CAPF 구성

CAPF(Certificate Authority Proxy Function) 설정

CAPF(Certificate Authority Proxy Function)는 LSC(Locally Significant Certificate)를 발급하고 Cisco 엔드포인트를 인증하는 Cisco 독점 서비스입니다. CAPF 서비스는 Unified Communications Manager에서 실행되며 다음 작업을 수행합니다.

- 지원되는 Cisco Unified IP Phone에 LSC를 발급합니다.
- 혼합 모드가 활성화된 경우 전화기를 인증합니다.
- 전화기에 대한 기존 LSC를 업그레이드합니다.
- 보기 및 문제해결을 위해 전화기 인증서를 검색합니다.

CAPF 실행 모드

다음 모드에서 작동하도록 CAPF를 구성할 수 있습니다.

- CAPF(Cisco Authority Proxy Function)—Unified Communications Manager의 CAPF 서비스는 CAPF 서비스에서 자체 서명한 LSC를 발급합니다. 이것이 기본 모드입니다.
- 온라인 CA—이 옵션을 사용하여 전화기에 대한 외부 온라인 CA 서명 LSC를 확보합니다. CAPF 서비스는 자동으로 외부 CA에 연결됩니다. CSR이 제출되면 CA는 서명 후 CA 서명된 LSC를 자동으로 반환합니다.
- 오프라인 CA—오프라인 외부 CA를 사용하여 전화기의 LSC를 서명하려는 경우, 이 옵션을 사용합니다. 이 옵션을 사용하려면 LSC를 수동으로 다운로드하여 CA에 제출한 다음, CA 서명 인증서가 준비되고 나면 이를 업로드해야 합니다.

참고 타사 CA를 사용하여 LSC에 서명하려는 경우, Cisco에서는 프로세스가 자동화되고 훨씬 더 빨라져 문제가 발생할 가능성이 적기 때문에 온라인 **CA**를 오프라인 **CA** 대신 사용할 것을 권장합니다.

CAPF 서비스인증서

Unified Communications Manager가 설치되면 CAPF 서비스가 자동으로 설치되고 CAPF에 따른 시스템 인증서가 생성됩니다. 보안이 적용되면 Cisco CTL 클라이언트에서 인증서를 모든 클러스터 노드에 복사합니다.

전화기 인증서 유형

Cisco에서는 전화기에 다음과 같은 전화기 X.509v3 인증서 유형을 사용합니다.

- LSC(Locally Significant Certificate)—CAPF(Certificate Authority Proxy Function)와 관련된 필수 구성 작업을 수행한 후 지원되는 전화기에 설치되는 인증서입니다. 인증 또는 암호화를 위한 디바이스 보안 모드를 구성하고 나면 LSC가 Unified Communications Manager와 전화기 간의 연결을 보호합니다.

참고 온라인 CA의 경우, LSC 유효성은 CA에 기반하며 CA가 허용하는 한 사용할 수 있습니다.

- MIC(Manufacturing Installed Certificate)—Cisco Manufacturing에서 지원되는 전화기 모델에 MIC를 자동으로 설치합니다. 제조업체에서 설치한 인증서는 LSC 설치를 위해 Cisco CAPF(Certificate Authority Proxy Function)를 인증합니다. 제조업체에서 설치한 인증서를 덮어쓰기하거나 삭제할 수 없습니다.

참고 Cisco에서는 LSC 설치용으로만 MIC(Manufacturer Installed Certificate)를 사용할 것을 권장합니다. Cisco에서는 LSC를 지원하여 Unified Communications Manager와 TLS 연결을 인증합니다. MIC 루트 인증서의 보안이 침해될 수 있으므로, TLS 인증을 위해 MIC를 사용하기 위해 또는 다른 목적으로 전화기를 구성하는 고객은 이러한 위험을 감수해야 합니다. MIC의 보안이 침해된 경우 Cisco에서는 어떤 책임도 지지 않습니다.

CAPF를 통한 **LSC** 세대

CAPF를 구성한 후에는 전화기에 구성된 인증 문자열을 추가합니다. 전화기와 CAPF 간에 키 및 인증서 교환이 발생하고 다음과 같은 상황이 발생합니다.

- 전화기에서 구성된 인증 방법을 사용하여 CAPF에 대해 자체 인증을 진행합니다.

