인증서 구성

인증서 개요

인증서는 ID를 보호하고 IM and Presence 서비스 및 다른 시스템 간의 신뢰 관계를 구축하는 데 사용됩니다. 인증서를 사용하여 IM and Presence 서비스를 Cisco Unified Communications Manager, Cisco Jabber 클라이언트 또는 모든 외부 서버에 연결할 수 있습니다. 인증서가 없으면 가짜 DNS 서버가 사용되었는지 또는 다른 서버로 라우팅되었는지 알 수 없습니다.

IM and Presence 서비스에서 사용할 수 있는 두 가지 주요 클래스의 인증서가 있습니다.

- 자체 서명 인증서 - 자체 서명 인증서는 인증서를 발급하는 서버와 동일한 서버에서 서명됩니다. 기업 내에서 비보안 네트워크를 통해 이동하는 연결이 없는 경우 자체 서명 인증서를 사용하여 다른 내부 시스템과 연결할 수 있습니다. 예를 들어 IM and Presence 서비스는 Cisco Unified Communications Manager에 대한 내부 연결을 위해 자체 서명 인증서를 생성할 수 있습니다.
- CA 서명 인증서 - 제 3자 인증 기관(CA)에서 서명된 인증서입니다. 서버/서비스 인증서의 유효성을 제어하는 공용 CA(예: Verisign, Entrust 또는 Digicert) 또는 서버(예: Windows 2003, Linux, Unix, IOS)로 서명할 수 있습니다. CA 서명 인증서는 자체 서명 인증서보다 안전하며 일반적으로 모든 WAN 연결에 사용됩니다. 예를 들어, 페더레이션 연결을 다른 엔터프라이즈 또는 WAN 연결을 사용하는 인터클러스터 피어 구성을 사용하려면 CA 서명 인증서가 외부 시스템과의 신뢰 관계를 구축해야 합니다.

CA 서명 인증서는 자체 서명 인증서보다 안전합니다. 일반적으로 자체 서명 인증서는 내부 연결에 적합하지만 WAN 연결 또는 공용 인터넷을 통과하는 연결의 경우 CA 서명 인증서를 사용해야 합니다.

다중 서버 인증서

또한 IM and Presence 서비스는 일부 시스템 서비스에 대해 다중 서버 SAN 인증서도 지원합니다. 다중 서버 인증서를 위한 CSR(Certificate Signing Request)을 생성하면 인증서가 클러스터 노드에 업로드된 후 결과 다중 서버 인증서 및 서명 인증서의 관련 체인이 모든 클러스터 노드에 자동으로 구축됩니다.

IM and Presence 서비스의 인증서 종류

IM and Presence 서비스 내에서 다른 시스템 구성 요소에는 다른 유형의 인증서가 필요합니다. 다음 표에서는 IM and Presence 서비스의 클라이언트와 서비스에 필요한 서로 다른 인증서에 대해 설명합니다.

참고 인증서 이름이 -ECDSA로 끝나면 인증서/키 유형은 Elliptic Curve(EC)입니다. 그렇지 않으면, RSA입니다.

표 ***1:*** 인증서 종류 및 서비스

인증서 종류	서비스	인증서 신뢰 저장	다중 서버 지원	참고 사항
tomcat, tomcat-ECDSA	Cisco 클라이언트 프로파일 에이전트, Cisco AXL 웹 서비스, Cisco Tomcat	tomcat- trust	예	IM and Presence 서비스에 대한 클라이언트 인증의 일부로서 Cisco Jabber 클라이언트에 표시됩니다. Cisco Unified CM IM and Presence 관리 사용자 인터페이스를 탐색할 때 웹 브라우저에 표시됩니다. 연결된 trust-store는 사용자 자격 증명을 구성된 LDAP 서버로 인증하기 위해 IM and Presence 서비스에서 설정한 연결을 확인하는 데 사용됩니다.
ipsec		ipsec-신뢰	아니요	IPSec 정책이 활성화될 때 사용됩니다.

인증서 종류	서비스	인증서 신뢰 저장	다중 서버 지원	참고 사항
cup, cup-ECDSA	Cisco SIP Proxy, Cisco Presence 엔진	cup-trust	아니요	SIP 페더레이션 사용자를 위해 IM and Presence를 가져오기 위해 Expressway-C에 인증서를 제공합니다. IM and Presence 프록시는 클라이언트와 서버 역할을 모두 수행합니다. 프레즌스 엔진은 Exchange/Office 365 통신에 이러한 인증서를 사용하여 일정 프레즌스를 얻습니다. 프레즌스 엔진은 클라이언트 전용으로 작동합니다.
cup-xmpp, cup-xmpp-ECDSA	Cisco XCP 연결 관리자, Cisco XCP Web 연결 관리자, Cisco XCP 디렉터리 서비스, Cisco XCP 라우터 서비스	cup-xmpp-trust	예	XMPP 세션을 생성하는 동안 Cisco Jabber 클라이언트, 타사 XMPP 클라이언트 또는 CAXL 기반 애플리케이션에 표시됩니다. 연결된 trust-store는 타사 XMPP 클라이언트에 대해 LDAP 검색 작업을 수행하는 과정에서 Cisco XCP 디렉터리 서비스가 설정한 연결을 확인하는 데 사용됩니다. 연결된 trust-store는 라우팅 통신 유형이 라우터 대 라우터로 설정된 경우 IM and Presence 서비스 서버 간 보안 연결을 설정할 때 Cisco XCP 라우터 서비스에 의해 사용됩니다.
cup-xmpp-s2s, cup-xmpp-s2s-ECDSA	Cisco XCP XMPP 페더레이션 연결 관리자	cup-xmpp-trust	예	외부에서 제휴된 XMPP 시스템을 연결할 때 XMPP 도메인 간 페더레이션에 대해 표시됩니다.

