Finesse와 CTI 서버 간 보안 통신 구성

목차

소개

이 문서에서는 Cisco Contact Center Enterprise(CCE) 솔루션에서 Cisco Finesse와 CTI(Computer Telephony Integration) 서버 간에 CA(Certificate Authority) 서명 인증서를 구현하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CCE 릴리스 12.0(1)
- Finesse 릴리스 12.0(1)
- CTI 서버

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- PCCE(Packaged CCE) 12.0(1)
- Finesse 12.0(1)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

CCE 버전 11.5에서 Cisco는 TLS(Transport Layer Security) 버전 1.2의 지원을 시작했으며, 이를 통해 SIP(Session Initiation Protocol) 및 RTP(Real-time Transport Protocol) 메시지가 TLS 1.2를 통해 안전하게 전송될 수 있습니다. CCE 12.0에서 그리고 데이터 인 동작 보안의 일부로서 Cisco는 대부분의 컨택 센터 통화에서 TLS 1.2 지원을 시작했습니다. 흐름:인바운드 및 아웃바운드 음성, 다중 채널 및 외부 데이터베이스 딥이 문서의 핵심은 인바운드 음성, 특히 Finesse와 CTI 서버 간의 통신입니다.

CTI 서버는 다음 연결 모드를 지원합니다.

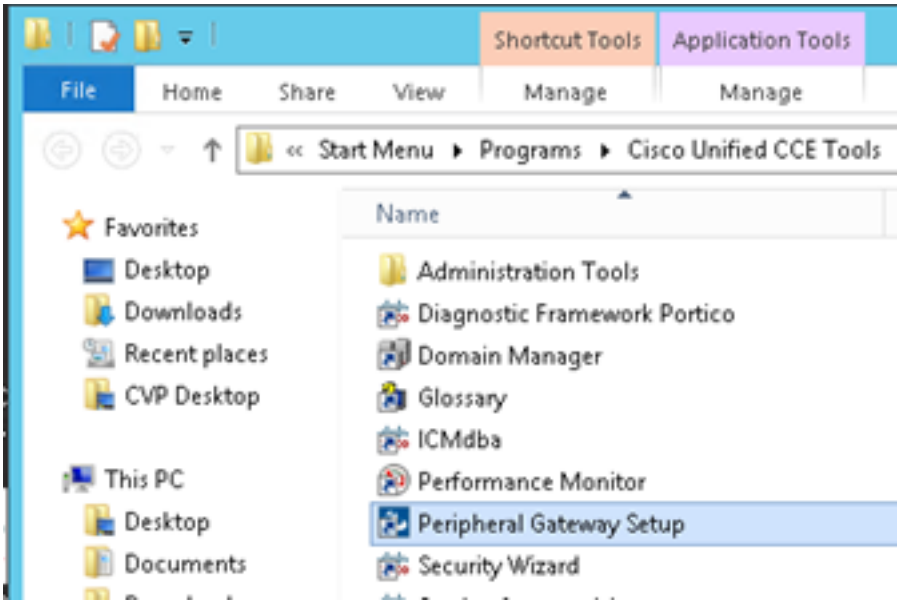
- **보안 전용 연결**:CTI 서버와 CTI 클라이언트(Finesse, dialer, CTIOS 및 ctitest) 간의 보안 연결을 허용합니다.
- **보안 연결 및 비보안 연결(혼합 모드):**보안은 물론 CTI 서버와 CTI 클라이언트 간의 비보안 연결을 허용합니다.이것이 기본 연결 모드입니다.이 모드는 이전 릴리스를 CCE 12.0(1)으로 업그레이드할 때 구성됩니다.

  참고:비보안 전용 모드는 지원되지 않습니다.

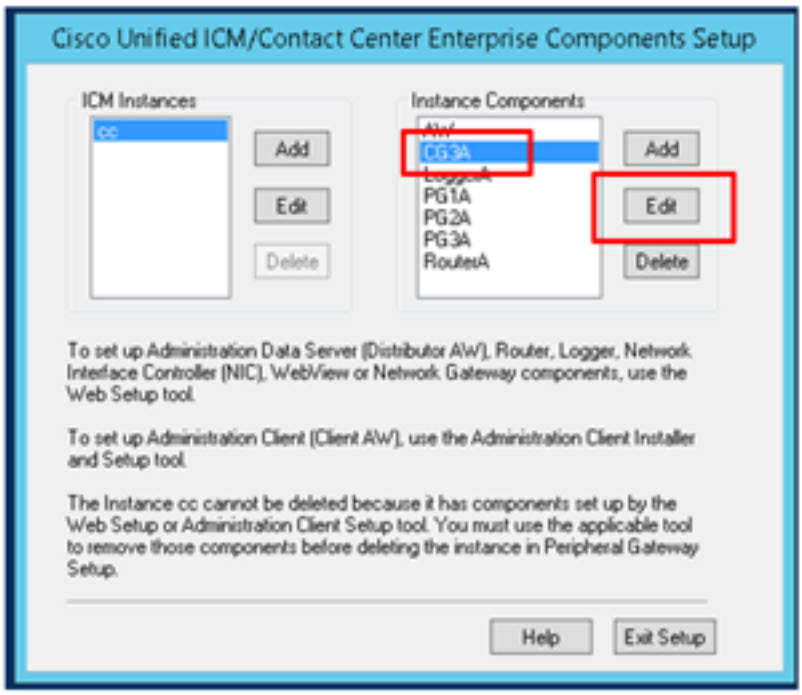
구성

CCE CTI 서버 보안

1단계. PCCE 관리 워크스테이션(AW)에서 **Unified CCE Tools** 폴더를 열고 주변 장치 게이트웨이 설정을 두 번 **클릭합니다**.

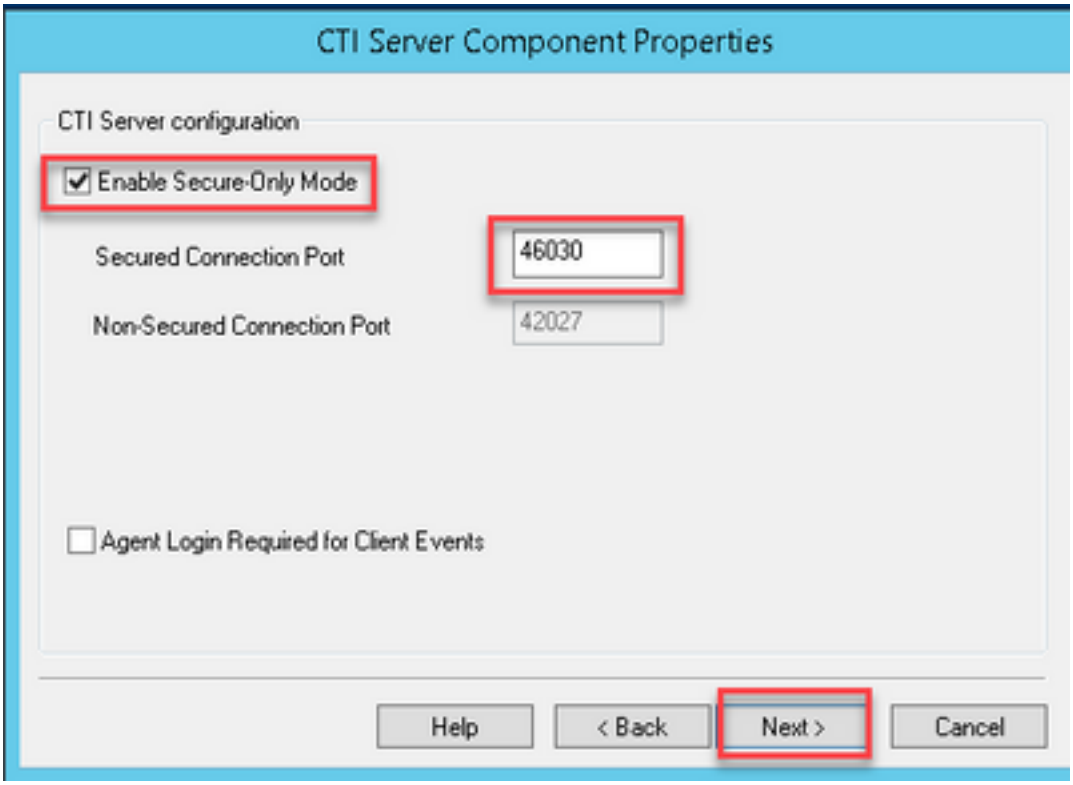


2단계. **CG3A를** 선택하고 Edit(**수정)**를 클릭합니다.