- 전화기에서 공개-개인 키 쌍을 생성합니다.
- 전화기에서 서명된 메시지로 공개 키를 CAPF로 착신 전송합니다.
- 개인 키는 전화기에 남아 있으며 외부에 절대 공개되지 않습니다.
- CAPF에서 전화기 인증서에 서명하고 서명된 메시지로 전화기에 인증서를 보냅니다.

참고 전화기 사용자가 인증서 작업을 중단하거나 전화기의 작동 상태를 볼 수 있으니, 주의하십시오.

참고 우선 순위가 낮게 설정되어 있는 키 생성을 통해 작업 수행 중에도 전화기가 작동할 수 있습니다. 인증 생성 중에 전화기가 작동하더라도 추가 TLS 트래픽으로 인해 전화기에 대한 최소 통화 처리 중단이 발생할 수 있습니다. 예를 들어, 설치가 끝날 때 인증서가 플래시에 기록되면 오디오 결함이 발생할 수 있습니다.

CAPF 사전 요건

LSC 생성을 위해 CAPF(Certificate Authority Proxy Function)를 구성하기 전에 다음 작업을 수행합니다.

- 타사 CA를 사용하여 LSC에 서명하려는 경우, 외부에서 CA를 구성합니다.
- 전화기 인증 방법을 계획합니다.
- LSC를 생성하기 전에 다음을 갖추고 있는지 확인하십시오.
  - Unified Communications Manager 릴리스 12.5 이상.
  - 인증서에 CAPF를 사용하는 엔드포인트(Cisco IP 전화기 및 Jabber 포함).
  - Microsoft Windows Server 2012 및 2016.
  - DNS(Domain name Service)가 구성되어 있습니다.
- CA 루트 및 HTTPS 인증서를 업로드한 다음 LSC를 생성해야 합니다. 보안 SIP 연결 중에, HTTPS 인증서는 CAPF-trust를 통과하고 CA 루트 인증서는 CAPF-trust 및 CallManager-trust를 통과합니다. IIS(인터넷 정보 서비스)에서 HTTPS 인증서를 호스팅합니다. CA 루트 인증서는 CSR(인증서 서명 요청)에 서명하기 위해 사용됩니다.

  다음은 인증서를 업로드해야 할 경우에 대한 시나리오입니다.

표 *1:* 인증서 업로드 시나리오

시나리오	결과
CA 루트 인증서 및 HTTPS 인증서는 동일합니다.	CA 루트 인증서를 업로드합니다.
CA 루트 인증서 및 HTTPS 인증서는 서로 다르며, HTTPS 인증서는 동일한 CA 루트 인증서에서 발급합니다.	CA 루트 인증서를 업로드합니다.
중간 CA 및 HTTPS 인증서는 서로 다르며, CA 루트 인증서에서 발급합니다.	CA 루트 인증서를 업로드합니다.
CA 루트 및 HTTPS 인증서가 서로 다르며, 동일한 CA 루트 인증서에서 발급합니다.	CA 루트 및 HTTPS 인증서를 업로드합니다.

참고 여러 인증서를 동시에 생성하면 통화 처리 중단이 발생할 수 있기 때문에 예약된 유지보수 일정 안에 CAPF를 사용하실 것을 강력하게 권장합니다.

CAPF(Certificate Authority Proxy Function) 구성 작업 플로우

다음 작업을 완료하여 엔드포인트에 대한 LSC를 발행하도록 CAPF(Certificate Authority Proxy Function)을 구성합니다.

참고 새 CAPF 인증서를 다시 생성하거나 업로드하고 나면 CAPF 서비스를 다시 시작할 필요가 없습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	타사 CA 루트 인증서 업로드	LSC를 타사 CA 서명을 받게하려면 CA 루트 인증서 체인을 CAPF-trust 저장소에 업로드합니다. 그렇지 않은 경우 이 작업을 생략할 수 있습니다.
단계 **2**	CA(인증기관) 루트 인증서 업로드 , 6 페이지	CA 루트 인증서를 Trust 저장소에Unified Communications Manager 업로 합니다.
단계 **3**	온라인 CA(인증기관) 설정 구성, 6 페이지	이 절차를 사용하여 전화기 LSC 인증서를 생성합니다.