인증서 필수 조건

Cisco Unified Communications Manager에서 다음 항목을 구성합니다.

- IM and Presence 서비스용 SIP 트렁크 보안 프로파일을 구성합니다.
- IM and Presence 서비스에 대한 SIP 트렁크를 구성합니다.
  - 보안 프로파일을 SIP 트렁크와 연결합니다.
  - IM and Presence 서비스 인증서의 주체 CN(공통 이름)으로 SIP 트렁크를 구성합니다.

Cisco Unified Communications Manager와 인증서 교환

Cisco Unified Communications Manager와 인증서를 교환하려면 이 작업을 완료하십시오.

참고 Cisco Unified Communications Manager와 IM and Presence 서비스 간의 인증서 교환은 설치 프로세스 중에 자동으로 처리됩니다. 그러나 인증서 교환을 수동으로 완료해야 하는 경우 이 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco Unified Communications Manager 인증서를 IM and Presence 서비스로 가져오기, 4 페이지	Cisco Unified Communications Manager의 인증서를 IM and Presence 서비스로 가져옵니다.
단계 **2**	IM and Presence 서비스에서 인증서 다운로드, 5 페이지	IM and Presence 서비스에서 인증서를 다운로드합니다. 인증서를 Cisco Unified Communications Manager로 가져와야 합니다.
단계 **3**	IM and Presence 인증서를 Cisco Unified Communications Manager로 가져오기, 6 페이지	인증서 교환을 완료하려면 IM and Presence 서비스 인증서를 Cisco Unified Communications Manager의 Callmanager-trust 저장소로 가져옵니다.

Cisco Unified Communications Manager 인증서를 IM and Presence 서비스로 가져오기

이 절차를 사용하여 Cisco Unified Communications Manager의 인증서를 IM and Presence 서비스로 가져옵니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 보안 > 인증서 가져오기 도구를 선택합니다.

단계 **2** 인증서 신뢰 저장 메뉴에서 **IM and Presence(IM/P)** 서비스 신뢰를 선택합니다.

단계 **3** Cisco Unified Communications Manager 노드의 IP 주소, 호스트 이름 또는 FQDN을 입력합니다.

단계 **4** Cisco Unified Communications Manager 노드와 통신하기 위한 포트 번호를 입력합니다.

단계 **5** 제출을 클릭합니다.

참고 인증서 가져오기 도구는 가져오기 작업을 완료한 후 Cisco Unified Communications Manager에 성공적으로 연결되었는지 여부, Cisco Unified Communications Manager에서 인증서가 성공적으로 다운로드되었는지 여부를 보고합니다. 인증서 가져오기 도구에서 실패를 보고하는 경우 온라인 도움말의 권장 작업을 참조하십시오. **Cisco Unified IM and Presence OS** 관리보안 > 인증서 관리를 선택하여 수동으로 인증서를 가져올 수도 있습니다.

참고 협상된 TLS 암호화에 따라 인증서 가져 오기 도구는 RSA 기반 인증서 또는 ECDSA 기반 인증서를 다운로드합니다.

단계 **6** Cisco SIP Proxy 서비스를 다시 시작합니다.

a) Cisco Unified IM and Presence 서비스 가용성의 IM and Presence에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.
b) 서버 드롭다운 목록 상자에서 IM and Presence 서비스 클러스터 노드를 선택하고 이동을 클릭합니다.
c) **Cisco SIP Proxy**를 선택하고 다시 시작을 클릭합니다.

다음에 수행할 작업

IM and Presence 서비스에서 인증서 다운로드, 5 페이지

IM and Presence 서비스에서 인증서 다운로드

이 절차를 사용하여 IM and Presence 서비스에서 인증서를 다운로드합니다. 인증서를 Cisco Unified Communications Manager로 가져와야 합니다.

프로시저

단계 **1** **Cisco Unified IM and Presence OS** 관리의 IM and Presence에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** `cup.pem` 파일을 선택합니다.

참고 `cup ECDSA.pem`도 사용할 수 있는 옵션입니다.

단계 **4** 다운로드를 클릭하고 파일을 로컬 컴퓨터에 저장합니다.

팁 cup.csr 파일 액세스와 관련하여 IM and Presence 서비스에 표시되는 오류는 무시하십시오. CA(인증 기관)에서는 사용자가 Cisco Unified Communications Manager와 교환하는 인증서에 서명할 필요가 없습니다.

