인증서 관리

인증서 개요

시스템은 자체 서명 인증서 및 타사 서명 인증서를 사용합니다. 인증서는 장치를 안전하게 인증하고 데이터를 암호화하고 데이터를 해싱하여 소스와 대상 간의 무결성을 보장하기 위해 시스템의 장치 간에 사용됩니다. 인증서를 사용하면 대역폭, 통신 및 작업을 안전하게 전송할 수 있습니다.

인증서의 가장 중요한 부분은 데이터를 암호화하고 대상 웹사이트, 전화 또는 FTP 서버와 같은 항목과 공유하는 방법을 숙지하고 정의하는 것입니다.

시스템이 인증서를 신뢰하는 경우 올바른 대상과 정보를 공유하는 것을 완벽하게 신뢰할 수 있도록 시스템에 인증서가 미리 설치되어 있음을 의미합니다. 그렇지 않으면, 이러한 지점 간 통신은 종료됩니다.

인증서를 신뢰하기 위해서는 타사 인증 기관(CA)과 미리 신뢰가 설정되어 있어야 합니다.

장치가 CA 및 중간 인증서를 먼저 신뢰할 수 있음을 알고 있어야 보안 소켓 레이어(SSL) 핸드셰이크라고 하는 메시지를 교환하여 제공되는 서버 인증서를 신뢰할 수 있습니다.

참고 Tomcat용 EC 기반 인증서가 지원됩니다. 이 새로운 인증서를 tomcat-ECDSA라고 합니다. 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence Service* 구성 및 관리의 IM and Presence Service 섹션에서 향상된 TLS 암호화를 참조하십시오.

Tomcat 인터페이스의 EC Ciphers는 기본적으로 비활성화됩니다. Cisco Unified Communications Manager 또는 IM and Presence Service에서 **HTTPS** 암호 엔터프라이즈 매개 변수를 사용하여 활성화할 수 있습니다. 이 매개 변수를 변경하는 경우 모든 노드에서 Cisco Tomcat 서비스를 다시 시작해야 합니다.

EC-기반 인증서에 대한 자세한 내용은 Cisco Unified Communications Manager 및 IM and Presence Service에서 릴리스 노트의 승인된 솔루션을 위한 일반 기준에 대한 ECDSA 지원을 참조하십시오.

타사 서명 인증서 또는 인증서 체인

애플리케이션 인증서를 서명한 인증 기관의 인증 기관 루트 인증서를 업로드합니다. 하위 인증 기관이 애플리케이션 인증서를 서명한 경우 하위 인증 기관의 인증 기관 루트 인증서를 업로드해야 합니다. 모든 인증 기관 인증서의 PKCS#7 형식 인증서 체인을 업로드할 수도 있습니다.

동일한 인증서 업로드 대화 상자를 사용하여 인증 기관 루트 인증서 및 애플리케이션 인증서를 업로드할 수 있습니다. 인증 기관 루트 인증서 또는 인증 기관 인증서만 포함된 인증서 체인을 업로드할 때는 형식 인증서 type-trust인 인증서 이름을 선택합니다. 애플리케이션 인증서 또는 애플리케이션 인증서와 인증 기관 인증서를 포함하는 인증서 체인을 업로드할 때는 인증서 유형만 포함하는 인증서 이름을 선택합니다.

예를 들어, Tomcat 인증 기관 인증서 또는 인증 기관 인증서 체인을 업로드할 때는 **tomcat-trust**를 선택하고 Tomcat 애플리케이션 인증서 또는 애플리케이션 인증서와 인증 기관 인증서를 포함하는 인증서 체인을 업로드할 때는 **tomcat** 또는 **tomcat ECDSA**를 선택합니다.

CAPF 인증 기관 루트 인증서를 업로드할 때 CallManager-trust 저장소로 복사되므로 하지 CallManager용 인증 기관 루트 인증서를 별도로 업로드할 필요가 없습니다.

참고 타사 인증 기관에서 서명한 인증서를 성공적으로 업로드하면 서명된 인증서를 가져오는 데 사용된 최근에 생성된 CSR을 삭제하고 타사에서 서명한 인증서(업로드한 경우)를 포함하여 기존 인증서를 덮어씁니다.

참고 시스템은 tomcat-trust, CallManager-trust 및 Phone-SAST-trust 인증서를 클러스터의 각 노드에 자동으로 복제합니다.