	명령 또는 동작	목적
단계 4	오프라인 CA(인증기관) 설정 구성	이 절차를 사용하여 오프라인 CA를 사용하는 전화기 LSC 인증서를 생성합니다.
단계 5	CAPF 서비스 활성화 또는 재시작	CAPF 시스템 설정을 구성한 후에 필수 CAPF 서비스를 활성화합니다.
단계 6	다음 절차 중 하나를 사용하여 Unified Communications Manager에서 CAPF 설정을 구성합니다. • 범용 디바이스 템플릿에서 CAPF 설정 구성, 9 페이지 • 벌크 관리자를 통한 CAPF 설정 업데이트, 10 페이지 • 전화기에 대한 CAPF 설정 구성, 12 페이지	다음 옵션 중 하나를 사용하여 CAPF 설정을 전화기 구성에 추가합니다. • LDAP 디렉터리를 동기화하지 않은 경우, CAPF 설정을 범용 디바이스 템플릿에 추가하고 초기 LDAP 동기화를 통해 설정을 적용합니다. • 벌크 관리 도구를 사용하여 단일 작업에서 여러 전화기에 CAPF 설정을 적용합니다. • 전화기 별로 CAPF 설정을 적용할 수 있습니다.
단계 7	KeepAlive 타이머 설정, 12 페이지	(선택 사항) CAPF 엔드포인트 연결에 대한 keepalive 값을 설정하여 방화벽에 의해 시간이 초과되지 않도록 합니다. 기본값은 15분입니다.

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.

CA(인증기관) 루트 인증서 업로드

클러스터 전체 인증서를 업로드 하 여 클러스터 내 모든 서버에 배포 합니다.

프로시저

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

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 **callManager-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.

중요 이 노트는 릴리스 14 SU2부터 적용할 수 있습니다.

참고 모든 루트 또는 중간 CA 인증서의 경우에는 다음과 같은 기본 X509 확장이 포함되어야 합니다.

X509v3 기본 제약조건:

CA:TRUE, pathlen:0

X509v3 키 사용:

디지털 서명, 인증서 서명

인증서에 이러한 확장이 누락된 경우 TLS 연결이 실패하게 됩니다.

중요 이 노트는 릴리스 14 SU3부터 IPsec 인증서에 대해서만 적용됩니다.

참고 CA 서명 IPsec 인증서의 경우 다음 확장을 포함하지 않아야 합니다.

X509v3 기본 제약조건:

CA:TRUE

온라인 CA(인증기관) 설정 구성

Unified Communications Manager에서 이 절차를 사용하여 온라인 CAPF를 사용하여 전화기 LSC를 생성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 서버 드롭다운 목록에서CAPF(Certificate Authority Proxy Function)(활성) 서비스를 활성화한 노드를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **CAPF(Certificate Authority Proxy Function)(**활성**)**을 선택합니다. 서비스 이름 옆에 "활성"이라는 단어가 표시되는지 확인하십시오.

단계 4 엔드포인트 대상 인증서 발급자 드롭다운 목록에서 온라인 **CA**를 선택합니다. CA 서명 인증서의 경우, 온라인 CA를 사용하는 것이 좋습니다.

단계 5 인증서 유효 기간**(**일**)** 필드에 1 ~ 1825 사이의 숫자를 입력하여 CAPF에서 발급한 인증서가 유효한 날짜의 수를 나타냅니다.

단계 6 온라인 **CA** 매개변수 섹션에서 다음 매개변수를 설정하여 온라인 CA 섹션에 대한 연결을 생성합니다.

- 온라인 CA 호스트네임—제목 이름 또는 CN(공통 이름)이 HTTPS 인증서의 FQDN(Fully Qualified Domain name)과 동일해야 합니다.

  참고 구성된 호스트네임은 Microsoft CA에서 실행되는 IIS(인터넷 정보 서비스)에서 호스팅하는 HTTP 인증서의 CN(공통 이름)과 동일 합니다.

- 온라인 CA 포트 - 온라인 CA에 대한 포트 번호를 입력합니다(예: 443).
- 온라인 CA 템플릿—템플릿의 이름을 입력합니다. Microsoft CA가 템플릿을 만듭니다.

  참고 이 필드는 온라인 CA 유형이 Microsoft CA인 경우에만 활성화됩니다.