다음에 수행할 작업

IM and Presence 인증서를 Cisco Unified Communications Manager로 가져오기, 6 페이지

IM and Presence 인증서를 Cisco Unified Communications Manager로 가져오기

인증서 교환을 완료하려면 IM and Presence 서비스 인증서를 Cisco Unified Communications Manager의 Callmanager-trust 저장소로 가져옵니다.

시작하기 전에

IM and Presence 서비스에서 인증서 다운로드, 5 페이지

프로시저

단계 **1** Cisco Unified OS 관리에 로그인합니다.

단계 **2** 보안 > 인증서 관리를 선택합니다.

단계 **3** 인증서 업로드를 클릭합니다.

단계 **4** 인증서 이름 메뉴에서 **Callmanager-trust**를 선택합니다.

단계 **5** 찾아보기를 선택하고 IM and Presence 서비스에서 이전에 다운로드한 인증서를 선택합니다.

단계 **6** 파일 업로드를 클릭합니다.

단계 **7** Cisco CallManager 서비스를 다시 시작합니다.

a) Cisco Unified Serviceability에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

b) 서버 드롭다운 목록 상자에서 Cisco Unified Communications Manager 노드를 선택하고 이동을 클릭합니다.

c) **Cisco CallManager** 서비스를 선택하고 다시 시작을 클릭합니다.

IM and Presence 서비스에 CA(인증 기관) 설치

IM and Presence 서비스에서 제3자 CA(인증 기관)에서 서명한 인증서를 사용하려면 먼저 해당 CA의 루트 신뢰 인증서 체인을 IM and Presence 서비스에 설치해야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	CA 루트 인증서 체인 업로드, 7 페이지	이 절차를 사용하여 제3자 인증 기관에서 IM and Presence 서비스로 CA 루트 인증서 체인을 업로드합니다.

	명령 또는 동작	목적
단계 2	Cisco 클러스터 간 동기화 에이전트 서비스 다시 시작, 7 페이지	인증서를 업로드한 후, Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작합니다.
단계 3	CA 인증서가 다른 클러스터에 동기화되었는지 확인, 8 페이지	CA 인증서 체인이 모든 피어 클러스터에 복제되었는지 확인합니다.

CA 루트 인증서 체인 업로드

이 절차를 사용하여 서명 인증 기관(CA)의 인증서를 IM and Presence 데이터베이스 게시자 노드로 업로드합니다. 체인은 체인의 여러 인증서로 구성될 수 있으며, 각 인증서는 후속 인증서에 서명합니다.

- 루트 인증서 > 중간 1 인증서 > 중간 2 인증서

프로시저

단계 1 IM and Presence 데이터베이스 게시자 노드에서 Cisco Unified IM and Presence OS 관리에 로그인합니다.

단계 2 보안 > 인증서 관리를 선택합니다.

단계 3 인증서/인증서 체인 업로드를 클릭합니다.

단계 4 인증서 이름 드롭다운 목록에서 다음 중 하나를 선택합니다.

- CA 서명 tomact 인증서를 업로드하는 경우 **tomcat-trust**를 선택합니다.
- CA 서명 cup-xmpp 인증서 또는 CA 서명 cup-xmpp-s2s를 업로드하는 경우 **cup-xmpp-trust**를 선택합니다.

단계 5 서명 인증서에 대한 설명을 입력합니다.

단계 6 찾아보기를 클릭하여 루트 인증서에 대한 파일을 찾습니다.

단계 7 파일 업로드를 클릭합니다.

단계 8 인증서/인증서 체인 업로드 창을 사용하여 같은 방법으로 각 중간 인증서를 업로드합니다. 각 중간 인증서에 대해 체인에 선행 인증서의 이름을 입력해야 합니다.

다음에 수행할 작업

Cisco 클러스터 간 동기화 에이전트 서비스 다시 시작, 7 페이지

Cisco 클러스터 간 동기화 에이전트 서비스 다시 시작

IM and Presence 데이터베이스 게시자 노드에 루트 및 중간 인증서를 업로드한 후에는 해당 노드에서 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작해야 합니다. 이 서비스를 다시 시작하면 CA 인증서가 다른 모든 클러스터에 즉시 동기화됩니다.

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록 상자에서 인증서를 가져온 IM and Presence 서비스 노드를 선택하고 이동을 클릭합니다.

참고 또한 명령줄 인터페이스에서 `utils service restart Cisco Intercluster Sync Agent` 명령을 사용하여 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작할 수도 있습니다.

단계 **3** **Cisco** 클러스터 간 동기화 에이전트 서비스를 선택하고 다시 시작을 클릭합니다.

다음에 수행할 작업

클러스터 간 동기화 확인, 11 페이지

CA 인증서가 다른 클러스터에 동기화되었는지 확인

Cisco 클러스터 간 동기화 에이전트 서비스가 다시 시작되면 CA 인증서가 다른 클러스터에 올바르게 동기화되었는지 확인해야 합니다. 다른 각 IM and Presence 데이터베이스 게시자 노드에서 다음 절차를 완료하십시오.

참고 다음 절차의 정보는 `-ECDSA`로 끝나는 인증서에도 적용됩니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 **2** 상호 클러스터링 문제 해결 도구 아래에서 각 **TLS** 사용 인터클러스터 피어가 보안 인증서를 성공적으로 교환했는지 확인하십시오**.** 테스트를 찾아보고 통과했는지 확인합니다.

