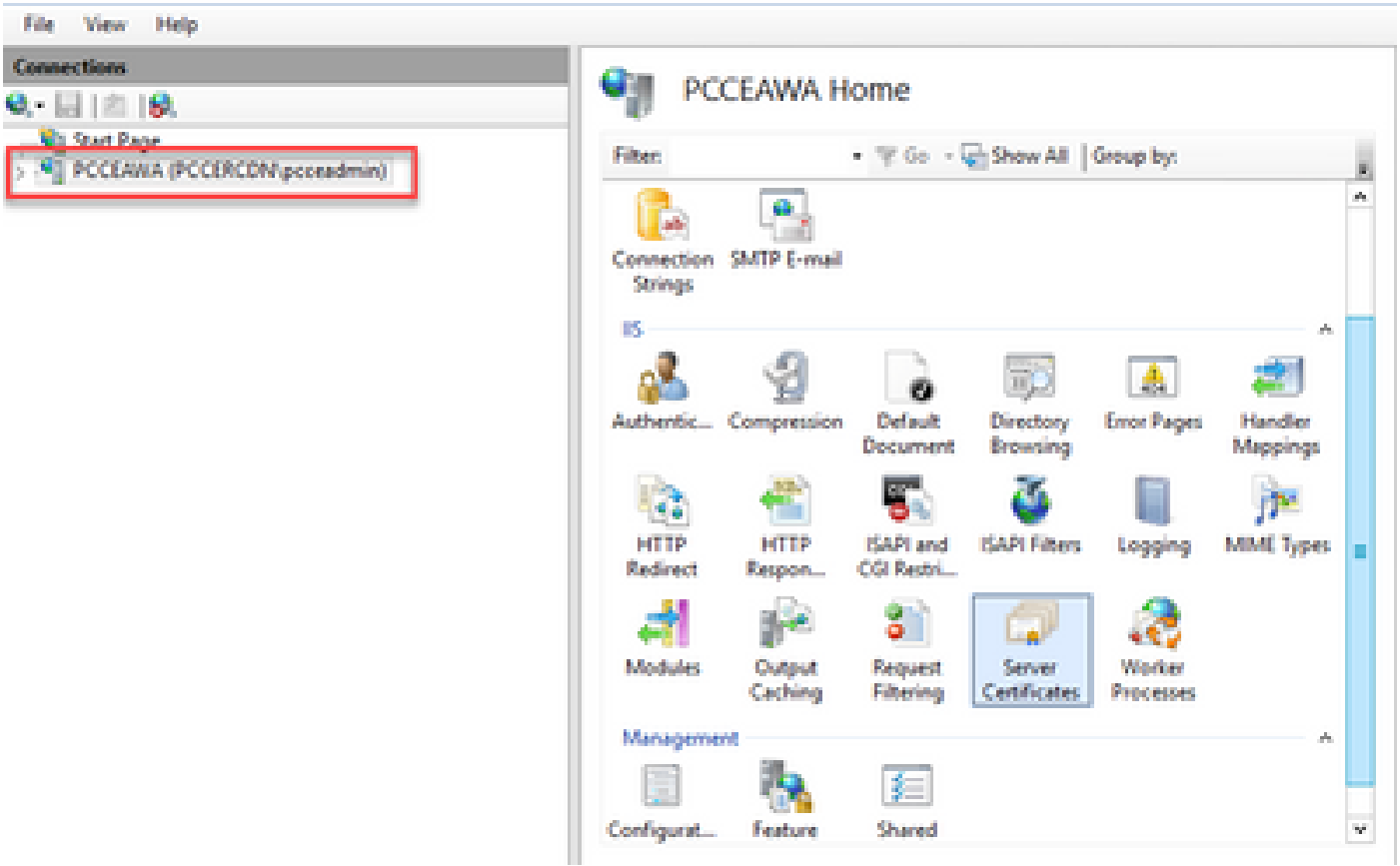
ステップ 2：CA署名付き証明書を認証局(ルート、アプリケーション、および中間（存在する場合）)から取得します。

3. CA署名付き証明書のアップロード

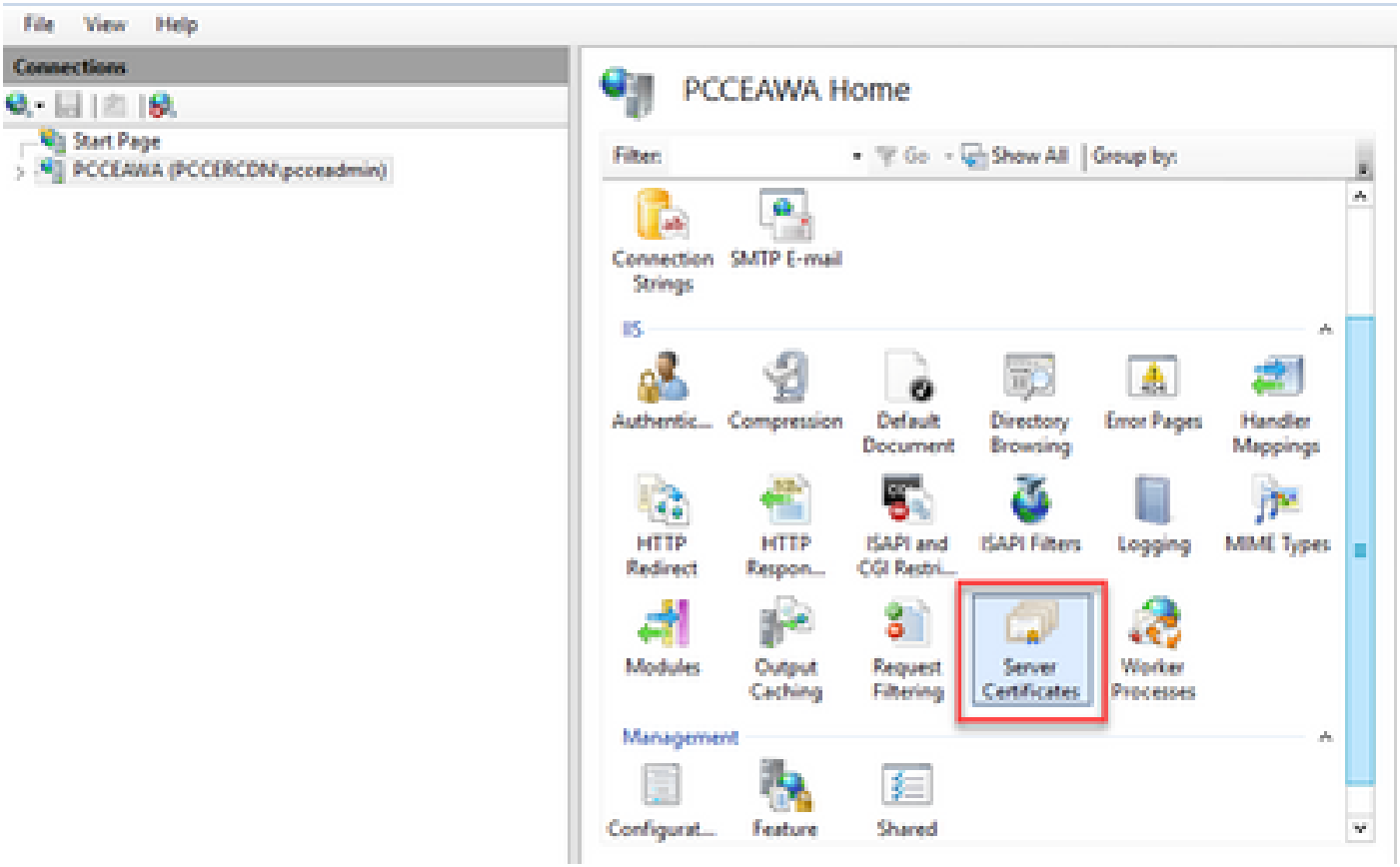
ステップ 1：Windowsにログインし、Control Panel > Administrative Tools > Internet Information Services (IIS) Managerの順に選択します。