- 온라인 CA 유형 - 엔드포인트 인증서의 자동 등록을 위해 Microsoft CA 또는 EST 지원 CA를 선택합니다.
  - Microsoft CA - CA가 디지털 인증서를 장치에 할당하는 Microsoft CA인 경우 이 옵션을 사용합니다.

    참고 FIPSS 활성화 모드는 Microsoft CA에서 지원되지 않습니다.

    - 중요 릴리스 14SU2부터 지원됩니다.

    EST 지원 CA - CA가 자동 등록을 위해 내장 EST 서버 모드를 지원하는 경우 이 옵션을 사용합니다.

- 온라인 CA 사용자 이름—CA 서버의 사용자 이름을 입력합니다.
- 온라인 CA 암호—CA 서버의 사용자 이름에 대한 암호를 입력합니다.
- 인증서 등록 프로파일 레이블 - 유효한 문자가 포함된 EST 지원 CA에 대한 디지털 ID를 입력합니다.

  참고 이 필드는 온라인 CA 유형이 EST 지원 CA인 경우에만 활성화됩니다.

단계 **7** 나머지 CAPF 서비스 매개변수를 완료합니다. 매개변수 이름을 클릭하여 서비스 매개변수 도움말 시스템을 봅니다.

단계 **8** 저장을 클릭합니다.

단계 **9** **CAPF(Certificate Authority Proxy Function)**를 다시 시작하여 변경 사항을 적용합니다. 그러면 Cisco 인증서 등록 서비스가 자동으로 다시 시작됩니다.

현재 온라인 **CA** 제한 사항

- CA 서버에서 영어 이외의 다른 언어를 사용하는 경우, 온라인 CA 기능이 작동하지 않습니다. CA 서버는 영어로만 응답해야 합니다.
- 온라인 CA 기능은 CA를 사용한 mTLS 인증을 지원하지 않습니다.
- LSC 작업에 온라인 CA를 사용하는 동안 LSC 인증서에 '디지털 서명' 및 '키 암호화' 키 사용이 제공되지 않을 경우 디바이스 보안 등록이 실패합니다.
- LSC 작업에 온라인 CA를 사용하는 동안 LSC 인증서에 '디지털 서명' 및 '키 암호화'를 제공하지 않을 경우 디바이스 보안 등록이 실패합니다.

오프라인 **CA(**인증기관**)** 설정 구성

오프라인 CA를 사용하여 전화기 LSC 인증서를 생성하기로 결정한 경우, 이 고급 프로세스를 수행합니다.

참고 오프라인 CA 옵션은 무수한 수동 단계와 관련이 있어 온라인 CA에 비해 시간이 더 오래 소요됩니다. 인증서 생성 및 전송 프로세스 중에 문제가 발생하는 경우(예: 네트워크 중단 또는 전화 재설정) 프로세스를 다시 시작합니다.

프로시저

단계 **1** 타사 CA(인증기관)에서 루트 인증서 체인을 다운로드합니다.

단계 **2** Unified Communications Manager에서 필수 신뢰(CallManager trust CAPF trust)에 루트 인증서 체인을 업로드합니다.

단계 **3** Unified Communications Manager을(를) 구성하여 엔드포인트에 인증서 발급 서비스 매개변수를 오프라인 CA로 설정하여 오프라인 CA를 사용합니다.

단계 **4** 전화기 LSC에 대한 **CSR**을 생성합니다.

단계 **5** **CSR**을 인증기관에 보냅니다

단계 **6** **CSR**에서 서명된 인증서를 가져옵니다.

오프라인 CA를 사용하여 전화기 LSC를 생성하는 방법에 대한 자세한 예는 CUCM 타사 CA 서명 LSC 생성 및 가져오기 구성을 참조하십시오.

CAPF 서비스 활성화 또는 재시작

CAPF 시스템 설정을 구성한 후에 필수 CAPF 서비스를 활성화합니다. CAPF 서비스가 이미 활성화된 경우 다시 시작합니다.

프로시저

단계 **1** Cisco 유니파이드 Serviceability에서 도구 > 서비스 활성화를 선택합니다.

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

단계 **3** [보안 서비스] 창에서 적용되는 서비스를 확인하십시오.

- **Cisco Certificate** 등록 서비스—온라인 CA를 사용하는 경우 이 서비스를 선택하고, 그렇지 않은 경우 선택하지 않은 상태로 둡니다.
- **CAPF(Certificate Authority Proxy Function)**—체크 표시되어 있지 않은 경우(비활성 상태), 이 서비스를 선택합니다. 서비스가 이미 활성화된 경우 다시 시작합니다.