단계 **3** 테스트에 오류가 표시되면 인터클러스터 피어 IP 주소를 확인합니다. CA 인증서를 업로드한 클러스터를 참조해야 합니다. 다음 단계를 진행하여 문제를 해결합니다.

단계 **4** 프레즌스 > 클러스터 간을 선택하고 시스템 문제 해결 도구 페이지에서 확인한 인터클러스터 피어와 관련된 링크를 클릭합니다.

단계 **5** 강제 수동 동기화를 클릭합니다.

단계 **6** 인터클러스터 피어 상태 패널에서 자동 새로 고침으로 60초를 허용합니다.

단계 **7** 인증서 상태 필드에 "연결이 안전합니다"가 표시되는지 확인합니다.

단계 **8** 인증서 상태 필드에 "연결이 안전합니다"가 표시되지 않으면 IM and Presence 데이터베이스 게시자 노드에서 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작하고 5~7단계를 반복합니다.

- 관리 CLI에서 서비스를 다시 시작하려면 utils service restart Cisco Intercluster Sync Agent 명령을 실행합니다.
- 또는 Cisco Unified IM and Presence 서비스 가용성 GUI에서 이 서비스를 다시 시작할 수도 있습니다.

단계 **9** 인증서 상태 필드에 이제 "연결이 안전합니다"가 표시되는지 확인합니다. 이 표시는 클러스터 간 동기화가 클러스터 사이에서 올바르게 설정되었고, 업로드한 CA 인증서가 다른 클러스터에 동기화되었음을 의미합니다.

다음에 수행할 작업

서명 인증서를 각 IM and Presence 서비스 노드에 업로드합니다.

IM and Presence 서비스로 인증서 업로드

IM and Presence 서비스에 인증서를 업로드하려면 다음 작업을 완료하십시오. CA 서명 인증서 또는 자체 서명 인증서를 업로드할 수 있습니다.

시작하기 전에

제3자 CA(인증 기관)에서 서명한 CA 서명 인증서를 사용하려면 해당 CA의 루트 인증서 체인이 IM and Presence 서비스에 이미 설치되어 있어야 합니다. 자세한 내용은 IM and Presence 서비스에 CA(인증 기관) 설치, 6 페이지의 내용을 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 업로드, 10 페이지	서명된 인증서를 IM and Presence 서비스에 업로드합니다.
단계 **2**	Cisco Tomcat 서비스 다시 시작, 11 페이지	(Tomcat 인증서만 해당). Cisco Tomcat 서비스를 다시 시작합니다.
단계 **3**	클러스터 간 동기화 확인, 11 페이지	(Tomcat 인증서만 해당). 클러스터 내 영향받는 모든 노드에 대해 Cisco Tomcat 서비스가 다시 시작되었으면 클러스터 간 동기화가 제대로 작동하는지 확인해야 합니다.
단계 **4**	모든 노드에서 Cisco XCP 라우터 서비스 다시 시작, 12 페이지	인증서를 cup-xmpp 저장소에 업로드한 경우 모든 클러스터 노드에서 Cisco XMP 라우터를 다시 시작합니다.
단계 **5**	Cisco XCP XMPP 페더레이션 연결 관리자 서비스 다시 시작, 12 페이지	(XMPP 페더레이션만 해당). XMPP 페더레이션을 위해 cup-xmpp 저장소로 인증서를 업로

	명령 또는 동작	목적
		드한 경우 Cisco XCPXMPP 페더레이션 연결 관리자 서비스를 다시 시작합니다.
단계 **6**	XMPP 페더레이션 보안 인증서에서 와일드카드 활성화, 13 페이지	(XMPP 페더레이션만 해당). TLS를 통한 XMPP 페더레이션을 위한 cup-xmpp 저장소로 인증서를 업로드한 경우 XMPP 보안 인증서에 대해 와일드카드를 활성화해야 합니다. 이는 그룹 채팅에 필요합니다.

인증서 업로드

이 절차를 사용하여 각 IM and Presence 서비스 노드에 업로드합니다.

참고 클러스터에 대한 모든 필수 tomcat 인증서에 서명하고 동시에 업로드하는 것이 좋습니다. 이 프로세스를 수행하면 클러스터 간 통신 복구에 소요되는 시간이 단축됩니다.

참고 다음 절차의 정보는 `-ECDSA`로 끝나는 인증서에도 적용됩니다.

시작하기 전에

인증서가 CA에 의해 서명된 경우 해당 CA의 루트 인증서 체인도 설치했어야 합니다. 그렇지 않으면 CA 서명 인증서를 신뢰하지 않습니다. CA 인증서가 모든 클러스터에 대해 올바르게 동기화되었으면 적절한 서명 인증서를 각 IM and Presence 서비스 노드에 업로드할 수 있습니다.