3단계. CTI 서버 속성에서 **다음**을 클릭합니다.**CG3A** 서비스 중지 설정에 대한 질문에 **예**를 선택합니다.

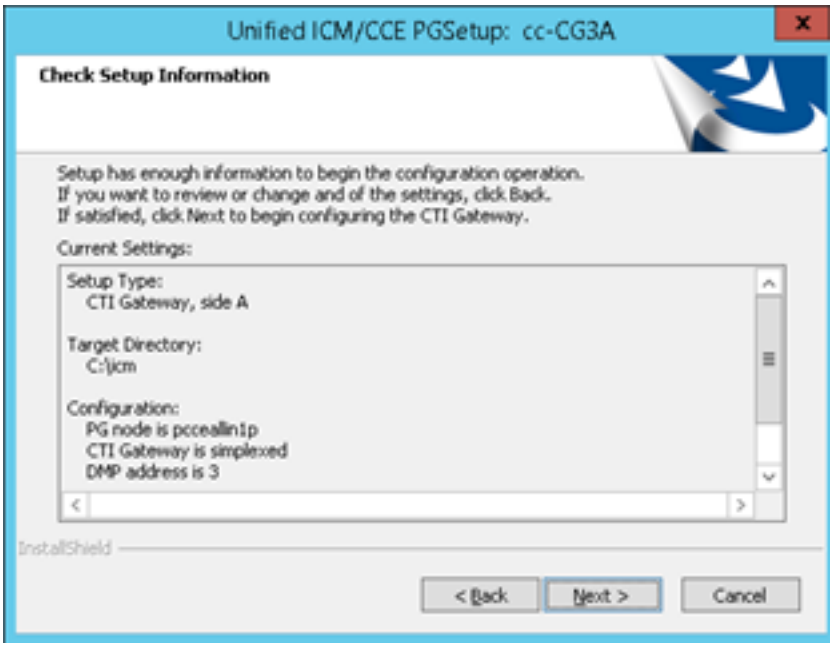
4단계. CTI **Server Components Properties(CTI 서버 구성 요소 속성)**에서 Enable **Secured-only mode(보안 전용 모드 활성화)를 선택합니다.**다음 연습에서는 **Finesse에서** 동일한 포트를 구성해야 하므로 Secured Connection Port**(46030)**에 유의하십시오.Next(**다음)를 클릭합니다**.



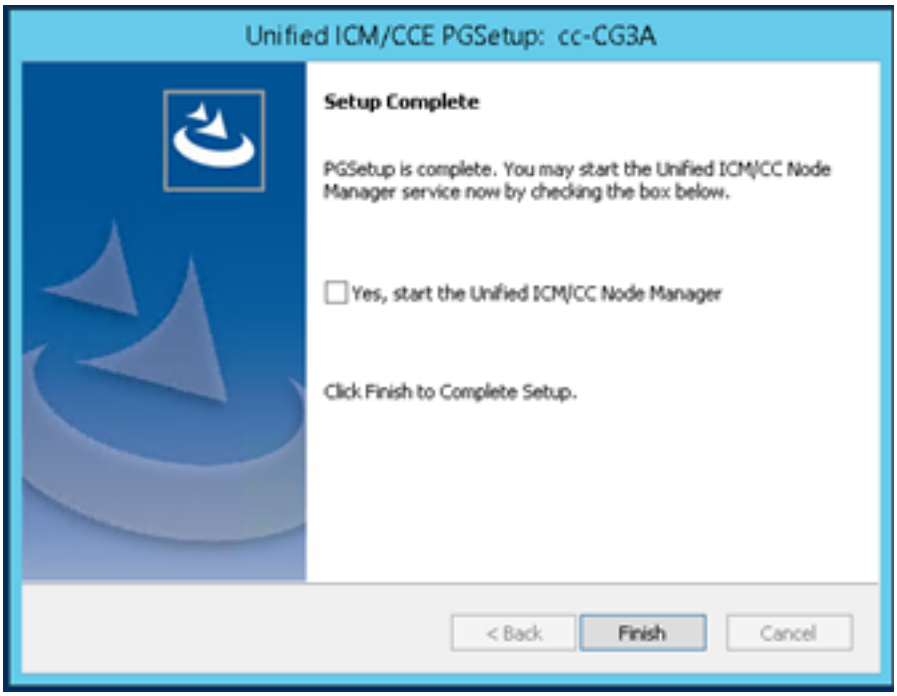
참고:기본 보안 통신은 42030이지만 이 문서에 사용되는 랩은 40630입니다. 포트 번호는 ICM 시스템 ID를 포함하는 수식의 일부입니다.시스템 ID가 1(CG1a)이면 기본 포트 번호는 일반적으로 42030입니다. 실습의 시스템 ID는 3(CG3a)이므로 기본 포트 번호는 46030입니다.

5단계. CTI **Network Interface Properties(CTI 네트워크 인터페이스 속성)에서 Next(다음)**를 클릭합

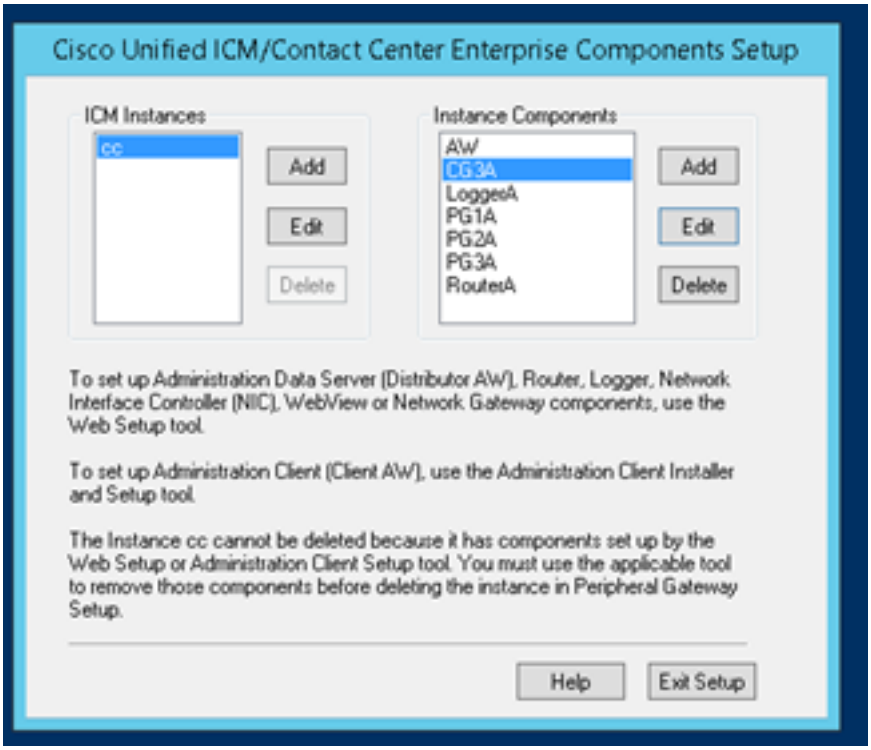
니다.Setup Information(**설정 정보)을** 확인하고 **Next(다음)**를 클릭합니다.



6단계. 이미지에 표시된 대로 **마침**을 클릭합니다.



7단계. Exit Setup(**설정 종료)**을 클릭하고 이미지에 표시된 대로 설정 창이 닫힐 때까지 기다립니다.



8단계. PCCEAllin1 데스크톱에서 Unified **CCE 서비스 제어**를 두 번 클릭합니다.

9단계. Cisco ICM cc CG3A를 선택하고 **시작**을 클릭합니다.

Finesse 보안 컨피그레이션

1단계. 웹 브라우저를 열고 Finesse **Administration**(Finesse 관리)**으로 이동합니다**.

2단계. 이미지에 표시된 대로 **Contact Center Enterprise CTI Server Settings(컨택 센터 엔터프라이즈 CTI 서버 설정) 섹션**으로 아래로 스크롤합니다.

3단계. 이전 연습에서 CG3A에 구성된 보안 통신 포트의 A측 포트를 변경합니다.**46030**. **[SSL 암호화 사용]을 선택하고 [저장]을 클릭합니다**.