참고 디렉터리 신뢰 인증서를 tomcat-trust에 업로드할 수 있으며, 이는 DirSync 서비스가 보안 모드에서 작동하는 데 필요합니다.

타사 인증 기관 인증서

타사 인증 기관이 발행하는 애플리케이션 인증서를 사용하려면 인증 기관 또는 PKCS #7 인증서 체인에서 서명된 애플리케이션 인증서 및 인증 기관 루트 인증서를 모두 얻어야 합니다(구별된 인코딩 규칙 [DER]). 여기에는 애플리케이션 인증서와 인증 기관 인증서가 모두 포함됩니다. 인증 기관에서 이러한 인증서를 받는 방법에 대한 정보를 검색합니다. 프로세스는 인증 기관마다 다릅니다. 서명 알고리즘은 RSA 암호화를 사용해야 합니다.

Cisco Unified Communications 운영 체제는 프라이버시 향상 메일(PEM) 인코딩 형식으로 CSR을 생성합니다. 시스템은 DER 및 PEM 인코딩 형식의 인증서와 PEM 형식의 PKCS #7 인증서 체인을 사용할 수 있습니다. CAPF(인증 기관 프록시 기능)를 제외한 모든 인증서 유형의 경우 인증 기관 루트 인증서와 애플리케이션 인증서를 받아 각 노드에 업로드해야 합니다.

CAPF의 경우 인증 기관 루트 인증서와 애플리케이션 인증서를 받아 첫 번째 노드에만 업로드합니다. CAPF 및 Unified Communications ManagerCSR은 인증 기관으로부터 애플리케이션 인증서 요청 시 포함해야 하는 확장을 포함합니다. 인증 기관이 ExtensionRequest 메커니즘을 지원하지 않을 경우 다음과 같이 X.509 확장을 활성화해야 합니다.

- CAPF CSR은 다음 확장을 사용합니다.

```
X509v3 확장 키 사용: TLS, 웹 서버 인증 X509v3 키 사용: 디지털 서명, 인증서 서명
```

- Tomcat 및 Tomcat-ECDSA용 CSR은 다음과 같은 확장을 사용합니다.

참고 Tomcat 또는 Tomcat-ECDSA 는 키 계약 또는 IPsec 엔드 시스템 키 사용을 요구하지 않습니다.

```
X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템
X509v3 키 사용: 디지털 서명, 키 암호화, 데이터 암호화, 키 계약
```

- IPsec용 CSR은 다음 확장을 사용합니다.

```
 X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템
X509v3 키 사용: 디지털 서명, 키 암호화, 데이터 암호화, 키 계약
```

- Unified Communications Manager용 CSR은 다음 확장을 사용합니다.

```
X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증 X509v3 키 사용: 디지털
 서명, 키 암호화, 데이터 암호화, 키 계약
```

- IM and Presence Service cup 및 cup-xmpp 인증서에 대한 CSR은 다음 확장을 사용합니다.

```
X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템
X509v3 키 사용: 디지털 서명, 키 암호화, 데이터 암호화, 키 계약,
```

참고 인증서에 대한 CSR을 생성하고 SHA256 서명을 사용하여 타사 인증 기관이 서명하도록 할 수 있습니다. 그런 다음 이 서명된 인증서를 다시 Unified Communications Manager에 업로드하여, Tomcat 및 기타 인증서가 SHA256을 지원할 수 있습니다.

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 ***1: 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 ***2: 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
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		

인증서 표시

인증서 목록 페이지의 필터 옵션을 사용하여 공통 이름, 만료 날짜, 키 유형 및 사용법을 기준으로 인증서 목록을 정렬하고 조회합니다. 따라서 필터 옵션을 사용하면 데이터를 효과적으로 정렬, 조회 및 관리할 수 있습니다.

Unified Communications Manager 릴리스 14에서, 사용 옵션을 선택하여 ID 또는 신뢰 인증서 목록을 정렬 및 조회할 수 있습니다.

프로시저

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

단계 **2** 인증서 목록 찾기 드롭다운 목록에서 필수 필터 옵션을 선택하고 찾기 필드에 검색 항목을 입력한 다음, 찾기 버튼을 클릭합니다.

