

CCE 솔루션에서 CA 서명 인증서 구현

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경](#)

[절차](#)

[CCE Windows 기반 서버](#)

[1. CSR 생성](#)

[2. CA 서명 인증서 얻기](#)

[3. CA 서명 인증서 업로드](#)

[4. CA 서명 인증서를 IIS에 바인딩합니다](#)

[5. CA 서명 인증서를 진단 포트에 바인딩합니다](#)

[6. 루트 및 중간 인증서를 Java 키 저장소로 가져옵니다.](#)

[CVP 솔루션](#)

[1. FQDN을 사용하여 인증서 생성](#)

[2. CSR 생성](#)

[3. CA 서명 인증서 얻기](#)

[4. CA 서명 인증서 가져오기](#)

[VOS 서버](#)

[1. CSR 인증서 생성](#)

[2. CA 서명 인증서 얻기](#)

[3. 애플리케이션 및 루트 인증서 업로드](#)

[다음은 확인합니다.](#)

[문제 해결](#)

[관련정보](#)

소개

이 문서에서는 Cisco CCE(Contact Center Enterprise) 솔루션에서 CA(Certificate Authority) 서명 인증서를 구현하는 방법에 대해 설명합니다.

기고자: Anuj Bhatia, Robert Rogier, Ramiro Amaya, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Unified Contact Center Enterprise(UCCE) 릴리스 12.5(1)
- Package Contact Center Enterprise 릴리스 12.5(1)

- CVP(Customer Voice Portal) 릴리스 12.5(1)
- Cisco VVB(Virtualized Voice Browser)
- Cisco CVP OAMP(Operations and Administration Console)
- Cisco CUIC(Unified Intelligence Center)
- CUCM(Cisco Unified Communication Manager)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- Finesss 12.5
- CUIC 12.5
- Windows 2016

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경

인증서는 클라이언트와 서버 간 인증과 통신이 안전하게 이루어지도록 하는 데 사용됩니다.

사용자는 CA에서 인증서를 구매하거나 자체 서명 인증서를 사용할 수 있습니다.

자체 서명 인증서(이름에서 알 수 있듯이)는 ID를 인증하는 엔티티와 동일한 엔티티에서 서명되며, 인증 기관에서 서명하지 않습니다. 자체 서명 인증서는 CA 인증서만큼 안전하지 않은 것으로 간주되지만, 기본적으로 많은 애플리케이션에서 사용됩니다.

PCCE(Package Contact Center Enterprise) 솔루션 버전 12.x에서는 솔루션의 모든 구성 요소가 SPOG(Single Pane of Glass)에 의해 제어되며, SPOG는 AW(Principal Admin Workstation) 서버에서 호스팅됩니다.

PCCE 12.5(1) 버전의 SRC(Security Management Compliance)로 인해 SPOG와 솔루션의 다른 구성 요소 간의 모든 통신은 보안 HTTP 프로토콜을 통해 수행됩니다. UCCE 12.5에서는 구성 요소 간의 통신도 보안 HTTP 프로토콜을 통해 이루어집니다.

이 문서에서는 보안 HTTP 통신을 위해 CCE 솔루션에서 CA 서명 인증서를 구현하는 데 필요한 단계에 대해 자세히 설명합니다. 기타 UCCE 보안 고려 사항은 UCCE [보안 지침을 참조하십시오](#). 보안 HTTP와 다른 추가 CVP 보안 통신에 대해서는 CVP 컨피그레이션 가이드: CVP 보안 지침의 보안 [지침을 참조하십시오](#).

절차

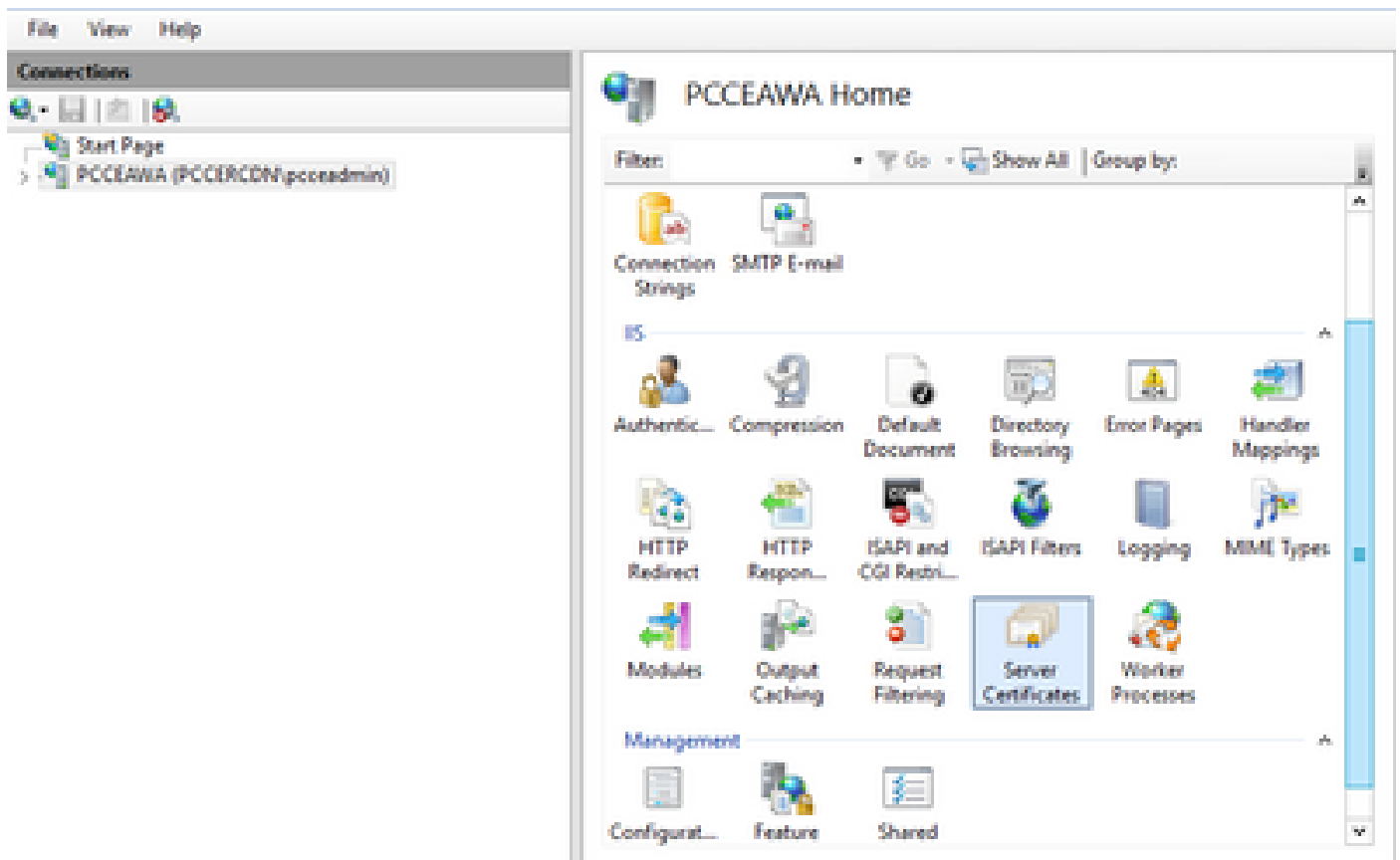
CCE Windows 기반 서버

1. CSR 생성

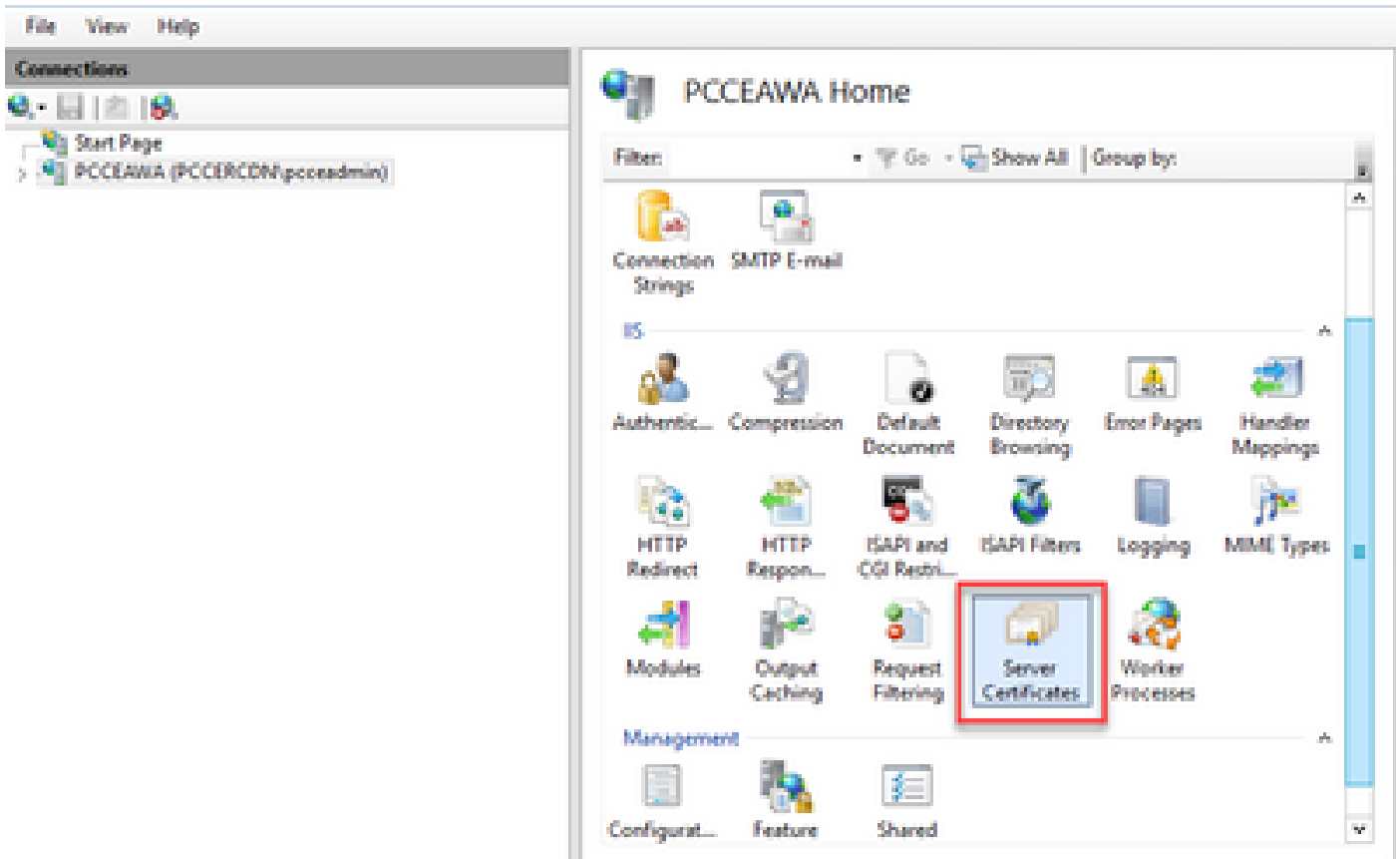
이 절차에서는 IIS(인터넷 정보 서비스) 관리자에서 CSR(인증서 서명 요청)을 생성하는 방법에 대해 설명합니다.

1단계. Windows에 로그인하고 제어판 > 관리 도구 > 인터넷 정보 서비스(IIS) 관리자를 선택합니다.

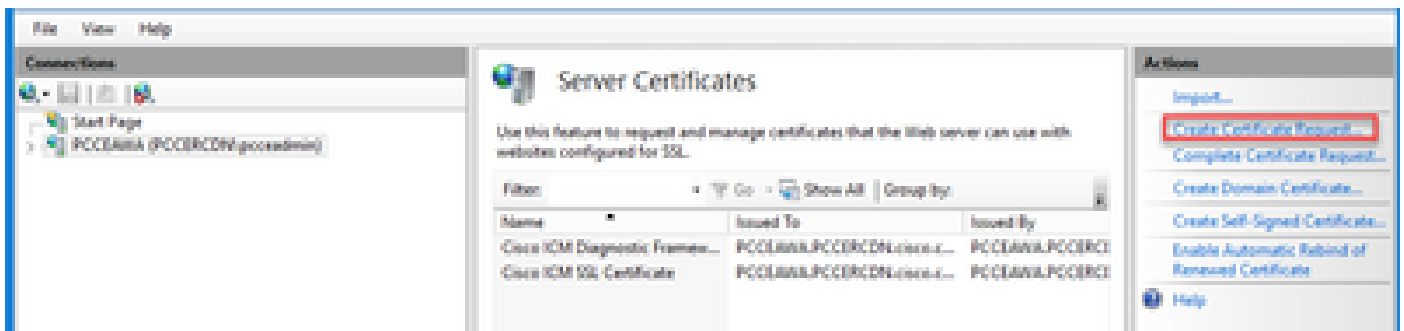
2단계. Connections 창에서 서버 이름을 클릭합니다. Server Home 창이 나타납니다.