프로시저

단계 **1** **Cisco Unified IM and Presence OS** 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서 목적을 선택합니다. 예를 들어 **tomcat**.
단계 **4** 서명 인증서에 대한 설명을 입력합니다.
단계 **5** 찾아보기를 클릭하고 업로드할 파일을 찾습니다.
단계 **6** 파일 업로드를 클릭합니다.
단계 **7** 각 IM and Presence 서비스 노드에 대해 반복합니다.

다음에 수행할 작업

Cisco Tomcat 서비스를 다시 시작합니다.

Cisco Tomcat 서비스 다시 시작

각 IM and Presence 서비스 노드에 tomcat 인증서를 업로드한 후에는 각 노드에서 Cisco Tomcat 서비스를 다시 시작해야 합니다.

프로시저

단계 **1** 관리자 CLI에 로그인합니다.

단계 **2** `utils service restart Cisco Tomcat` 명령을 실행합니다.

단계 **3** 각 노드에 대해 반복합니다.

다음에 수행할 작업

클러스터 간 동기화가 제대로 작동하는지 확인합니다.

클러스터 간 동기화 확인

클러스터 내 영향받는 모든 노드에 대해 Cisco Tomcat 서비스가 다시 시작되었으면 클러스터 간 동기화가 제대로 작동하는지 확인해야 합니다. 다른 클러스터의 각 IM and Presence 데이터베이스 게시자 노드에서 다음 절차를 완료하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 **2** 상호 클러스터링 문제 해결 도구 아래에서 각 **TLS** 사용 인터클러스터 피어가 보안 인증서를 성공적으로 교환했는지 확인하십시오**.** 테스트를 찾아보고 통과했는지 확인합니다.

단계 **3** 테스트에 오류가 표시되면 인터클러스터 피어 IP 주소를 확인합니다. CA 인증서를 업로드한 클러스터를 참조해야 합니다. 다음 단계를 진행하여 문제를 해결합니다.

단계 **4** 프레즌스 > 클러스터 간을 선택하고 시스템 문제 해결 도구 페이지에서 확인한 인터클러스터 피어와 관련된 링크를 클릭합니다.

단계 **5** 강제 수동 동기화를 클릭합니다.

단계 **6** 피어의 **Tomcat** 인증서도 재동기화 확인란을 선택하고 확인을 클릭합니다.

단계 **7** 인터클러스터 피어 상태 패널에서 자동 새로 고침으로 60초를 허용합니다.

단계 **8** 인증서 상태 필드에 "연결이 안전합니다"가 표시되는지 확인합니다.

단계 **9** 인증서 상태 필드에 "연결이 안전합니다"가 표시되지 않으면 IM and Presence 데이터베이스 게시자 노드에서 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작하고 5~8단계를 반복합니다.

- 관리자는 다음 명령을 실행 하는 CLI에서 서비스를 다시 시작 하려면: utils 서비스 Cisco 클러스터 간 동기화 에이전트를 다시 시작 합니다.
- 또는 Cisco Unified IM and Presence 서비스 가용성 GUI에서 이 서비스를 다시 시작할 수도 있습니다.

단계 **10** 인증서 상태 필드에 이제 "연결이 안전합니다"가 표시되는지 확인합니다. 표시되면, 이 클러스터와 인증서가 업로드된 클러스터 사이에 클러스터 간 동기화가 다시 설정된 것입니다.

모든 노드에서 **Cisco XCP** 라우터 서비스 다시 시작

cup-xmpp 및/또는 cup-xmpp-ECDSA 인증서를 각 IM and Presence 서비스 노드에 업로드한 후에는 각 노드에서 Cisco XCP 라우터 서비스를 다시 시작해야 합니다.

참고 Cisco Unified IM and Presence 서비스 가용성 GUI에서 Cisco XCP 라우터 서비스를 다시 시작할 수도 있습니다.

프로시저

단계 **1** 관리자 CLI에 로그인합니다.

단계 **2** utils service restart Cisco XCP Router 명령을 실행합니다.

단계 **3** 각 노드에 대해 반복합니다.

Cisco XCP XMPP 페더레이션 연결 관리자 서비스 다시 시작

cup-xmpp-s2s 및/또는 cup-xmpp-s2s-ECDSA 인증서를 각 IM and Presence 서비스 페더레이션 노드에 업로드한 후에는 각 페더레이션 노드에서 Cisco XCP XMPP 페더레이션 연결 관리자 서비스를 다시 시작해야 합니다.

프로시저

단계 **1** 관리자 CLI에 로그인합니다.

단계 **2** utils service restart Cisco XCP XMPP Federation Connection Manager 명령을 실행합니다.

단계 **3** 각 페더레이션 노드에 대해 반복합니다.

XMPP 페더레이션 보안 인증서에서 와일드카드 활성화

TLS를 통한 XMPP 페더레이션 파트너 간 그룹 채팅을 지원하려면 XMPP 보안 인증서에 대한 와일드카드를 활성화해야 합니다.