참고: 연결을 테스트하려면 먼저 Finesse Tomcat 서비스를 다시 시작하거나 Finesse 서버를 다시 시작해야 합니다.

4단계. Finesse 관리 페이지에서 로그아웃합니다.

5단계. Finesse를 사용하여 SSH 세션을 엽니다.

6단계. FINESSEA SSH 세션에서 다음 명령을 실행합니다.

유틸리티 시스템 재시작

시스템을 다시 시작할지 묻는 메시지가 나타나면 **yes**를 입력합니다.

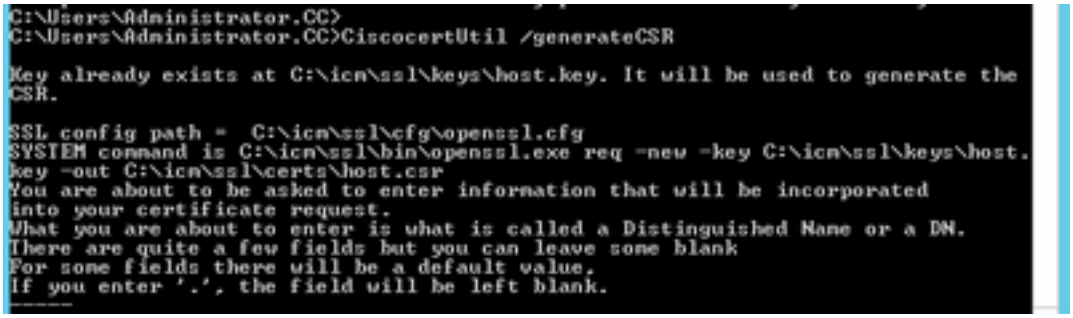
```
Using username "administrator".
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
        Disk 1: 146GB, Partitions aligned
        8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes


 Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

에이전트 PG 인증서 생성(CTI 서버)

CiscoCertUtils는 CCE 버전 12에서 릴리스된 새로운 툴입니다. 이 툴을 사용하여 인바운드 음성에 대한 모든 CCE 인증서를 관리합니다.이 문서에서는 이러한 CiscoCertUtils를 사용하여 PG(주변 장

치 게이트웨이) CSR(인증서 서명 요청)을 생성합니다.

1단계. CSR 인증서를 생성하려면 다음 명령을 실행합니다.**CiscoCertUtil /generateCSR**



다음과 같이 요청된 정보를 제공합니다.

국가 이름:미국

시/도 이름:MA

지역 이름:BXB

조직 이름:Cisco

조직 단위:CX

일반 이름:PCCEAllin1.cc.lab

Email:jdoe@cc.lab

챌린지 비밀번호:기차 1번!

선택적 회사 이름:Cisco

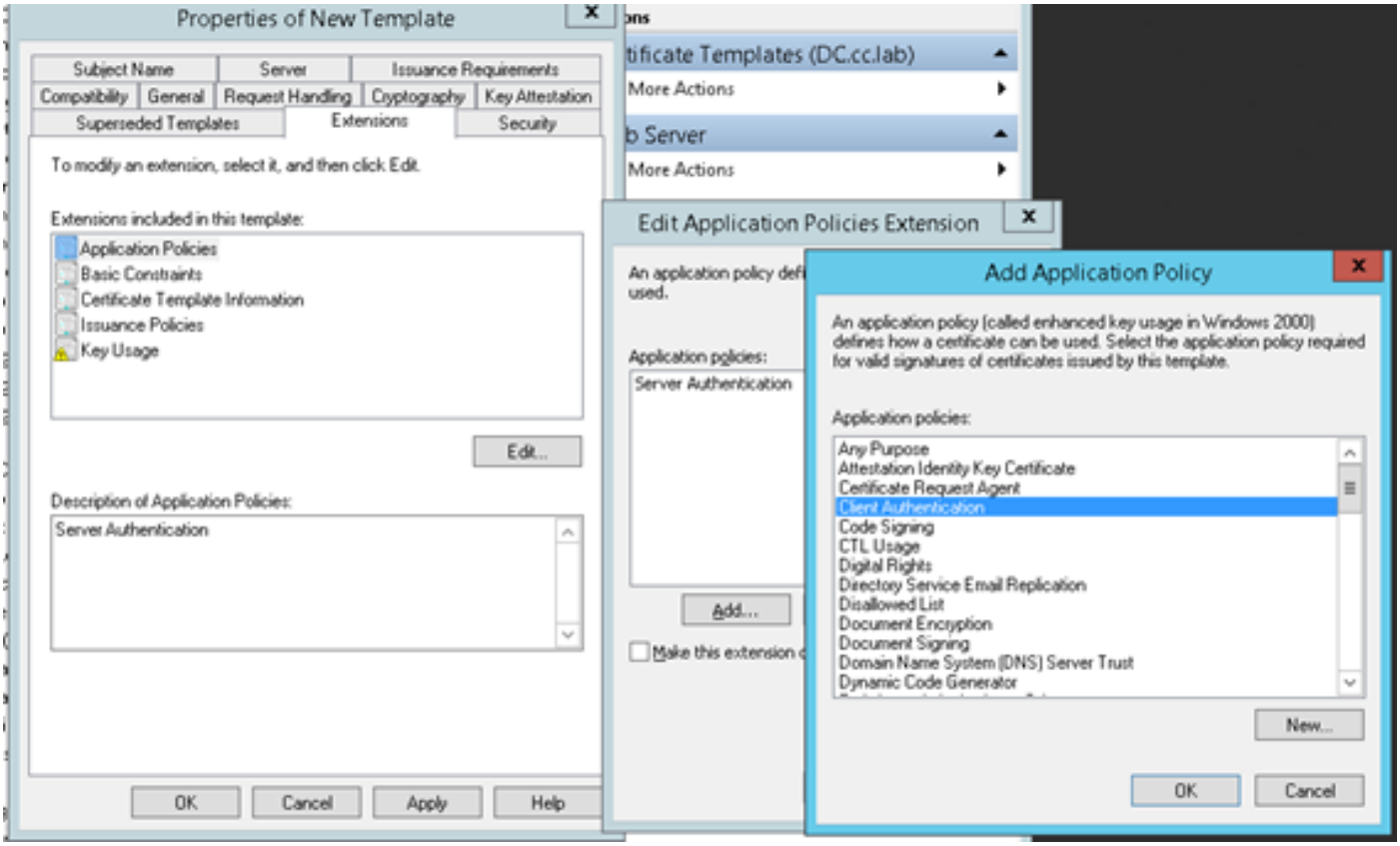
