전화 마이그레이션을 위한 CUCM 클러스터 간 벌크 인증서 관리 절차

목차

소개

이 문서에서는 전화 마이그레이션을 위해 Cisco CUCM(Unified Communications Manager) 클러스터 간 대량 인증서 관리를 위한 방법 절차를 제공합니다.

기고자: Cisco TAC 엔지니어 Adrian Esquillo

> **참고:**이 절차는 CUCM 릴리스 12.5(1)용 관리 설명서의 벌크 인증서 관리 섹션에서도 간략하게 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.
·SFTP(Secure File Transfer Protocol) 서버
·CUCM 인증서

사용되는 구성 요소

·이 문서의 정보는 CUCM 10.X를 기반으로 합니다.

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

배경 정보

Bulk Certificate Management에서는 CUCM 클러스터 간에 인증서 집합을 공유할 수 있습니다.이 단계는 EMCC(Extension Mobility Cross Cluster)와 같은 개별 클러스터 간에 신뢰를 설정해야 하는 개별 클러스터의 시스템 기능과 클러스터 간 전화 마이그레이션에 대한 요구 사항입니다.

절차의 일부로 클러스터의 모든 노드에서 인증서를 포함하는 PKCS12(Public Key Cryptography Standards #12) 파일이 생성됩니다.모든 클러스터는 동일한 SFTP 서버의 동일한 SFTP 디렉토리로 인증서를 내보내야 합니다.소스 및 대상 클러스터의 CUCM 게시자에서 벌크 인증서 관리 컨피그레이션을 수동으로 수행해야 합니다.마이그레이션할 전화기가 두 클러스터에 모두 연결되도록 소스 및 대상 클러스터가 작동 및 작동해야 합니다.소스 클러스터 전화기가 대상 클러스터로 마이그레이션됩니다.

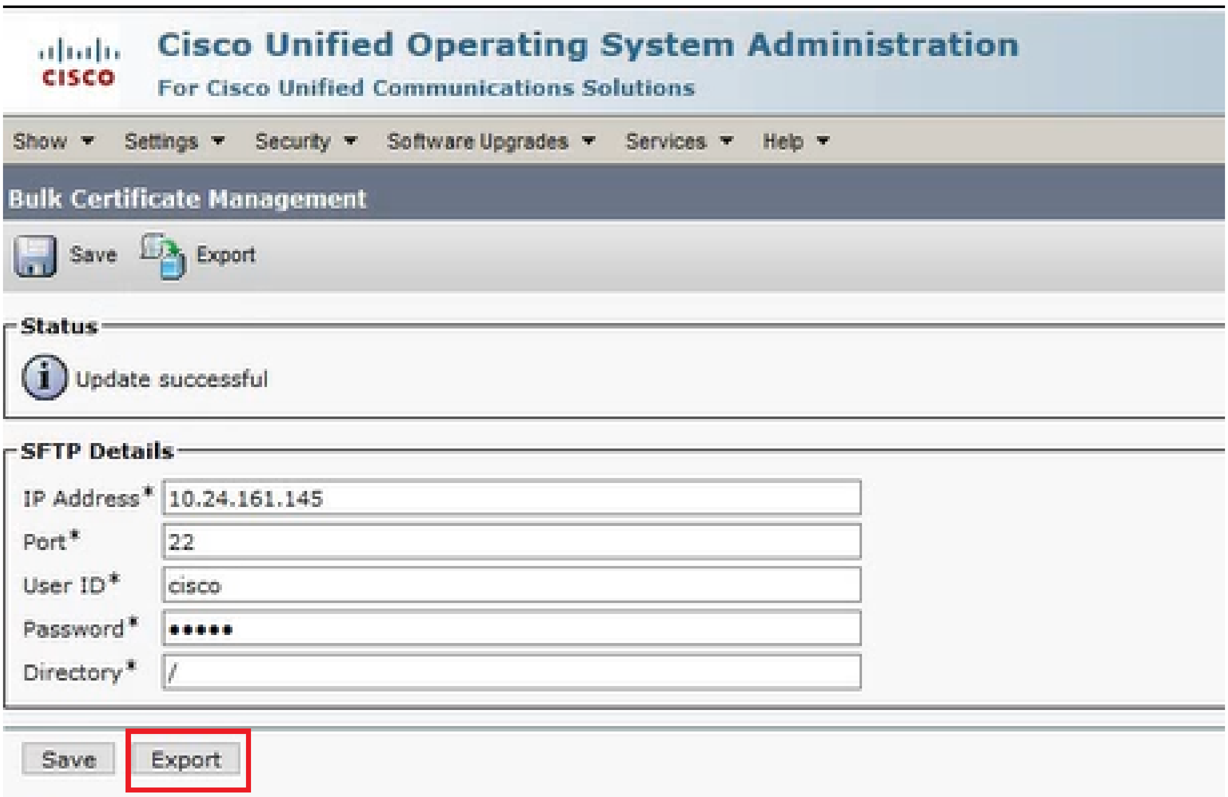
대량 인증서 관리 절차

대상 클러스터 인증서 내보내기

1단계. 대상 클러스터의 CUCM 게시자에서 대량 인증서 관리를 위한 SFTP 서버를 구성합니다.

