기본 보안 구성

보안 구성 정보

이 섹션에서는 Cisco Unified Communications Manager를 설정하기 위해 수행해야 하는 기본 보안 구성 작업에 대한 정보를 제공합니다.

보안 구성 작업

다음 작업을 수행하여 기본 보안 구성을 설정합니다.

클러스터에 대한 혼합 모드 활성화

이 절차를 사용하여 클러스터에서 혼합 모드를 활성화합니다.

프로시저

단계 **1** 퍼블리셔 노드의 CLI(Command Line Interface)에 로그인합니다.

단계 **2** **utils ctl set-cluster mixed-mode** CLI 명령을 실행합니다.

참고 Communications Manager가 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 등록되어 있는지, 스마트 어카운트 또는 가상 어카운트에서 수신한 등록 토큰에 이 클러스터에 등록 중인 동안 내보내기 제어 기능 허용이 활성화되어 있는지 확인하십시오.

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.

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.

타사 **CA** 루트 인증서 업로드

CA 루트 인증서를 CAPF-trust 저장소 및 Unified Communications Manager trust 저장소에 업로드하여 외부 CA를 사용하여 LSC 인증서에 서명합니다.

참고 타사 CA를 사용하여 LSC에 서명하지 않으려면 이 작업을 건너뜁니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서 용도 드롭다운 목록에서 **CAPF-trust**를 선택합니다.
단계 **4** 인증서에 대한 설명을 입력합니다. 예를 들어, 외부 **LSC** 서명 **CA**에 대한 인증서입니다.
단계 **5** 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.
단계 **6** 업로드를 클릭합니다.
단계 **7** 이 작업을 반복하여 인증서 용도에 대한 **callmanager-trust**에 인증서를 업로드합니다.

TLS 사전 요건:

최소 TLS 버전을 구성하기 전에, 네트워크 디바이스 및 애플리케이션에서 모두 TLS 버전을 지원하는지 확인하십시오. 또한 Unified Communications Manager 및 IM and Presence 서비스를 사용하여 구성하려는 TLS에 대해서도 활성화되어 있는지 확인하십시오. 다음 제품 중 하나가 구축된 경우, 최소 TLS 요구 사항을 충족하고 있는지 확인하십시오. 이러한 요구 사항을 충족되지 않은 경우, 다음과 같은 제품을 업그레이드해야 합니다.

- SCCP(Skinny Client Control Protocol) 전화회의 브리지
- 트랜스코더
- 하드웨어 MTP(미디어 터미네이션 포인트)
- SIP Gateway
- Cisco Prime Collaboration 보증
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element(CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

컨퍼런스 브리지, MTP(Media Termination Point), Xcoder, Prime Collaboration Assurance, Prime Collaboration Provisioning, Cisco Unity Connection, Cisco Meeting Server, Cisco IP Phones, Cisco Room 장치, FOS(Fusion Onboarding Service), Common Identity Service, SLM(Smart License Manager), Push REST 서비스, Cisco Jabber 및 Webex 앱 클라이언트와 다른 타사 응용 프로그램 등 클라우드 서비스를 업그레이드할 수 없습니다.

참고 이전 버전의 Unified Communications Manager를 업그레이드하는 경우, 모든 디바이스 및 애플리케이션에서 더 높은 버전의 TLS를 지원하는지 확인하십시오. 예를 들어, Unified Communications Manager 및 IM and Presence 서비스, 릴리스 9.x는 TLS 1.0만 지원합니다.

최저 TLS 버전 설정

기본값으로 Unified Communications Manager에서는 1.0의 최소 TLS 버전을 지원합니다. 이 절차를 사용하여 Unified Communications Manager에 대해 지원되는 최소 TLS 버전을 재설정하고, IM and Presence 서비스를 1.1 또는 1.2와 같은 상위 버전으로 재설정합니다.

네트워크 디바이스 및 애플리케이션에서 구성하려는 TLS 버전을 지원하는지 확인하십시오. 자세한 내용은 TLS 사전 요건:, 4 페이지를 참조하십시오.

프로시저

단계 **1** **CLI(Command Line Interface)**에 로그인합니다.

단계 **2** 기존 TLS 버전을 확인하려면, **show tls min-version** CLI 명령을 실행합니다.

단계 **3** <*minimum*>가 TLS 버전을 나타내는 **set tls min-version**<*minimum*> CLI 명령어를 실행합니다.

예를 들어, **set tls min-version 1.2**을 실행하여 최소 TLS 버전을 1.2로 설정합니다.

참고 릴리스 15SU1까지 모든 Unified Communications Manager 및 IM and Presence 서비스 서비스 클러스터 노드에서 **3**단계를 수행합니다.

TLS 암호화 설정

SIP 인터페이스에 사용 가능한 가장 강력한 암호를 선택하여 더 약한 암호를 비활성화할 수 있습니다. 이 절차를 사용하여 Unified Communications Manager에서 TLS 연결 설정을 위해 지원하는 암호를 구성합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 보안 매개변수에서 **TLS** 암호화 엔터프라이즈 매개변수에 대한 값을 구성합니다. 사용 가능한 옵션에 대한 도움말은 엔터프라이즈 매개변수 온라인 도움말을 참조하십시오.

단계 **3** 저장을 클릭합니다.

참고 모든 TLS 암호는 클라이언트 암호화 기본 설정에 따라 조정됩니다.