단계 **4** 모든 설정을 수정한 경우, 저장을 클릭합니다.

단계 **5** **CAPF(Certificate Authority Proxy Function)**서비스가 이미 선택된 된 경우(활성 상태), 다음과 같이 다시 시작합니다.

a) 관련 링크 드롭다운 목록에서 컨트롤 센터 - 기능 서비스를 선택하고 이동을 클릭합니다.
b) 보안 설정 창에서 **CCAPF(Certificate Authority Proxy Function)**를 선택하고 재시작을 클릭합니다.

단계 **6** 다음 절차 중 하나를 완료하여 개별 전화기 대비 CAPF 설정을 구성합니다.

a) 범용 디바이스 템플릿에서 CAPF 설정 구성, 9 페이지
b) 벌크 관리자를 통한 CAPF 설정 업데이트, 10 페이지
c) 전화기에 대한 CAPF 설정 구성, 12 페이지

범용 디바이스 템플릿에서 CAPF 설정 구성

이 절차를 사용하여 범용 디바이스 템플릿에 CAPF 설정을 구성합니다. 기능 그룹 템플릿 구성을 통해 LDAP 디렉터리 동기화에 대해 템플릿을 적용합니다. 템플릿의 CAPF 설정은 이 템플릿을 사용하는 모든 동기화된 디바이스에 적용됩니다.

참고 동기화되지 않은 LDAP 디렉터리에 범용 디바이스 템플릿을 추가만 할 수 있습니다. 초기 LDAP 동기화가 발생한 경우, 벌크 관리를 사용하여 전화기를 업데이트합니다. 자세한 내용은 벌크 관리자를 통한 CAPF 설정 업데이트, 10 페이지를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 디바이스 템플릿을 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 템플릿을 선택합니다.
- 새로 추가를 클릭합니다.

단계 3 **CAPF(Certificate Authority Proxy Function)** 설정 영역을 확장합니다.

단계 4 인증서 작업 드롭다운 목록에서 설치/업그레이드를 선택합니다.

단계 5 인증 모드 드롭다운 목록 메뉴에서 디바이스가 자체 인증할 수 있는 옵션을 선택합니다.

단계 6 인증 문자열을 사용하기로 선택한 경우, 텍스트 상자에 인증 문자열을 입력하거나 문자열 생성을 클릭하여 시스템에서 문자열을 생성합니다.

참고 이 문자열이 디바이스 자체에 구성지 않은 경우 인증이 실패합니다.

단계 7 나머지 필드에서 키 정보를 구성합니다. 필드에 대해 도움이 필요한 경우, 온라인 도움말을 참조하십시오.

단계 8 저장을 클릭합니다.

참고 이 템플릿을 사용하는 디바이스를 이 절차에서 할당한 것과 동일한 인증 방법으로 구성했는지 확인하십시오. 그렇지 않으면 디바이스 인증이 실패합니다. 전화기 인증 구성 방법에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

단계 9 이 프로파일을 사용하는 디바이스에 템플릿 설정을 적용합니다.

a) 기능 그룹 템플릿 구성에 범용 디바이스 템플릿을 추가합니다.
b) 기능 그룹 템플릿을 동기화되지 않은 LDAP 디렉터리 구성에 추가합니다.
c) LDAP 동기화를 완료합니다. CAPF 설정은 동기화된 모든 디바이스에 적용됩니다.

기능 그룹 템플릿 및 LDAP 디렉터리 구성에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "엔드 유저 구성" 섹션을 참조하십시오.

벌크 관리자를 통한 CAPF 설정 업데이트

벌크 관리의 전화기 업데이트 쿼리를 사용하여 단일 작업에서 많은 기존 전화기에 대한 CAPF 설정 및 LSC 인증서를 구성합니다.

참고 전화기를 프로비저닝하지 않은 경우, 벌크 관리의 전화기 삽입 메뉴를 사용하여 CSV 파일의 CAPF 설정으로 새 전화기를 프로비저닝합니다. CSV 파일에서 전화기를 삽입하는 방법에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서의 "전화기 삽입" 섹션을 참조하십시오.