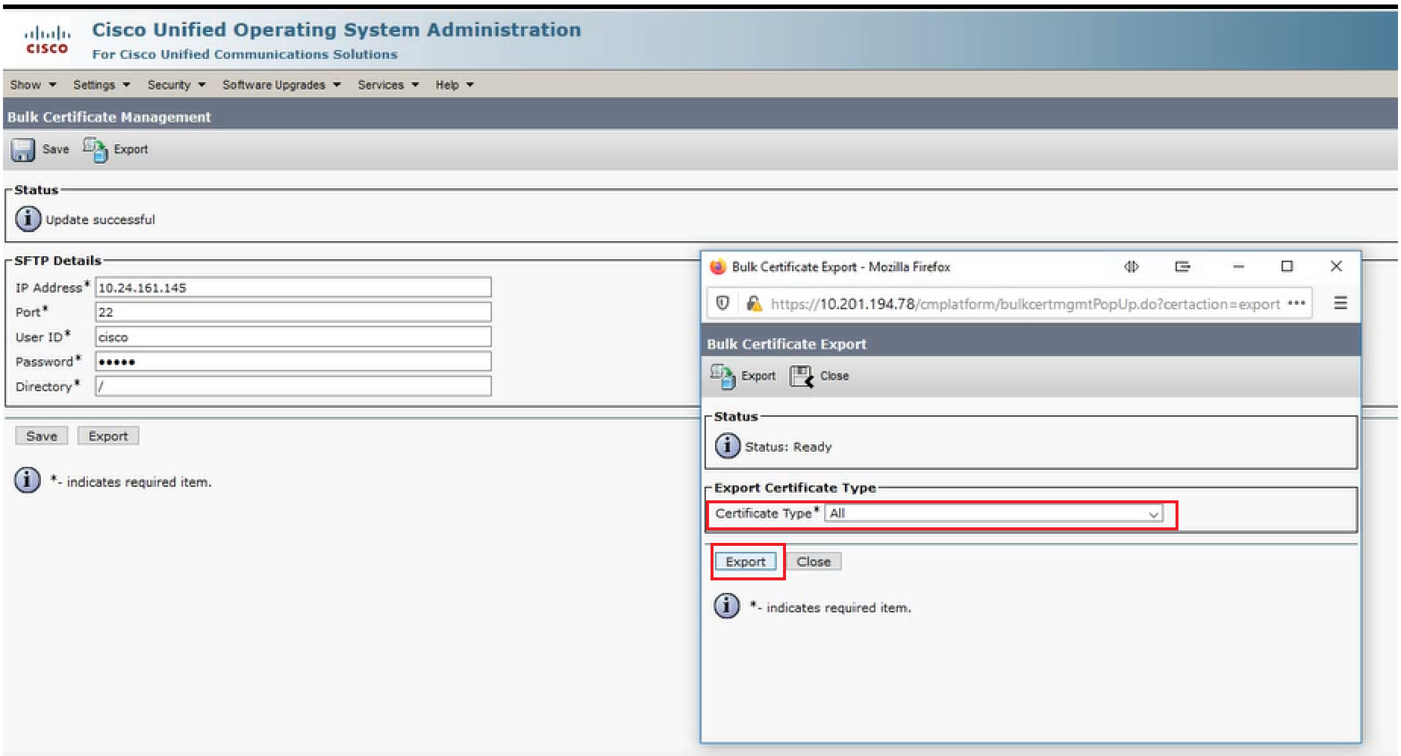
이 예에서는 대상 클러스터 CUCM 버전이 11.5.1입니다.

·**Cisco Unified OS 관리(Cisco Unified OS Administration) > Security(보안) > Bulk Certificate Management(대량 인증서 관리)**로 이동하여 SFTP 서버 세부 정보를 입력하고 이미지에 표시된 대로 Export(내보내기)를 **클릭합니다**.

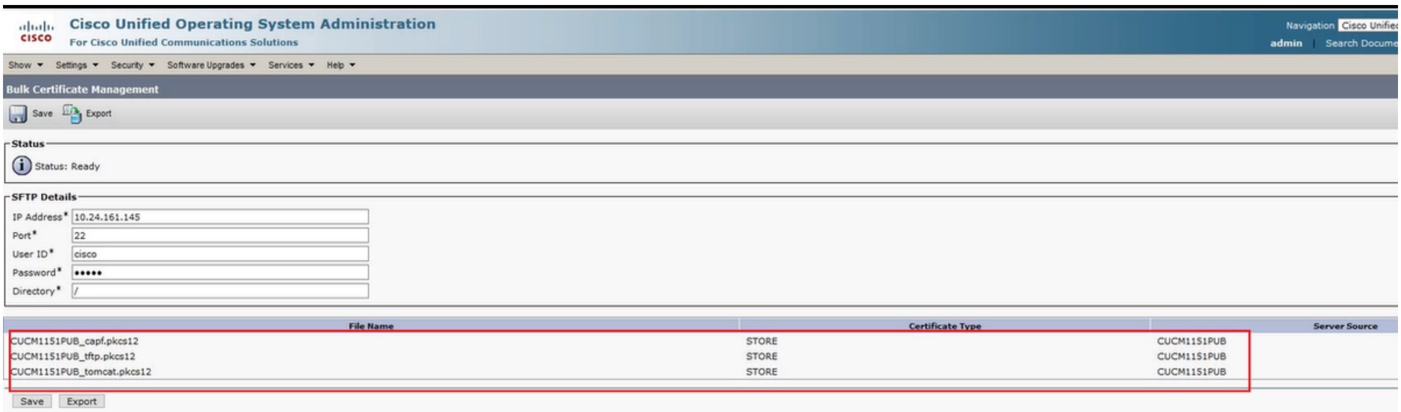


2단계. 대상 클러스터의 모든 노드에서 SFTP 서버로 모든 인증서를 내보냅니다.