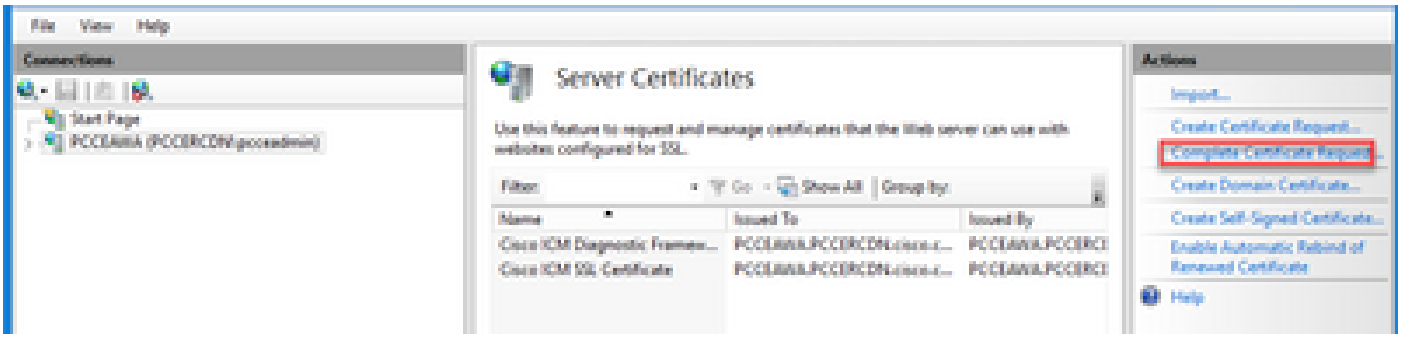
ステップ2.[接続]ウィンドウで、サーバー名をクリックします。



手順 3：IIS領域で、Server Certificatesをダブルクリックします。



ステップ4.ActionsペインでComplete Certificate Requestをクリックします。



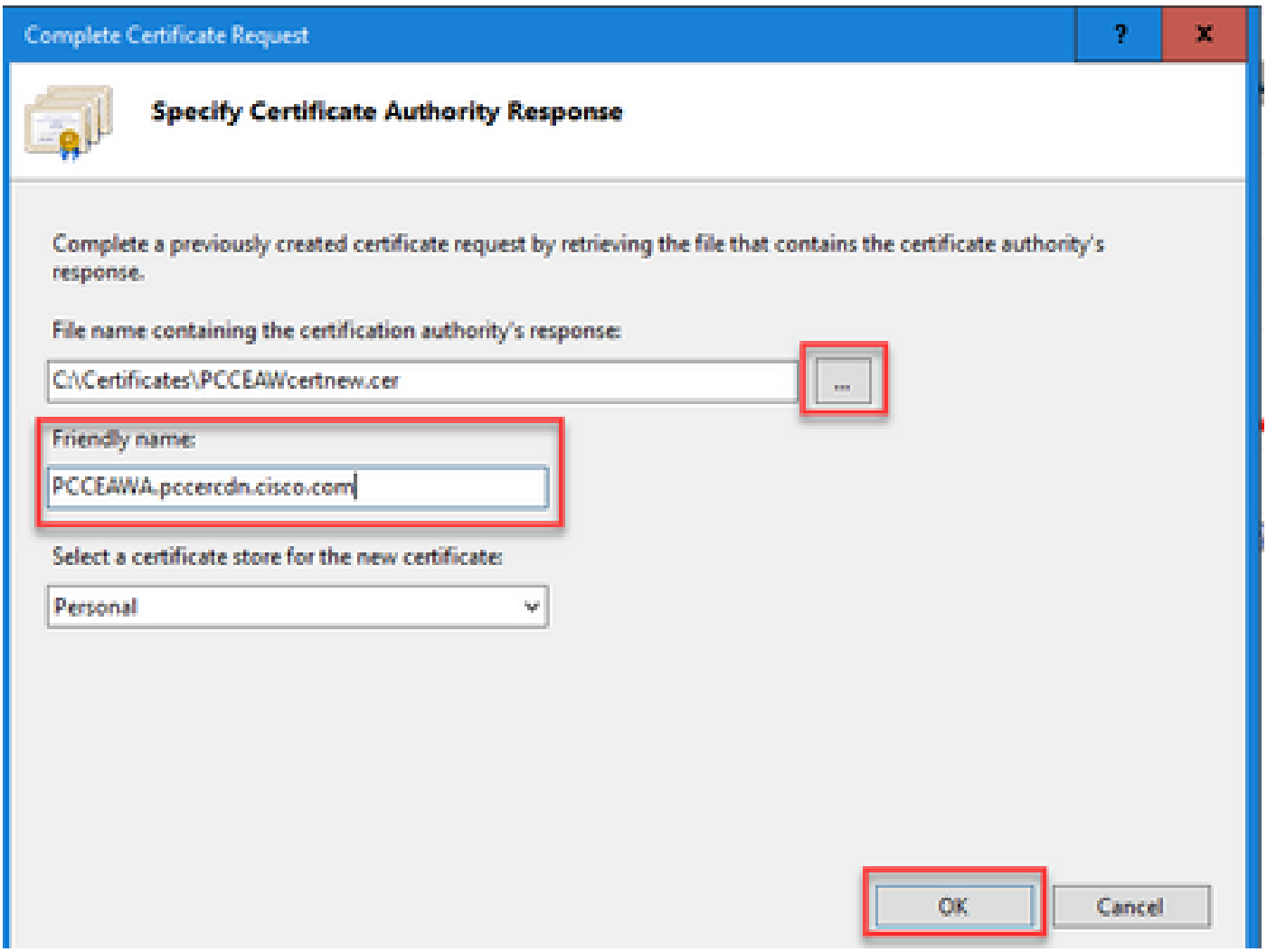
ステップ5:Complete Certificate Requestダイアログボックスで、次のフィールドに値を入力します。

[File name which contains the certification authority response]フィールドで、[...]ボタンをクリックします。

署名されたアプリケーション証明書が保存されている場所を参照し、[開く]をクリックします。

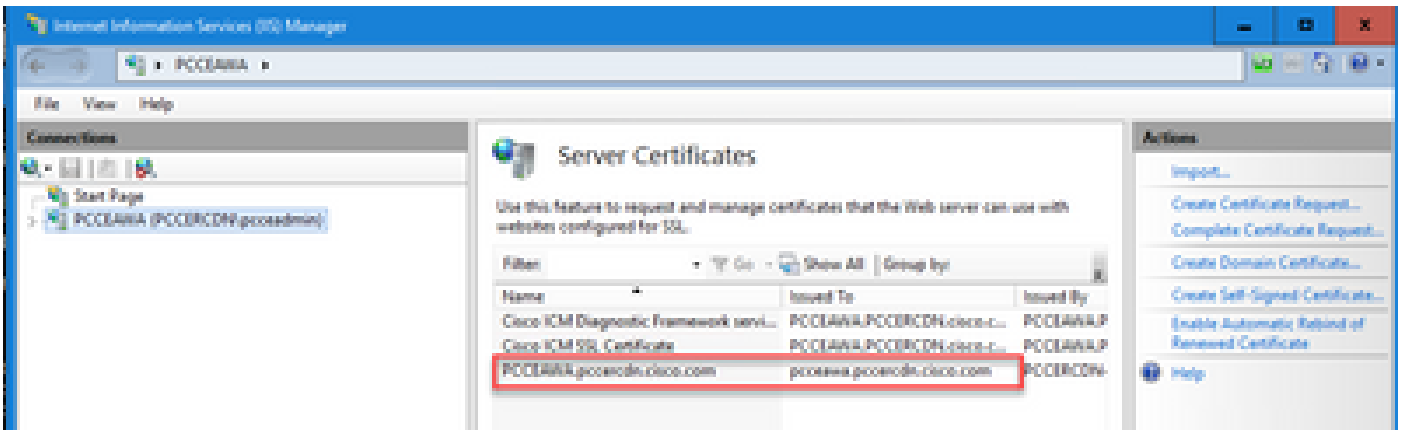
注：これが2-Tier CA実装であり、ルート証明書がまだサーバ証明書ストアにない場合は、署名付き証明書をインポートする前に、ルートをWindowsストアにアップロードする必要があります。ルートCAをWindowsストアhttps://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificateにアップロードする必要がある場合は、このドキュメントを参照してください。

[フレンドリ名]フィールドに、サーバーの完全修飾ドメイン名(FQDN)または任意の有効な名前を入力します。Select a certificate store for the new certificateドロップダウンがPersonalのままであることを確認します。



ステップ 6：[OK] をクリックして証明書をアップロードします。

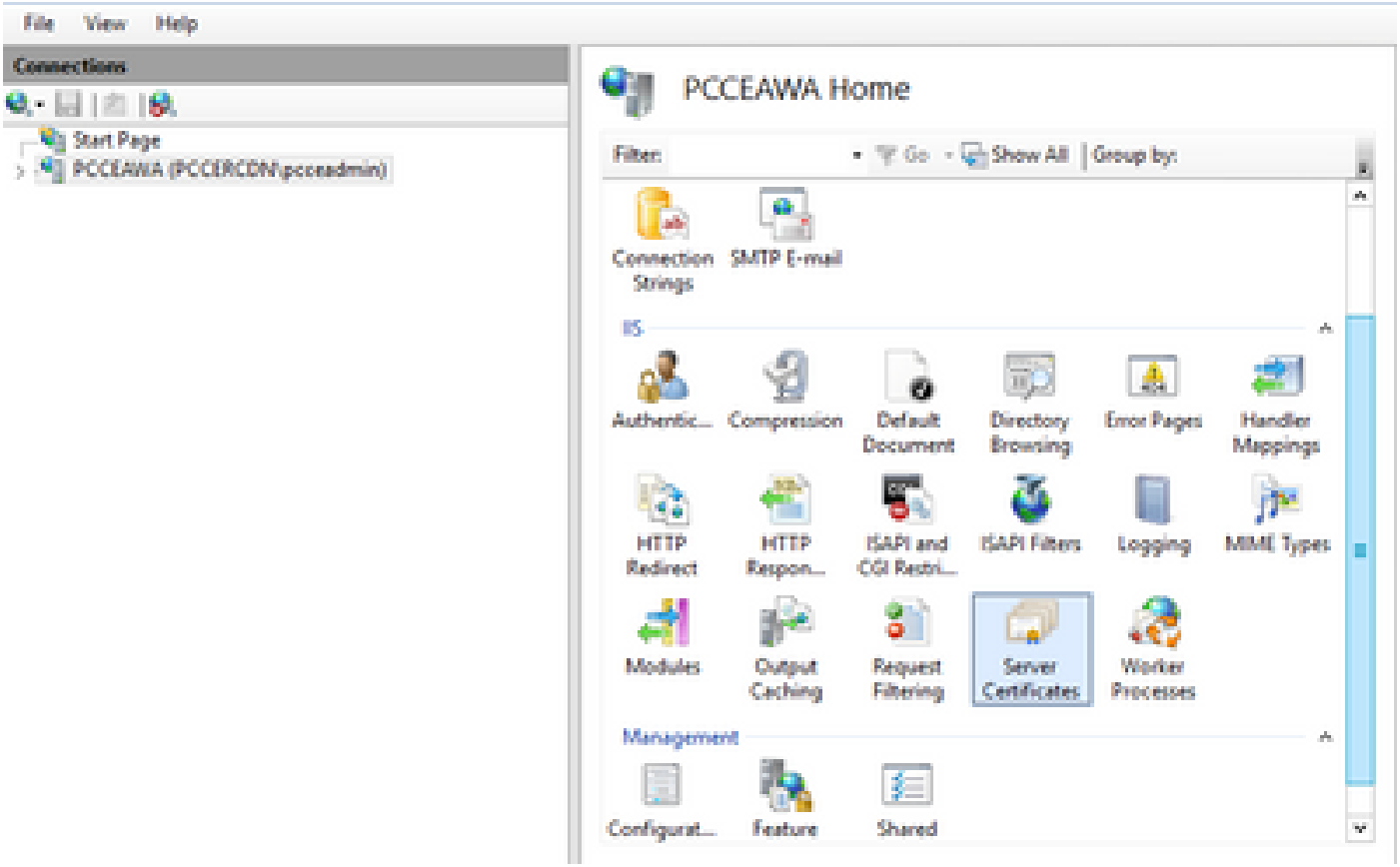
証明書のアップロードが成功すると、証明書が[サーバ証明書]ペインに表示されます。