호스트 인증서 및 키는 C:\icm\ssl\certs 및 **C:\icm\ssl\keys**에 **저장됩니다**.

2단계. C:\icm\ssl\certs 폴더로 이동하고 **host.csr** 파일**이** 생성되었는지 확인합니다.

CSR 인증서 가져오기 CA에서 서명

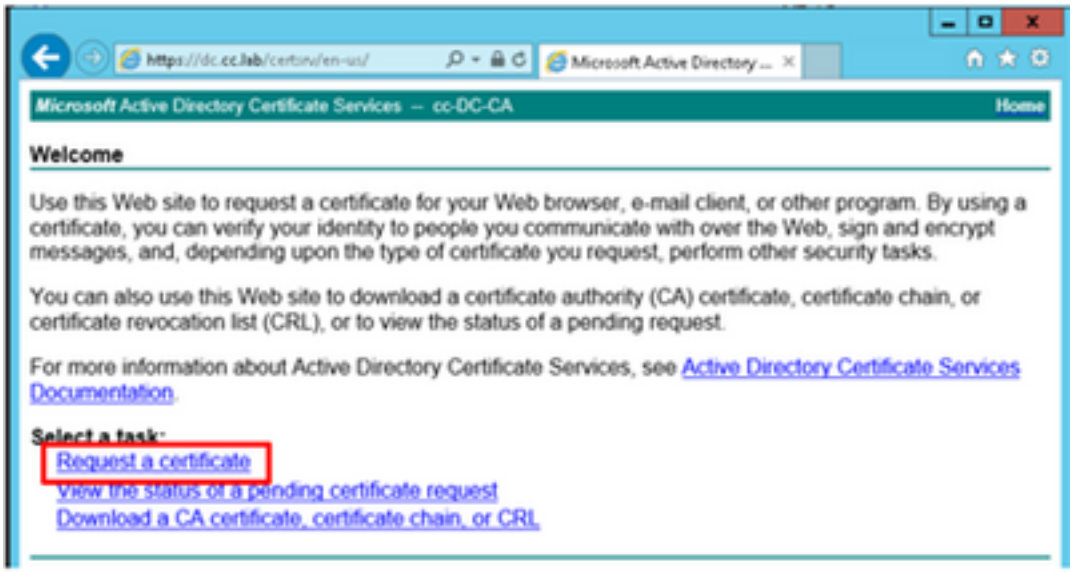
CSR 인증서가 생성된 후에는 서드파티 CA에서 서명해야 합니다.이 연습에서는 도메인 컨트롤러에 설치된 Microsoft CA가 서드파티 CA로 사용됩니다.

Microsoft CA를 사용할 때 이미지에 표시된 대로 CA에서 사용하는 인증서 템플릿에 클라이언트 및 서버 인증이 포함되어 있는지 확인합니다.

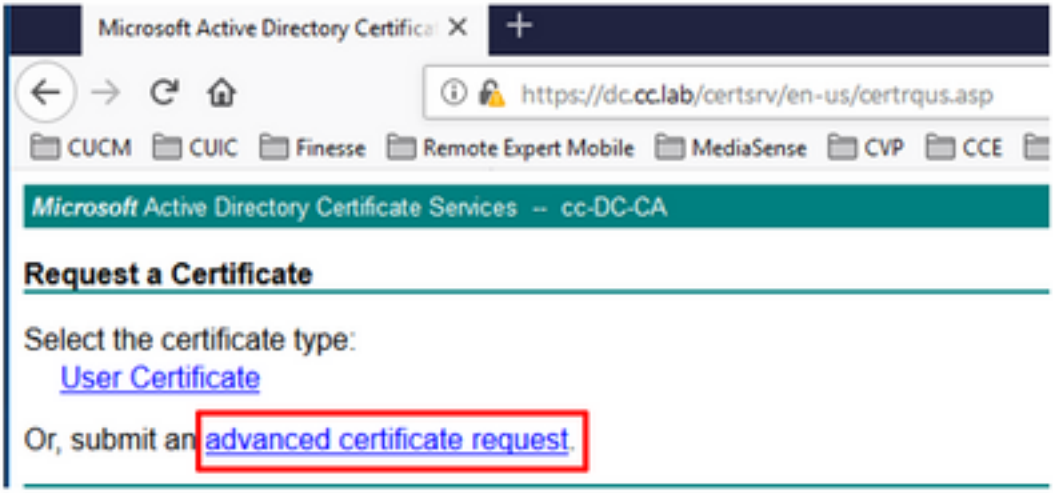


1단계. 웹 브라우저를 열고 CA로 이동합니다.

2단계. **Microsoft Active Directory 인증서 서비스**에서 **인증서 요청**을 선택합니다.

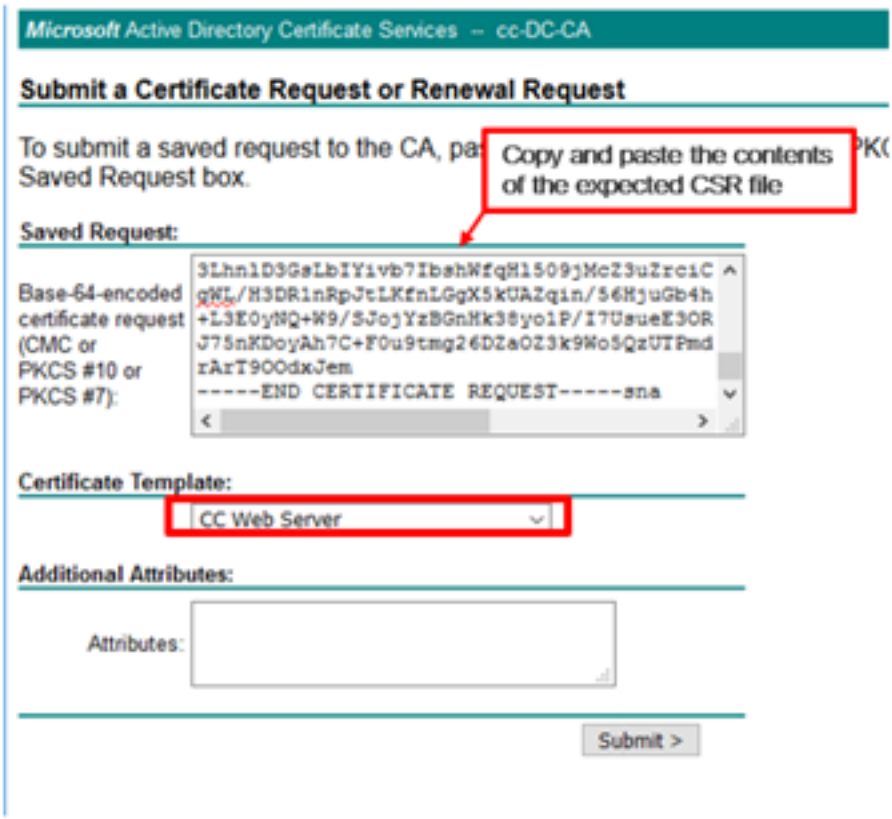


3단계. **고급 인증서 요청** 옵션을 선택합니다.



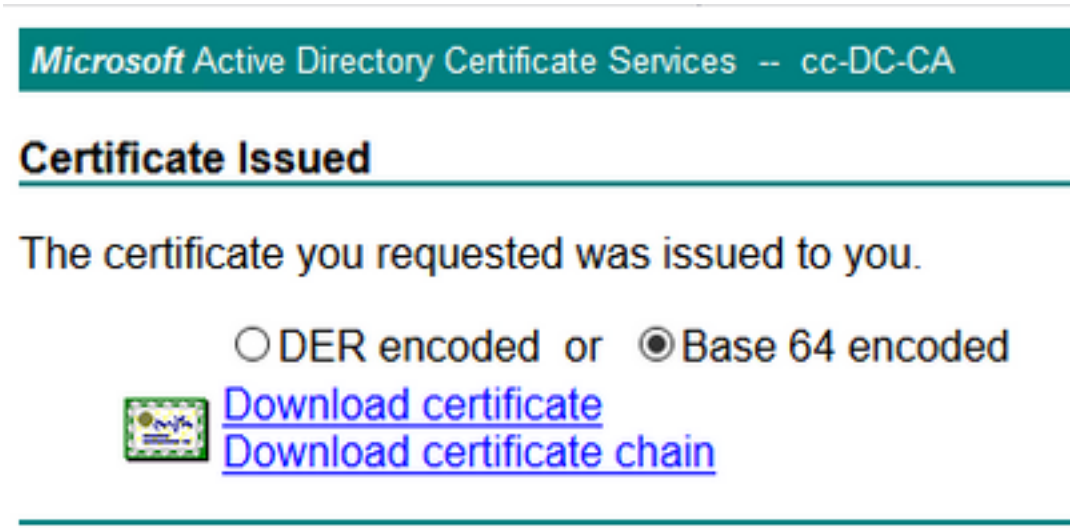
4단계. **고급 인증서 요청**에서 PG 에이전트 CSR 인증서의 내용을 Saved Request(**저장된 요청)** 상자에 복사하여 붙여넣습니다.

5단계. 클라이언트 및 서버 인증이 있는 **웹 서버** 템플릿을 선택합니다.Lab에서 CC Web Server 템플릿은 클라이언트 및 서버 인증으로 생성되었습니다.



6단계. Submit(제출)을 **클릭합니다**.

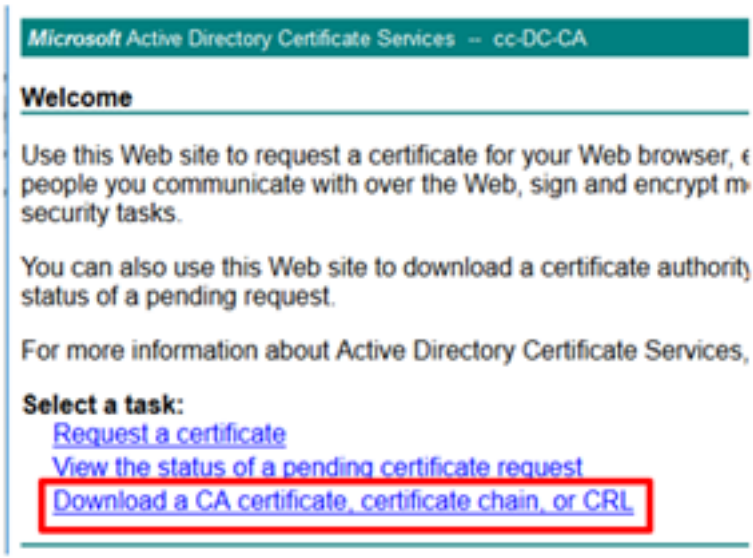
7단계. **Base 64 인코딩**을 선택하고 이미지에 표시된 **Download Certificate(인증서 다운로드**)를 클릭합니다.



8단계. 파일을 저장하고 **확인**을 클릭합니다.파일이 **다운로드** 폴더에 저장됩니다.