예를 들면, ID 인증서만 조회하려면 사용을 인증서 목록 찾기 드롭다운 목록에서 선택하고, 찾기 필드에 ID를 입력한 다음, 찾기 버튼을 클릭합니다.

인증서 다운로드

인증서 다운로드 작업을 사용하여 인증서 사본을 가져오거나 CSR 요청을 제출할 때 인증서를 업로드할 수 있습니다.

프로시저

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

단계 **2** 검색 기준을 지정하고 찾기를 클릭합니다.

단계 **3** 필요한 파일 이름을 선택하고 다운로드를 클릭합니다.

중간 인증서 설치

중간 인증서를 설치하려면 먼저 루트 인증서를 설치하고 서명된 인증서를 업로드해야 합니다. 이 단계는 특정 체인에서 여러 인증서가 있는 서명된 인증서를 인증기관에서 제공하는 경우에만 필요합니다.

프로시저

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

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 적절한 신뢰 저장소를 선택하여 루트 인증서를 설치합니다.

단계 **4** 선택한 인증서 용도에 대한 설명을 입력합니다.

단계 **5** 다음 단계 중 하나를 수행하여 업로드할 파일을 선택합니다.

- 파일 업로드 텍스트 상자에서 파일의 경로를 입력합니다.
- 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.

단계 **6** 업로드를 클릭합니다.

단계 **7** 고객 인증서를 설치한 후 FQDN을 사용하여 Cisco Unified Intelligence Center URL에 액세스합니다. IP 주소를 사용하여 Cisco Unified Intelligence Center에 액세스하는 경우 사용자 지정 인증서를 성공적으로 설치한 후에도 "계속 하려면 여기를 클릭해야 합니다." 메시지가 표시됩니다.

참고
- Tomcat 인증서가 업로드되면 TFTP 서비스를 비활성화하고 나중에 활성화해야 합니다. 그렇지 않으면 TFTP는 이전 캐시된 자체 서명 tomcat 인증서를 계속 제공하게 됩니다.

신뢰 인증서 삭제

신뢰할 수 있는 인증서는 삭제할 수 있는 유일한 인증서 유형입니다. 시스템에서 생성되는 자체 서명된 인증서는 삭제할 수 없습니다.

⚠

주의 인증서를 삭제하면 시스템 작동에 영향을 미칠 수 있습니다. 또한 인증서가 기존 체인의 일부인 경우 인증서 체인이 끊어질 수 있습니다. 인증서 목록 창에서 관련 인증서의 사용자 이름 및 제목 이름에서 이 관계를 확인합니다. 이 작업은 취소할 수 없습니다.

프로시저

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

단계 **2** 찾기 제어를 사용하여 인증서 목록을 필터링합니다.

단계 **3** 인증서의 파일 이름을 선택합니다.

단계 **4** 삭제를 클릭합니다.

단계 **5** 확인을 클릭합니다.

참고
- “CAPF-trust”, “tomcat-trust”, “CallManager-trust” 또는 “Phone-SAST-trust” 인증서 유형을 삭제하는 경우 클러스터의 모든 서버에서 인증서가 삭제됩니다.
- CAPF-trust로 인증서를 가져오는 경우 해당 특정 노드에서만 활성화되고 클러스터 전체에 복제되지 않습니다.

인증서 다시 생성

인증서가 만료되기 전에 재생성하는 것이 좋습니다. 인증서가 만료될 때 RTMT(Syslog 뷰어)와 이메일 알림을 받게 됩니다.

그러나 만료된 인증서를 재생성할 수도 있습니다. 전화기를 다시 시작하고 서비스를 다시 부팅해야 하기 때문에 업무 시간이 끝난 후 이 절차를 수행합니다. Cisco Unified OS 관리에서 유형이 "cert"로 나열되는 인증서만 재생성할 수 있습니다.

⚠

주의 인증서를 다시 생성하면 시스템 작동에 영향을 미칠 수 있습니다. 인증서를 다시 생성하면 업로드된 경우 타사 서명 인증서를 포함하여 기존 인증서를 덮어씁니다.

프로시저

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

검색 매개변수를 입력하여 인증서를 찾고 해당 구성 세부 정보를 봅니다. 인증서 목록 창의 모든 기준과 일치하는 레코드가 표시됩니다.

인증서 세부 정보 페이지에서 재생성 버튼을 클릭하면 키 길이가 동일한 자체 서명 인증서가 재생성됩니다.