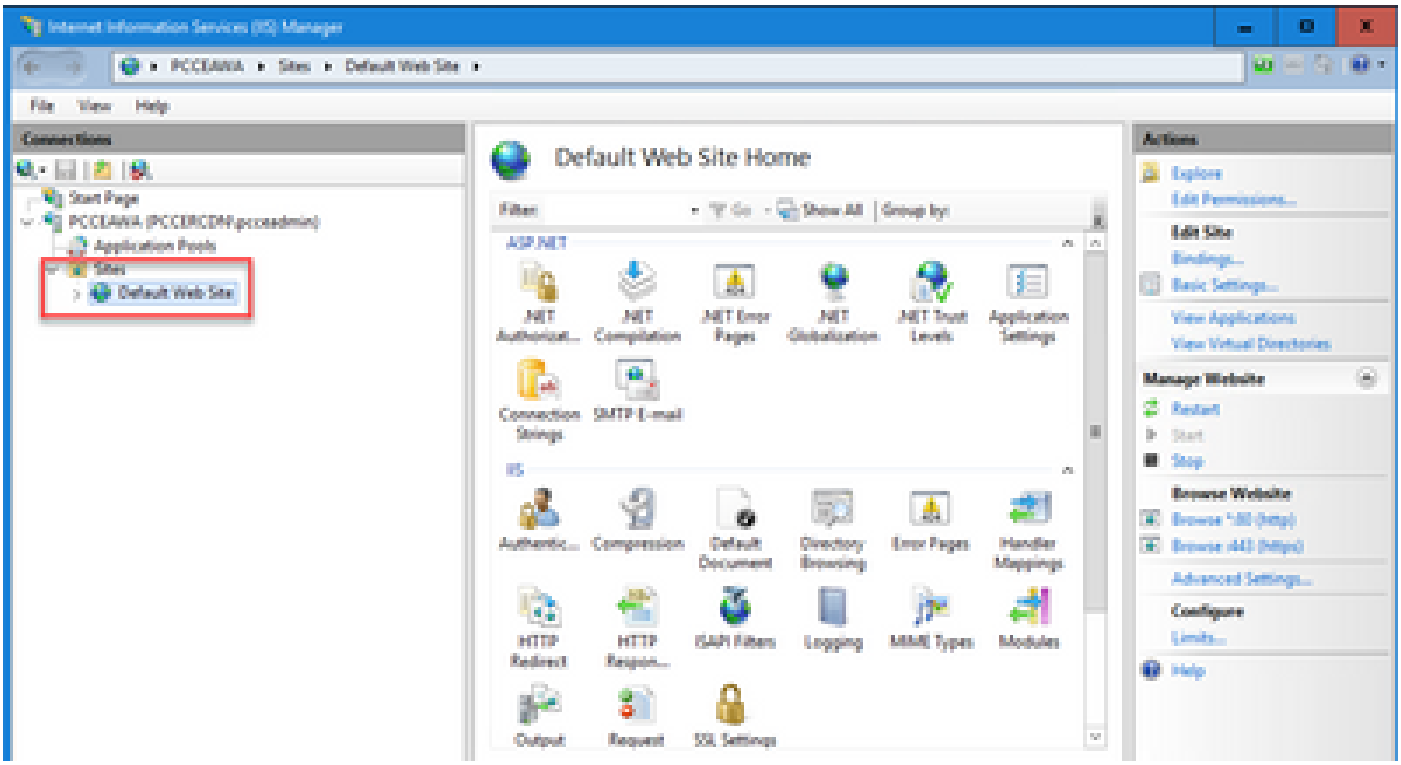
4. CA署名付き証明書のIISへのバインド

この手順では、IISマネージャでCA署名付き証明書をバインドする方法について説明します。

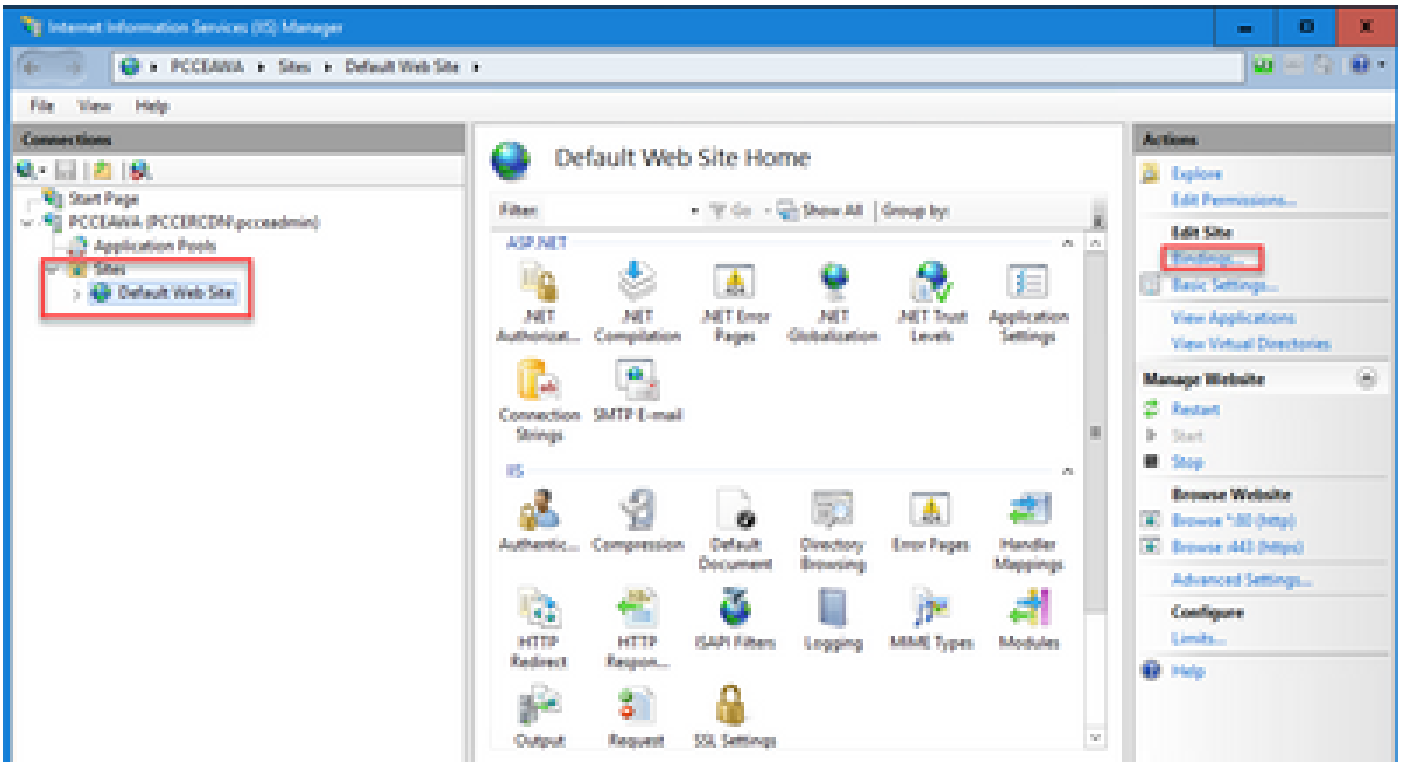
ステップ 1：Windowsにログインし、Control Panel > Administrative Tools > Internet Information Services (IIS) Managerの順に選択します。



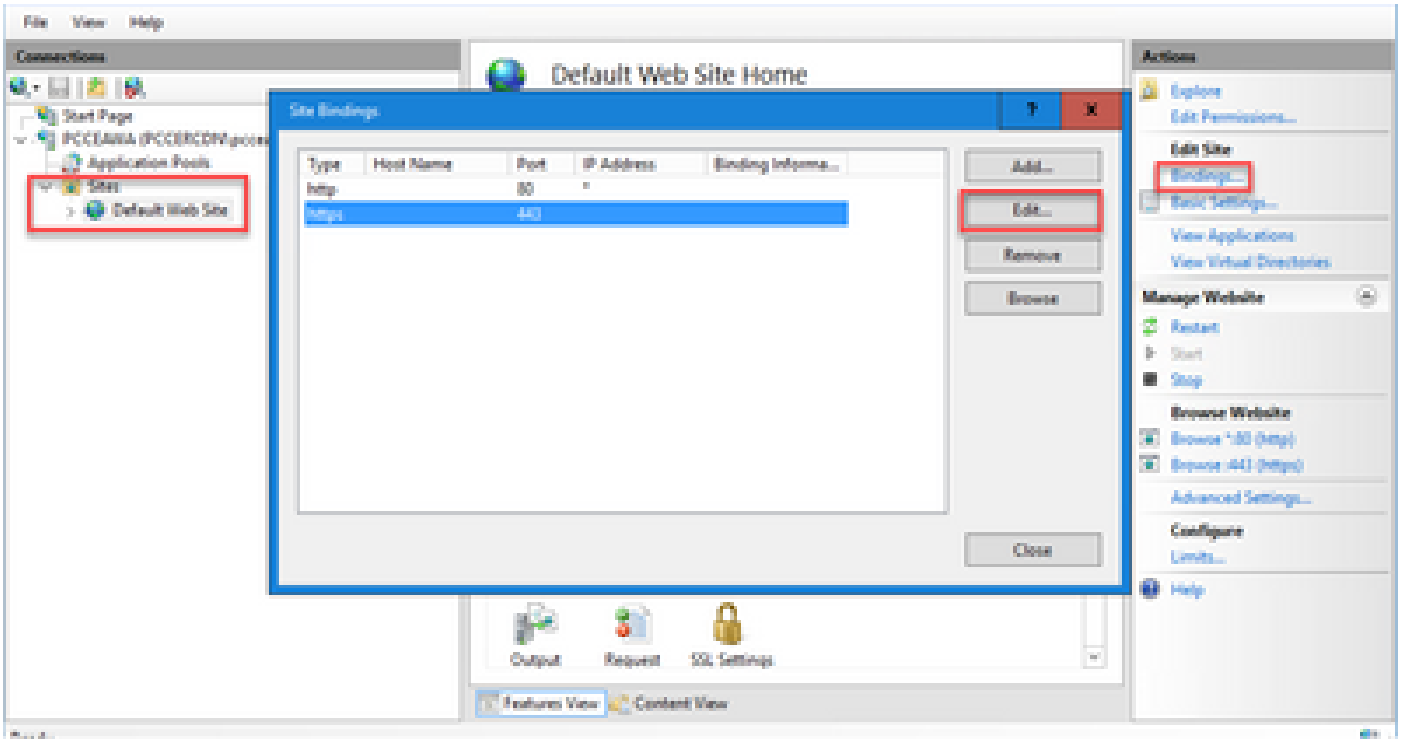
ステップ2.Connectionsペインで、<server_name> > Sites > Default Web Siteの順に選択します。