이 절차에서 추가하려는 것과 동일한 문자열 및 인증 방법을 사용하여 전화기를 구성하였는지 확인하십시오. 그렇지 않으면 전화기가 CAPF에 인증되지 않습니다. 전화기에서 인증을 구성하는 방법에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.벌크 관리 > 전화기 > 전화기 업데이트 > 쿼리.

단계 **2** 필터 옵션을 사용하여 업데이트하려는 전화기로 검색을 제한하고 찾기를 클릭합니다.

예를 들어, 전화기 찾기 위치 드롭다운 목록을 사용하여 모든 전화기를 선택합니다. 여기서 LSC는 특정 날짜 이전에 또는 특정 디바이스 풀 내에서 만료됩니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 로그아웃/재설정/재시작 섹션에서 구성 적용 라디오 버튼을 선택합니다. 작업이 실행되면 CAPF 업데이트가 업데이트된 모든 전화기에 적용됩니다.

단계 **5** **CAPF(Certificate Authority Proxy Function)** 정보에서 인증서 작업 확인란에 체크 표시합니다.

단계 **6** 인증서 작업 드롭다운 목록에서 설치/업그레이드를 선택하여 CAPF가 전화기에 새 LSC 인증서를 설치하도록 합니다.

단계 **7** 인증 모드 드롭다운 목록에서 LSC 설치 중 전화기의 자체 인증 방법을 선택합니다.

참고 전화기에서 동일한 인증 방법을 구성합니다.

단계 **8** 인증 문자열을 인증 모드로 선택한 경우, 다음 단계 중 하나를 완료합니다.

- 각 디바이스에 대한 고유한 인증 문자열을 사용하려는 경우, 각 디바이스에 고유한 인증 문자열 생성을 선택합니다.
- 인증 문자열 텍스트 상자에 문자열을 입력하거나, 모든 디바이스에 대해 동일한 인증 문자열을 사용하려면 문자열 생성을 클릭합니다.

단계 **9** 전화기 업데이트 창의 **CAPF(Certificate Authority Proxy Function)** 정보 섹션에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **10** 작업 정보에서 즉시 실행을 선택합니다.

참고 예약된 시간에 작업을 실행하려면 나중에 실행을 선택합니다. 작업 예약에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서에서 "예약된 작업 관리" 섹션을 참조하십시오.

단계 **11** 제출을 클릭합니다.

참고 이 절차에서 설정 적용 옵션을 선택하지 않은 경우, 업데이트된 모든 전화기에 대해 전화기 설정 창에서 설정을 적용합니다.

전화기에 대한 **CAPF** 설정 구성

이 절차를 사용하여 개별 전화기의 LSC 인증서에 대한 CAPF 설정을 구성합니다.

참고 벌크 관리 또는 동기화 LDAP 디렉터리를 사용하여 많은 수의 전화기에 CAPF 설정을 적용합니다.

이 절차에서 추가하려는 것과 동일한 문자열 및 인증 방법을 사용하여 전화기를 구성합니다. 그렇지 않으면, 전화기가 CAPF에 자체 인증되지 않습니다. 전화기에서 인증을 구성하는 방법에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기.

단계 **2** 찾기를 클릭하고 기존 전화기를 선택합니다. 전화기 구성 페이지가 나타납니다.

단계 **3** **CAPF(Certificate Authority Proxy Function)** 정보 창으로 이동합니다.

단계 **4** 인증서 작업 드롭다운 목록에서 CAPF에 대한 설치/업그레이드를 선택하여 전화기에 새 LSC 인증서를 설치합니다.

단계 **5** 인증 모드 드롭다운 목록에서 LSC 설치 중 전화기의 자체 인증 방법을 선택합니다.

참고 동일한 인증 방법을 사용하도록 전화기를 구성해야 합니다.

단계 **6** 텍스트 문자열을 입력하거나 문자열 생성을 클릭하여 인증 문자열을 선택하는 경우 문자열을 생성합니다.

단계 **7** 전화기 설정 페이지의 **CAPF(Certificate Authority Proxy Function)** 정보 창에 있는 나머지 필드에 세부 정보를 입력합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

KeepAlive 타이머 설정

이 절차를 사용하여 CAPF-엔드포인트 연결에 대한 클러스터 수준 keepalive 타이머를 설정하여 방화벽에 의해 연결이 시간 초과되지 않도록 합니다. 타이머의 기본값은 15분입니다. 각 간격 이후 CAPF 서비스는 연결을 계속 유지할 수 있도록 keepalive 신호를 전화기로 보냅니다.