·후속 팝업 창에서 Certificate Type(인증서 유형)에 대해 **All(모두)**을 선택한 다음 **Export(내보내기)**를 클릭합니다(이미지에 표시됨).



·팝업 창을 닫고 대상 클러스터의 각 노드에 대해 생성된 PKCS12 파일을 사용하여 Bulk Certificate Management(대량 인증서 관리)를 업데이트합니다. 웹 페이지는 이미지에 표시된 대로 이 정보로 새로 고쳐집니다.



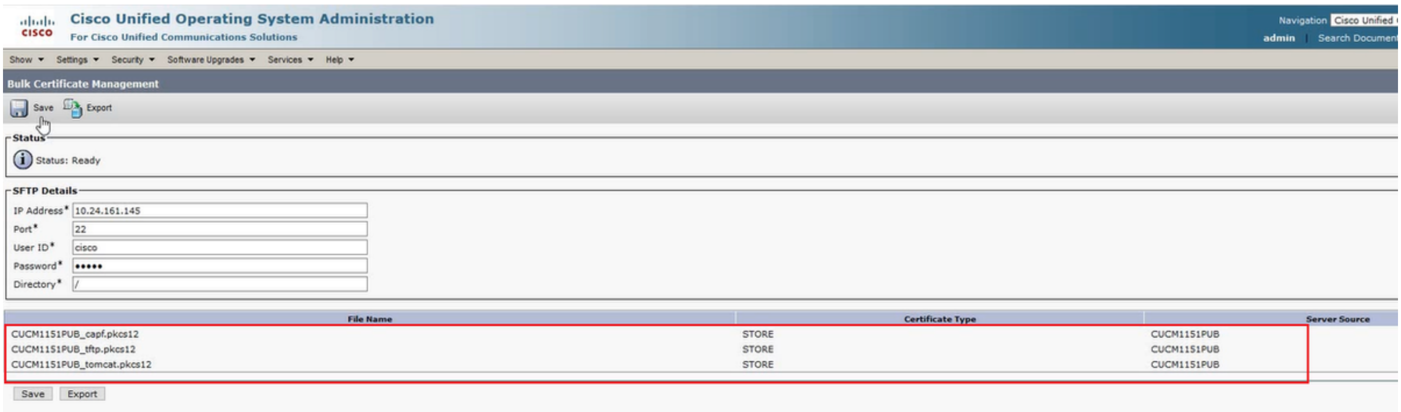
소스 클러스터 인증서 내보내기

1단계. 소스 클러스터의 CUCM 게시자에서 대량 인증서 관리를 위한 SFTP 서버를 구성합니다.

이 예에서는 소스 클러스터 CUCM 버전이 10.5.2입니다.

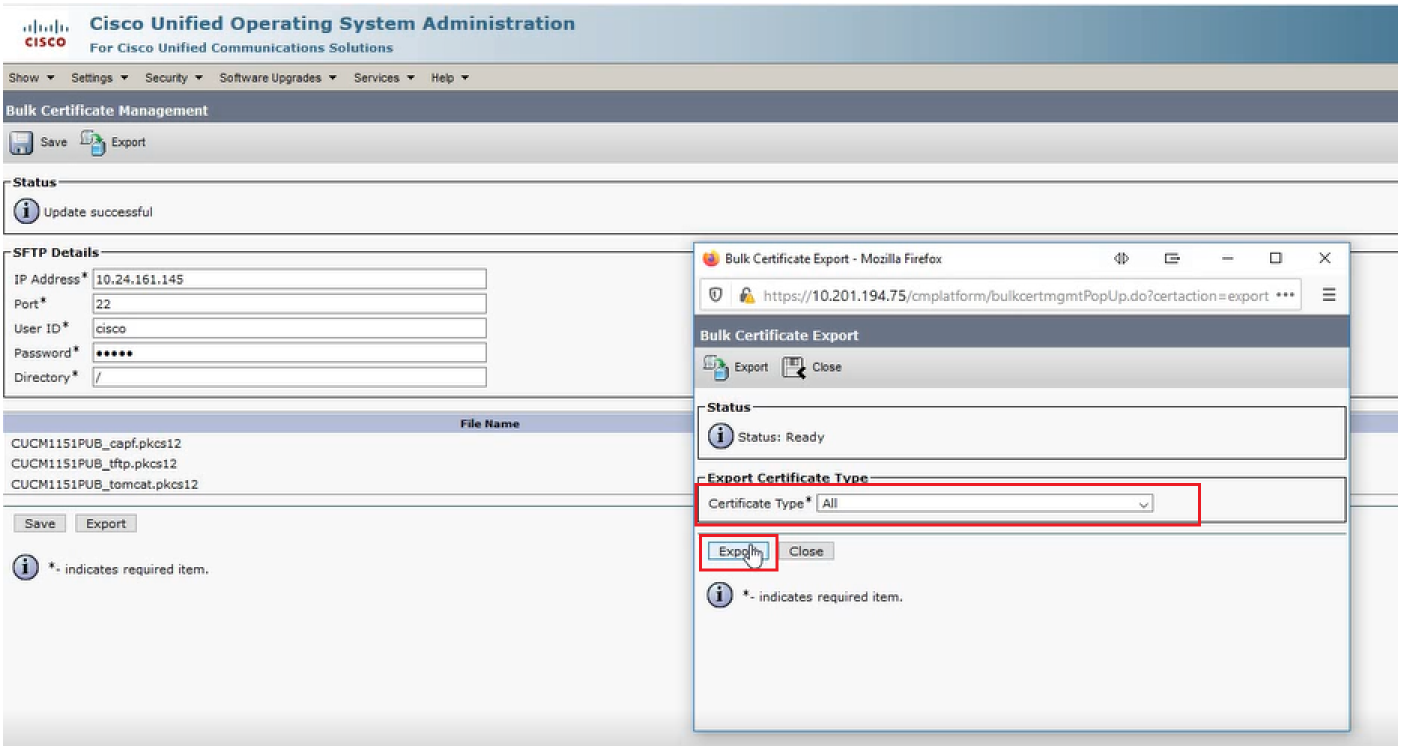
·**Cisco Unified OS 관리(Cisco Unified OS Administration) > Security(보안) > Bulk Certificate Management(대량 인증서 관리)**로 이동하여 SFTP 서버 세부 정보를 입력하고 이미지에 표시된 대로 Export(내보내기)를 **클릭합니다**.