3단계. IIS 영역에서 Server Certificates를 두 번 클릭합니다.



4단계. Actions(작업) 창에서 Create Certificate Request(인증서 요청 생성)를 클릭합니다.



5단계. Request Certificate 대화 상자에서 다음을 수행합니다.

표시된 필드에 필수 정보를 지정하고 다음을 클릭합니다.

Request Certificate

Distinguished Name Properties

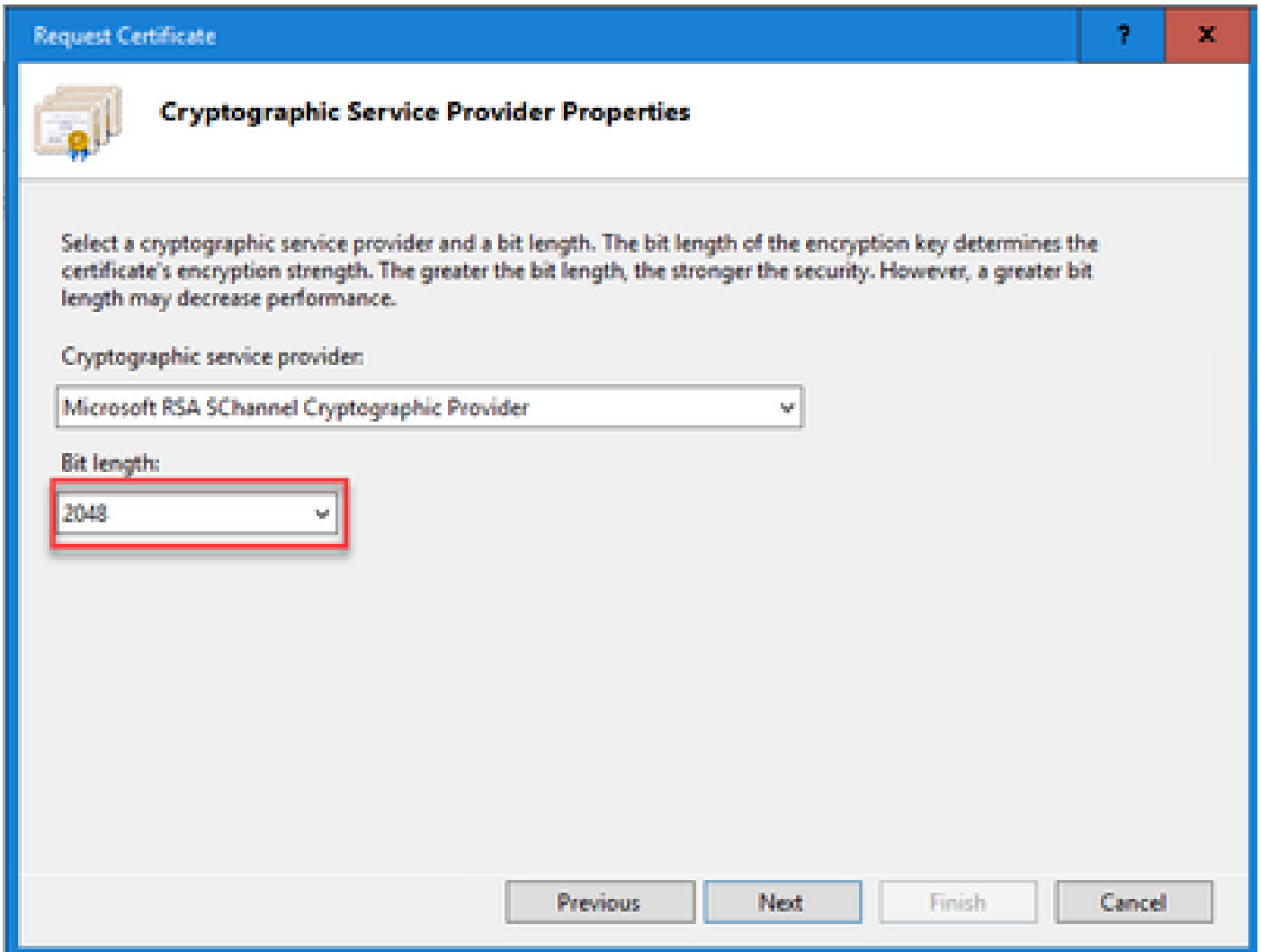
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

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"/>

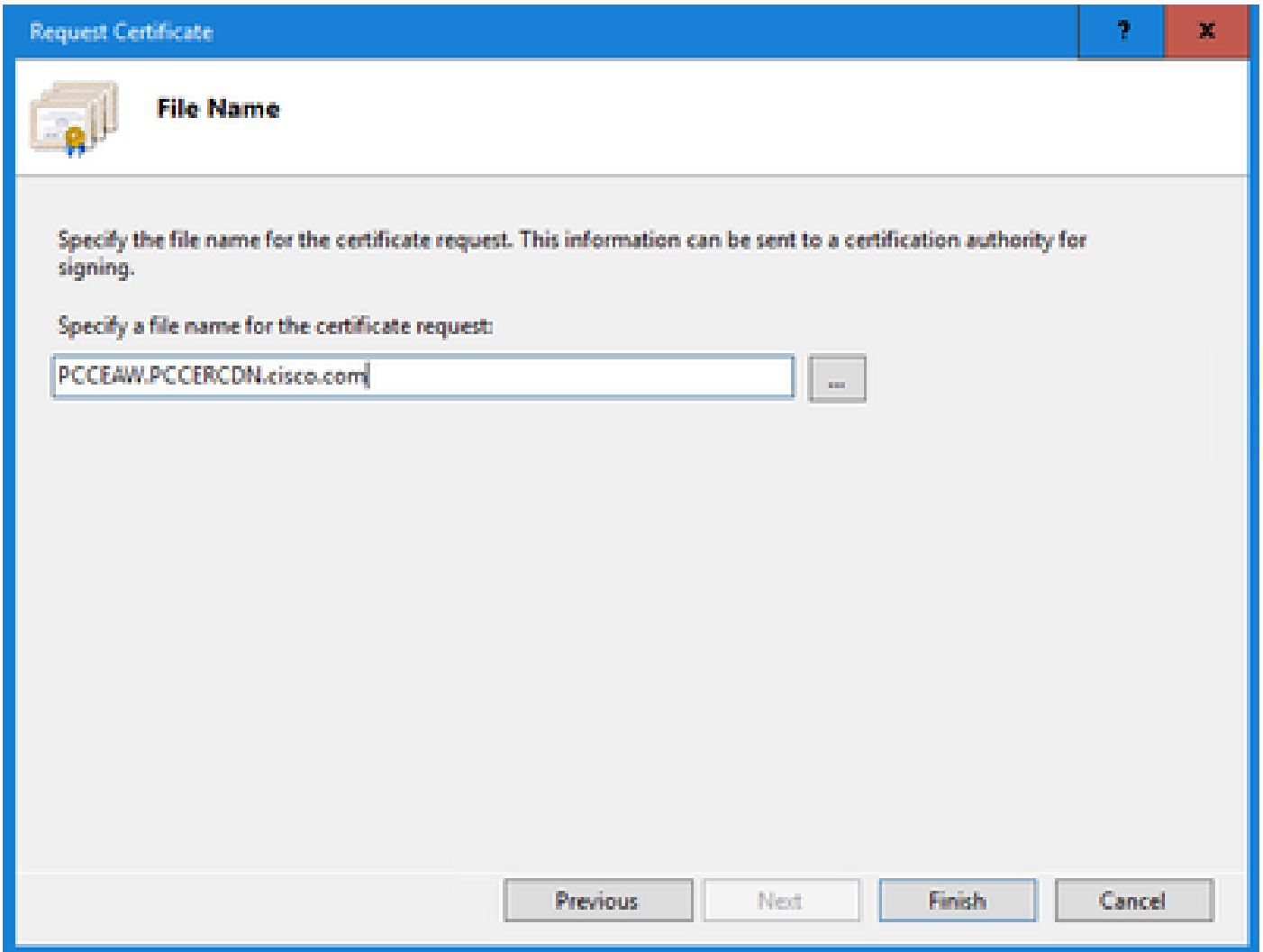
Previous Next Finish Cancel

Cryptographic service provider(암호화 서비스 공급자) 드롭다운 목록에서 기본 설정을 유지합니다.

Bit length(비트 길이) 드롭다운 목록에서 2048을 선택합니다.




6단계. 인증서 요청에 대한 파일 이름을 지정하고 Finish(마침)를 클릭합니다.



2. CA 서명 인증서 얻기

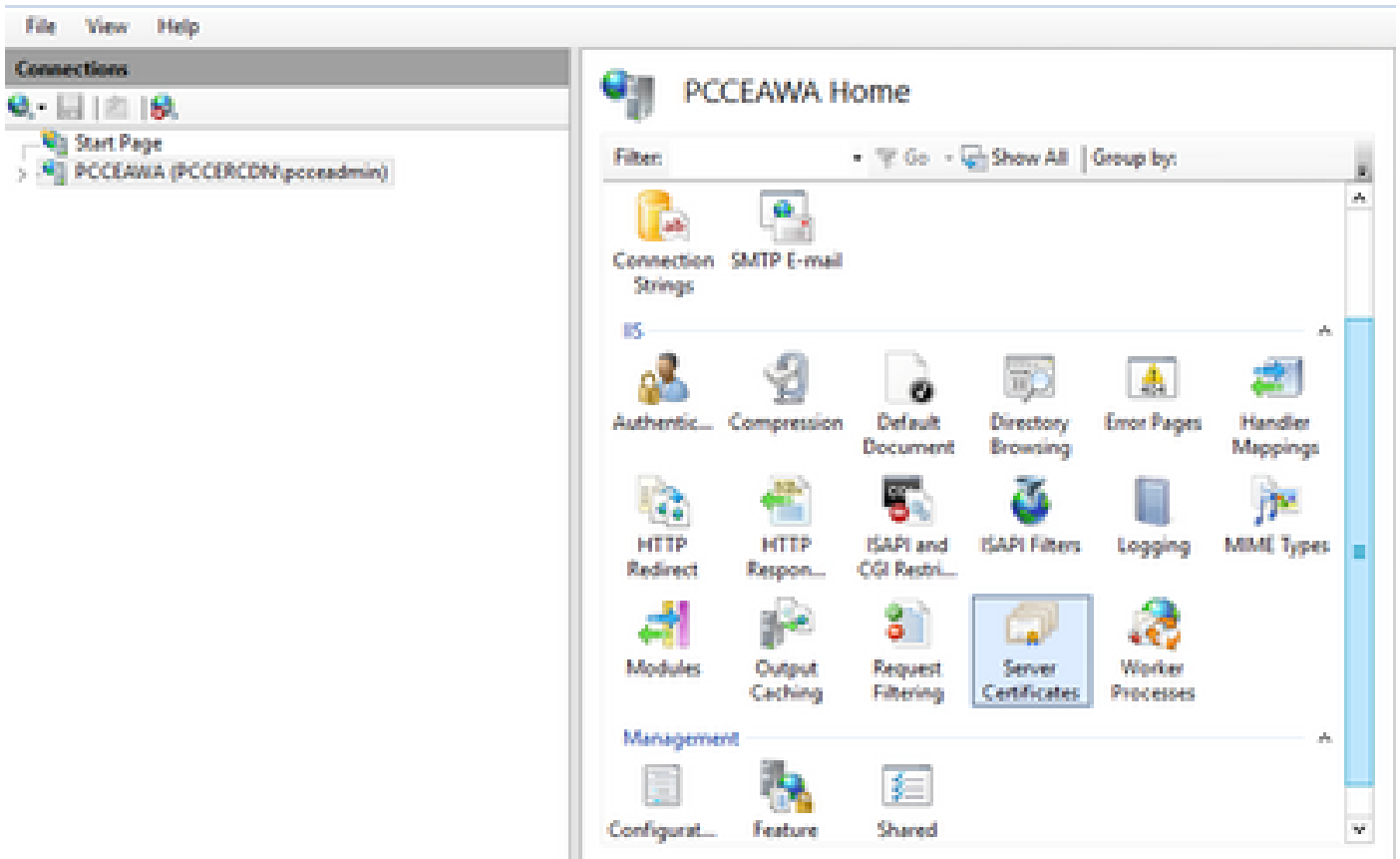
1단계. CA에서 인증서를 서명합니다.

 참고: CA에서 사용하는 인증서 템플릿에 클라이언트 및 서버 인증이 포함되어 있는지 확인하십시오.