기본적으로 XMPP 페더레이션 보안 인증서 `cup-xmpp-s2s` 및 `cup-xmpp-s2s-ECDSA`에는 IM and Presence 서비스 구축에서 호스트하는 모든 도메인이 포함됩니다. 이들은 SAN(Subject Alternative Name) 항목으로서 인증서 내에 추가됩니다. 호스트된 모든 도메인에 대한 와일드카드를 동일한 인증서 내에서 제공해야 합니다. 따라서 XMPP 보안 인증서에는 SAN 항목 "example.com" 대신 SAN 항목 "*.example.com"을 포함해야 합니다. 그룹 채팅 서버 별칭은 IM and Presence 서비스 시스템에 호스트된 도메인 중 하나의 하위 도메인이므로 와일드카드가 필요합니다. 예: “conference.example.com”.

참고 모든 노드에서 `cup-xmpp-s2s` 또는 `cup-xmpp-s2s-ECDSA` 인증서를 보려면 **Cisco Unified IM and Presence OS** 관리 > 보안 > 인증서 관리를 선택하고 **cup-xmpp-s2s** 또는 **cup-xmpp-s2s-ECDSA** 링크를 클릭합니다.

프로시저

단계 **1** 시스템 > 보안 설정을 선택합니다.

단계 **2** **XMPP** 페더레이션 보안 인증서에서 와일드카드 활성화를 선택합니다.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

Cisco XMPP 페더레이션 연결 관리자 서비스가 실행되고 있으며 XMPP 페더레이션이 활성화된 클러스터 내 모든 노드에서 XMPP 페더레이션 보안 인증서를 다시 생성해야 합니다. TLS를 통한 XMPP 페더레이션 그룹 채팅을 지원하려면 모든 IM and Presence 서비스 클러스터에서 이 보안 설정을 활성화해야 합니다.

Generate a CSR(CSR 생성)

이 절차를 사용하여 인증서 서명 요청(CSR)을 생성합니다. CA 서명 인증서를 제공할 수 있도록 제3자 CA에 제출할 CSR이 필요합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** **CSR** 생성 버튼을 클릭합니다. 인증서 서명 요청 생성 팝업 창이 나타납니다.

단계 **3** 인증서 목적 드롭다운 목록에서 생성하는 인증서의 유형을 선택합니다.

단계 **4** 서버 드롭다운 목록에서 IM and Presence 서버를 선택합니다. 다중 서버 인증서의 경우 다중 서버**(SAN)**를 선택합니다.

단계 **5** 키 길이 및 해시 알고리즘을 입력합니다.

단계 **6** 나머지 필드를 작성하고 생성을 클릭합니다.

단계 **7** CSR을 로컬 컴퓨터에 다운로드합니다.

a) **CSR** 다운로드를 클릭합니다.
b) 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.
c) **CSR** 다운로드

다음에 수행할 작업

CA 서명 인증서를 발급할 수 있도록 CSR을 제3자 인증 기관에 제출합니다.

인증서 서명 요청 키 사용 확장

다음 표에는 Unified Communications Manager 및 IM and Presence Service CA 인증서에 대한 인증서 서명 요청(CSR)의 주요 용도 확장이 나와 있습니다.

표 ***2: Cisco Unified Communications Manager CSR*** 키 용도 확장

	다중 서버	확장 키 사용			키 사용				
		서버 인증 **(1.3.6.1.5.5.7.3.1)**	클라이언트 인증 **(1.3.6.1.5.5.7.3.2)**	**IP** 보안 엔드 시스템 **(1.3.6.1.5.5.7.3.5)**	디지털 서명	키 암호화	데이터 암호화	키 인증서 서명	키 계약
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF(게시자에만 해당)	N	Y	Y		Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	Y	Y	Y		Y	Y	Y		

표 ***3: IM and Presence Service CSR*** 키 사용 확장

	다중 서버	확장 키 사용			키 사용				
		서버 인증 **(1.3.6.1.5.5.7.3.1)**	클라이언트 인증 **(1.3.6.1.5.5.7.3.2)**	**IP** 보안 엔드 시스템 **(1.3.6.1.5.5.7.3.5)**	디지털 서명	키 암호화	데이터 암호화	키 인증서 서명	키 계약
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		Y

	다중 서버	확장 키 사용			키 사용				
		서버 인증 **(1.3.6.1.5.5.7.3.1)**	클라이언트 인증 **(1.3.6.1.5.5.7.3.2)**	**IP** 보안 엔드 시스템 **(1.3.6.1.5.5.7.3.5)**	디지털 서명	키 암호화	데이터 암호화	키 인증서 서명	키 계약
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

셀프 서명 인증서 생성

이 절차를 사용하여 자체 서명 인증서를 생성합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 자체 서명 생성을 클릭합니다. 새 자체 서명 인증서 생성 팝업 창이 나타납니다.
단계 **3** 인증서 목적 드롭다운 목록에서 생성하는 인증서의 유형을 선택합니다.
단계 **4** 구축 드롭다운에서 서버의 이름을 입력합니다.
단계 **5** 적절한 키 길이를 선택합니다.
단계 **6** 해시 알고리즘에서 암호화 알고리즘을 선택합니다. 예를 들어 SHA256.
단계 **7** 생성을 클릭합니다.

IM and Presence 서비스에서 자체 서명 신뢰 인증서 삭제

동일한 클러스터에서 노드 간 서비스 가용성에 대한 교차 탐색을 지원하기 위해, IM and Presence 서비스와 Cisco Unified Communications Manager 간 Cisco Tomcat 서비스 신뢰 저장소가 자동으로 동기화됩니다.