참고:대상 클러스터에서 SFTP 서버로 내보낸 PKCS12 파일은 액세스 시 소스 클러스터 CUCM 게시자의 Bulk Certificate Management 웹 페이지에 표시됩니다.

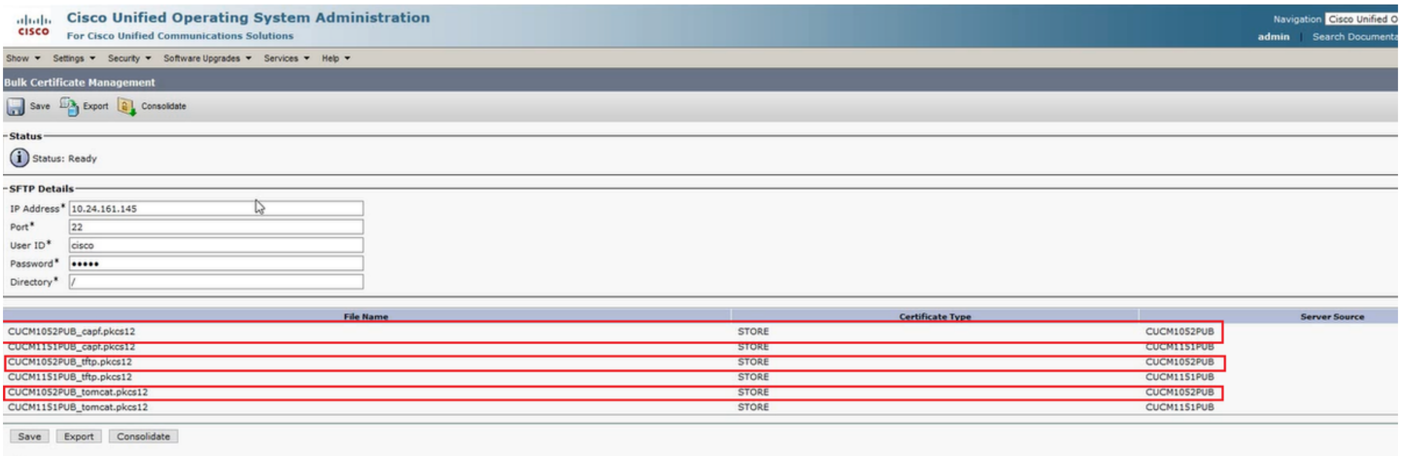


2단계. 소스 클러스터의 모든 노드에서 SFTP 서버로 모든 인증서를 내보냅니다.

·후속 팝업 창에서 Certificate Type(인증서 유형)에 대해 **All(모두)**을 선택한 다음 **Export(내보내기)**를 클릭합니다(이미지에 표시됨).