프로시저

단계 **1** 명령줄 인터페이스를 사용하여 퍼블리셔 노드에 로그인합니다.

단계 **2** `Utils capt set keep_alive` CLI 명령을 실행합니다.

단계 **3** 5에서 60(분) 사이의 숫자를 입력하고 입력을 클릭합니다.

CAPF 관리 작업

CAPF를 구성하고 LSC 인증서를 발급한 후에는 다음 작업을 사용하여 LSC 인증서를 지속적으로 관리합니다.

인증서 상태 모니터링

시스템을 구성하여 인증서 상태를 자동으로 모니터링할 수 있습니다. 시스템에서 인증서 만료가 다가오면 이메일을 보내 며, 만료 후에는 인증서를 철회합니다.

인증서 모니터링 확인 작업을 구성하는 방법에 대한 자세한 내용은, "인증서 관리" 관리 장의 인증서 모니터링 및 철회 작업 플로우를 참조하십시오.

오래된 LSC 보고서 실행

이 절차를 사용하여 Cisco Unified Reporting에서 오래된 LSC 보고서를 실행합니다. 오래된 LSC는 엔드포인트 CSR에 대한 응답으로 생성되었지만, 새로운 CSR이 오래된 LSCS가 설치되기 전에 엔드포인트에 의해 생성 되었기 때문에 한 번도 설치된 적이 없었던 인증서입니다.

참고 퍼블리셔 노드에서 `utils capf stale-lsc list` CLI 명령을 실행하여 오래된 LSC 인증서 목록을 가져올 수도 있습니다.

프로시저

단계 **1** Cisco Unified Reporting Administration에서 시스템 보고서를 선택합니다.

단계 **2** 왼쪽 내비게이션 바에서 오래된 **LSC**를 선택합니다.

단계 **3** 새 보고서 생성을 클릭합니다.

보류 중인 CSR 목록 조회

이 절차를 사용하여 보류 중인 CAPF CSR 파일 목록을 봅니다. 모든 CSR 파일에는 타임스탬프가 찍혀 있습니다.

프로시저

단계 **1** 명령줄 인터페이스를 사용하여 퍼블리셔 노드에 로그인합니다.

단계 **2** `utils capf csr list` CLI 명령을 실행합니다.

보류기 중인 CSR 파일의 타임스탬프가 찍힌 목록이 표시됩니다.

오래된 LSC 인증서 삭제

이 절차를 사용하여 시스템에서 오래된 LSC 인증서를 삭제합니다.

프로시저

단계 1 명령줄 인터페이스를 사용하여 퍼블리셔 노드에 로그인합니다.

단계 2 `utils capf stale-lsc delete all` CLI 명령어 실행
시스템에서 모든 오래된 LSC 인증서를 삭제합니다.

CAPF 시스템 상호 작용 및 제한 사항

기능	상호 작용
인증 문자열	전화기에 대한 CAPF 인증 방법의 경우, 작업 후에 동일한 인증 문자열을 전화기에 입력해야 합니다. 그렇지 않으면 작업이 실패합니다. TFTP 암호화 구성 엔터프라이즈 매개변수가 활성화되어 있고 인증 문자열을 입력하지 못한 경우, 일치하는 인증 문자열이 전화기에 입력될 때까지 전화기가 실패하고 복구되지 않을 수 있습니다.
클러스터 서버 자격 증명	Unified Communications Manager 클러스터의 모든 서버는 동일한 관리자 사용자 이름 및 암호를 사용해야 합니다. 그래야 CAPF에서 클러스터의 모든 서버를 인증할 수 있습니다.
보안 전화기 마이그레이션	보안 전화기가 다른 클러스터로 이동되는 경우, Unified Communications Manager에서는 인증서가 CTL 파일에 존재하지 않는 다른 CAPF에서 발급했기 때문에 전화기에서 전송하는 LSC 인증서를 신뢰하지 않습니다. 보안 전화에서 등록을 진행하게 하려면, 기존 CTL 파일을 삭제합니다. 그런 다음, 설치/업그레이드 옵션을 사용하여 새 CAPF를 통해 새 LSC 인증서를 설치하고 새 CTL 파일에 대한 전화기를 재설정합니다(또는 MIC를 사용합니다). 전화기를 이동하기 전에 [전화기 구성] 창의 [CAPF] 섹션에서 [삭제] 옵션을 사용하여 기존 LSC를 삭제합니다.