원래의 자체 서명 신뢰 인증서를 CA 서명 인증서로 바꾼 경우 원래의 자체 서명 신뢰 인증서가 서비스 신뢰 저장소에 유지됩니다. 이 절차를 사용하여 IM and Presence 서비스 및 Cisco Unified Communications Manager 노드에서 자체 서명 인증서를 삭제할 수 있습니다.

시작하기 전에

중요 CA 서명 인증서를 추가한 경우 Cisco 클러스터 간 동기화 에이전트 서비스가 지정된 IM and Presence 서비스 노드에서 정기적인 정리 작업을 수행하기 위해서는 30분을 대기해야 합니다.

프로시저

단계 **1** Cisco Unified IM and Presence Operating System 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 찾기를 클릭합니다.

인증서 목록이 나타납니다.

참고 인증서 이름은 서비스 이름 및 인증서 유형의 두 부분으로 구성됩니다. 예를 들어 tomcat-trust에서 tomcat은 서비스 이름이고 trust는 인증서 유형입니다.

삭제할 수 있는 자체 서명 신뢰 인증서는 다음과 같습니다.

- Tomcat 및 Tomcat-ECDSA — tomcat-trust
- Cup-xmpp 및 Cup-xmpp-ECDSA — cup-xmpp-trust
- Cup-xmpp-s2s 및 Cup-xmpp-s2s-ECDSA — cup-xmpp-trust
- Cup 및 Cup-ECDSA — cup-trust
- Ipsec - ipsec-trust

단계 **3** 삭제하고자 하는 자체 서명 신뢰 인증서의 링크를 클릭합니다.

중요 서비스 신뢰 저장소와 연결된 서비스에 대해 CA 서명 인증서를 구성했는지 확인하십시오.

인증서 상세정보를 표시하는 새 창이 나타납니다.

단계 **4** 삭제를 클릭합니다.

참고 해당 인증서를 삭제할 권한이 있는 경우에만 삭제 버튼이 나타납니다.

단계 **5** 구축 전체에서 불필요한 자체 서명 신뢰 인증서를 모두 제거하려면 클러스터의 각 IM and Presence 서비스 노드 및 인터클러스터 피어에 대해 위 절차를 반복하십시오.

다음에 수행할 작업

서비스가 Tomcat이면 Cisco Unified Communications Manager 노드에서 IM and Presence 서비스 노드의 자체 서명 tomcat-trust 인증서를 확인해야 합니다. Cisco Unified Communications Manager에서 자체 서명 Tomcat-Trust 인증서 삭제, 17 페이지를 참조하십시오.

Cisco Unified Communications Manager에서 자체 서명 Tomcat-Trust 인증서 삭제

클러스터의 각 노드에 대한 Cisco Unified Communications Manager 서비스 신뢰 저장소에는 자체 서명 tomcat-trust 인증서가 있습니다. Cisco Unified Communications Manager 노드에서 삭제할 인증서는 이러한 인증서뿐입니다.

참고 다음 절차에 있는 정보는 EC 인증서에도 적용됩니다.

시작하기 전에

CA 서명 인증서로 클러스터의 IM and Presence 서비스 노드를 구성한 다음, Cisco Unified Communications Manager 노드로 인증서가 전파되기까지 30분 정도 기다렸는지 확인합니다.

프로시저

단계 **1** **Cisco Unified Operating System** 관리에서 보안 > 인증서 관리를 선택합니다.

인증서 목록 창이 표시됩니다.

단계 **2** 검색 결과를 필터링하려면 드롭다운 목록에서 인증서 및 시작 단어를 선택하고 빈 필드에 tomcat-trust를 입력합니다. 찾기를 클릭합니다.

인증서 목록 창이 확장되면서 tomcat-trust 인증서가 나열됩니다.

단계 **3** 이름에 IM and Presence 서비스 노드의 호스트 이름 또는 FQDN이 포함된 링크를 확인합니다. 이들은 이 서비스 및 IM and Presence 서비스 노드와 연결된 자체 서명 인증서입니다.

단계 **4** IM and Presence 서비스 노드의 자체 서명 tomcat-trust 인증서에 대한 링크를 클릭합니다.

tomcat-trust 인증서 상세정보를 표시하는 새 창이 나타납니다.

단계 **5** 인증서 상세정보에서 발급자 이름 CN= 값 및 주체 이름 CN= 값이 일치하는지 검토하여 이것이 자체 서명 인증서인지 확인합니다.

단계 **6** 이것이 자체 서명 인증서인지를 확인했으며 CA 서명 인증서가 Cisco Unified Communications Manager 노드로 전파된 것이 확실하면 삭제를 클릭합니다.

참고 삭제 권한이 있는 인증서에 대해서만 삭제 버튼이 나타납니다.

단계 **7** 클러스터의 각 IM and Presence 서비스 노드에 대해 4~6단계를 반복합니다.

인증서 모니터링 작업 흐름

이 작업을 수행하여 인증서 상태 및 만료를 자동으로 모니터링하도록 시스템을 구성하십시오.