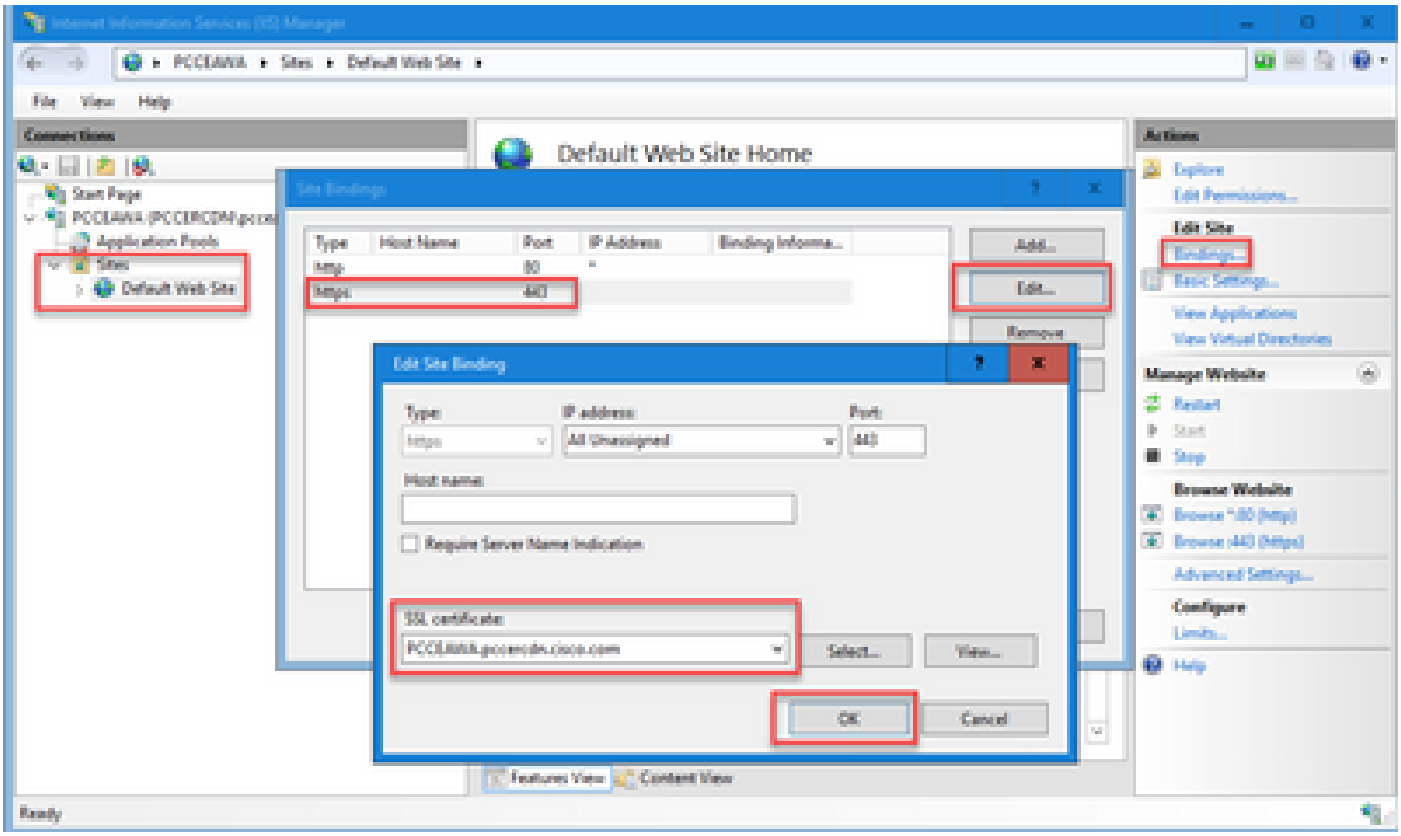
手順 3：[操作]ウィンドウで、[バインド...]をクリックします。



ステップ4.httpsと入力し、ポート443をクリックして、Edit...をクリックします。

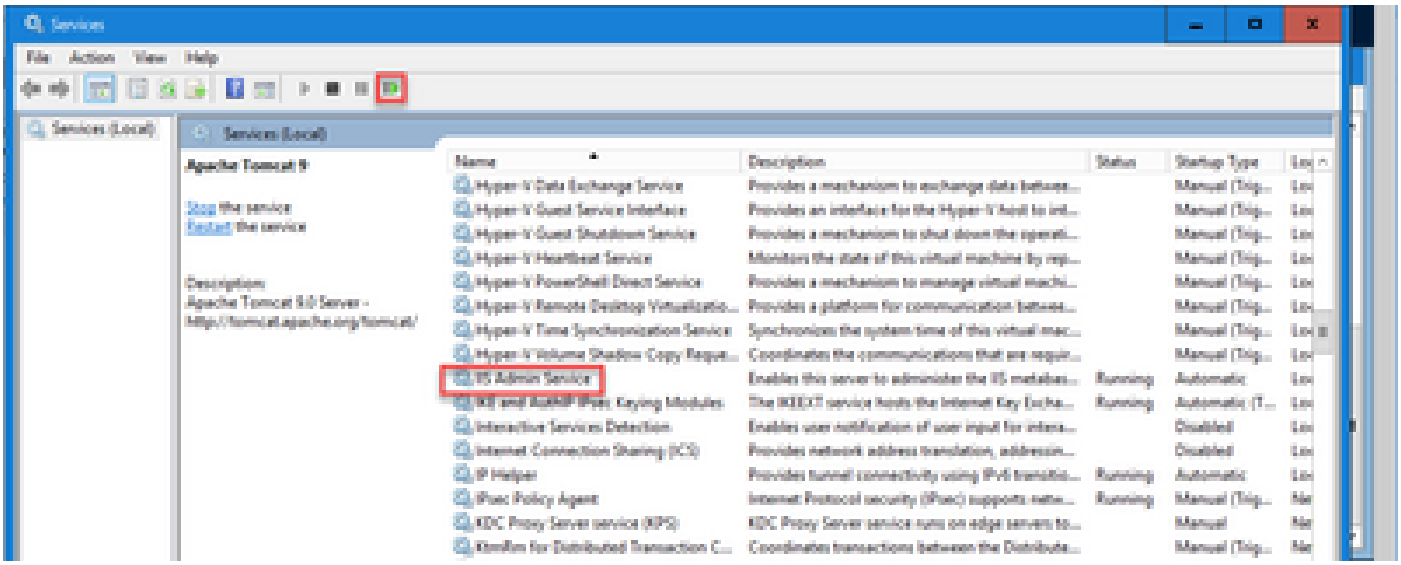


ステップ5:SSL証明書のドロップダウンリストから、前の手順で指定したフレンドリ名と同じ名前を持つ証明書を選択します。



ステップ 6：[OK] をクリックします。

ステップ 7：Start > Run > services.mscの順に移動し、IIS Admin Serviceを再起動します。



IISが正常に再起動すると、アプリケーションの起動時に証明書エラーの警告が表示されません。

5. Diagnostic PorticoへのCA署名付き証明書のバインド

この手順では、Diagnostic PorticoでCA署名付き証明書をバインドする方法について説明します。

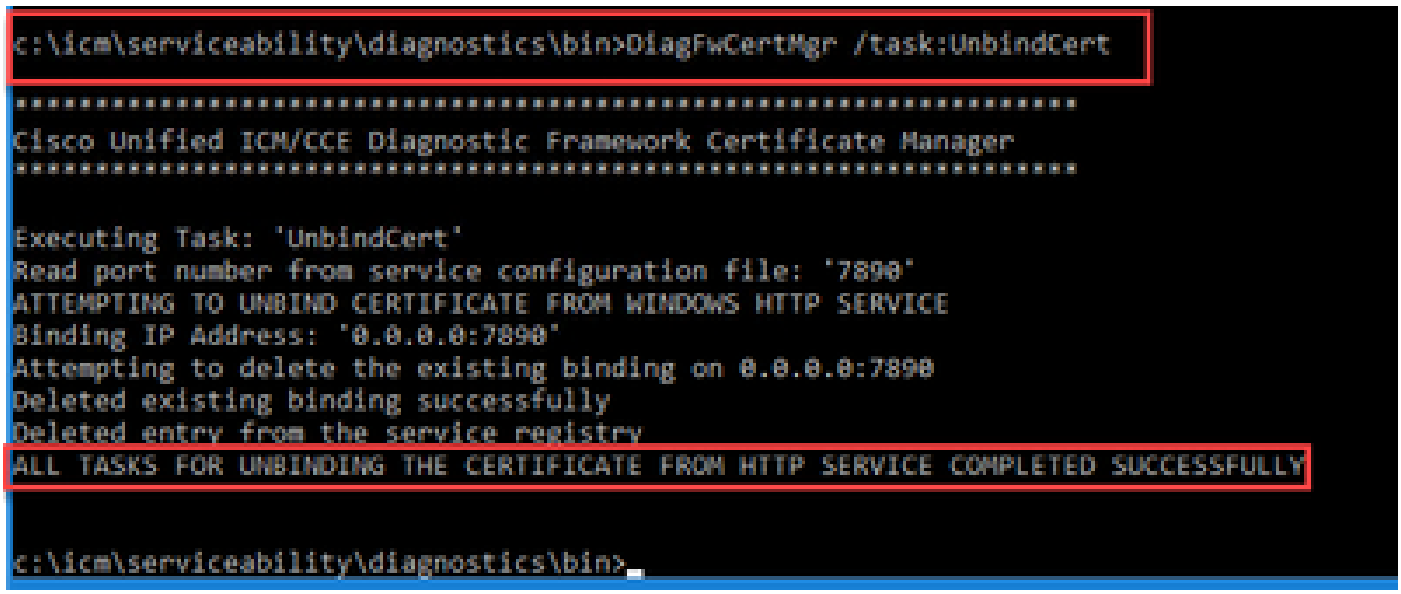
ステップ 1：コマンドプロンプトを開きます（[管理者として実行]）。

ステップ2.Diagnostic Porticoホームフォルダに移動します。次のコマンドを実行します。

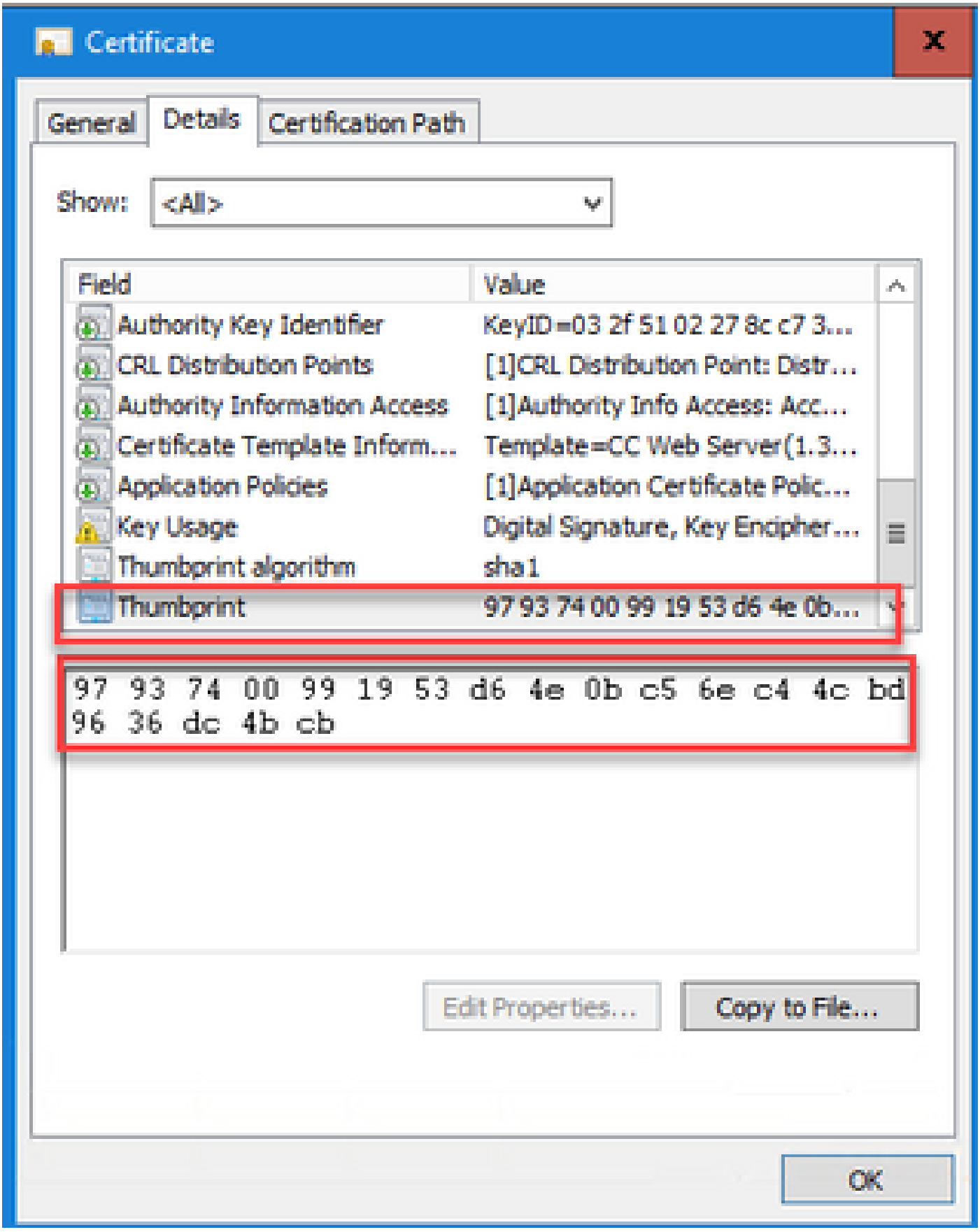
```
cd c:\icm\serviceability\diagnostics\bin
```