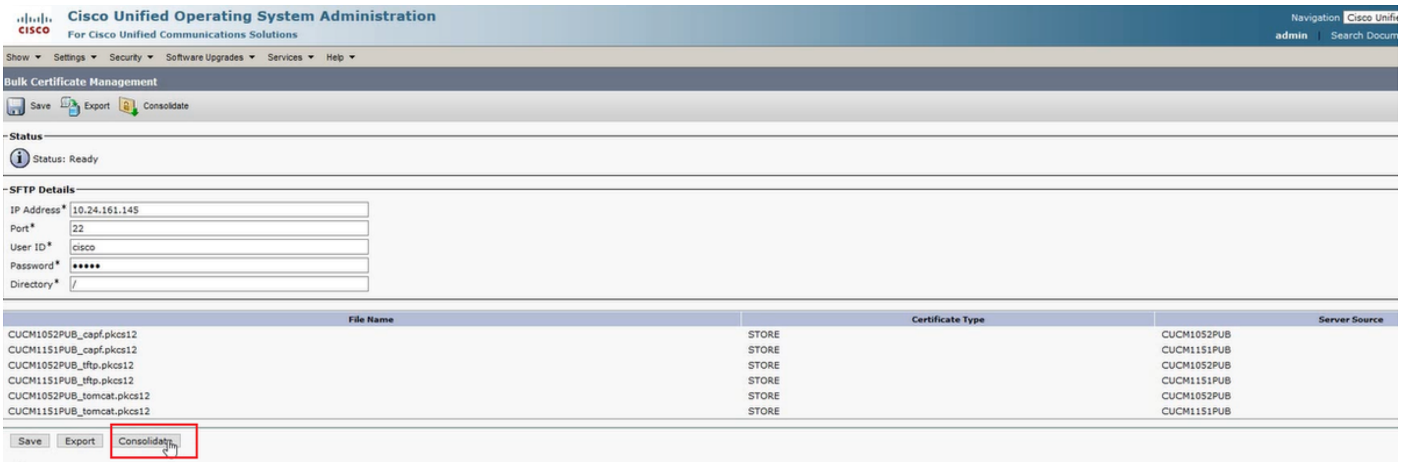
·팝업 창을 닫고 소스 클러스터의 각 노드에 대해 생성된 PKCS12 파일을 사용하여 Bulk Certificate Management(대량 인증서 관리) 업데이트를 실행하면 웹 페이지가 이 정보로 새로 고쳐집니다.소스 클러스터의 Bulk Certificate Management에 대한 웹 페이지에는 이제 이미지에 표시된 것처럼 SFTP로 내보낸 소스 및 대상 PKCS12 파일이 모두 표시됩니다.



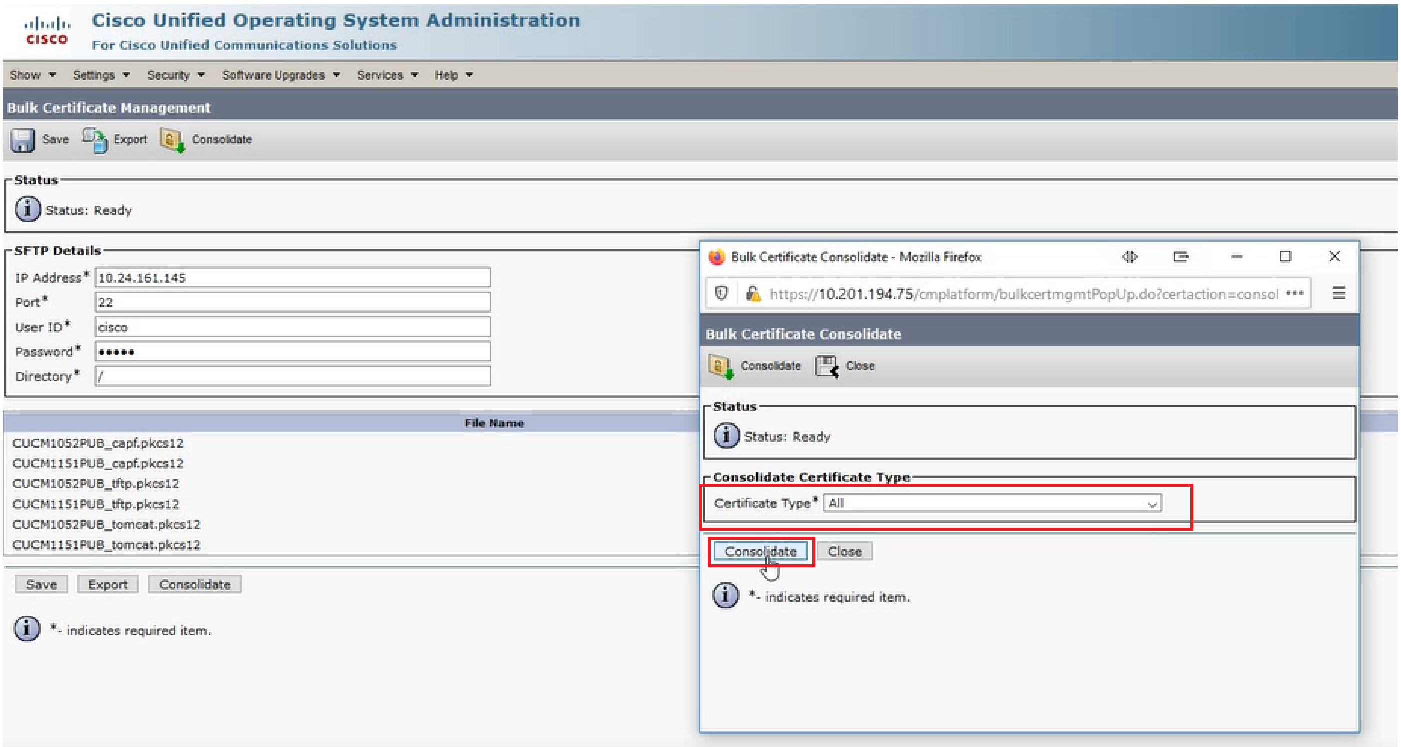
소스 및 대상 PKCS12 파일 통합

> **참고:**Bulk Certificate Management 내보내기는 소스 및 대상 클러스터 모두에서 수행되는 반면, 통합은 클러스터 중 하나에서만 CUCM 게시자를 통해 수행됩니다.