- 인증서가 만료에 도달하면 전자 메일을 보냅니다.
- 만료된 인증서를 해지합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 모니터 알림 구성, 18 페이지	자동 인증서 모니터링을 구성합니다. 시스템은 인증서 상태를 주기적으로 확인하고 인증서의 만료가 다가오면 사용자에게 전자 메일을 보냅니다.
단계 **2**	OCSP를 통해 인증서 해지 구성, 19 페이지	시스템이 만료된 인증서를 자동으로 취소하도록 OCSP를 구성합니다.

인증서 모니터 알림 구성

Unified Communications Manager 또는 IM and Presence Service에 대한 자동화된 인증서 모니터링을 구성합니다. 시스템은 인증서 상태를 주기적으로 확인하고 인증서의 만료가 다가오면 사용자에게 전자 메일을 보냅니다.

참고 **Cisco** 인증서 만료 모니터 네트워크 서비스가 실행 중이어야 합니다. 이 서비스는 기본적으로 활성화되어 있지만 도구 > 제어 센터 - 네트워크 서비스를 선택하고 **Cisco** 인증서 만료 모니터 서비스 상태가 실행 중인지 확인하여 Cisco 통합 서비스 가용성에서 서비스가 실행 중인지 확인할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리(Unified Communications Manager 인증서 모니터링의 경우) 또는 Cisco Unified IM and Presence 관리(IM and Presence Service 인증서 모니터링의 경우)에 로그인합니다.

단계 **2** 보안 > 인증서 모니터를 선택합니다.

단계 **3** 알림 시작 시간 필드에 숫자 값을 입력합니다. 이 값은 시스템이 만료 예정을 통지하기 시작한 인증서 만료 전 일 수를 나타냅니다.

단계 **4** 알림 빈도 필드에 알림 빈도를 입력합니다.

단계 **5** (선택 사항) 시스템이 예정된 인증서 만료에 대한 전자 메일 알림을 보내도록 하려면 전자 메일 알림 활성화 확인란을 선택합니다.

단계 **6** 인증서 상태 검사에 LSC 인증서를 포함시키려면 **LSC** 모니터링 활성화 확인란을 선택합니다.

단계 **7** 전자 메일 **ID** 필드에 시스템에서 알림을 보낼 전자 메일 주소를 입력합니다. 세미콜론으로 구분하여 여러 개의 전자 메일 주소를 입력할 수 있습니다.

단계 **8** 저장을 클릭합니다.

참고 인증서 모니터 서비스는 기본적으로 24시간 마다 실행됩니다. 인증서 모니터 서비스를 다시 시작하면 서비스를 시작한 다음 24시간 후에만 실행되도록 다시 일정을 계산합니다. 간격은 인증서가 만료일 7일 전까지도 변경되지 않습니다. 인증서가 만료되었거나 만료 1일 전이 되면 1시간 마다 실행됩니다.

다음에 수행할 작업

시스템이 만료된 인증서를 자동으로 취소하도록 OCSP(온라인 인증서 상태 프로토콜)를 구성합니다. 자세한 내용은 OCSP를 통해 인증서 해지 구성, 19 페이지을 참조하십시오.

OCSP를 통해 인증서 해지 구성

OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서 상태를 정기적으로 확인하고 만료된 인증서를 자동으로 해지할 수 있습니다.

시작하기 전에

시스템에 OCSP 검사에 필요한 인증서가 있는지 확인하십시오. OCSP 응답 특성으로 구성된 루트 또는 중간 CA 인증서를 사용하거나 tomcat-trust에 업로드된 지정된 OCSP 서명 인증서를 사용할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리(Unified Communications Manager 인증서 해지의 경우) 또는 Cisco Unified IM and Presence 관리(IM and Presence Service 인증서 해지의 경우)에 로그인합니다.

단계 **2** 보안 > 인증서 해지를 선택합니다.

단계 **3** **OCSP** 활성화 확인란을 선택하고 다음 작업 중 하나를 수행합니다.

- OCSP 확인을 위해 OCSP 응답자를 지정하려면 구성된 **OCSP URI** 사용 버튼을 선택하고 **OCSP** 가 구성된 **URI** 필드에 응답자의 URI를 입력합니다.
- 인증서가 OCSP 응답자 URI로 구성된 경우 인증서에서 **OCSP URI** 사용 버튼을 선택합니다.

단계 **4** 해지 확인 활성화 확인란을 선택합니다.

단계 **5** 해지 확인을 위한 간격 기간과 함께 모두 확인 필드를 완료합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** (선택 사항) CTI, IPsec 또는 LDAP 링크가있는 경우 수명이 긴 연결에 OCSP 해지 지원을 활성화하려면 위의 단계 외에도 다음 단계를 완료해야 합니다.

a) [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
b) 인증서 해지 및 만료 아래에서 인증서 유효성 확인 매개 변수를 **True**로 설정합니다.
c) 유효성 확인 빈도 매개 변수에 대한 값을구성합니다.

   참고 인증서 해지 창의 해지 확인 활성화 매개 변수의 간격 값은 유효성 확인 빈도 엔터프라이즈 매개 변수의 값보다 우선합니다.

d) 저장을 클릭합니다.