手順 3：Diagnostic Porticoにバインドされている現在の証明書を削除します。次のコマンドを実行します。

```
DiagFwCertMgr /task:UnbindCert
```

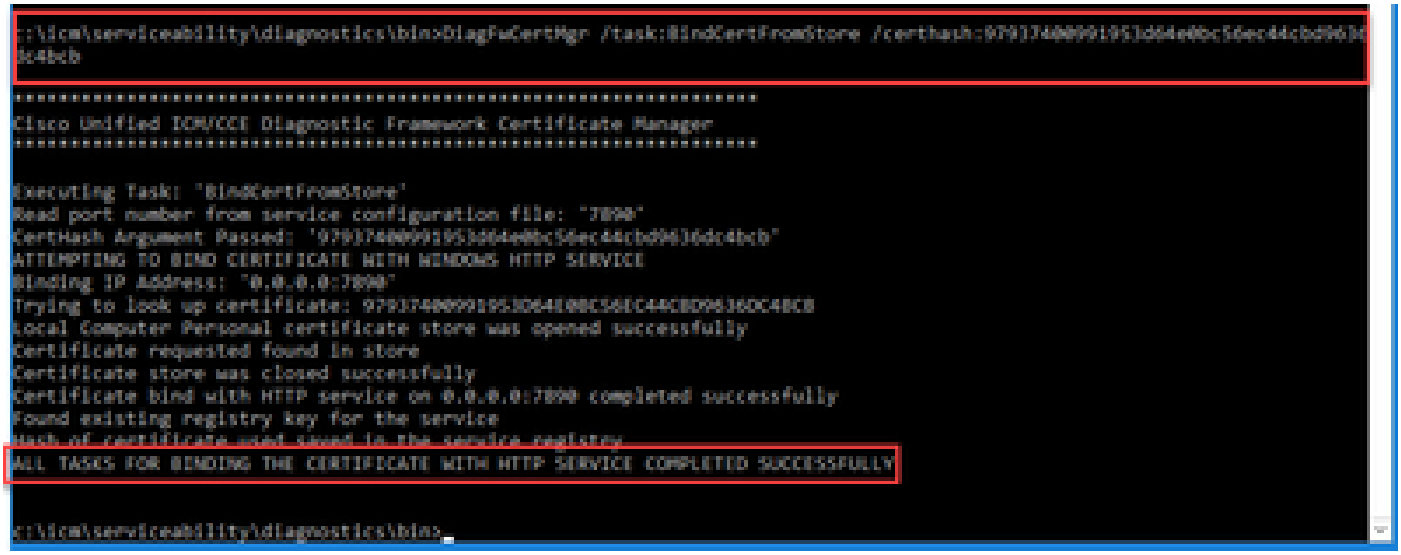


ステップ4.署名付き証明書を開き、[拇印]フィールドのハッシュコンテンツ（スペースなし）をコピーします。



ステップ 5：次のコマンドを実行して、ハッシュの内容を貼り付けます。

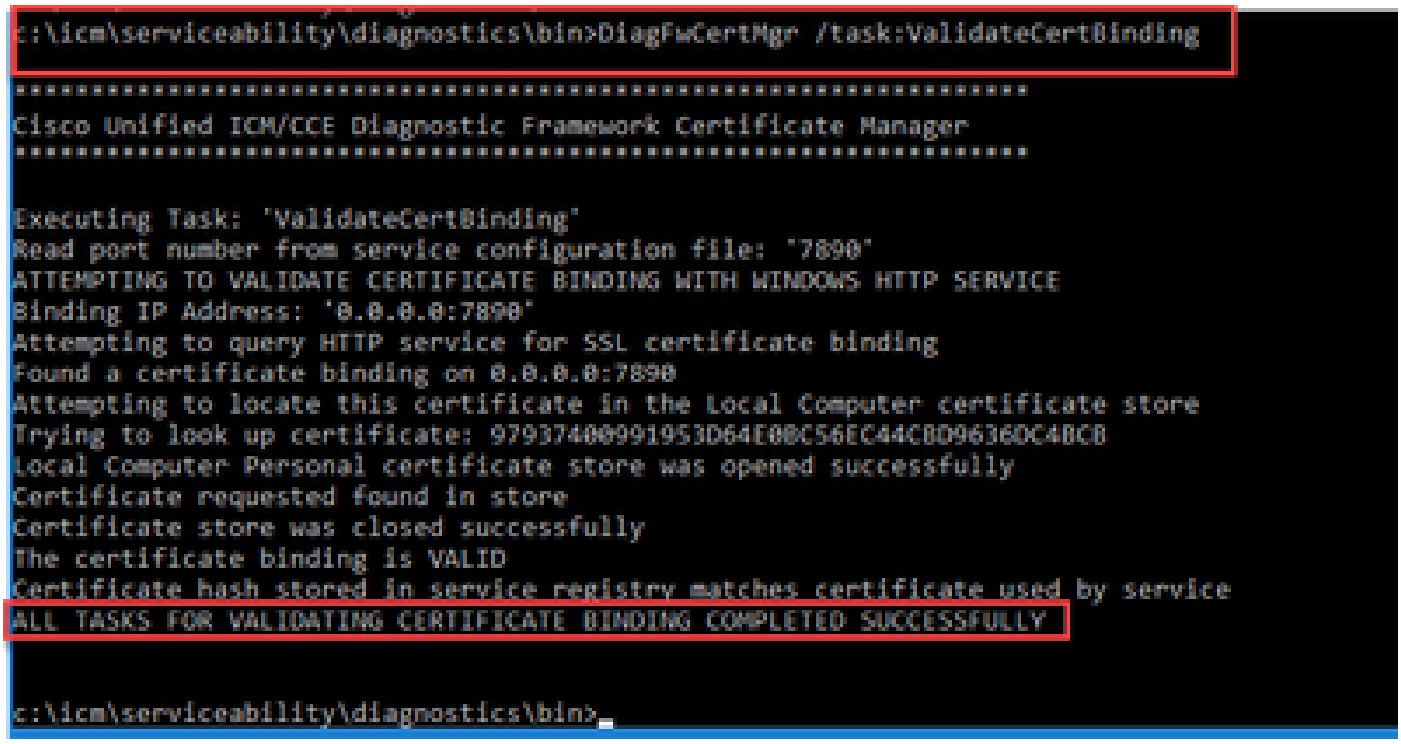
```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```



証明書のバインドが成功すると、「The certificate binding is VALID」というメッセージが表示されます。

手順 6：証明書のバインドが正常に行われたかどうかを検証します。次のコマンドを実行します。