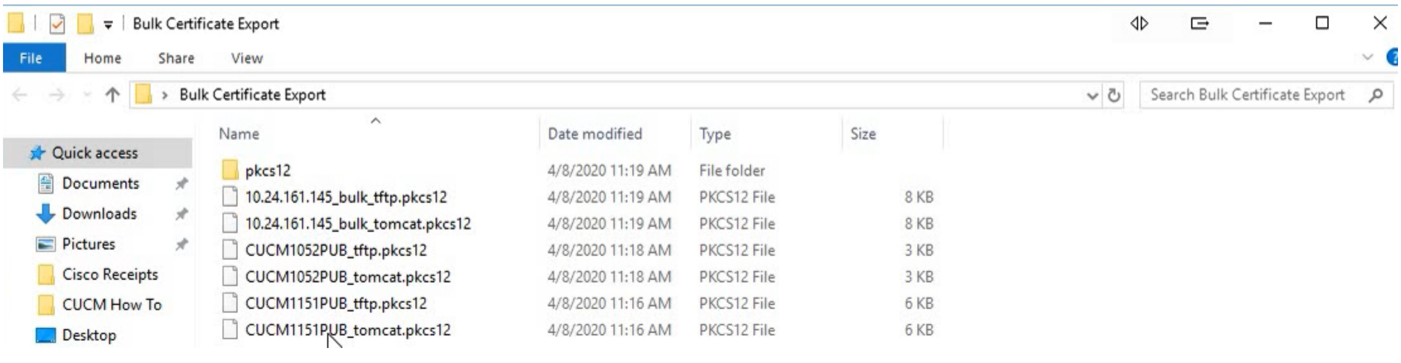
1단계. 소스 클러스터의 CUCM 게시자의 Bulk Certificate Management 페이지로 돌아가서 이미지에 표시된 대로 Consolidate(통합)를 **클릭합니다**.

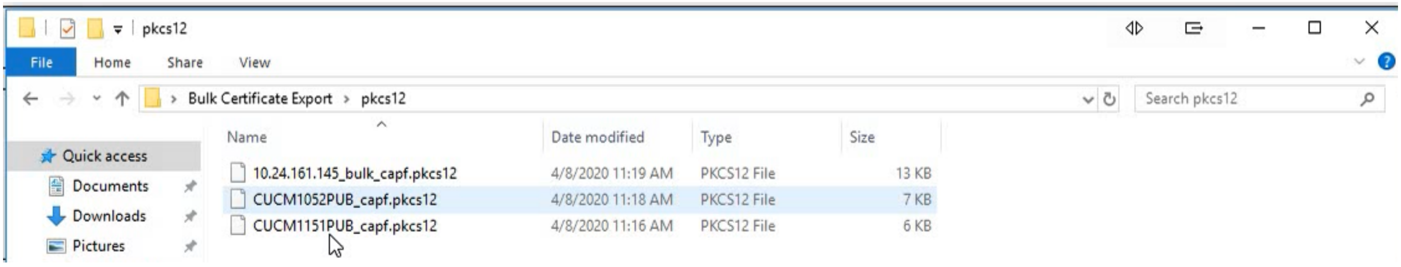


·후속 팝업 창에서 Certificate Type(인증서 유형)에 대해 **All(모두)**을 선택한 다음 **Consolidate(통합)**를 클릭합니다.



· 언제든지 SFTP 디렉토리를 확인하여 소스 및 대상 클러스터에 모두 포함된 pkcs12 파일을 확인할 수 있습니다.이미지에 표시된 대로, 대상 및 소스 클러스터에서 모든 인증서를 내보낸 후 SFTP 디렉토리의 내용이 완료되었습니다.