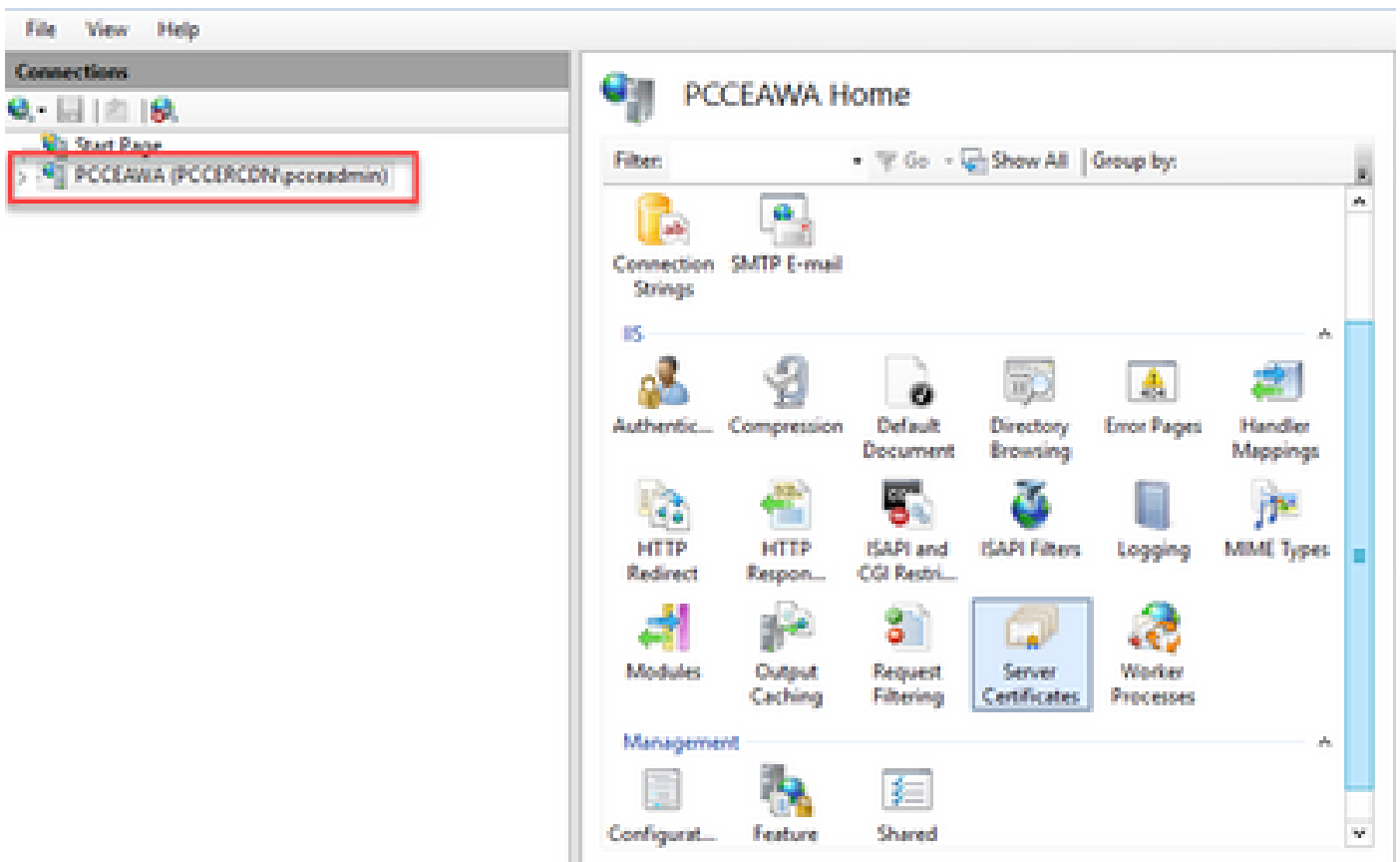
2단계. 인증 기관(루트, 애플리케이션 및 중간(있는 경우))에서 CA 서명 인증서를 가져옵니다.

3. CA 서명 인증서 업로드

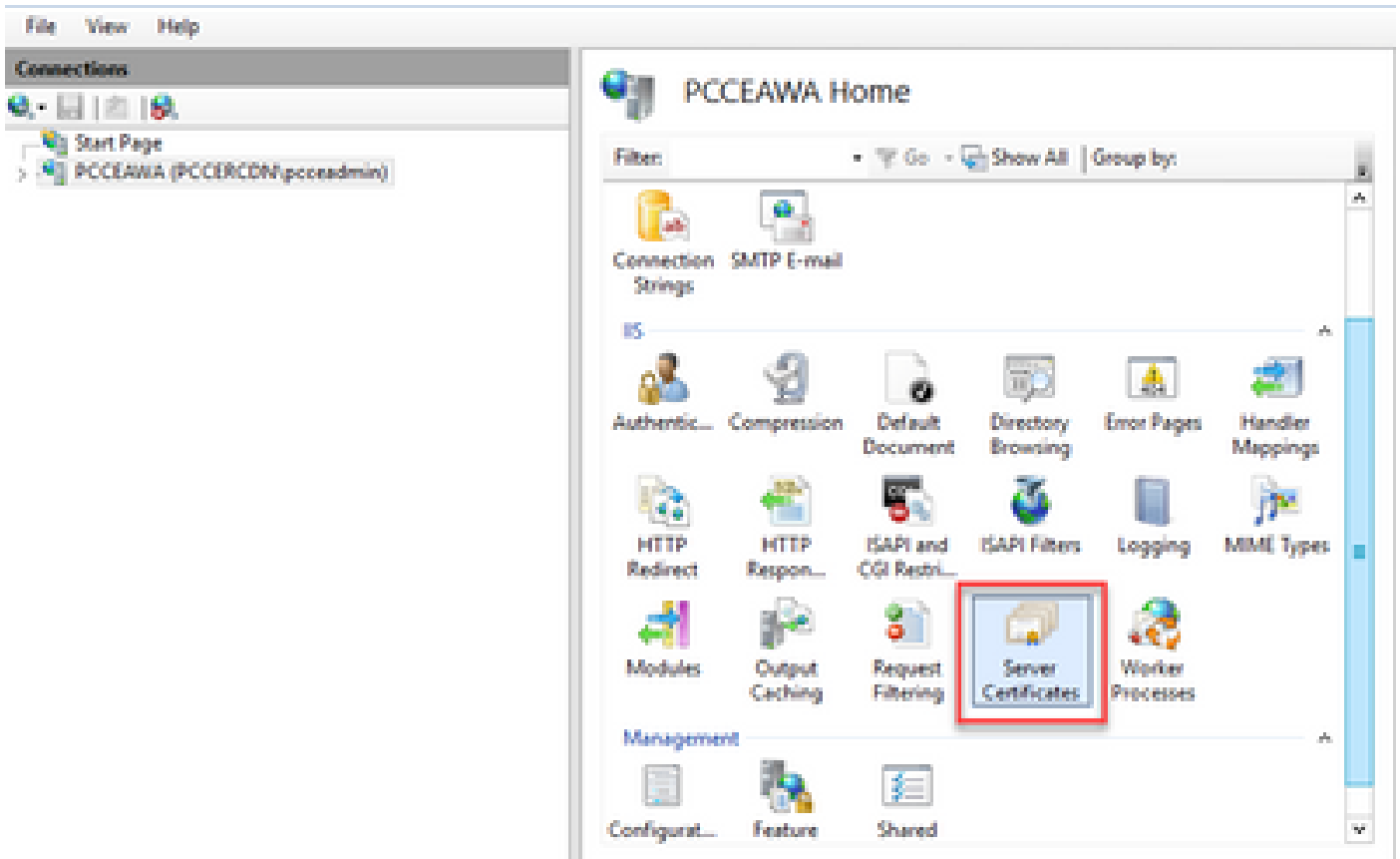
1단계. Windows에 로그인하고 제어판 > 관리 도구 > 인터넷 정보 서비스(IIS) 관리자를 선택합니다.



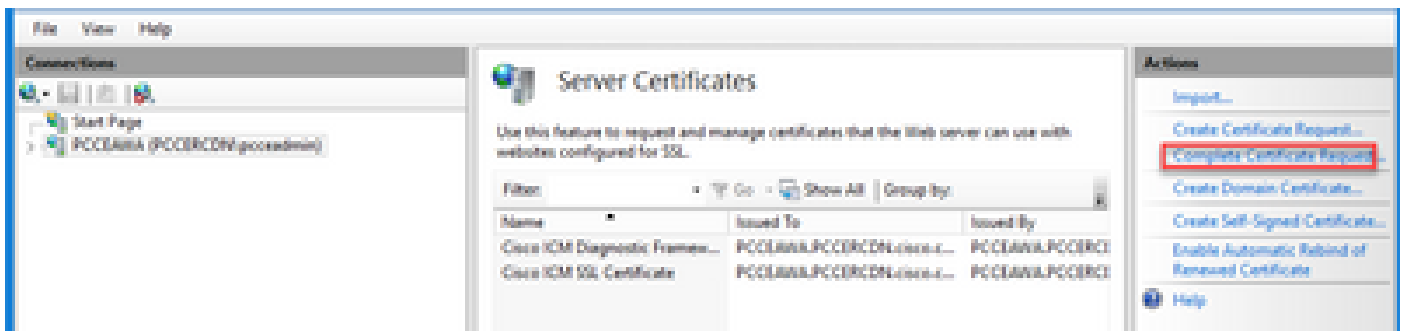
2단계. Connections 창에서 서버 이름을 클릭합니다.



3단계. IIS 영역에서 서버 인증서를 두 번 클릭합니다.




4단계. Actions(작업) 창에서 Complete Certificate Request(인증서 요청 완료)를 클릭합니다.



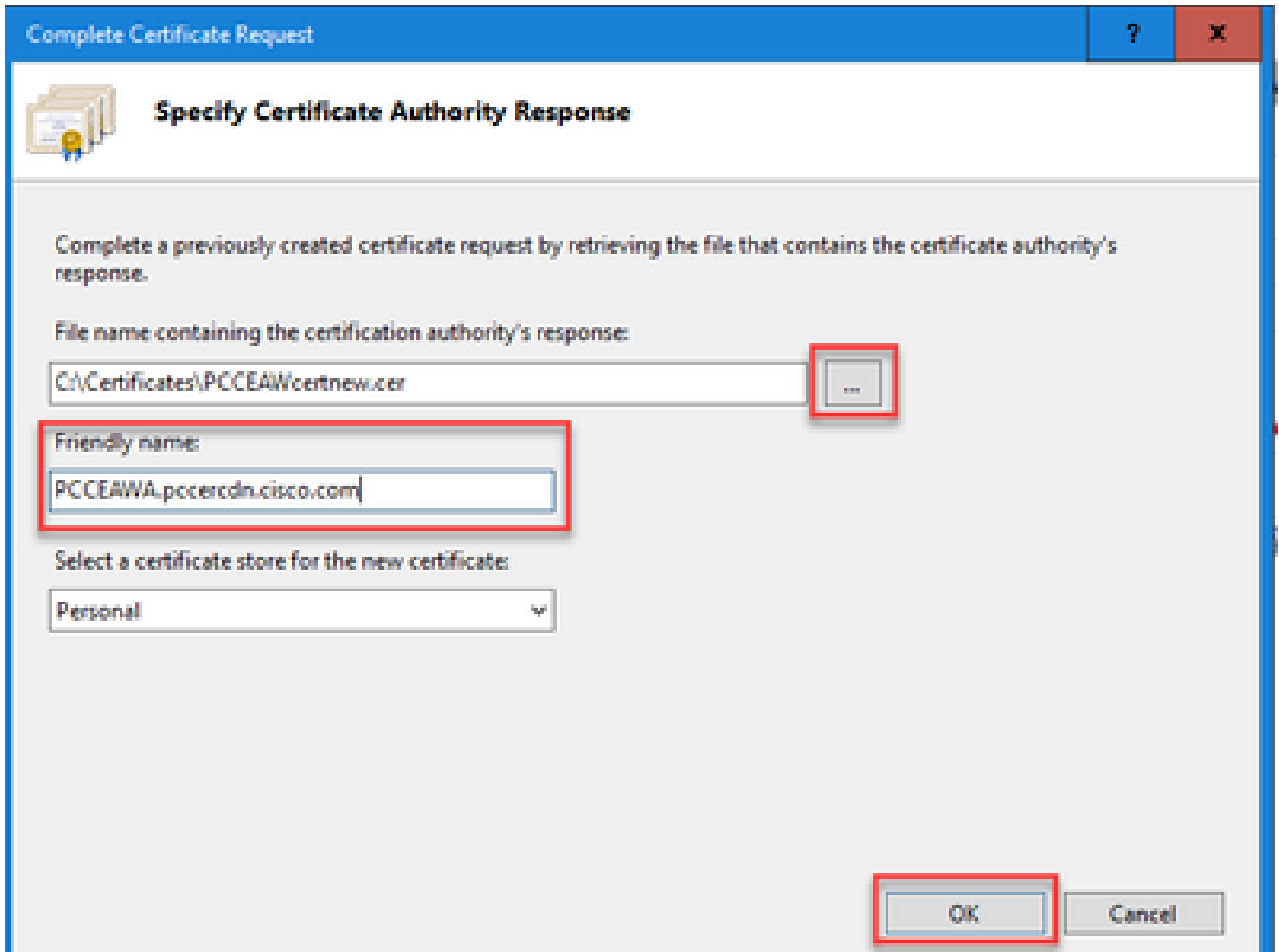
5단계. 인증서 요청 완료 대화 상자에서 다음 필드를 완료합니다.