```
DiagFwCertMgr /task:ValidateCertBinding
```



注:DiagFwCertMgrはデフォルトでポート7890を使用します。

証明書のバインドが成功すると、「The certificate binding is VALID」というメッセージが表示されます。

手順 7：Diagnostic Frameworkサービスを再起動します。次のコマンドを実行します。

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

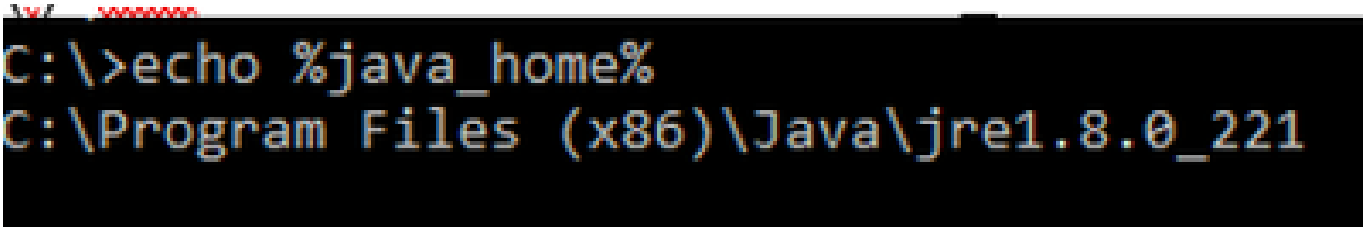
診断フレームワークが正常に再起動すると、アプリケーションの起動時に証明書エラー警告が表示されません。

6. Javaキーストアへのルートおよび中間証明書のインポート

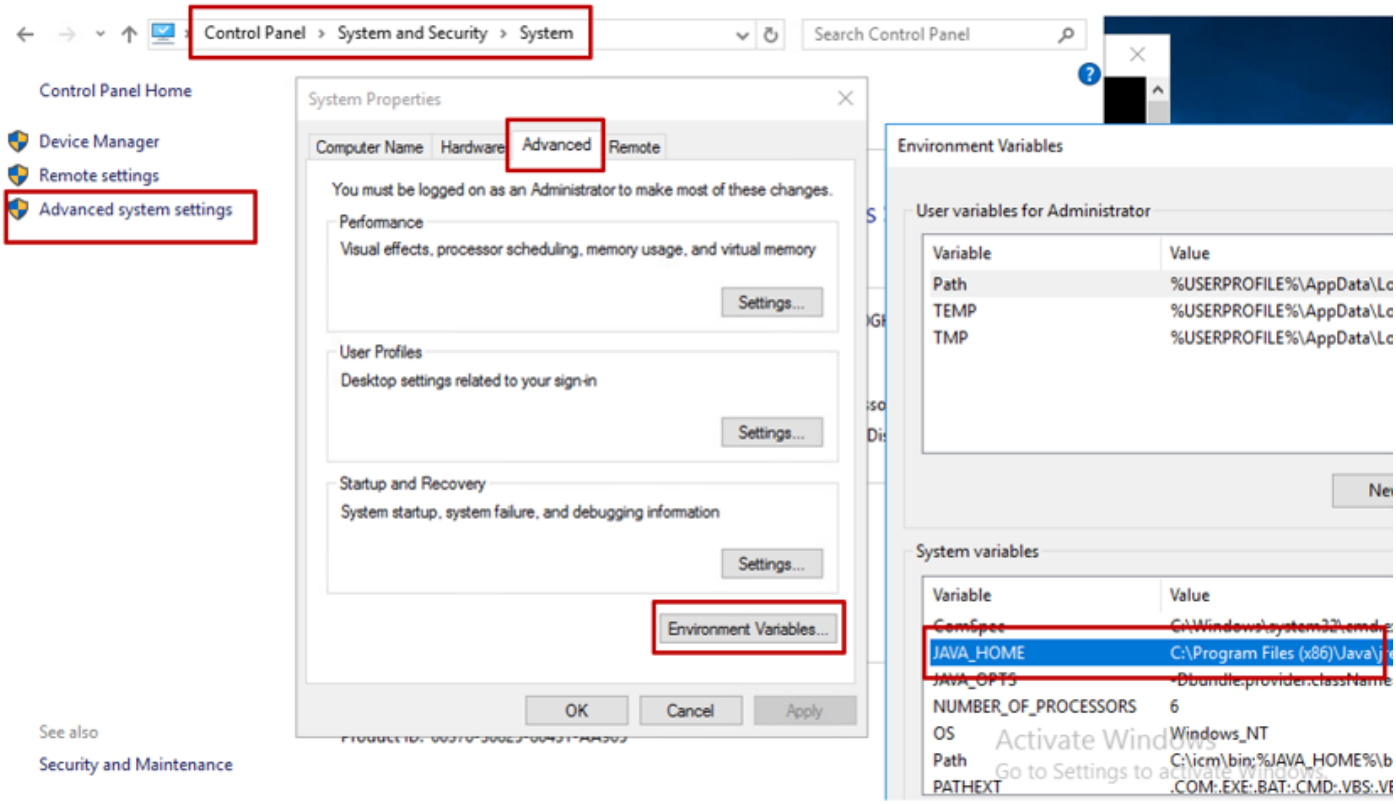
⚠ 注意：作業を開始する前に、キーストアをバックアップし、管理者としてJavaホームからコマンドを実行する必要があります。

ステップ1:Javaキーツールがホストされている場所を確認するためにJavaホームパスを知ります。Javaホームパスを見つける方法はいくつかあります。

オプション1:CLIコマンド：echo %JAVA_HOME%



オプション2：図に示すように、高度なシステム設定を使用して手動で



注:UCCE 12.5のデフォルトパスはC:\Program Files (x86)\Java\jre1.8.0_221\binです。ただし、12.5(1a)インストーラを使用しているか、12.5 ES55（必須のOpenJDK ES）がインストールされている場合は、データストアのパスがOpenJDKによって変更されているため、JAVA_HOMEではなくCCE_JAVA_HOMEを使用してください。CCEおよびCVPでのOpenJDKの移行についての詳細は、CCE 2.5(1)でのOpenJDKのインストールと移行、およびCVP 12.5(1)でのOpenJDKのインストールと移行を参照してください。

ステップ 2：C:\Program Files (x86)\Java\jre1.8.0_221\lib\securityフォルダからcacertsファイルをバックアップします。 別の場所にコピーできます。

ステップ 3：Administratorとしてコマンドウィンドウを開き、コマンドを実行します。

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

注：必要な特定の証明書は、証明書の署名に使用するCAによって異なります。パブリックCAの一般的な2層CAでは、内部CAよりもセキュリティが高いため、ルート証明書と中間証明書の両方をインポートする必要があります。中間証明書がないスタンドアロンCA（通常はラボまたはよりシンプルな内部CAで見られる）では、ルート証明書をインポートするだけで済みます。

CVPソリューション

1. FQDNを使用した証明書の生成

この手順では、Web Service Manager(WSM)、Voice XML(VXML)、Call Server and Operations Management(OAMP)サービスのFQDNを使用して証明書を生成する方法について説明します。

注:CVPをインストールする場合、証明書名にはサーバの名前のみが含まれ、FQDNは含まれないため、証明書を再生成する必要があります。

注意：作業を開始する前に、次の操作を行う必要があります。
1.キーストアパスワードを取得します。more %CVP_HOME%\conf\security.propertiesコマンドを実行します。このパスワードは、keytoolコマンドを実行するときに必要です。
2. %CVP_HOME%\conf\securityフォルダを別のフォルダにコピーします。
3.コマンドウィンドウを管理者として開き、コマンドを実行します。

CVPサーバ

ステップ 1：CVPサーバの証明書を削除するには、次のコマンドを実行します。

```
%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
```

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 2：WSM証明書を生成するには、次のコマンドを実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

注：デフォルトでは、証明書は2年間生成されます。-validity XXXXを使用して、証明書が再生成される有効期限を設定します。そうでない場合、証明書は90日間有効であり、この時間の前にCAによって署名される必要があります。これらの証明書のほとんどでは、3 ~ 5年は妥当な検証期間である必要があります。

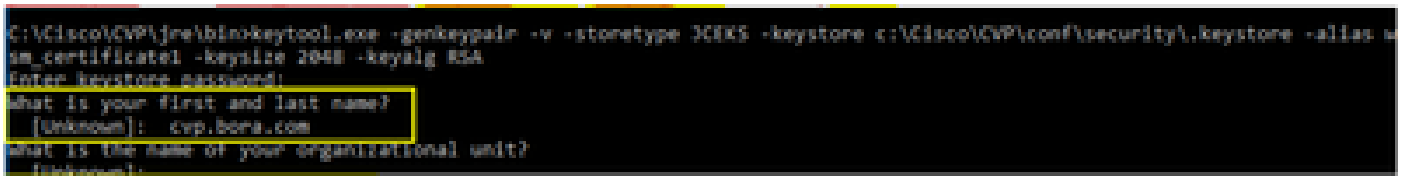
標準的な有効性の入力を次に示します。

1年	365

2年	730
三年	1095
4年	1460
五年	1895
十年	3650

⚠ 注意:12.5の証明書はSHA 256、キーサイズ2048、および暗号化アルゴリズムRSAである必要があります。次のパラメータを使用して、これらの値を設定します。-keyalg RSAおよび– keysize 2048。CVPキーストアコマンドには – storetype JCEKSパラメータを含めることが重要です。これを行わないと、証明書、キー、またはキーストアが破損する可能性があります。

質問に対して、サーバのFQDNを指定します。最初と最後の名前は何ですか。



次の質問に答えてください。

組織ユニットの名前は何ですか。

[不明]: <OUを指定>

組織の名前は何ですか。

[不明]: <組織名を指定>

市区町村の名前は何ですか。

[不明]: <都市/地域の名前を指定>

都道府県の名前は何ですか。

[不明]: <都道府県の名前を指定>

このユニットの2文字の国番号は何ですか。

[不明]: <2文字の国番号を指定>

次の2つの入力にyesを指定します。

ステップ 3：vxml_certificateとcallserver_certificateに対して同じ手順を実行します。

```
%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 レポート サーバ

ステップ 1：WSMとReporting Serverの証明書を削除するには、次のコマンドを実行します。

```
%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
```

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 2：WSM証明書を生成するには、次のコマンドを実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

クエリのサーバのFQDNとして名と姓を指定し、CVPサーバで行った手順と同じ手順を続行します。

ステップ 3：callserver_certificateに対して同じ手順を実行します。

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

CVP OAMP（UCCE導入）

PCCEソリューションバージョン12.xでは、ソリューションのすべてのコンポーネントがSPOGによって制御され、OAMPがインストールされていないため、これらの手順が必要になるのはUCCE導入ソリューションだけです。

ステップ 1：WSMとOAMPサーバの証明書を削除するには、次のコマンドを実行します。

```
%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
```

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 2：WSM証明書を生成するには、次のコマンドを実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

クエリのサーバのFQDNとして名と姓を指定し、CVPサーバで行った手順と同じ手順を続行します。

ステップ 3：oamp_certificateに対して同じ手順を実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

2. CSRの生成

注:RFC5280準拠のブラウザでは、各証明書にサブジェクトの別名(SAN)が含まれている必要があります。これは、CSRの生成時にSANで – extパラメータを使用して実行できます。

サブジェクト代替名

-extパラメータを使用すると、ユーザは特定の拡張子を指定できます。この例では、サーバの完全修飾ドメイン名(FQDN)とlocalhostを使用して、サブジェクト代替名(SAN)を追加します。追加のSANフィールドは、カンマ区切り値として追加できます。

有効なSANタイプは次のとおりです。

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

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

CVPサーバ

ステップ 1：エイリアスの証明書要求を生成します。次のコマンドを実行し、ファイル（wsm_certificateなど）に保存します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 2：vxml_certificateとcallserver_certificateに対して同じ手順を実行します。

```
%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 -
```

プロンプトが表示されたら、キーストアのパスワードを入力します。

CVP レポート サーバ

ステップ 1：エイリアスの証明書要求を生成します。次のコマンドを実行し、ファイル（wsmreport_certificateなど）に保存します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 2：callserver_certificateに対して同じ手順を実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

CVP OAMP（UCCE導入）

ステップ 1：エイリアスの証明書要求を生成します。次のコマンドを実行し、ファイル（oamp_certificateなど）に保存します。

```
%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.
```

ステップ 2：oamp_certificateに対して同じ手順を実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。

3. CA署名付き証明書の取得

ステップ 1：CA上の証明書に署名します（CVPサーバの場合はWSM、CallserverおよびVXMLサーバ、CVP OAMPサーバの場合はWSMおよびOAMP、レポートサーバの場合はWSMおよびCallserver）。

ステップ 2：CA認証局からアプリケーション証明書とルート証明書をダウンロードします。

ステップ 3：ルート証明書とCA署名付き証明書を各サーバのフォルダ%CVP_HOME%\conf\security\にコピーします。

4. CA署名付き証明書のインポート

これらの手順をCVPソリューションのすべてのサーバに適用します。 CA署名付き証明書をインポートする必要があるのは、そのサーバ上のコンポーネントの証明書だけです。

ステップ 1：ルート証明書をインポートします。次のコマンドを実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロンプトで、Yesと入力します。

中間証明書がある場合は、次のコマンドを実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロンプトで、Yesと入力します。

ステップ 2：そのサーバ証明書用のCA署名付きWSMをインポートします（CVP、Reporting、およびOAMP）。次のコマンドを実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロンプトで、Yesと入力します。

ステップ 3：CVPサーバとレポートサーバで、Callserver CA署名付き証明書をインポートします。次のコマンドを実行します。

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

プロンプトが表示されたら、キーストアのパスワードを入力します。Trust this certificateプロンプトで、Yesと入力します。

ステップ 4：CVPサーバで、VXMLサーバのCA署名付き証明書をインポートします。次のコマンドを実行します。

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

ステップ 5：CVP OAMPサーバ（UCCEのみ）で、OAMPサーバCA署名付き証明書をインポートします。次のコマンドを実行します。

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

手順 6：サーバをリブートします。

注:UCCEの導入では、CSRの生成時に指定したFQDNを使用して、CVP OAMP内のサーバ（Reporting、CVP Serverなど）を追加してください。