9단계. 파일의 이름을 host.**cer**(선택 사항)로 바꿉니다.

10단계. 루트 인증서도 생성해야 합니다.CA 인증서 페이지로 돌아간 다음 **Download a CA certificate, certificate chain or CRL(CA 인증서, 인증서 체인 또는 CRL 다운로드)을** 선택합니다.루트 인증서는 모든 서버(PG 에이전트 및 Finesse)에서 동일하므로 이 단계를 한 번만 수행하면 됩니다.



11단계. Base **64**를 클릭하고 **CA 인증서 다운로드**를 선택합니다.

12단계. [파일 저장]을 클릭하고 [확인]을 **선택합니다**.파일이 기본 위치인 Downloads(다운로드)에 **저장됩니다**.

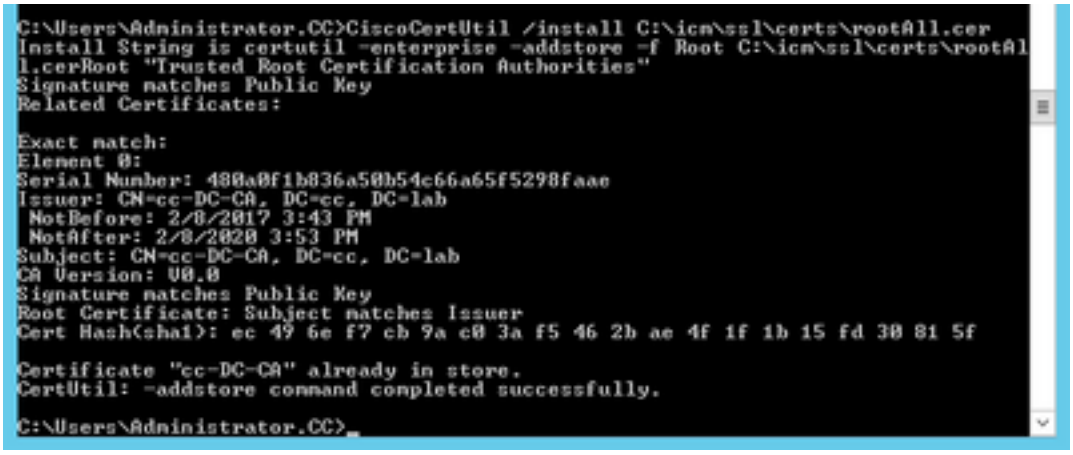
CCE PG CA 서명 인증서 가져오기

1단계. PG 에이전트에서 **C:\icm\ssl\certs**으로 이동하여 루트와 PG 에이전트 서명 파일을 여기에 붙여넣습니다.

2단계. c:\icm\ssl\certs 에서 host.pem 인증서를 **selfhost.pem**으로 **바꿉니다**.

3단계. host.cer의 이름을 c:\icm\ssl\certs 폴더에서 host.pem으로 **바꿉니다**.

4단계. 루트 인증서를 설치합니다.명령 프롬프트에서 다음 명령을 실행합니다. CiscoCertUtil **/install C:\icm\ssl\certs\rootAll.cer**



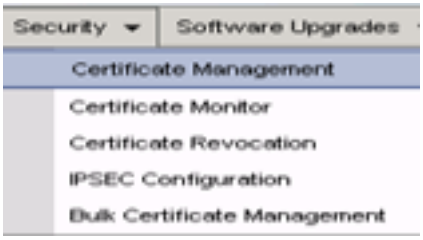
5단계. 동일한 명령을 실행하는 응용 프로그램 서명 인증서를 설치합니다.**CiscoCertUtil /install C:\icm\ssl\certs\host.pem**

6단계. PG를 순환합니다.Unified CCE 서비스 제어를 열고 Cisco ICM 에이전트 PG를 순환합니다.

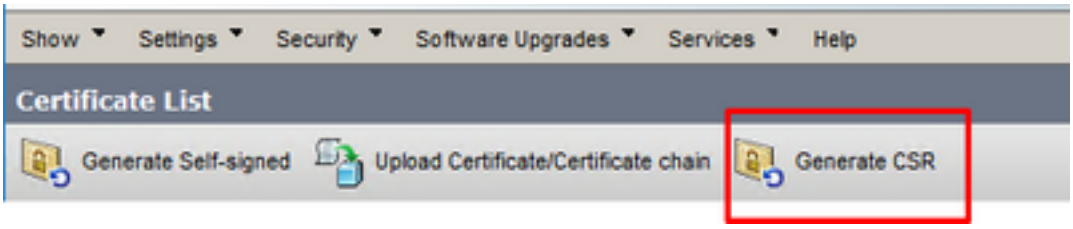