인증 기관 응답 필드가 포함된 파일 이름에서 ... 버튼을 클릭합니다.

서명된 애플리케이션 인증서가 저장된 위치를 찾은 다음 Open(열기)을 클릭합니다.

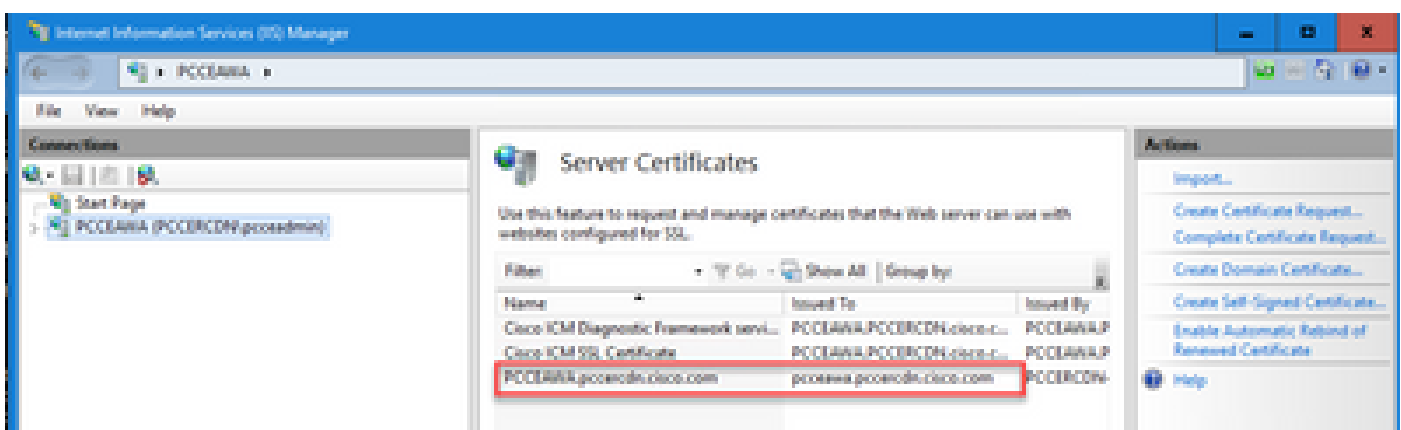
 참고: 2-tier CA 구현이고 루트 인증서가 서버 인증서 저장소에 없으면 서명된 인증서를 가져 오기 전에 루트를 Windows 저장소에 업로드해야 합니다. 루트 CA를 Windows 스토어 <https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate>에 업로드해야 하는 경우 이 문서를 [참조하십시오](#).

Friendly name(친숙한 이름) 필드에 서버의 FQDN(Fully Qualified Domain Name) 또는 중요한 이름을 입력합니다. Select a certificate store for the new certificate(새 인증서에 대한 인증서 저장소 선택) 드롭다운이 Personal(개인)으로 유지되는지 확인합니다.



6단계. 인증서를 업로드하려면 OK를 클릭합니다.

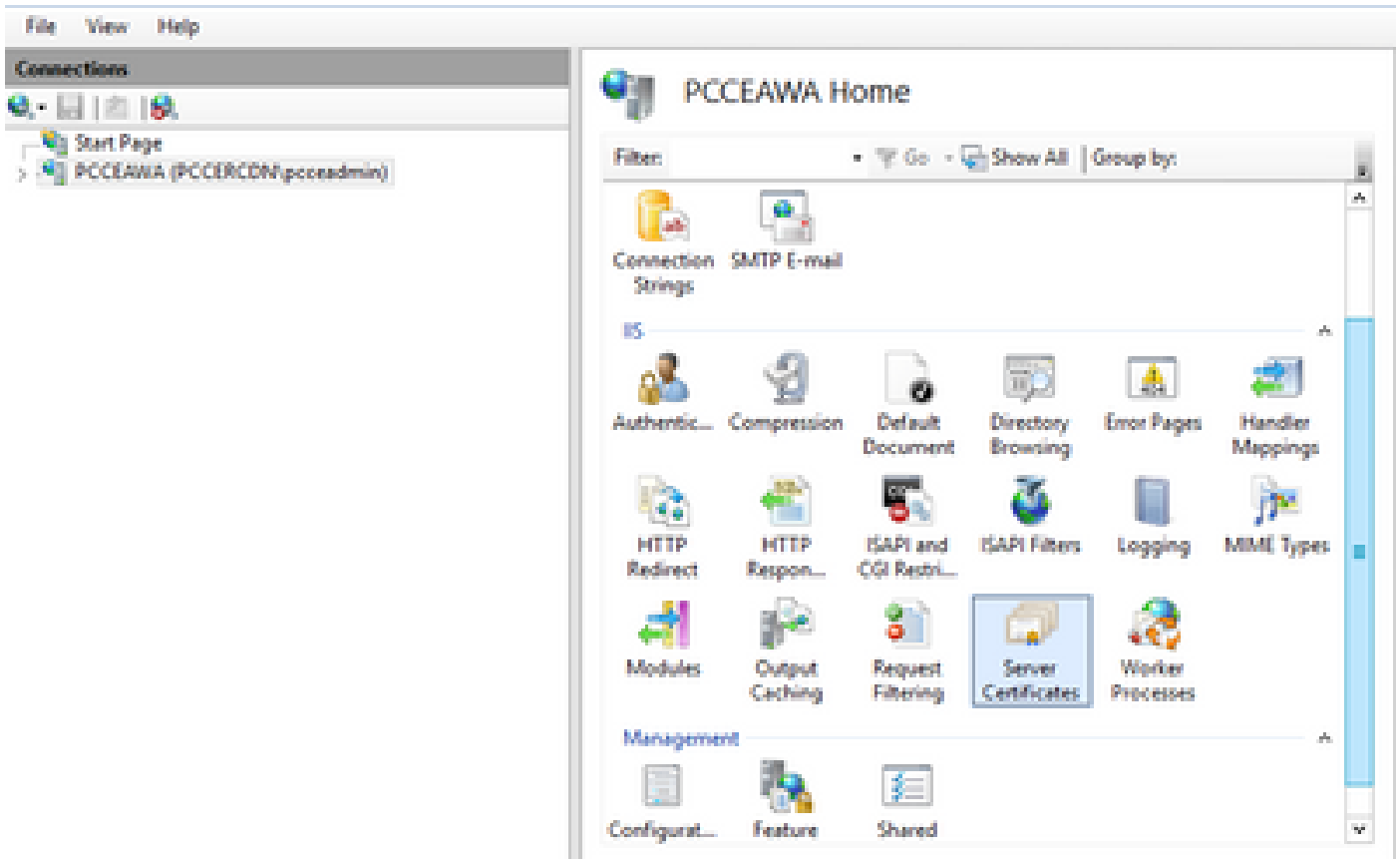
인증서 업로드에 성공하면 인증서가 Server Certificates 창에 나타납니다.



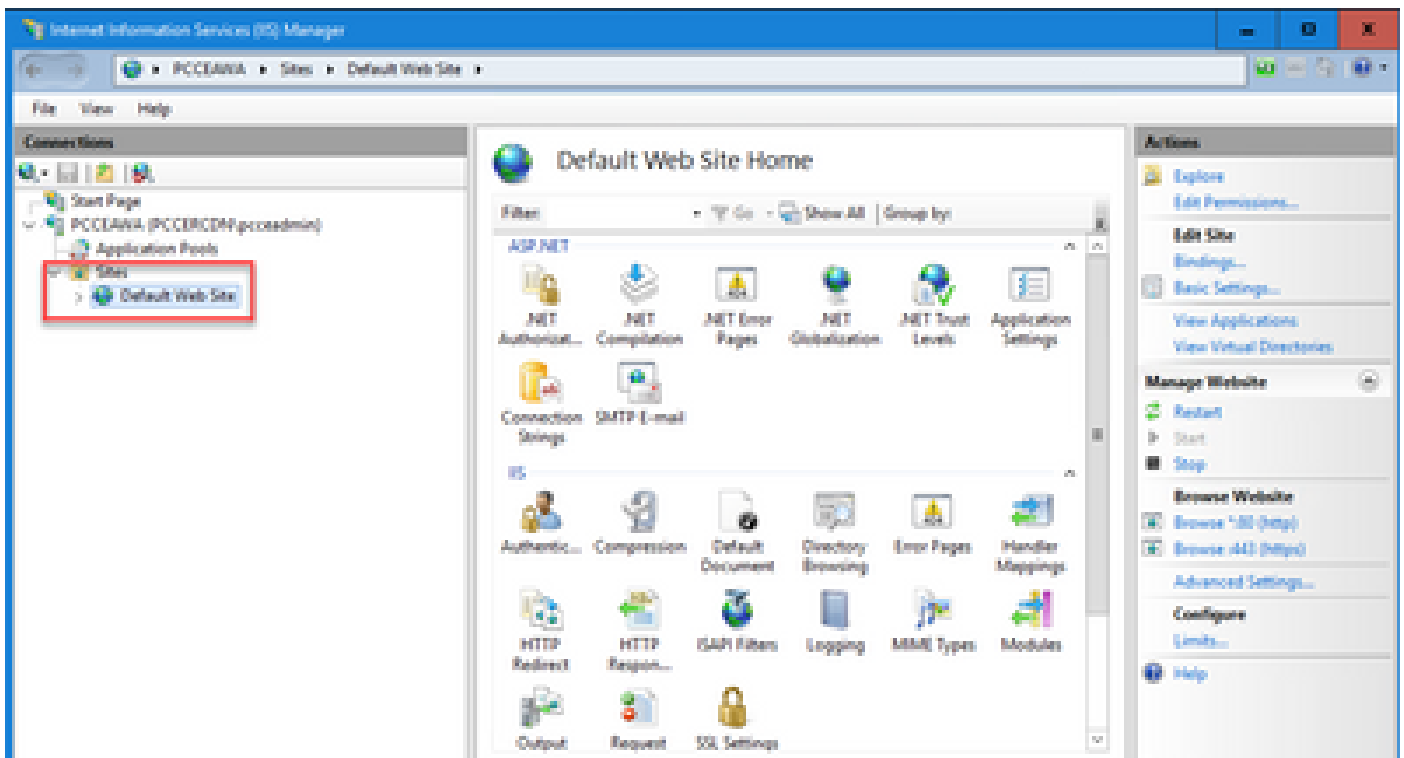
4. CA 서명 인증서를 IIS에 바인딩합니다

이 절차에서는 IIS 관리자에서 CA 서명 인증서를 바인딩하는 방법에 대해 설명합니다.

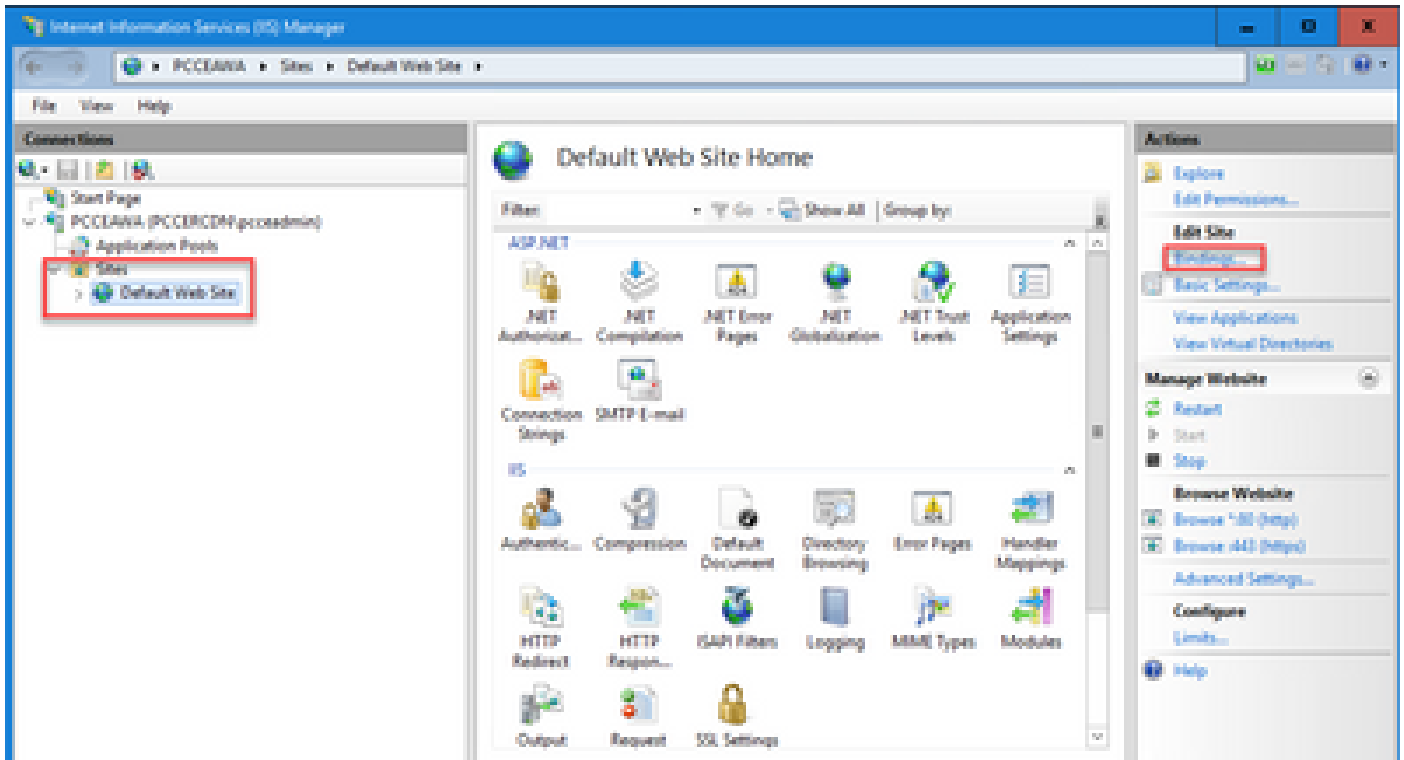
1단계. Windows에 로그인하고 제어판 > 관리 도구 > 인터넷 정보 서비스(IIS) 관리자를 선택합니다.