VOSサーバ

1. CSR証明書の生成

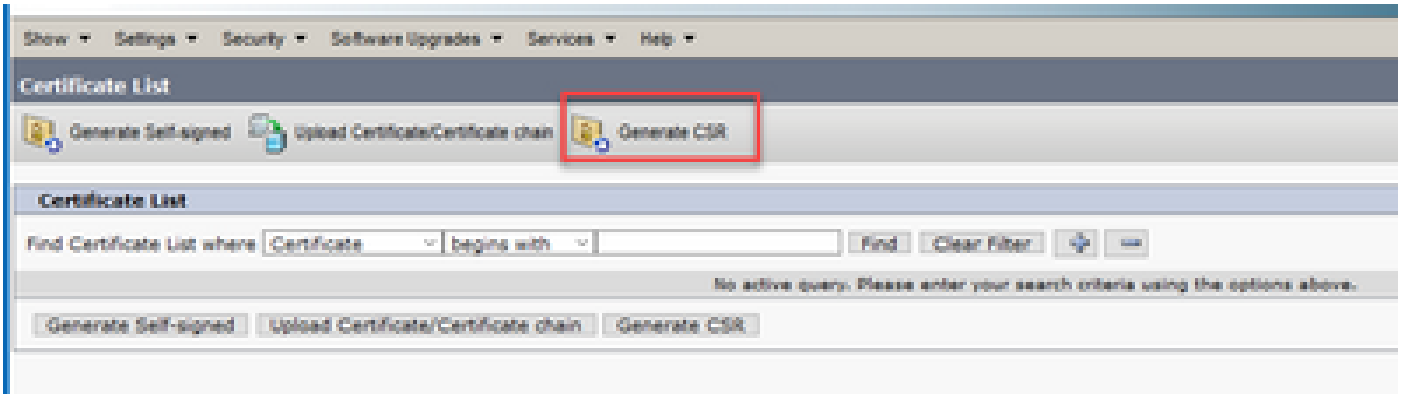
この手順では、Cisco Voice Operating System(VOS)ベースのプラットフォームからTomcat

CSR証明書を生成する方法について説明します。このプロセスは、次のようなすべてのVOSベースのアプリケーションに適用されます。

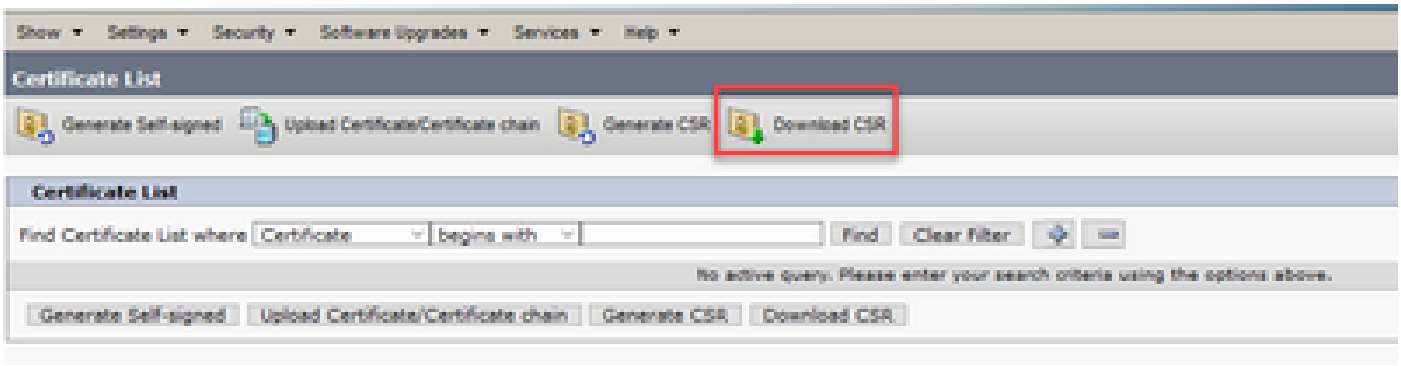
- CUCM
- Finesse
- CUIC \ライブデータ(LD) \アイデンティティサーバ(IDS)
- Cloud Connect
- Cisco VVB

ステップ 1：Cisco Unified Communications Operating System Administrationページ(https://FQDN:<8443または443>/cmplatform)に移動します。

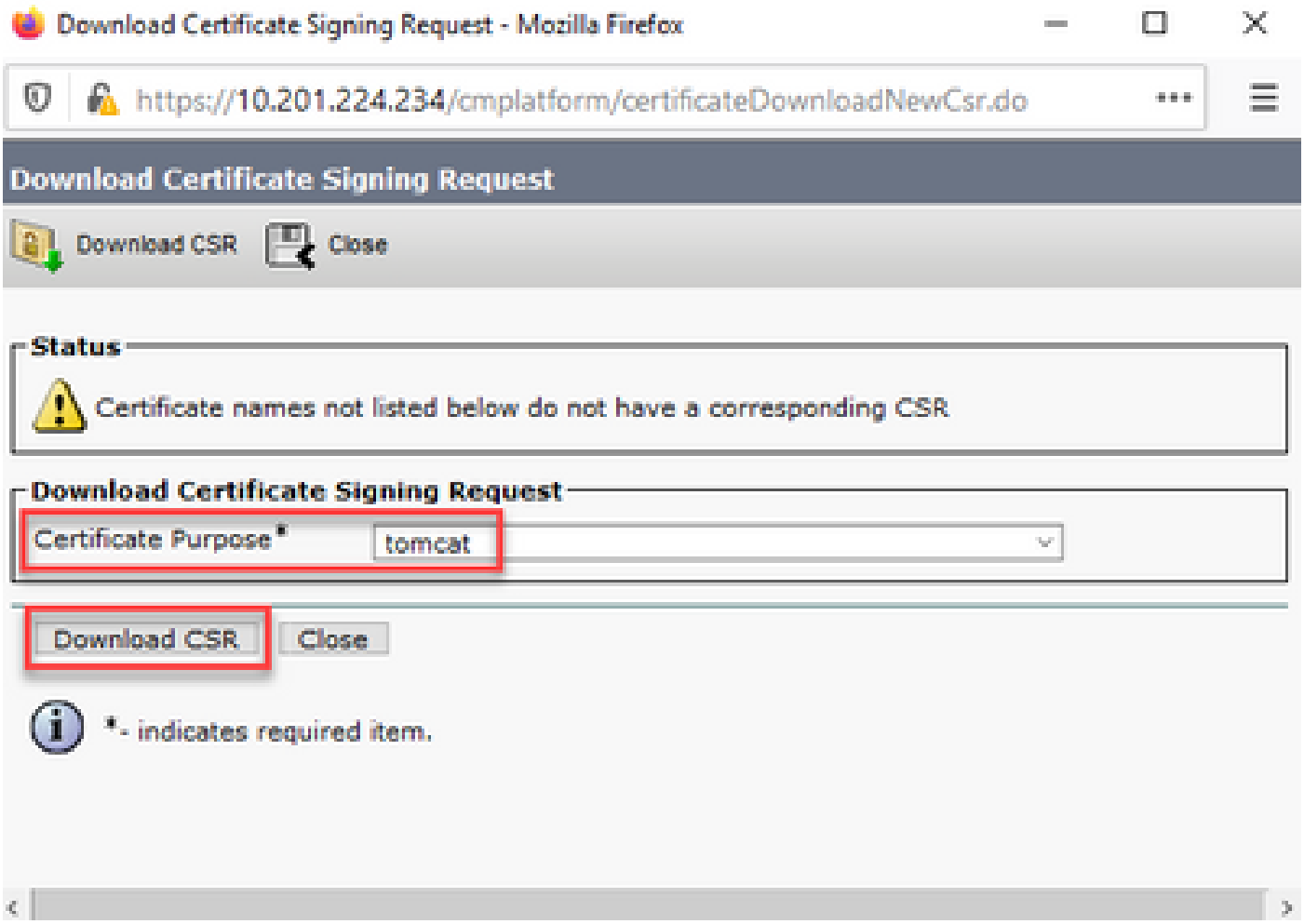
ステップ 2：Security > Certificate Managementの順に移動し、Generate CSRを選択します。



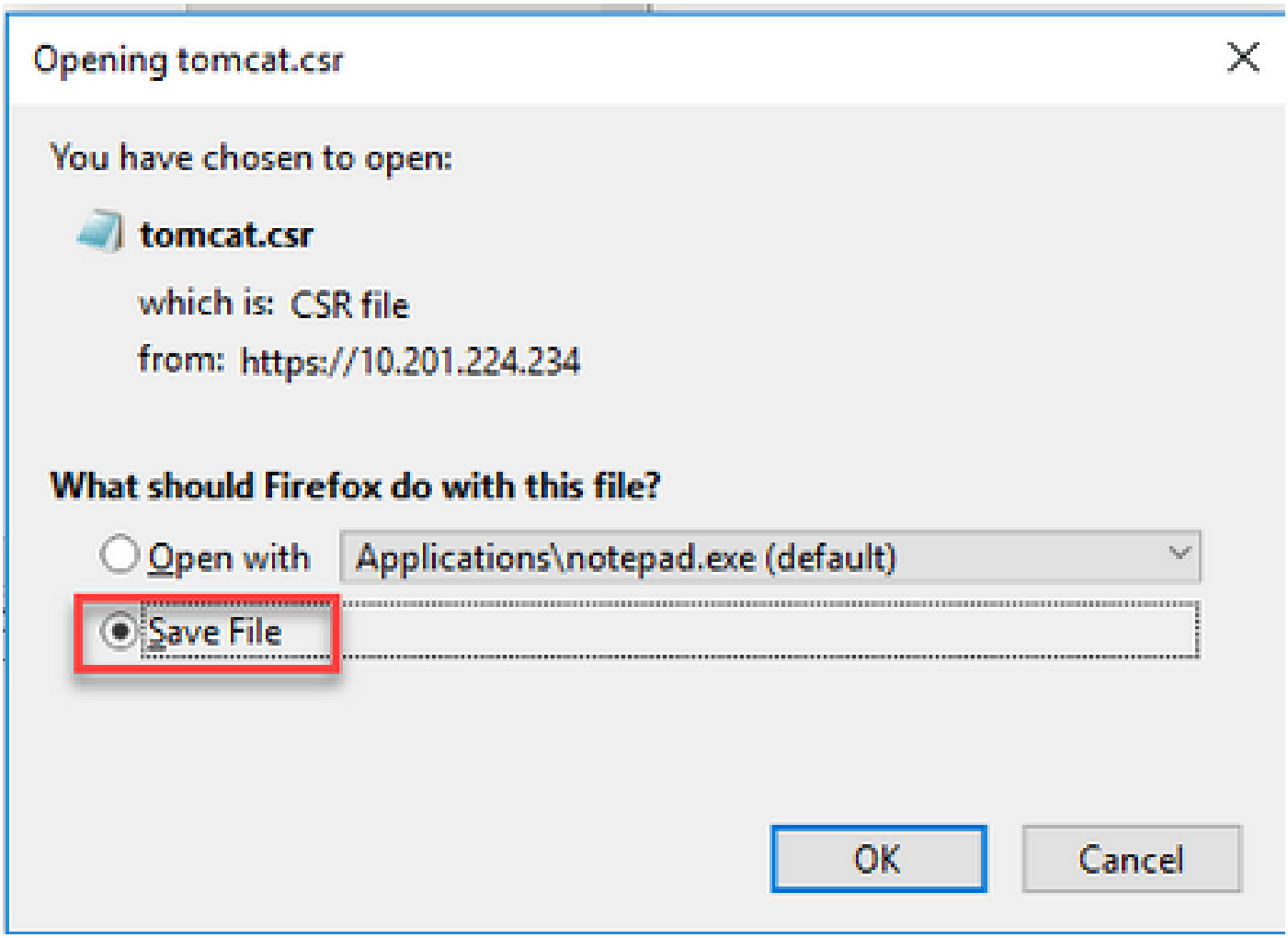
ステップ 3：CSR証明書が生成されたら、ウィンドウを閉じてDownload CSRを選択します。