Finesse 인증서 생성

1단계. 웹 브라우저를 열고 Finesse **OS Admin으로 이동합니다**.

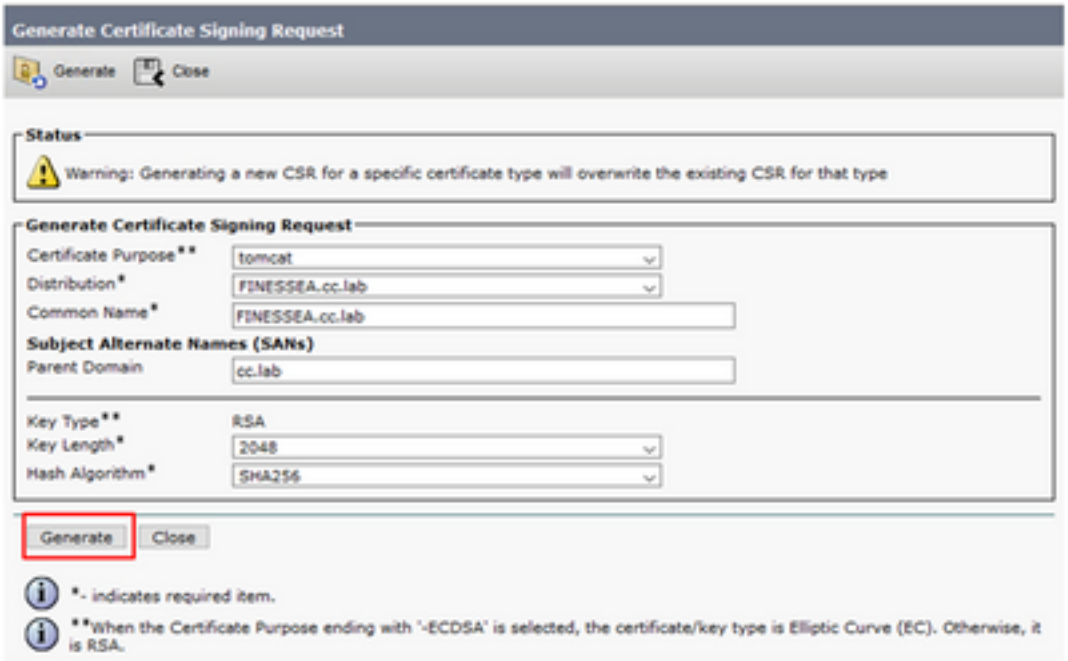
2단계. OS 관리자 자격 증명으로 로그인하고 이미지에 표시된 대로 **Security > Certificate Management**로 이동합니다.



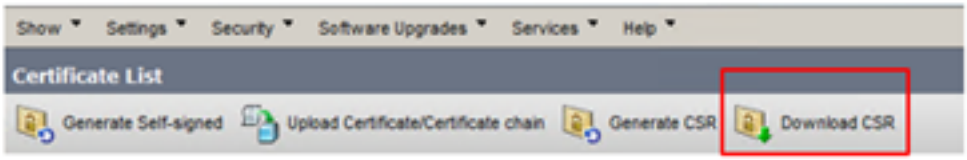
3단계. 이미지**에** 표시된 대로 Generate CSR(CSR 생성)을 클릭합니다.



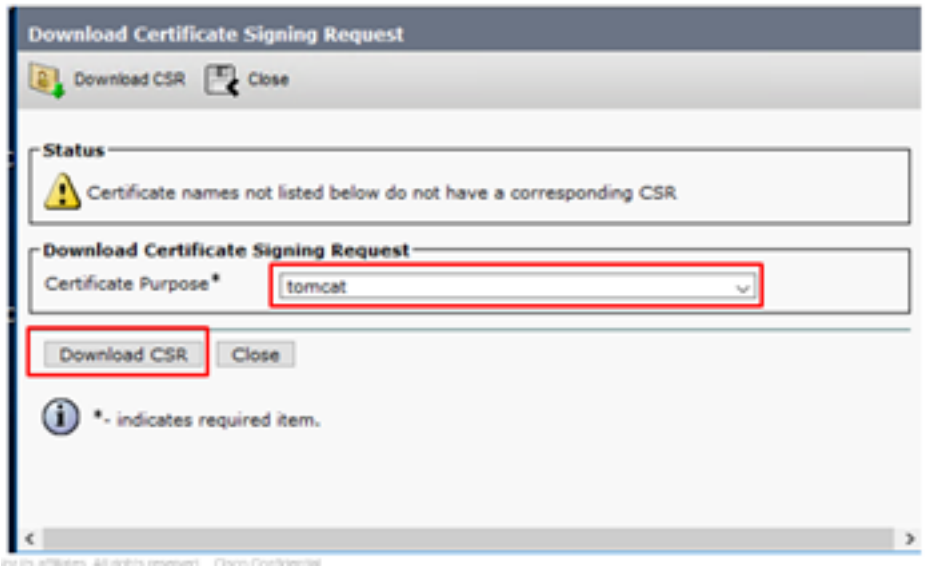
4단계. **Generate Certificate Signing Request(인증서 서명 요청 생성)**에서 기본값을 사용하고 Generate(생성)를 **클릭합니다.**



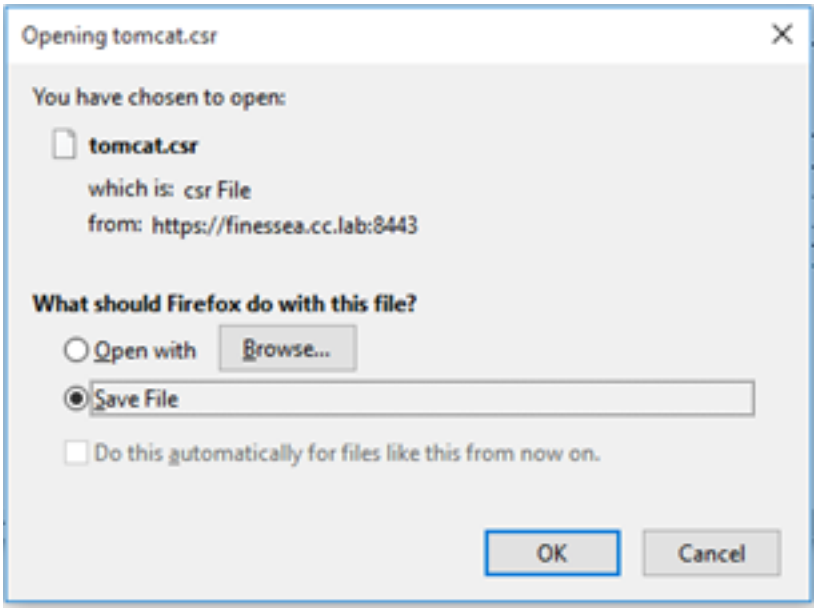
5단계. Generate Certificate **Signing Request(인증서 서명 요청 생성)** 창을 닫고 Download CSR(CSR **다운로드)을 선택합니다**.



6단계. Certificate Purpose(인증서 용도)에서 tomcat을 선택하고 **Download CSR(CSR 다운로드)을 클릭합니다**.



7단계. **Save File(파일 저장)**을 선택하고 이미지에 표시된 대로 **OK(확인)**를 클릭합니다.



8단계. **Download Certificate Signing Request(인증서 서명 요청 다운로드)** 창을 닫습니다.인증서가 기본 위치**(This PC > Downloads)에 저장됩니다**.

9단계. Windows 탐색기를 열고 해당 폴더로 이동합니다.이 인증서를 마우스 오른쪽 단추로 클릭하고 이름을 바꿉니다.**finestetomcat.csr**

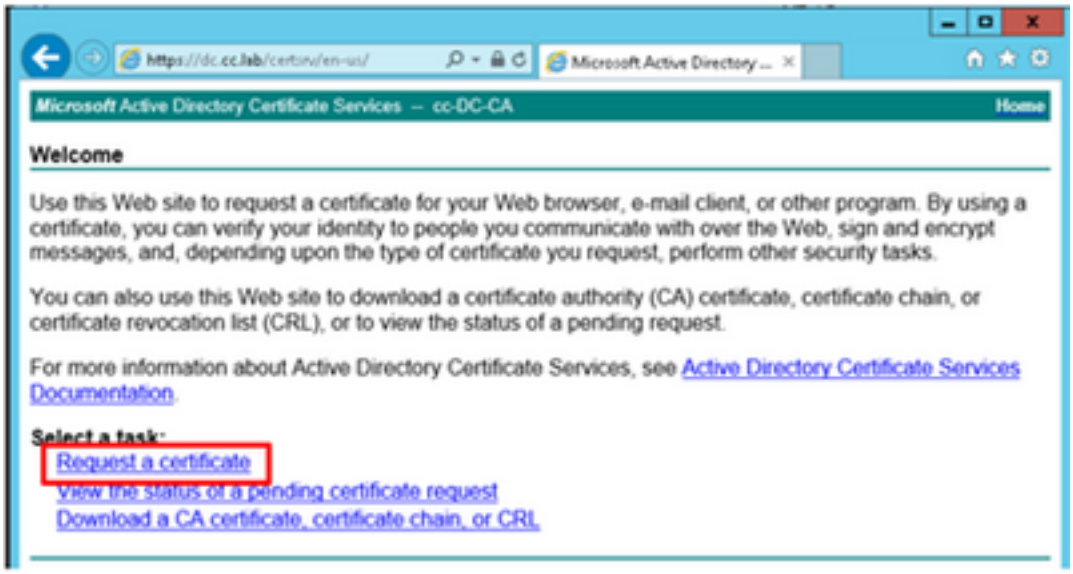