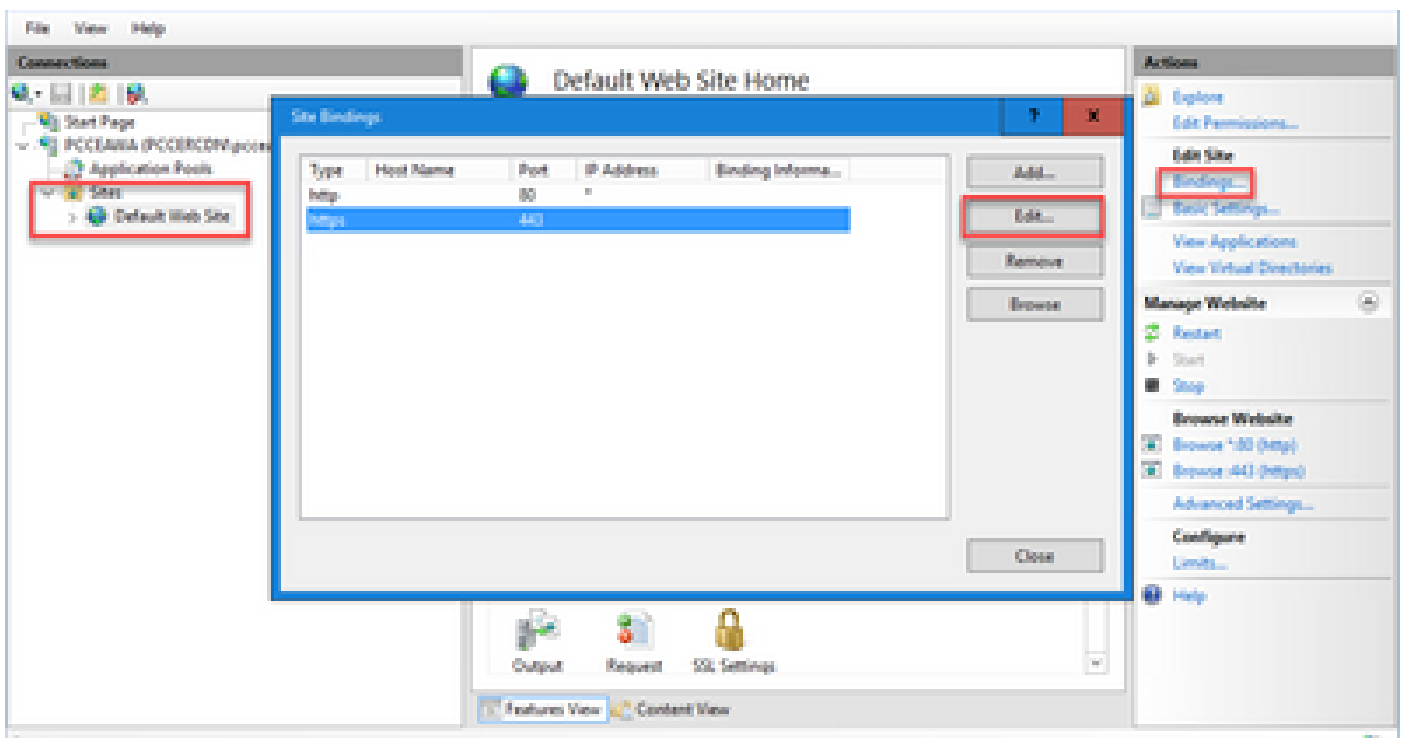
2단계. Connections(연결) 창에서 <server_name> > Sites(사이트) > Default Web Site(기본 웹 사이트)를 선택합니다.



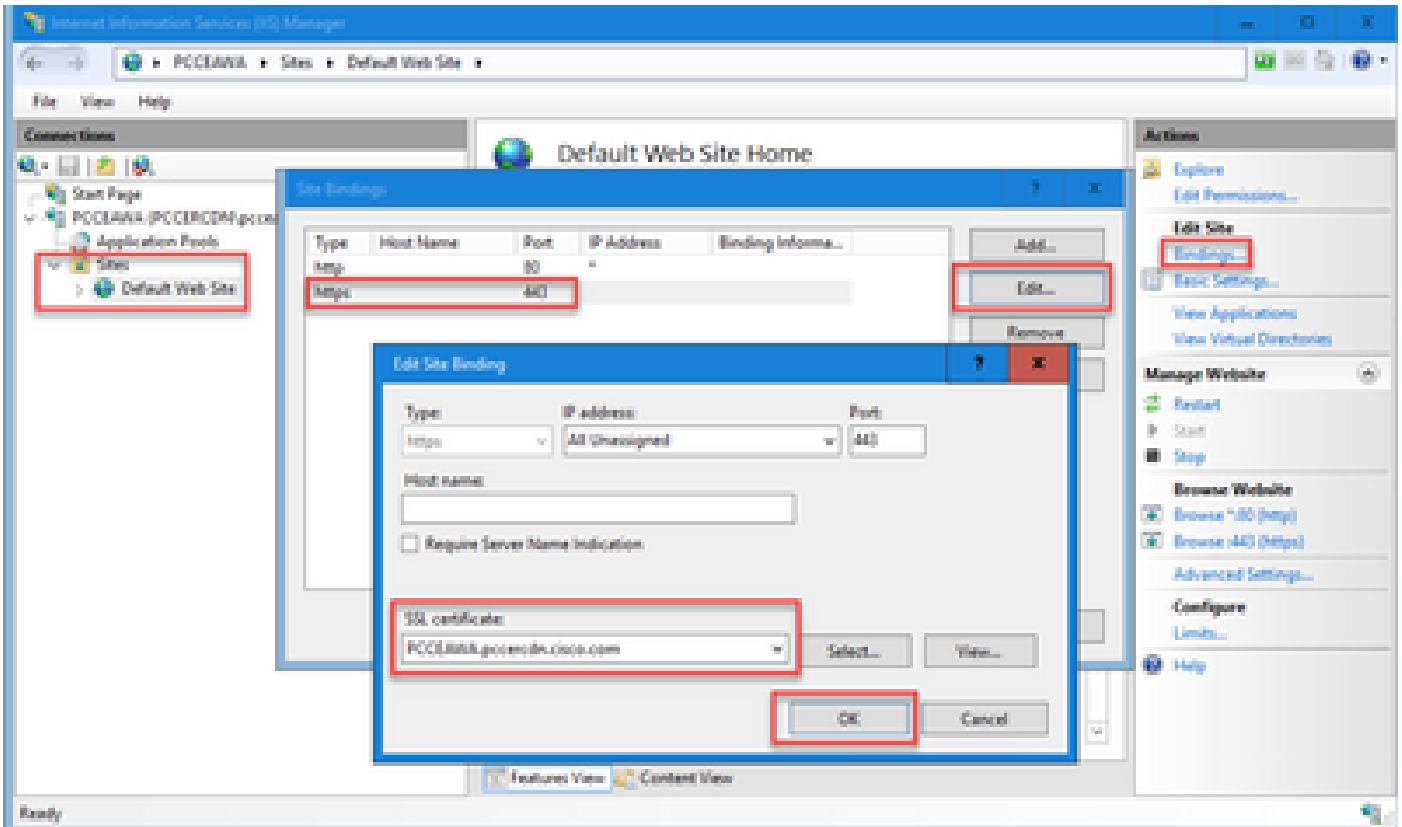
3단계. Actions(작업) 창에서 Bindings...를 클릭합니다.



4단계. 유형 https with port 443을 클릭한 다음 Edit...(수정...)를 클릭합니다.

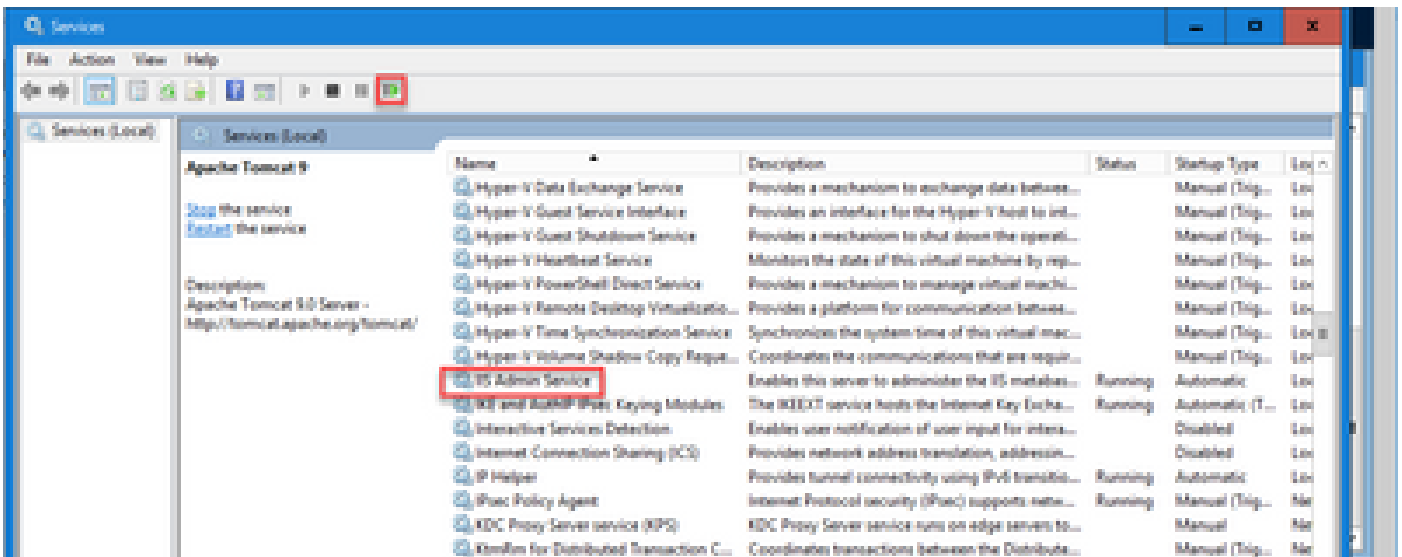


5단계. SSL certificate(SSL 인증서) 드롭다운 목록에서 이전 단계에서 지정된 것과 동일한 친숙한 이름의 인증서를 선택합니다.



6단계. OK(확인)를 클릭합니다.

7단계. 시작 > 실행 > services.msc로 이동하여 IIS 관리 서비스를 다시 시작합니다.



IIS를 다시 시작하면 응용 프로그램을 시작할 때 인증서 오류 경고가 나타나지 않습니다.

5. CA 서명 인증서를 진단 포트코에 바인딩합니다

이 절차에서는 진단 포털에서 CA 서명 인증서를 바인딩하는 방법에 대해 설명합니다.

1단계. 명령 프롬프트를 엽니다(관리자로 실행).

2단계. Diagnostic Portico 홈 폴더로 이동합니다. 다음 명령을 실행합니다.

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

3단계. 진단 포털에 대한 현재 인증서 바인딩을 제거합니다. 다음 명령을 실행합니다.