자체 서명 인증서 생성을 클릭하여 새 키 길이가 3072 또는 4096인 자체 서명 인증서를 재생성합니다.

단계 **2** 새 자체 서명 인증서 생성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **3** 생성을 클릭합니다.

단계 **4** 다시 생성된 인증서의 영향을 받는 모든 서비스를 다시 시작합니다.자세한 내용은 인증서 이름 및 설명, 8 페이지을 참조하십시오.

단계 **5** CAPF, ITLRecovery 인증서 또는 CallManager 인증서를 재생성한 후에 CTL 파일(필요한 경우)을 업데이트합니다.

참고 인증서를 다시 생성한 후 최신 백업이 다시 생성된 인증서를 포함하도록 시스템 백업을 수행해야 합니다. 백업에 다시 생성된 인증서가 포함되어 있지 않고 시스템 복원 작업을 수행하는 경우 전화기를 등록할 수 있도록 시스템에서 각 전화기를 수동으로 잠금 해제해야 합니다.

인증서 이름 및 설명

다음 표에서는 다시 생성할 수 있는 시스템 보안 인증서 및 다시 시작해야 하는 관련 서비스에 대해 설명합니다. TFTP 인증서 다시 생성에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html 에서 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

표 ***3:*** 인증서 이름 및 설명

이름	설명	관련 서비스
tomcat tomcat-ECDSA	이 인증서는 SIP Oauth 모드가 활성화되어 있는 경우 WebServices, Cisco DRF 서비스 및 Cisco CallManager 서비스에서 사용합니다.	Cisco 톰캣 서비스, Cisco 콜매니저 서비스, HAProxy 서비스, CISCO DRS(재해 복구 시스템) 로컬 및 마스터 서비스
ipsec	이 자체 서명 루트 인증서는 설치하는 동안 Unified Communications Manager, MGCP, H.323 및 IM and Presence 서비스와 IPsec 연결을 위해 생성됩니다.	IPsec 서비스
CallManager CallManager-ECDSA	이는 SIP, SIP 트렁크, SCCP, TFTP 등에 사용됩니다.	CallManager - HAProxy 서비스 CallManager-ECDSA - Cisco CallManager 서비스
CAPF	Unified Communications Manager 퍼블리셔에서 실행되는 CAPF 서비스에서 사용합니다. 이 인증서는 엔드포인트에 LSC를 발급하기 위해 사용됩니다(온라인 및 오프 라인 CAPF 모드 제외).	해당 없음

이름	설명	관련 서비스
TVS	이는 서버 인증서가 변경되는 경우 전화기에 대한 보조 신뢰 확인 방법의 역할을 담당하는 TVS(Trust Verification Service, 신뢰 확인 서비스)에서 사용합니다.	해당 없음

참고 보안 매개변수 섹션의 인증서 업데이트에 대한 새 엔터프라이즈 매개변수 전화기 상호 작용은 TVS, CAPF 또는 TFTP 인증서 중 하나가 업데이트될 때 적용 가능한 대로 수동으로 또는 자동으로 전화기를 재설정하는 데 사용됩니다. 이 매개변수는 전화기를 자동으로 재설정하는 것을 기본값으로 설정되어 있습니다.

OAuth 새로 고침 로그인을 위해 키 다시 생성

명령줄 인터페이스를 사용하여 암호화 키와 서명 키를 다시 생성하려면 이 절차를 사용합니다. Cisco Jabber가 Unified Communications Manager의 OAuth 인증을 위해 사용하는 암호화 키 또는 서명 키가 손상된 경우 이 작업을 완료합니다. 서명 키는 비대칭이고 RSA 기반인 반면 암호화 키는 대칭 키입니다.

이 작업을 완료한 후 이러한 키를 사용하는 현재 액세스 및 새로 고침 토큰은 무효화됩니다.

최종 사용자에게 미치는 영향을 최소화하기 위해 근무 시간 이후에 이 작업을 수행하는 것이 좋습니다.

암호화 키는 아래의 CLI를 통해서만 다시 생성될 수 있지만 서명 키는 퍼블리셔의 Cisco Unified OS 관리 GUI를 사용하여 다시 생성할 수도 있습니다. 보안 > 인증서 관리를 선택하고 **AUTHZ** 인증서를 선택한 다음, 다시 생성을 클릭합니다.