CA에서 Finesse 인증서 서명

이 섹션에서는 이전 단계에서 사용한 것과 동일한 Microsoft CA가 서드파티 CA로 사용됩니다.

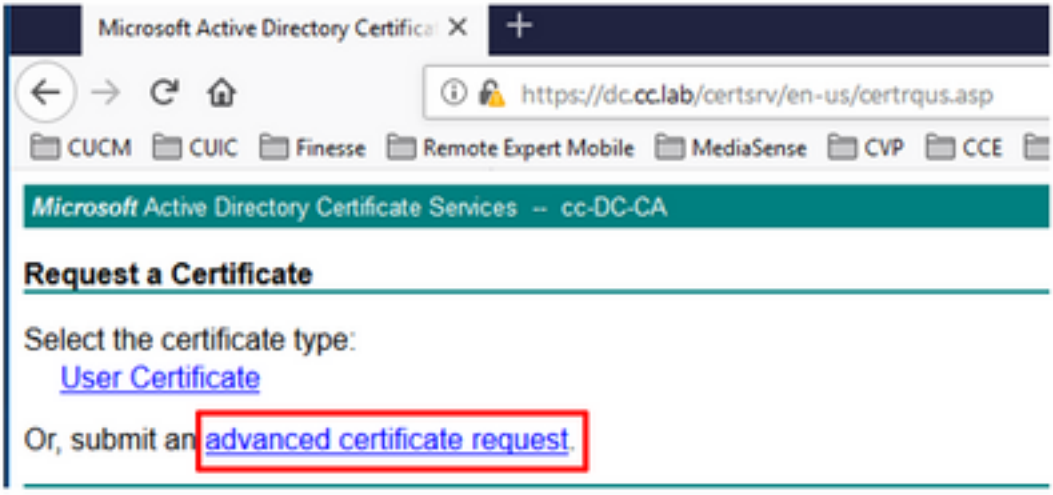
참고: CA에서 사용하는 인증서 템플릿에 클라이언트 및 서버 인증이 포함되어 있는지 확인합니다.

1단계. 웹 브라우저를 열고 CA로 이동합니다.

2단계. **Microsoft Active Directory 인증서 서비스**에서 **인증서 요청**을 선택합니다.

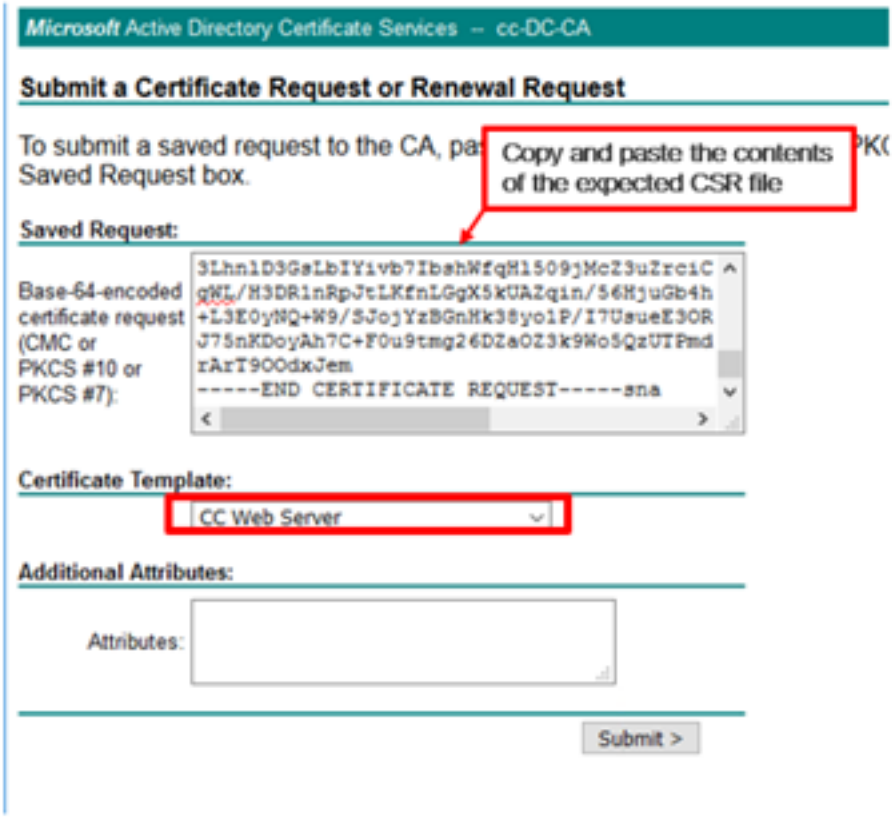


3단계. 이미지에 표시된 대로 **고급 인증서 요청** 옵션을 선택합니다.



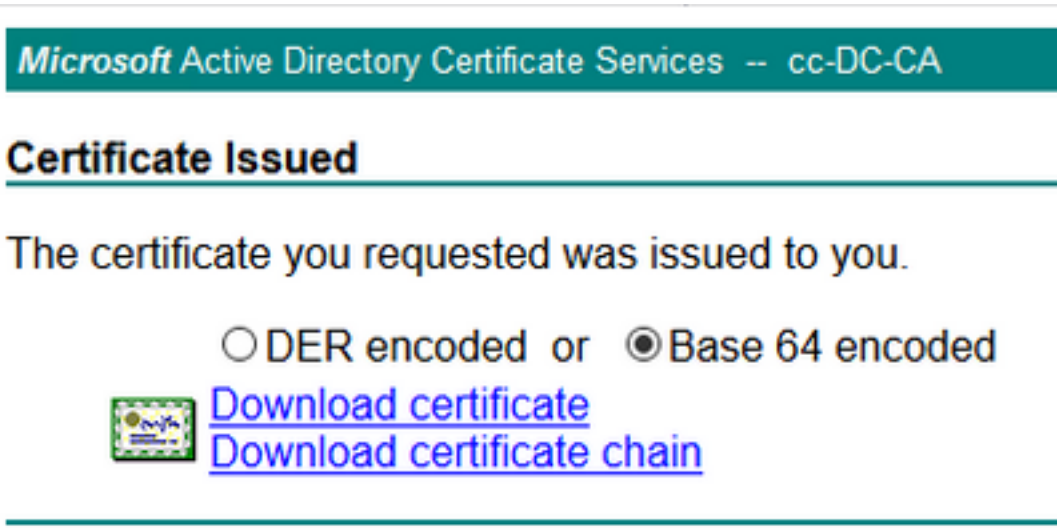
4단계. **고급 인증서 요청**에서 Finesse CSR 인증서의 내용을 Saved Request(**저장된 요청**) 상자에 복사하여 붙여넣습니다.

5단계. 클라이언트 및 서버 인증이 있는 웹 서버 템플릿을 선택합니다.이 Lab에서는 클라이언트 및 서버 인증을 사용하여 CC 웹 서버 템플릿을 만들었습니다.



6단계. Submit(제출)을 **클릭합니다**.

7단계. **Base 64 인코딩**을 선택하고 이미지에 표시된 **인증서 다운로드**를 클릭합니다.



8단계. 파일을 저장하고 **확인**을 클릭합니다.파일이 **다운로드** 폴더에 저장됩니다.

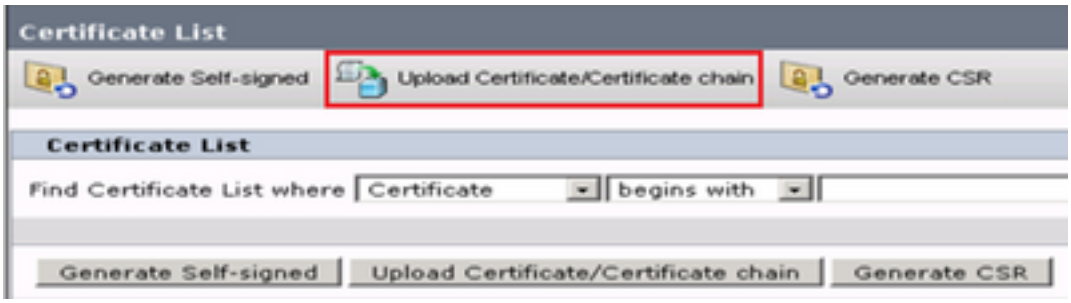
9단계. 파일의 이름을 finesse.**cer로 바꿉니다**.

Finesse 애플리케이션 및 루트 서명 인증서 가져오기

1단계. 웹 프로세서에서 Finesse **OS Admin** 페이지를 열고 **Security > Certificate Management**로 **이동합니다**.

2단계. 이미지에 표시된 대로 **Upload Certificate/Certificate chain(인증서/인증서 체인 업로드)** 버튼