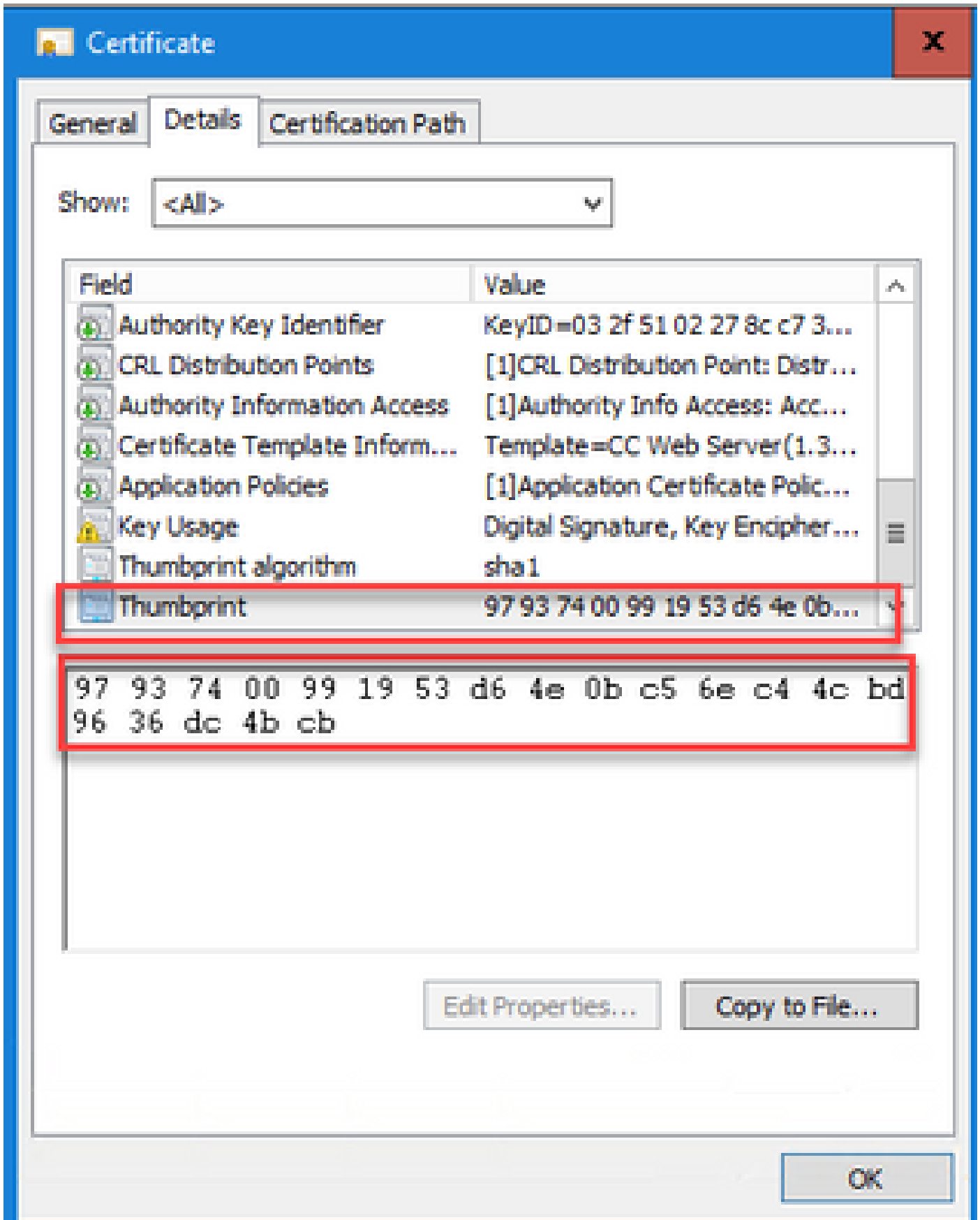
```
DiagFwCertMgr /task:UnbindCert
```

```
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>
```

4단계. 서명된 인증서를 열고 Thumbprint(지문) 필드의 해시 콘텐츠(공백 없음)를 복사합니다.



5단계. 이 명령을 실행하고 해시 내용을 붙여넣습니다.

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

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953D64E08C56EC44C8D9636DC4BCB
4C4BCB

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

Executing Task: 'BindCertFromStore'
Read port number from service configuration file: '7890'
CertHash Argument Passed: '97937400991953D64E08C56EC44C8D9636DC4BCB'
ATTEMPTING TO BIND CERTIFICATE WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Trying to look up certificate: 97937400991953D64E08C56EC44C8D9636DC4BCB
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>
```

인증서 바인딩에 성공하면 인증서 바인딩이 VALID(유효) 메시지가 표시됩니다.

6단계. 인증서 바인딩이 성공했는지 확인합니다. 다음 명령을 실행합니다.


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: 97937400991953D64E08C56EC44C8D9636DC4BCB
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>
```

 참고: DiagFwCertMgr은 기본적으로 포트 7890을 사용합니다.


인증서 바인딩에 성공하면 인증서 바인딩이 VALID(유효) 메시지가 표시됩니다.

7단계. 진단 프레임워크 서비스를 다시 시작합니다. 다음 명령을 실행합니다.

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

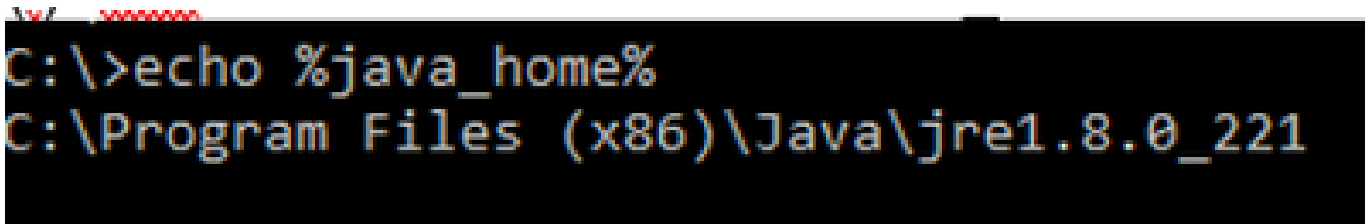
진단 프레임워크가 성공적으로 다시 시작되면 애플리케이션이 시작될 때 인증서 오류 경고가 나타나지 않습니다.

6. 루트 및 중간 인증서를 Java 키 저장소로 가져옵니다.

 주의: 시작하기 전에 키 저장소를 백업하고 Java 홈에서 관리자로 명령을 실행해야 합니다.

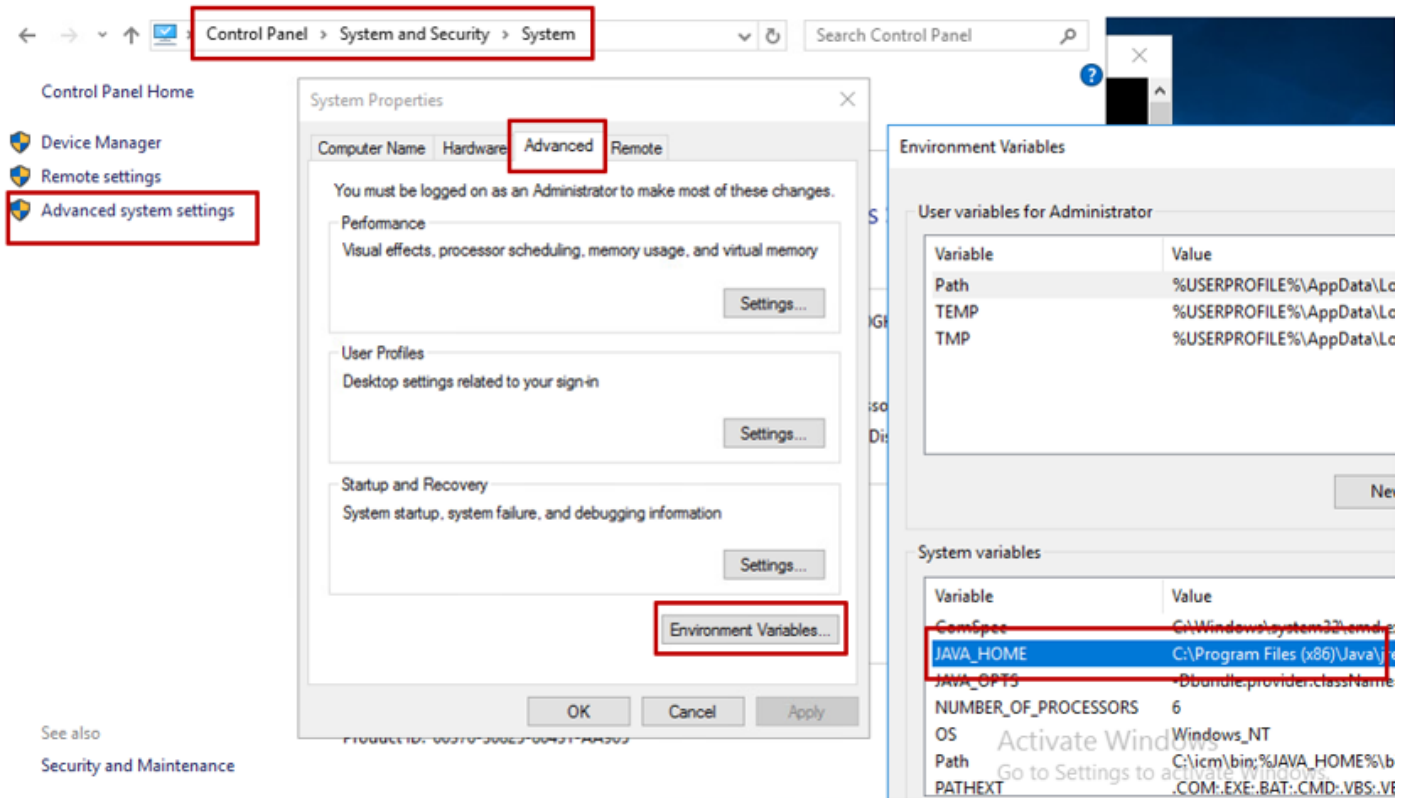
1단계. Java 홈 경로를 파악하여 Java 키틀이 호스팅되는 위치를 확인합니다. Java 홈 경로를 찾을 수 있는 방법에는 두 가지가 있습니다.

옵션 1: CLI 명령: `echo %JAVA_HOME%`



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

옵션 2: 그림과 같이 Manually via Advanced system setting(고급 시스템 설정을 통해 수동으로)



참고: UCCE 12.5의 기본 경로는 C:\Program Files (x86)\Java\jre1.8.0_221\bin입니다. 그러나 12.5(1a) 설치 관리자를 사용했거나 12.5 ES55가 설치된 경우(필수 OpenJDK ES), OpenJDK를 사용하여 데이터 저장소 경로가 변경되었으므로 JAVA_HOME 대신 CCE_JAVA_HOME을 사용합니다. CCE 및 CVP의 OpenJDK 마이그레이션에 대한 자세한 내용은 다음 문서에서 [Install and Migrate to OpenJDK in CCE 2.5\(1\)](#) 및 [Install and Migrate to OpenJDK in CVP 12.5\(1\)](#)를 참조하십시오.

2단계. C:\Program Files (x86)\Java\jre1.8.0_221\lib\security 폴더에서 cacerts 파일을 백업합니다. 다른 곳으로 복사하시면 됩니다.

3단계. 명령을 실행하려면 관리자 권한으로 명령 창을 엽니다.


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


참고: 필요한 특정 인증서는 인증서를 서명하는 데 사용하는 CA에 따라 다릅니다. 공용 CA의 전형적이며 내부 CA보다 안전한 2계층 CA에서는 루트 인증서와 중간 인증서를 모두 가져와야 합니다. 중간체가 없는 독립형 CA에서는 일반적으로 랩 또는 더 간단한 내부 CA에서 볼 수 있으므로 루트 인증서만 가져오면 됩니다.

CVP 솔루션

1. FQDN을 사용하여 인증서 생성

이 절차에서는 WSM(Web Service Manager), VXML(Voice XML), OAMP(Call Server and Operations Management) 서비스에 대해 FQDN을 사용하여 인증서를 생성하는 방법에 대해 설명합니다.

 참고: CVP를 설치할 때 인증서 이름에는 서버의 이름만 포함되고 FQDN은 포함되지 않으므로 인증서를 다시 생성해야 합니다.

-  주의: 시작하기 전에 다음을 수행해야 합니다.
1. 키 저장소 비밀번호를 가져옵니다. 다음 명령을 실행합니다.
%CVP_HOME%\conf\security.properties. keytool 명령을 실행할 때 이 비밀번호가 필요합니다.
 2. %CVP_HOME%\conf\security 폴더를 다른 폴더에 복사합니다.
 3. 관리자로 명령 창을 열어 명령을 실행합니다.