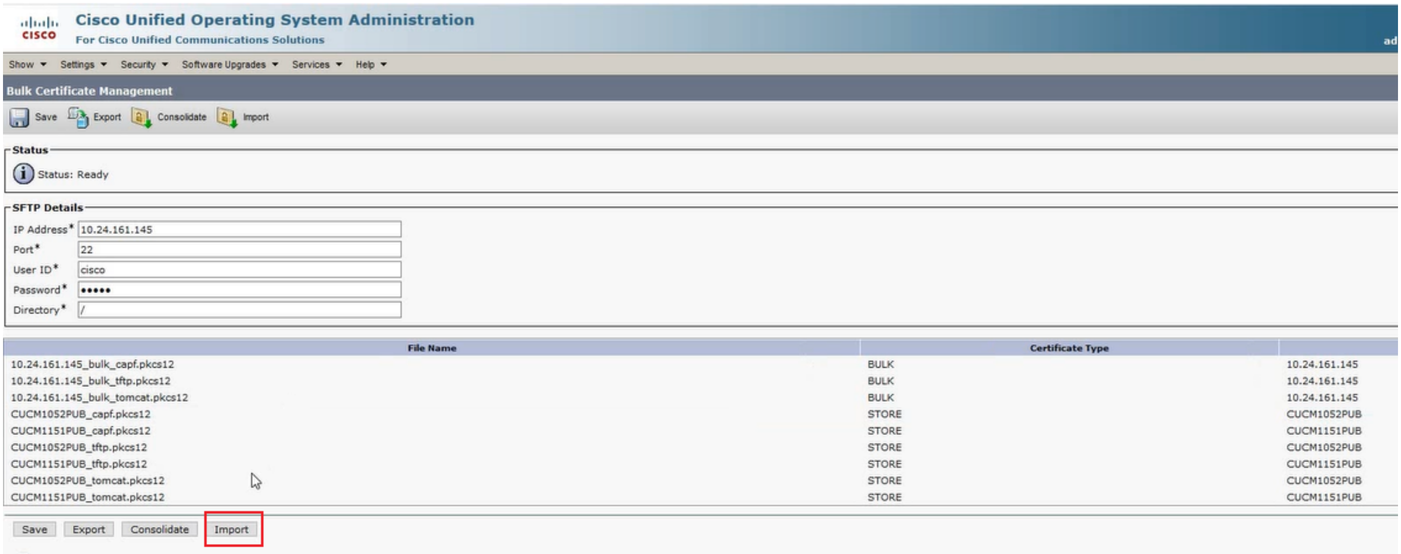




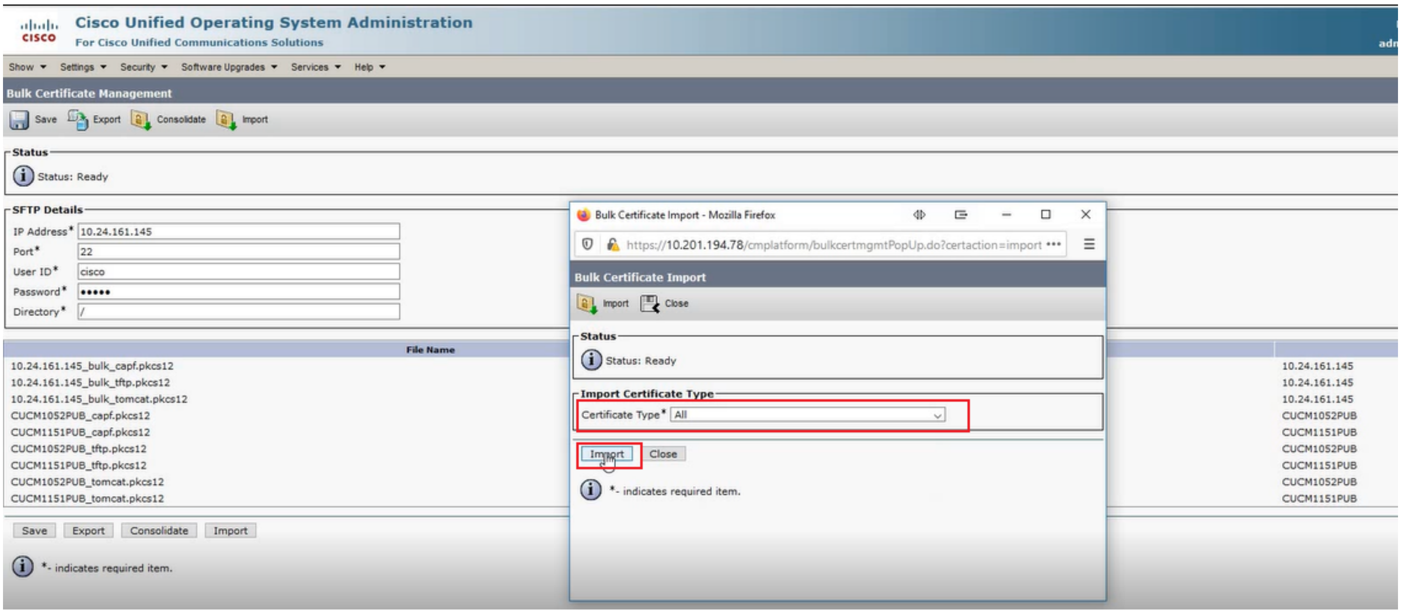
대상 및 소스 클러스터로 인증서 가져오기

1단계. 대상 클러스터로 인증서 가져오기

·대상 클러스터의 CUCM 게시자에서 **Cisco Unified OS 관리 > 보안 > 대량 인증서 관리**로 이동하여 페이지를 새로 고침한 다음 이미지에 표시된 대로 Import(가져오기)를 **클릭합니다**.



·후속 팝업 창에서 Certificate Type(인증서 유형)에 대해 **All(모두)**을 선택한 다음 이미지에 표시된 대로 Import(**가져오기**)를 클릭합니다.



2단계. 소스 클러스터에 대해 1단계를 반복합니다.

참고:대량 인증서 가져오기가 수행되면 인증서는 다음과 같이 원격 클러스터에 업로드됩니다.
·CAPF(Certificate Authority Proxy Function) 인증서가 CallManager-trust로 업로드됩니다.
·Tomcat 인증서가 tomcat-trust로 업로드됨
·CallManager 인증서가 Phone-SAST-trust 및 CallManager-trust로 업로드됩니다.
·ITLRecovery(Identity Trust List Recovery) 인증서가 Phone-SAST-trust 및 CallManager-trust로 업로드됩니다.

대상 클러스터 TFTP 서버 정보로 소스 클러스터 폰 구성

대상 클러스터 CUCM TFTP 서버를 가리키도록 TFTP(Trivial File Transfer Protocol) 옵션 150을 사용하여 소스 클러스터 전화기의 DHCP 범위를 구성합니다.

마이그레이션 프로세스를 완료하기 위해 대상 클러스터 ITL/CTL 파일을 가져오기 위해 소스 클러스터 폰 재설정

마이그레이션 프로세스의 일환으로 소스 클러스터 폰은 소스 클러스터의 Cisco TVS(Trust Verification Service)에 대한 보안 연결을 설정하여 대상 클러스터의 CallManager 또는 ITLRecovery 인증서를 확인합니다.