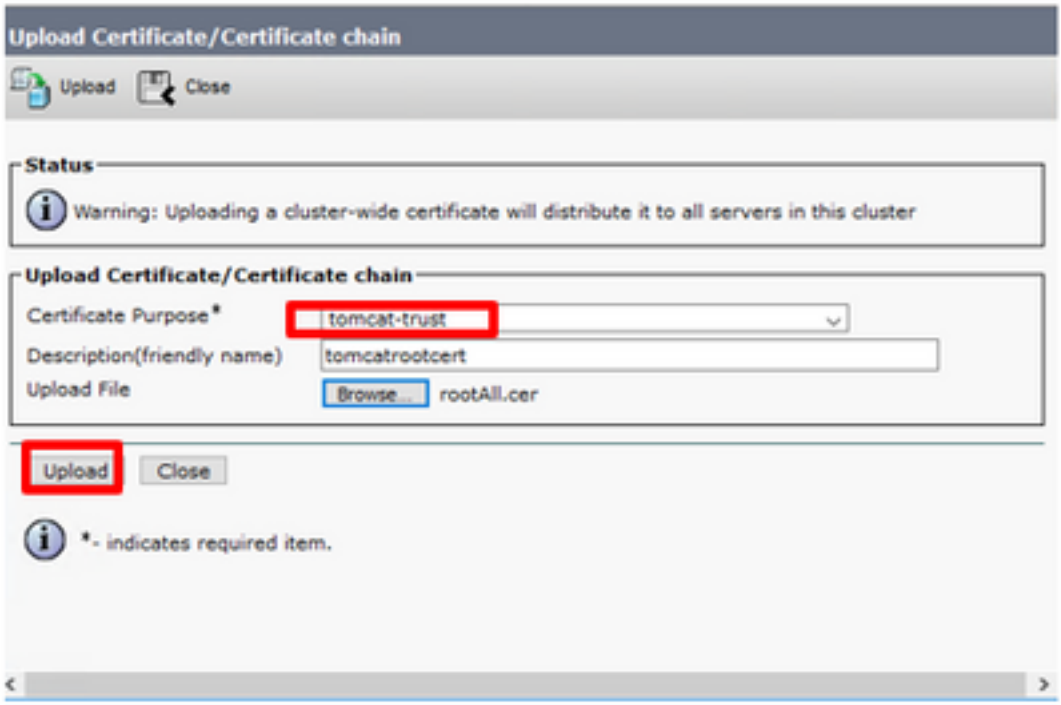
을 클릭합니다.



3단계. 팝업 창에서 Certificate Purpose(인증서 용도)를 **위해 tomcat-trust를 선택합니다**.

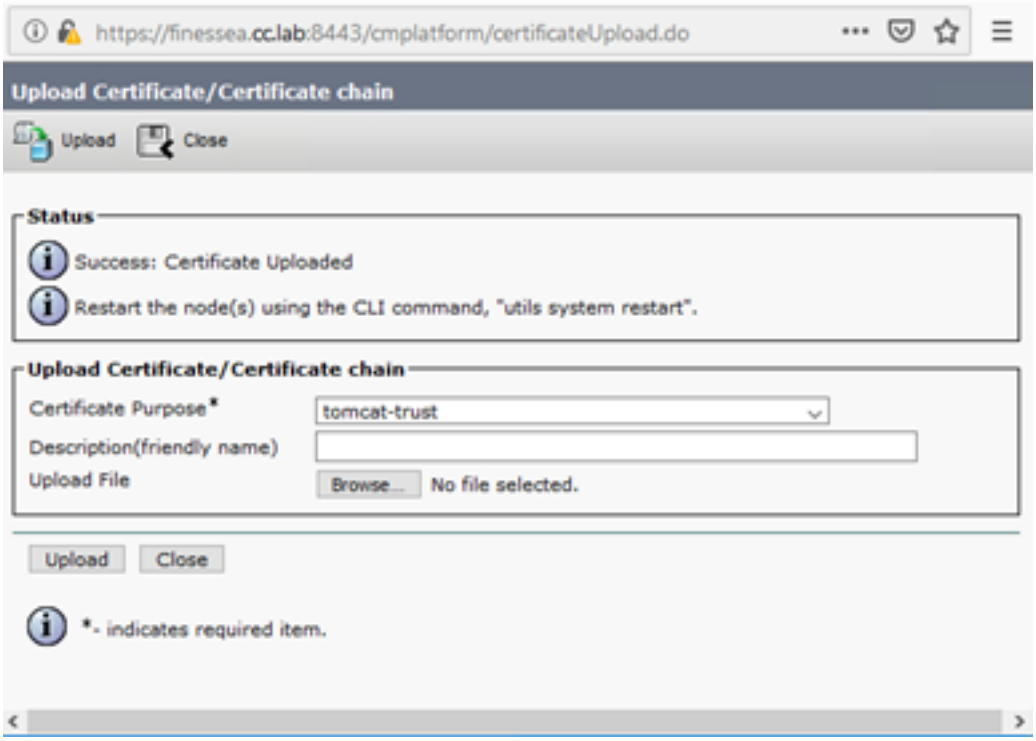
4단계. Browse.. 버튼을 클릭하고 가져올 루트 인증서 파일을 선택합니다.그런 다음 **열기** 버튼을 클릭합니다.

5단계. 설명에서 tomcatrootcert와 같은 내용을 **기록하고**, 이미지에 표시된 대로 **Upload** 버튼을 클릭합니다.

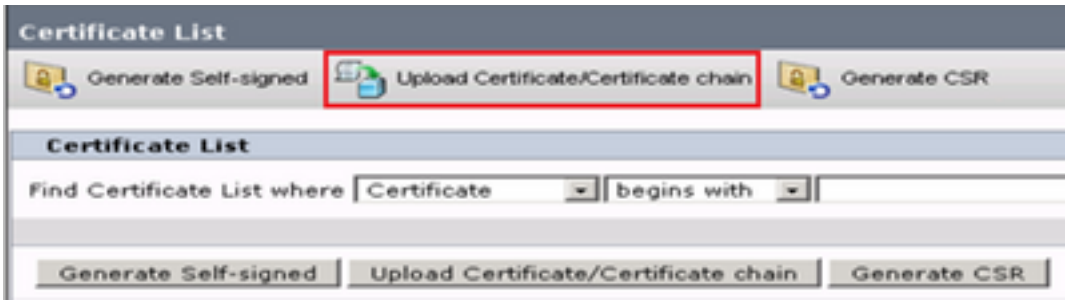


6단계. **성공**이 표시될 때까지 기다립니다.**Certificate Uploaded** 메시지를 표시하여 창을 닫습니다.

시스템을 다시 시작하라는 메시지가 표시되지만, 먼저 Finesse 애플리케이션 서명 인증서 업로드를 계속한 다음 시스템을 다시 시작할 수 있습니다.



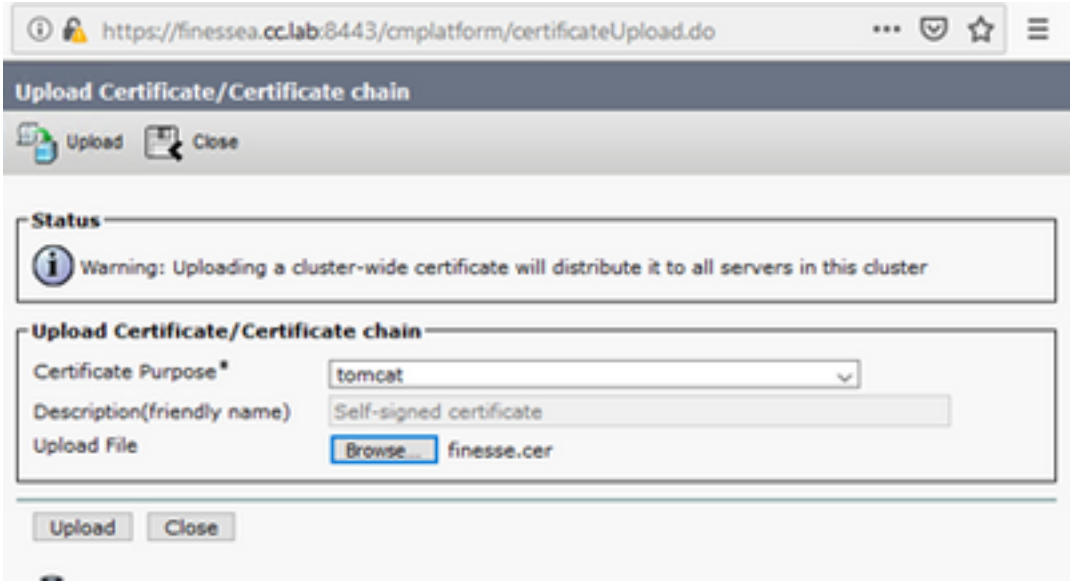
7단계. Finesse 애플리케이션 인증서를 가져오려면 Upload **Certificate/Certificate chain(인증서/인증서 체인 업로드**) 버튼을 더 길게 클릭합니다.



8단계. 팝업 창에서 Certificate Purpose(**인증서 용도**)를 선택합니다.

9단계. Browse.. 버튼을 클릭하고 Finesse CA 서명 파일 finesse.cer를 **선택합니다**.그런 다음 **열기** 버튼을 클릭합니다.

10단계. **Upload** 버튼을 클릭합니다.



11단계. **성공**이 표시될 때까지 기다립니다.**인증서 업로드됨** 메시지

다시 한 번 시스템 재시작을 요청합니다.창을 닫고 시스템을 다시 시작합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.