ステップ 4：証明書の目的がtomcatであることを確認し、Download CSRをクリックします。



ステップ 5：Save Fileをクリックします。ファイルはDownloadフォルダに保存されます。



2. CA署名付き証明書の取得

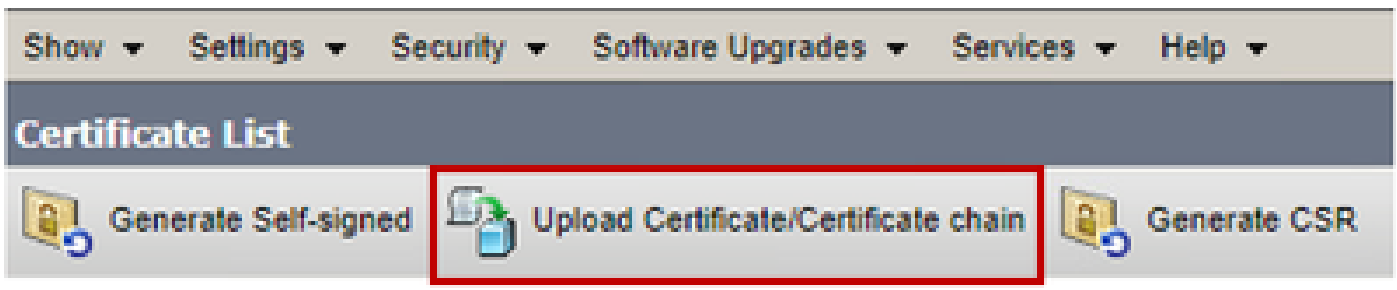
ステップ 1：CAにエクスポートされたtomcat証明書に署名します。

ステップ 2：CA認証局から認証されたアプリケーションとルートをダウンロードします。

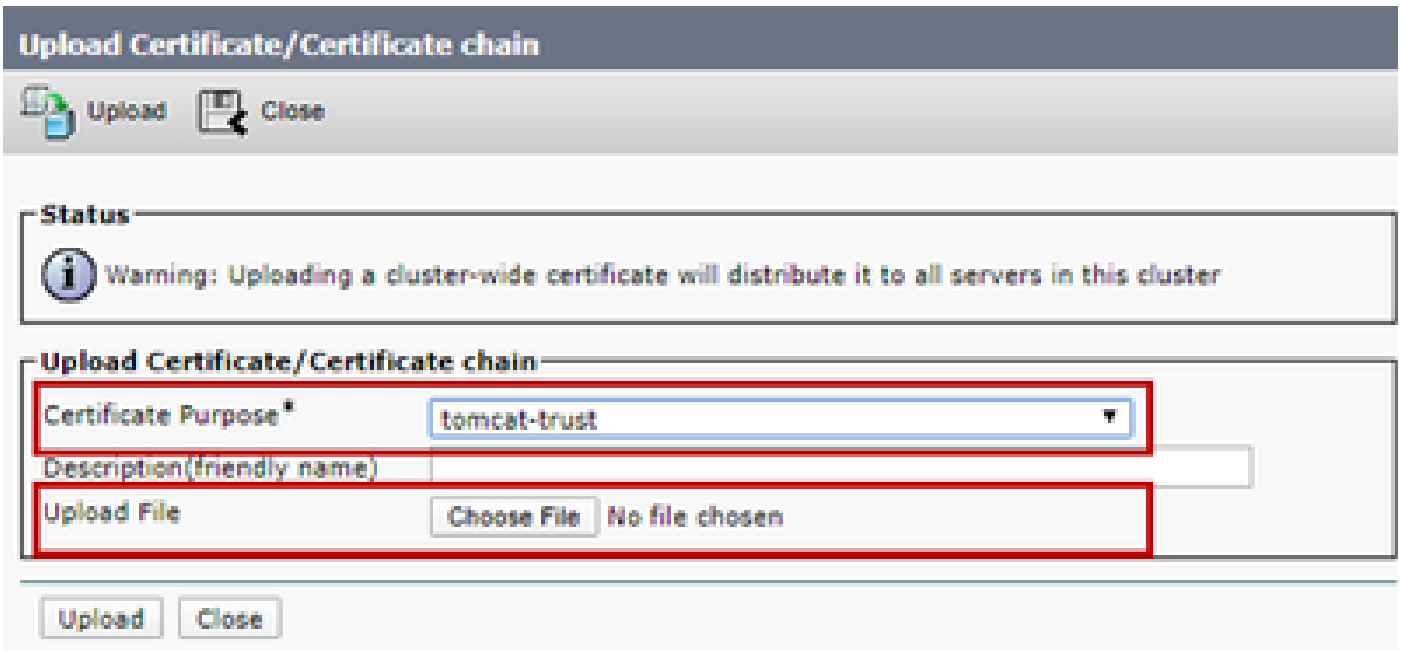
3.アプリケーション証明書とルート証明書のアップロード

ステップ 1：Cisco Unified Communications Operating System Administrationページ (https://FQDN:<8443または443>/cmplatform)に移動します。

ステップ 2：Security > Certificate Managementの順に移動し、Upload Certificate/Certificate chainを選択します。

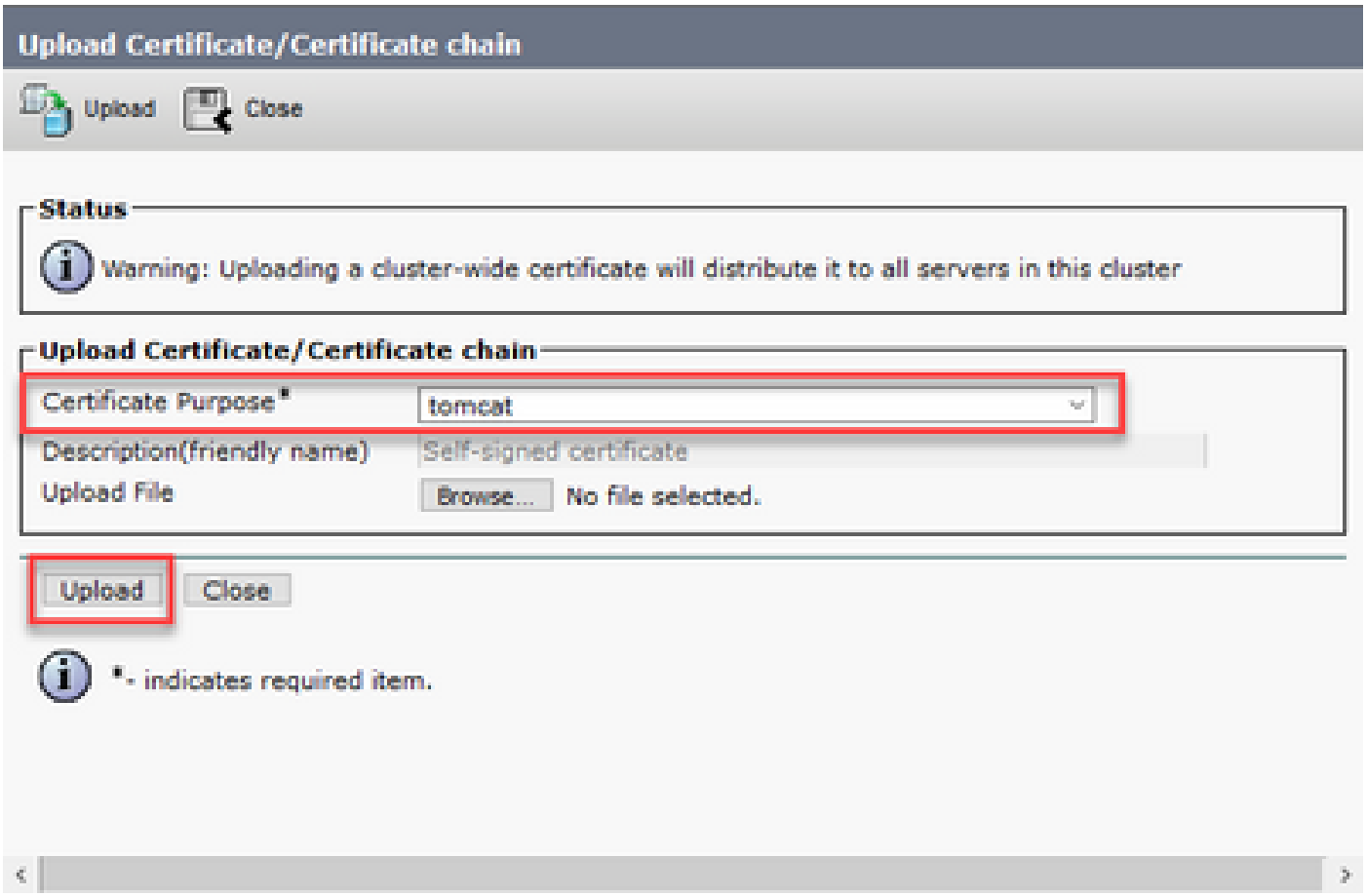


ステップ 3：Upload certificate/Certificate chainウィンドウのcertificate purposeフィールドで tomcat-trustを選択し、ルート証明書をアップロードします。



ステップ 4：中間証明書（存在する場合）をtomcat-trustとしてアップロードします。

ステップ 5：Upload certificate/Certificate chainウィンドウで、Certificate Purposeフィールドで now tomcatを選択し、アプリケーションCA署名付き証明書をアップロードします。



手順 6：サーバをリブートすると、

確認

サーバをリブートした後、次の手順を実行してCA署名付き実装を確認します。

ステップ 1：Webブラウザを開き、キャッシュをクリアします。

ステップ 2：ブラウザを閉じて、もう一度開きます。

ここで、CA署名付き証明書を開始するための証明書スイッチが表示され、証明書が自己署名であるため信頼できないことを示すメッセージがブラウザウィンドウに表示されなくなります。

トラブルシュート

このガイドには、CA署名付き証明書の実装をトラブルシューティングする手順はありません。

関連情報

- CVP設定ガイド：CVP設定ガイド – セキュリティ
- UCCEコンフィギュレーションガイド：UCCEコンフィギュレーションガイド – セキュリティ
- PCCEアドミニストレーションガイド：PCEアドミニストレーションガイド – セキュリティ

- UCCE自己署名証明書：Exchange UCCE自己署名証明書
- PCCE自己署名証明書：Exchange PCCE自己署名証明書
- CCE 12.5(1)でのOpenJDKのインストールと移行：CCE OpenJDKの移行
- CVP 12.5(1)でのOpenJDKのインストールと移行：CVP OpenJDKの移行

テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。