프로시저

단계 **1** Unified Communications Manager 퍼블리셔 노드에서 명령줄 인터페이스에 로그인합니다.

단계 **2** 암호화 키를 다시 생성하려면:

a) `set key regen authz encryption` 명령을 실행합니다.

b) `yes`를 입력합니다.

단계 **3** 서명 키를 다시 생성하려면:

a) `set key regen authz signing` 명령을 실행합니다.

b) `yes`를 입력합니다.
Unified Communications Manager 게시자 노드는 키를 다시 생성하고 새 키를 IM and Presence Service 노드를 포함한 모든 Unified Communications Manager 클러스터 노드에 복제합니다.

모든 UC 클러스터에 새 키를 다시 생성하고 동기화해야 합니다.

- IM and Presence 중앙 클러스터—IM and Presence 중앙 집중식 배포가 있는 경우 IM and Presence 노드는 텔레포니의 개별 클러스터에서 실행됩니다. 이 경우 IM and Presence Service 중앙 클러스터의 Unified Communications Manager 게시자 노드에서 이 절차를 반복합니다.
- Cisco Expressway 또는 Cisco Unity Connection—이러한 클러스터에서도 키를 다시 생성합니다. 자세한 내용은 Cisco Expressway 및 Cisco Unity Connection 설명서를 참조하십시오.

참고 다음 시나리오에서는 Cisco XCP 인증 서비스를 다시 시작해야 합니다.

- Authz 인증서를 재생성하는 경우
- IM and Presence 관리자 콘솔에서 중앙 집중식 배포에 대한 새 항목을 만들 경우

인증서 또는 인증서 체인 업로드

시스템이 신뢰하도록 하려는 새 인증서 또는 인증서 체인을 업로드합니다.

프로시저

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

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.

단계 **4** 다음 단계 중 하나를 수행하여 업로드할 파일을 선택합니다.

- 파일 업로드 텍스트 상자에서 파일의 경로를 입력합니다.
- 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.

단계 **5** 서버에 파일을 업로드하려면 파일 업로드를 클릭합니다.

참고 인증서를 업로드 한 후 영향을 받는 서비스를 다시 시작합니다. 서버가 다시 켜지면 CCMAdmin 또는 CCMUser GUI에 액세스하여 새로 추가되어 사용 중인 인증서를 확인할 수 있습니다.

타사 **CA(**인증기관**)** 인증서 관리

이 작업 플로우은 순서대로 각 단계를 참조하여 타사 인증 프로세스의 개요를 제공합니다. 이 시스템은 타사 인증기관이 PKCS # 10 인증서 서명 요청(CSR)으로 발행하는 인증서를 지원합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 서명 요청 생성, 11 페이지	인증서 애플리케이션 정보, 공개 키, 조직 이름, 일반 이름, 지역 및 국가를 포함하는 암호화된 텍스트 블록인 인증서 서명 요청(CSR)을 생성합니다. 인증기관은 이 CSR을 사용하여 시스템에 대한 신뢰할 수 있는 인증서를 생성합니다.
단계 **2**	CSR(Certificate Signing Request) 다운로드, 12 페이지	CSR을 생성 후 다운로드하고 인증기관에 제출할 준비를 합니다.
단계 **3**	인증기관 설명서를 참조하십시오.	인증기관에서 애플리케이션 인증서를 가져옵니다.
단계 **4**	인증기관 설명서를 참조하십시오.	인증기관에서 루트 인증서를 가져옵니다.
단계 **5**	인증기관 서명 CAPF 루트 인증서를 신뢰 저장소에 추가 , 12 페이지	루트 인증서를 신뢰 저장소에 추가합니다. 인증기관에서 서명한 CAPF 인증서를 사용할 때는 이 단계를 수행합니다.
단계 **6**	인증서 또는 인증서 체인 업로드, 10 페이지	노드에 인증기관 루트 인증서를 업로드합니다.
단계 **7**	CAPF 또는 Cisco Unified Communications Manager용 인증서를 업데이트한 경우 새 CTL 파일을 생성합니다.	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오. 타사에서 서명한 CAPF 또는 CallManager 인증서를 업로드한 후에 CTL 클라이언트(구성된 경우)를 다시 실행합니다.
단계 **8**	서비스 다시 시작, 13 페이지	새 인증서의 영향을 받는 서비스를 다시 시작합니다. 모든 인증서 유형에 대해 해당 서비스를 다시 시작합니다(예를 들어, Tomcat 또는 Tomcat-ECDSA 인증서를 업데이트한 경우 Cisco Tomcat 서비스를 다시 시작).