CVP 서버

1단계. CVP 서버 인증서를 삭제하려면 다음 명령을 실행합니다.


```
%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
```

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

2단계. WSM 인증서를 생성하려면 다음 명령을 실행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

 참고: 기본적으로 인증서는 2년간 생성됩니다. -validity XXXX를 사용하여 인증서가 재생성될 때 만료 날짜를 설정합니다. 그렇지 않으면 인증서가 90일 동안 유효하며 이 시간 전에 CA에 서명해야 합니다. 이러한 인증서의 대부분은 3-5년이 적절한 검증 시간이어야 합니다.

다음은 몇 가지 표준 유효성 입력입니다.

1년	365
----	-----

2년	730
3년	1095
4년	1460
5년	1895
10년	3650

⚠ 주의: 12.5 인증서는 SHA 256, Key Size 2048 및 Encryption Algorithm RSA여야 합니다. -keyalg RSA 및 -keysize 2048 매개변수를 사용하여 이 값을 설정합니다. CVP 키 저장소 명령에는 -storetype JCEKS 매개 변수가 포함되어야 합니다. 이 작업을 수행하지 않으면 인증서, 키 또는 더 나쁜 키 저장소가 손상될 수 있습니다.

질문에 서버의 FQDN을 지정합니다. 이름과 성이 무엇입니까?

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\usecurity\keystore -alias w
sm_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]:
```

다음 기타 질문을 완료합니다.

조직 구성 단위의 이름은 무엇입니까?

[알 수 없음]: <OU 지정>

귀사의 이름은 무엇입니까?

[알 수 없음]: <조직 이름 지정>

시 또는 지역의 이름이 무엇입니까?

[알 수 없음]: <시/군/구 이름 지정>

시/도 이름이 어떻게 됩니까?

[알 수 없음]: <시/도 이름 지정>

이 유닛의 국가 번호는 몇 번입니까?

[알 수 없음]: <두 글자로 된 국가 코드 지정>

다음 두 입력에 대해 yes를 지정합니다.

3단계. vxml_certificate 및 callserver_certificate에 대해 동일한 단계를 수행합니다.

```
%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
```

CVP 보고 서버

1단계. WSM 및 보고 서버 인증서를 삭제하려면 다음 명령을 실행합니다.

```
%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
```

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

2단계. WSM 인증서를 생성하려면 다음 명령을 실행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

쿼리에 대한 서버의 FQDN을 지정하고 성과 이름을 지정하고 CVP 서버와 동일한 단계를 계속합니다.

3단계. callserver_certificate에 대해 동일한 단계를 수행합니다.

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

CVP OAMP(UCCE 구축)

PCCE 솔루션 버전 12.x에서는 솔루션의 모든 구성 요소가 SPOG에 의해 제어되며 OAMP가 설치되지 않으므로 이러한 단계는 UCCE 구축 솔루션에만 필요합니다.

1단계. WSM 및 OAMP 서버 인증서를 삭제하려면 다음 명령을 실행합니다.

```
%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
```

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

2단계. WSM 인증서를 생성하려면 다음 명령을 실행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.


쿼리에 대한 서버의 FQDN을 지정하고 성과 이름을 지정하고 CVP 서버와 동일한 단계를 계속합니다.

3단계. oamp_certificate에 대해 동일한 단계를 수행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

2. CSR 생성

 참고: RFC5280 호환 브라우저에서는 각 인증서에 Subject Alternative Name(SAN)을 포함해야 합니다. 이는 CSR을 생성할 때 SAN과 함께 -ext 매개변수를 사용하여 수행할 수 있습니다

주체 대체 이름

-ext 매개 변수는 사용자가 특정 내선 번호를 사용할 수 있도록 허용합니다. 표시된 예에서는 서버의 FQDN(정규화된 도메인 이름)과 localhost가 포함된 SAN(주체 대체 이름)을 추가합니다. SAN 필드를 쉼표로 구분된 값으로 추가할 수 있습니다.

유효한 SAN 유형은 다음과 같습니다.

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

예: -ext san=dns:mycwp.mydomain.com,dns:localhost

CVP 서버

1단계. 별칭에 대한 인증서 요청을 생성합니다. 다음 명령을 실행하여 파일에 저장합니다(예: wsm_certificate).

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

2단계. vxml_certificate 및 callserver_certificate에 대해 동일한 단계를 수행합니다.

```
%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 -
```

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

CVP 보고 서버

1단계. 별칭에 대한 인증서 요청을 생성합니다. 다음 명령을 실행하여 파일에 저장합니다(예: wsmreport_certificate).

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

2단계. callserver_certificate에 대해 동일한 단계를 수행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

CVP OAMP(UCCE 구축)

1단계. 별칭에 대한 인증서 요청을 생성합니다. 다음 명령을 실행하여 파일에 저장합니다(예: 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.
```

2단계. oamp_certificate에 대해 동일한 단계를 수행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

3. CA 서명 인증서 얻기

1단계. CA의 인증서(CVP 서버의 경우 WSM, Callserver 및 VXML 서버, CVP OAMP 서버의 경우 WSM 및 OAMP, 보고 서버의 경우 WSM 및 Callserver)에 서명합니다.

2단계. CA 기관에서 애플리케이션 인증서 및 루트 인증서를 다운로드합니다.

3단계. 루트 인증서 및 CA 서명 인증서를 각 서버의 %CVP_HOME%\conf\security\ 폴더에 복사합니다.

4. CA 서명 인증서 가져오기

CVP 솔루션의 모든 서버에 이 단계를 적용합니다. 해당 서버의 구성 요소에 대한 인증서만 CA 서명 인증서를 가져와야 합니다.

1단계. 루트 인증서를 가져옵니다. 다음 명령을 실행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다. Trust this certificate 프롬프트에 Yes를 입력합니다.

중간 인증서가 있는 경우 다음 명령을 실행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다. Trust this certificate 프롬프트에 Yes를 입력합니다.

2단계. 해당 서버 인증서(CVP, Reporting and OAMP)에 대해 CA 서명 WSM을 가져옵니다. 다음 명

령을 실행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다. Trust this certificate 프롬프트에 Yes를 입력합니다.

3단계. CVP 서버 및 보고 서버에서 Callserver CA 서명 인증서를 가져옵니다. 다음 명령을 실행합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다. Trust this certificate 프롬프트에 Yes를 입력합니다.


4단계. CVP 서버에서 VXML 서버 CA 서명 인증서를 가져옵니다. 다음 명령을 실행합니다.

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

5단계. CVP OAMP 서버(UCCE만 해당)에서 OAMP 서버 CA 서명 인증서를 가져옵니다. 다음 명령을 실행합니다.

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

6단계. 서버를 재부팅합니다.

 참고: UCCE 구축에서는 CSR을 생성할 때 제공한 FQDN을 사용하여 CVP OAMP에 서버(보고, CVP 서버 등)를 추가해야 합니다.

VOS 서버

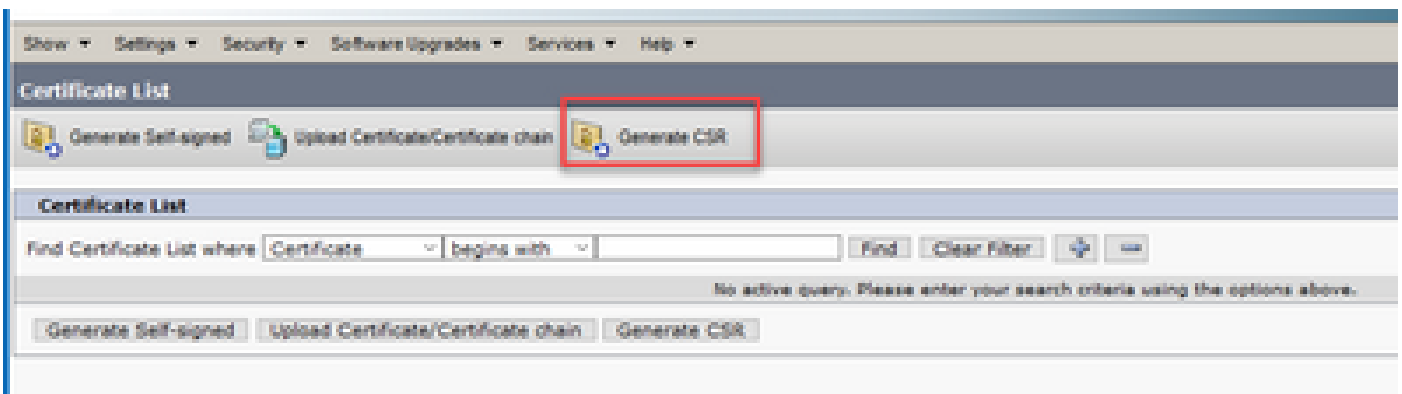
1. CSR 인증서 생성

이 절차에서는 Cisco VOS(Voice Operating System) 기반 플랫폼에서 Tomcat CSR 인증서를 생성하는 방법에 대해 설명합니다. 이 프로세스는 다음과 같은 모든 VOS 기반 애플리케이션에 적용 가능합니다.

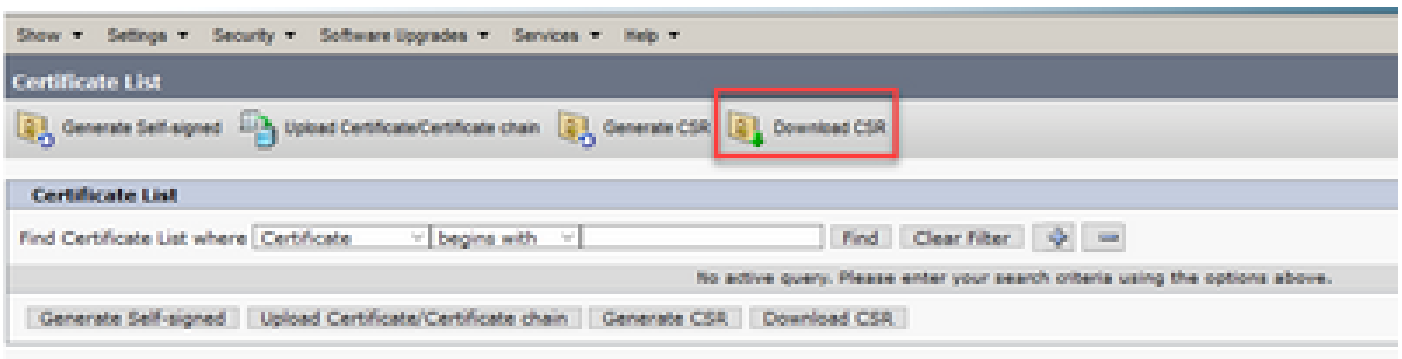
- CUCM
- Finesse
- CUIC \ LD(Live Data) \ID 서버(IDS)
- 클라우드 연결
- Cisco VVB

1단계. Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지(<https://FQDN:<8443 또는 443>/cmplatform>)로 이동합니다.

2단계. Security(보안) > Certificate Management(인증서 관리)로 이동하고 Generate CSR(CSR 생성)을 선택합니다.



3단계. CSR 인증서가 생성되면 창을 닫고 Download CSR(CSR 다운로드)을 선택합니다.



4단계. Certificate purpose(인증서 용도)가 tomcat인지 확인하고 Download CSR(CSR 다운로드)을 클릭합니다.


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.