참고:TFTP 서비스(TFTP 인증서라고도 함)를 실행하는 CUCM 서버의 소스 클러스터의 CallManager 인증서 또는 ITLRecovery 인증서는 소스 클러스터 CUCM 노드의 CTL(Certificate Trust List) 및/또는 ITL(Identity Trust List) 파일에 서명합니다.마찬가지로, TFTP 서비스를 실행하는 CUCM 서버의 대상 클러스터의 CallManager 인증서 또는 ITLRecovery 인증서는 대상 클러스터 CUCM 노드의 CTL 및/또는 ITL 파일에 서명합니다 .CTL 및 ITL 파일은 TFTP 서비스를 실행하는 CUCM 노드에 생성됩니다.대상 클러스터의 CTL 및/또는 ITL 파일이 소스 클러스터 TVS에서 검증되지 않은 경우 대상 클러스터로의 폰 마이그레이션이 실패합니다.

참고:소스 클러스터 전화 마이그레이션 프로세스를 시작하기 전에 해당 전화기에 유효한 CTL 및/또는 ITL 파일이 설치되어 있는지 확인합니다.또한 소스 클러스터에 대해 엔터프라이즈 기능 "Prepare Cluster for Rollback to Pre 8.0"이 False로 설정되어 있는지 확인합니다.또한 TFTP 서비스를 실행하는 대상 클러스터 CUCM 노드에 유효한 CTL 및/또는 ITL 파일이 설치되어 있는지 확인합니다.

전화기 마이그레이션을 완료하기 위해 대상 클러스터 ITL 파일을 가져오기 위해 소스 전화기에 대한 비보안 클러스터의 프로세스:

1단계. 재설정할 때 소스 클러스터 전화기에 표시되는 대상 클러스터의 ITL 파일에 포함된 CallManager 및 ITLRecovery 인증서는 현재 설치된 ITL 파일의 유효성을 검사하는 데 사용할 수 없습니다.이렇게 하면 소스 클러스터 전화기가 소스 클러스터의 TVS에 대한 연결을 설정하여 대상 클러스터의 ITL 파일을 검증합니다.
2단계. 전화기가 tcp 포트 2445에서 소스 클러스터 TVS에 대한 연결을 설정합니다.
3단계. 소스 클러스터의 TVS가 인증서를 전화기에 표시합니다.전화가 연결을 확인하고 소스 클러스터 TVS에서 대상 클러스터의 CallManager 또는 ITLRecovery 인증서를 확인하여 전화기가 대상 클러스터의 ITL 파일을 다운로드할 수 있도록 합니다.
4단계. 대상 클러스터 ITL 파일의 검증 및 설치 후 소스 클러스터 폰에서 대상 클러스터에서 서명된 컨피그레이션 파일을 검증하고 다운로드할 수 있습니다.

대상 클러스터 CTL 파일을 가져와 폰 마이그레이션을 완료하기 위해 소스 폰에 대한 보안 클러스터의 프로세스:

1단계. 전화기가 부팅되고 대상 클러스터에서 CTL 파일을 다운로드하려고 시도합니다.
2단계. CTL 파일은 전화의 현재 CTL 또는 ITL 파일에 없는 대상 클러스터의 CallManager 또는 ITLRecovery 인증서에 의해 서명됩니다.
3단계. 따라서 전화기가 소스 클러스터의 TVS에 도달하여 CallManager 또는 ITLRecovery 인증서를 확인합니다.

참고:이 시점에서는 소스 클러스터 TVS 서비스의 IP 주소를 포함하는 이전 컨피그레이션이 여전히 전화기에 있습니다.전화기 구성에 지정된 TVS 서버는 Callmanager 그룹과 동일합니다.

4단계. 전화기는 소스 클러스터의 TVS에 대한 TLS(Transport Layer Security) 연결을 설정합니다.
5단계. 소스 클러스터 TVS가 인증서를 전화기에 표시하는 경우 전화기는 이 TVS 인증서를 현재 ITL 파일의 인증서와 비교하여 확인합니다.
6단계. 동일하면 핸드셰이크가 성공적으로 완료됩니다.

7단계. 소스 전화기는 대상 클러스터 CTL 파일에서 소스 클러스터 TVS가 CallManager 또는 ITLRecovery 인증서를 확인하도록 요청합니다.
8단계. 소스 TVS 서비스는 인증서 저장소에서 대상 클러스터 CallManager 또는 ITLRecovery를 찾아 검증하고 소스 클러스터 전화기가 목적지 클러스터 CTL 파일로 업데이트되도록 진행합니다.
9단계. 소스 전화기는 현재 포함된 대상 클러스터 CTL 파일에 대해 검증된 대상 클러스터의 ITL 파일을 다운로드합니다.이제 소스 전화기의 CTL 파일에 대상 클러스터의 CallManager 또는 ITLRecovery 인증서가 포함되어 있으므로 소스 전화기는 소스 클러스터의 TVS에 연결하지 않고도 CallManager 또는 ITLRecovery 인증서를 확인할 수 있습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

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

구성 연습 비디오

이 링크는 CUCM 클러스터 간 벌크 인증서 관리 를 통해 표시되는 비디오에 대한 액세스를 제공합니다.

CUCM 클러스터 간 벌크 인증서 관리