인증서 서명 요청 생성

인증서 애플리케이션 정보, 공개 키, 조직 이름, 일반 이름, 지역 및 국가를 포함하는 암호화된 텍스트 블록인 인증서 서명 요청(CSR)을 생성합니다. 인증기관은 이 CSR을 사용하여 시스템에 대한 신뢰할 수 있는 인증서를 생성합니다.

참고 새 CSR을 생성하는 경우 기존 CSR을 덮어씁니다.

프로시저

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

단계 **2** **CSR** 생성을 클릭합니다.

단계 **3** 인증서 서명 요청 생성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 생성을 클릭합니다.

CSR(Certificate Signing Request) 다운로드

CSR을 생성 후 다운로드하고 인증기관에 제출할 준비를 합니다.

프로시저

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

단계 **2** **CSR** 다운로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.

단계 **4** **CSR** 다운로드를 클릭합니다.

단계 **5** (선택 사항) 프롬프트가 표시되면 저장을 클릭합니다.

인증기관 서명 **CAPF** 루트 인증서를 신뢰 저장소에 추가

인증기관에서 서명한 CAPF 인증서를 사용할 때 신뢰 저장소에Unified Communications Manager 루트 인증서를 추가합니다.

프로시저

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

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서/인증서 체인 업로드 팝업 창의 인증서 용도 드롭다운 목록에서 **CallManager-trust**를 선택하고 인증기관에서 서명한 CAPF 루트 인증서로 이동합니다.

단계 **4** 파일 업로드 필드에 인증서가 나타나면 업로드를 클릭합니다.

서비스 다시 시작

시스템이 클러스터의 특정 노드에서 기능 또는 네트워크 서비스를 다시 시작해야 하는 경우 이 절차를 사용합니다.

프로시저

단계 **1** 다시 시작하는 서비스 유형에 따라 다음 작업 중 하나를 수행합니다.

- 도구제어 센터 > - 기능 서비스를 선택합니다.
- 도구제어 센터 > - 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 시스템 노드를 선택하고 이동을 클릭합니다.

단계 **3** 다시 시작할 서비스 옆의 라디오 버튼을 클릭하고 다시 시작을 클릭합니다.

단계 **4** 다시 시작하는 데 약간 시간이 걸린다는 메시지가 표시되면 확인을 클릭합니다.

온라인 인증서 상태 프로토콜을 통한 인증서 해지

Unified Communications Manager는 인증서 해지를 모니터링하기 위한 OCSP를 제공합니다. 시스템은 예약된 간격 동안, 그리고 인증서가 업로드될 때마다 유효성을 확인하기 위해 인증서 상태를 확인합니다.

OCSP(온라인 인증서 상태 프로토콜)는 관리자가 시스템의 인증서 요구 사항을 관리하는 데 도움을 줍니다. OCSP가 구성된 경우 인증서 유효성을 확인하고 만료된 인증서를 실시간으로 해지하는 간단하고 안전하며 자동화된 방법을 제공합니다.

일반 기준 모드를 사용하는 FIPS 배포의 경우, OCSP도 일반 기준 요구 사항을 준수하는 데 도움이 됩니다.

유효성 확인

Unified Communications Manager는 인증서 상태를 확인하고 유효성을 확인합니다.

인증서는 다음과 같이 확인됩니다.

- Unified Communications Manager는 DTM(위임 신뢰 모델)을 사용하고 루트 CA 또는 중간 CA에 OCSP 서명 특성을 확인합니다. 루트 CA 또는 중간 CA는 상태를 확인하기 위해 OCSP 인증서에 서명해야 합니다. 위임 신뢰 모델이 실패하면 Unified Communications Manager가 TRP(신뢰 응답기 모델)로 대체하고 OCSP 서버의 지정 된 OCSP 응답 서명 인증서를 사용하여 인증서를 확인합니다.

참고 인증서의 해지 상태를 확인하려면 OCSP 응답자를 실행하고 있어야 합니다.