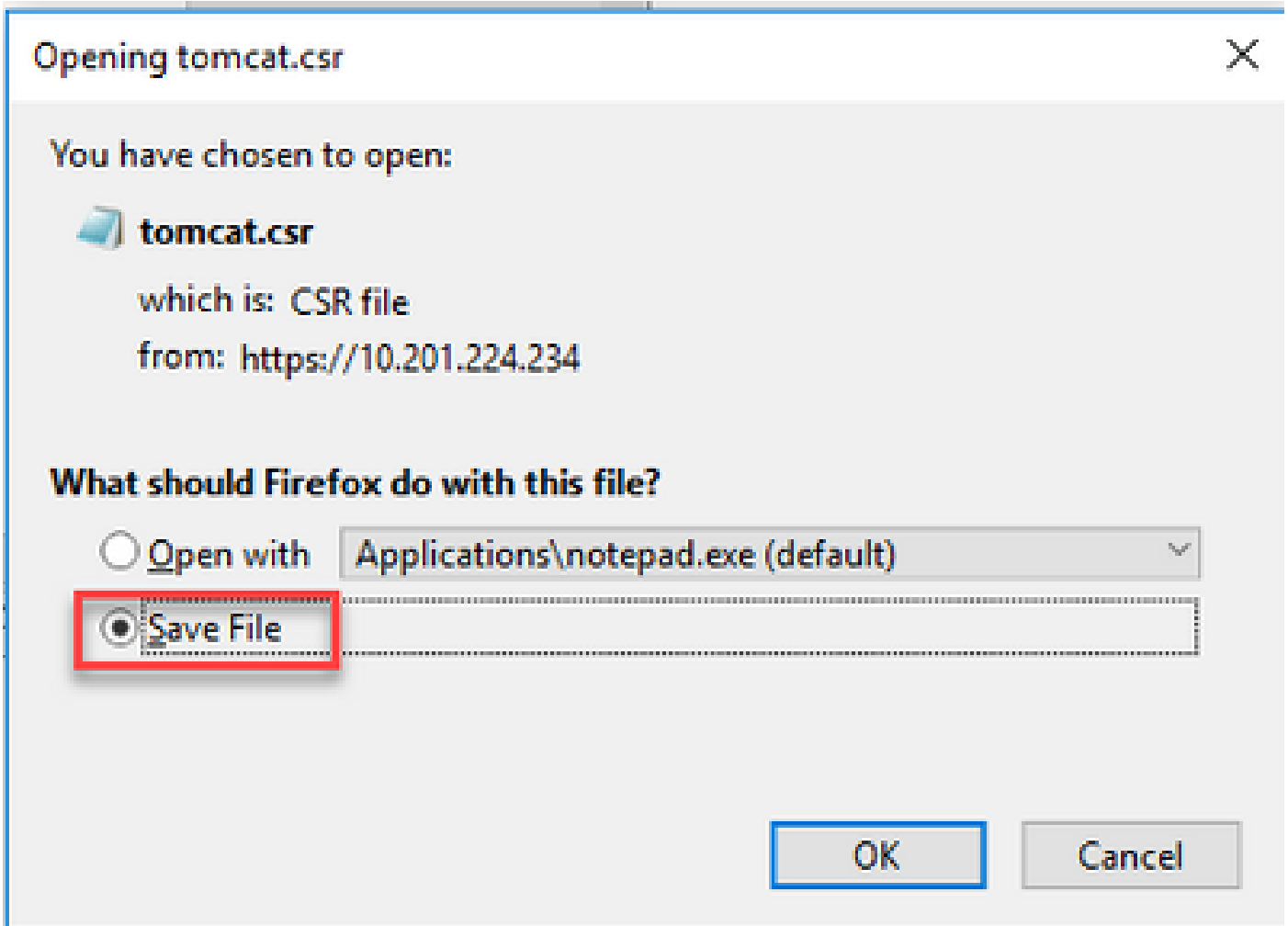
Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR Close

 *- indicates required item.

5단계. Save File(파일 저장)을 클릭합니다. 파일은 다운로드 폴더에 저장됩니다.



2. CA 서명 인증서 얻기

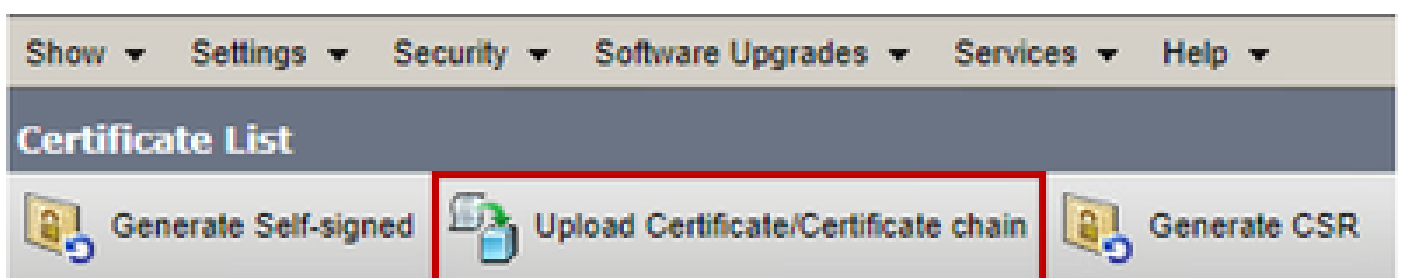
1단계. CA에서 내보낸 tomcat 인증서에 서명합니다.

2단계. CA 기관에서 인증한 애플리케이션과 루트를 다운로드합니다.

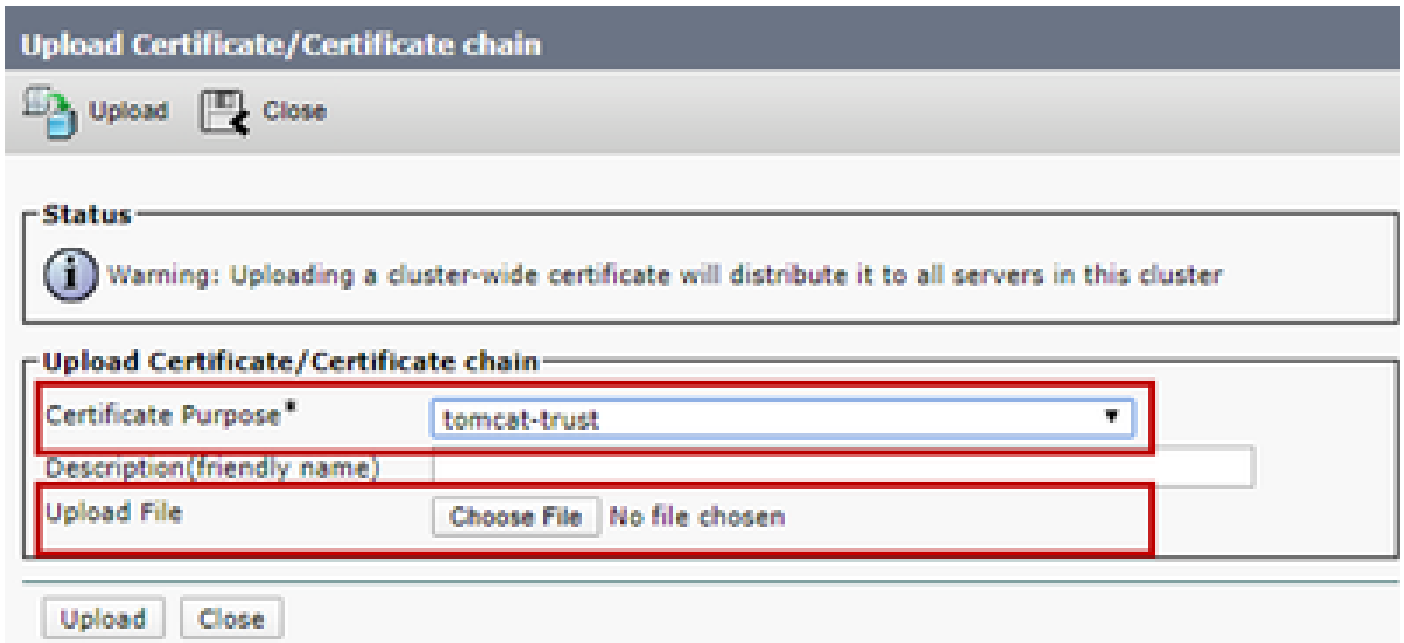
3. 애플리케이션 및 루트 인증서 업로드

1단계. Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지(<https://FQDN:<8443 또는 443>/cmplatform>)로 이동합니다.

2단계. Security(보안) > Certificate Management(인증서 관리)로 이동하고 Upload Certificate/Certificate chain(인증서/인증서 체인 업로드)을 선택합니다.



3단계. Upload certificate/Certificate chain(인증서/인증서 체인 업로드) 창에서 certificate purpose(인증서 용도) 필드에서 tomcat-trust를 선택하고 루트 인증서를 업로드합니다.



Upload Certificate/Certificate chain

Upload Close

Status

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

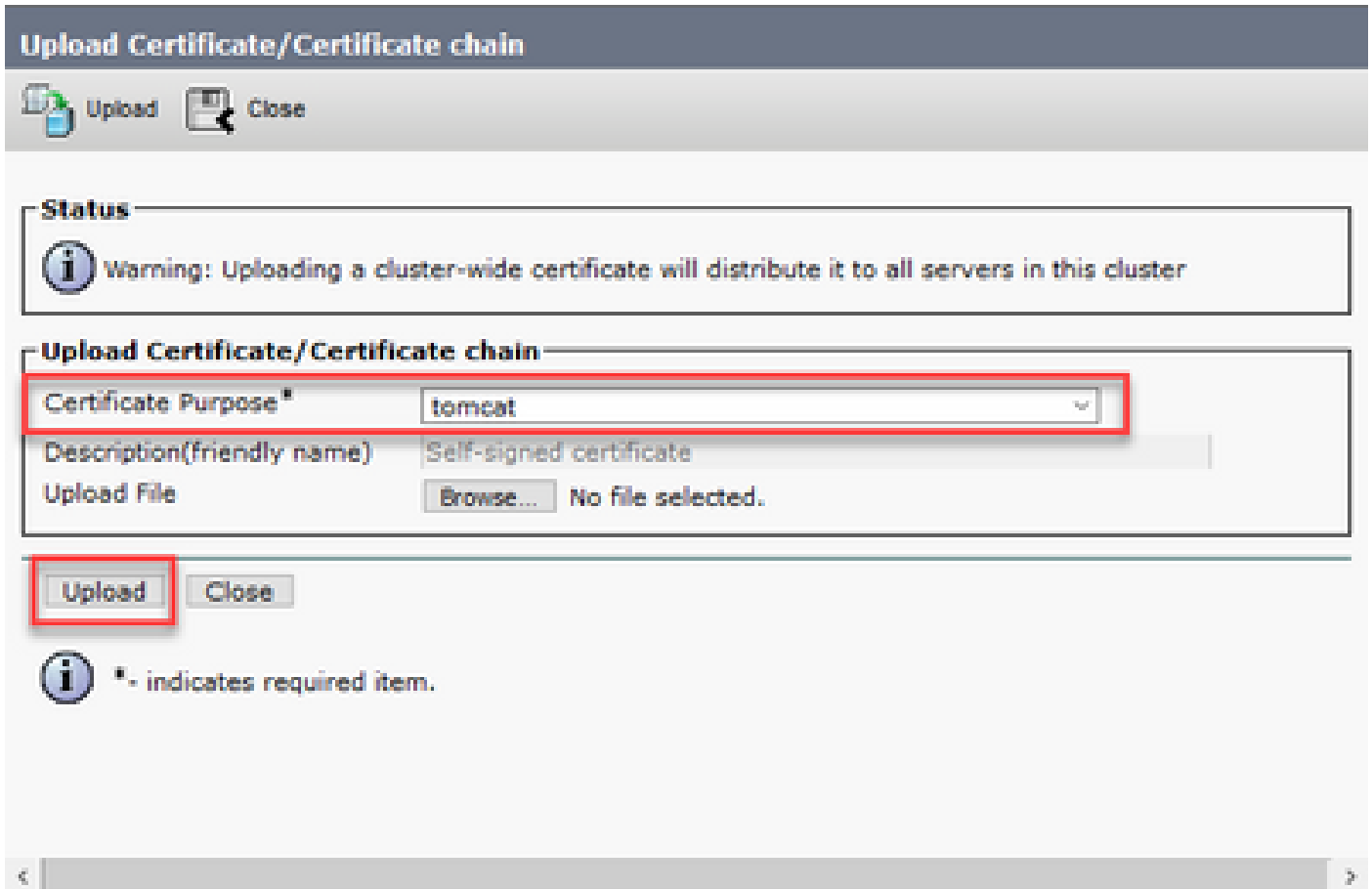
Upload Certificate/Certificate chain

Certificate Purpose [*]	tomcat-trust
Description(friendly name)	
Upload File	Choose File No file chosen

Upload Close

4단계. 중간 인증서(있는 경우)를 tomcat-trust로 업로드합니다.

5단계. Upload certificate/Certificate chain(인증서/인증서 체인 업로드) 창의 Certificate Purpose(인증서 용도) 필드에서 tomcat now tomcat을 선택하고 애플리케이션 CA 서명 인증서를 업로드합니다.



6단계. 서버를 재부팅합니다.

다음을 확인합니다.

서버를 재부팅한 후 다음 단계를 실행하여 CA 서명 구현을 확인합니다.

1단계. 웹 브라우저를 열고 캐시를 지웁니다.

2단계. 브라우저를 닫았다가 다시 엽니다.

이제 CA 서명 인증서를 시작하려면 인증서 스위치를 확인해야 하며, 브라우저 창에서 인증서가 자체 서명되어 있으므로 신뢰할 수 없다는 표시는 사라져야 합니다.

문제 해결

이 가이드에는 CA 서명 인증서의 구현 문제를 해결하는 단계가 없습니다.

관련 정보

- CVP 컨피그레이션 가이드: [CVP 컨피그레이션 가이드 - 보안](#)
- UCCE 컨피그레이션 가이드: [UCCE 컨피그레이션 가이드 - 보안](#)
- PCCE 관리 가이드: [PCE 관리 가이드 - 보안](#)
- UCCE 자체 서명 인증서: [Exchange UCCE 자체 서명 인증서](#)

- PCCE 자체 서명 인증서: [Exchange PCCE 자체 서명 인증서](#)
- CCE 12.5(1)에서 OpenJDK로 설치 및 마이그레이션: CCE [OpenJDK 마이그레이션](#)
- CVP 12.5(1)에서 OpenJDK 설치 및 마이그레이션: [CVP OpenJDK 마이그레이션](#)

[기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.