- 인증서 해지 창에서 OCSP 옵션을 활성화하여 실시간으로 인증서 해지를 확인하는 가장 안전한 방법을 제공합니다. 인증서 또는 구성된 OCSP URI에서 OCSP URI를 사용하려면 옵션에서 선택합니다. 수동 OCSP 구성에 대한 자세한 내용은 OCSP를 통해 인증서 해지 구성을 참조하십시오.

참고 리프 인증서의 경우 syslog, FileBeat, SIP, ILS, LBM 등과 같은 TLS 클라이언트는 OCSP 응답자에게 OCSP 요청을 보내고 OCSP 응답자로부터 실시간으로 인증서 해지 응답을 받습니다.

유효성 검사가 수행되고 일반 기준 모드가 켜지면 다음 상태 중 하나가 인증서에 반환됩니다.

- 정상 --정상 상태는 상태 질의에 대한 긍정적 응답을 나타냅니다. 최소한 이 긍정 응답은 인증서가 해지되지 않은 것으로 표시되지만 반드시 인증서가 발급되었음을 의미하는 것이 아니라 응답이 생성된 시간이 인증서의 유효 간격 내에 있음을 나타냅니다. 응답 확장은 발급, 유효성 등에 대한 긍정적 진술과 같은 인증서의 상태와 관련하여 응답자에 의한 추가 정보를 전달하는 데 사용될 수 있습니다.
- 해지됨 - 해지됨 상태는 인증서가 해지되었음을 나타냅니다(영구 또는 임시적(보류 중)).
- 알 수 없음-- 알 수 없음 상태는 OCSP 응답기에서 요청 중인 인증서를 알지 못하는 것을 나타냅니다.

참고 일반 기준 모드에서는 연결이 해지됨과 알 수 없음 케이스 모두에서 실패하는 반면, 연결은 일반 기준이 활성화되지 않은 경우 알 수 없음 응답 케이스에서 성공합니다.

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, 15 페이지	자동 인증서 모니터링을 구성합니다. 시스템은 인증서 상태를 주기적으로 확인하고 인증서의 만료가 다가오면 사용자에게 전자 메일을 보냅니다.
단계 **2**	OCSP를 통해 인증서 해지 구성, 16 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, 16 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.

인증서 오류 문제 해결

시작하기 전에

IM and Presence Service 노드의 Unified Communications Manager 서비스 또는 Unified Communications Manager 노드의 IM and Presence Service 기능에 액세스하려 할 때 오류가 발생하는 경우 문제의 원인은 tomcat-trust 인증서입니다. 오류 메시지 서버에 연결할 수 없습니다(원격 노드에 연결할 수 없음)이 다음 서비스 가용성 인터페이스 창에 나타납니다.

- 서비스 활성화
- 컨트롤 센터 - 기능 서비스
- 컨트롤 센터 - 네트워크 서비스

이 절차를 사용하여 인증서 오류를 해결합니다. 첫 단계부터 시작하고 필요한 경우 계속 진행합니다. 때때로 첫 단계만 완료해도 오류를 해결할 수 있으며 기타의 경우 모든 단계를 완료해야 합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택하여 필수 tomcat-trust 인증서가 있는지 확인합니다.

필수 인증서가 없는 경우 30분 기다렸다가 다시 확인합니다.

단계 **2** 해당 정보를 보려는 인증서를 선택합니다. 콘텐츠가 원격 노드에 있는 해당 인증서와 일치하는지 확인합니다.

단계 **3** CLI에서 Cisco 인터클러스터 동기화 에이전트 서비스를 다시 시작합니다. **utils service restart Cisco Intercluster Sync Agent**.

단계 **4** Cisco 인터클러스터 동기화 에이전트 서비스가 다시 시작되면 Cisco Tomcat 서비스를 다시 시작합니다. **utils service restart Cisco Tomcat**.

단계 **5** 30분이 소요됩니다. 이전 단계로 인증서 오류가 해결되지 않고 tomcat-trust 인증서가 있는 경우 인증서를 삭제합니다. 인증서를 삭제한 후 각 노드에 대한 Tomcat 및 Tomcat-ECDSA 인증서를 다운로드하고 피어에 tomcat-trust 인증서로 업로드하여 수동으로 교환해야 합니다.

단계 **6** 인증서 교환이 완료된 후 각 영향을 받는 서버에서 Cisco Tomcat을 다시 시작합니다. **utils service restart Cisco Tomcat**.