기능	상호 작용
Cisco Unified IP Phone 6900 시리즈, 7900 시리즈, 8900 시리즈 및 9900 시리즈	Cisco에서는 Cisco Unified IP Phone 6900 시리즈, 7900 시리즈, 8900 시리즈 및 9900 시리즈를 업그레이드하여 Unified Communications Manager에 대한 TLS 연결을 위해 LSC를 사용할 것과, 예상되는 호환성 문제를 방지하기 위해 CallManager 신뢰 저장소에서 MIC 루트 인증서를 제거할 것을 권장합니다. Unified Communications Manager에 대한 TLS 연결을 위해 MIC를 사용하는 일부 전화기 모델은 등록되지 않을 수도 있습니다. 관리자는 CallManager 신뢰 저장소에서 다음과 같은 MIC 루트 인증서를 제거해야 합니다. • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
정전	다음 정보는 통신 두절 또는 정전 발생 시 적용됩니다. • 전화기에서 인증서 설치가 진행디는 동안 통신 두절이 발생하는 경우, 전화기는 30초 간격으로 3회 이상 인증서를 가져오려고 시도합니다. 이러한 값은 구성할 수 없습니다. • 전화기에서 CAPF를 사용하여 세션을 시도하는 동안 정신이 발생하는 경우, 전화기에서는 플래시에 저장된 인증 모드를 사용합니다. 즉, 전화기가 다시 부팅된 후에 전화기가 TFTP 서버에서 새 구성 파일을 로드할 수 없는 경우가 이에 해당됩니다. 인증서 작업이 완료되면 시스템에서 바로 해당 값을 소거합니다.
인증서 암호화	Unified Communications Manager 릴리스 11.5(1) SU1에서 시작하여 CAPF 서비스에서 발급한 모든 LSC 인증서는 SHA-256 알고리즘으로 서명됩니다. 따라서 IP 전화기 7900/8900/9900 시리즈 모델은 SHA-256 서명된 LSC 인증서 및 외부 SHA2 ID 인증서(Tomcat, CallManager, CAPF, TVS 등)를 지원합니다. 서명 확인이 필요한 다른 암호화 작업의 경우, SHA-1만 지원됩니다. 참고 소프트웨어 유지보수 종료 또는 단종 단계에 있는 전화기 모델을 사용하는 경우, 11.5(1) SU1 릴리스를 사용하기 전에 Unified Communications Manager를 사용할 것을 강력 권장합니다.

7942 및 7962 전화기를 이용한 CAPF 예

사용자 또는 Unified Communications Manager에서 전화기를 재설정할 때는, CAPF가 Cisco Unified IP Phone 7962 및 7942와 상호 작용하는 방식에 대한 다음 정보를 고려하십시오.

참고 다음 예에서, LSC가 아직 전화기에 존재하지 않고 CAFP 인증 모드에 대해 기존 인증서 사용을 선택한 경우, CAPF 인증서 작업이 실패합니다.

예-비보안 디바이스 보안 모드

이 예에서는, 디바이스 보안 모드를 비보안으로 그리고 CAPF 인증 모드를 **Null** 문자열 사용 또는 기존 인증서 사용**(**우선순위**...)**으로 설정한 후에 전화기가 재설정됩니다. 전화기가 재설정되고 나면, 즉시 기본 Unified Communications Manager에 등록되고 구성 파일을 수신합니다. 그런 다음 전화기가 자동으로 CAPF를 사용하여 세션을 시작하여 LSC를 다운로드합니다. 전화기에서 LSC를 설치한 후에는 디바이스 보안 모드를 인증됨 또는 암호화됨으로 구성합니다.

예-인증된/암호화된 디바이스 보안 모드

이 예에서는, 디바이스 보안 모드를 비보안으로 인증됨 또는 암호화됨으로 그리고 CAPF 인증 모드를 **Null** 문자열 사용 또는 기존 인증서 사용**(**우선순위**...)**으로 설정한 후에 전화기가 재설정됩니다. CAPF 세션이 종료되고 전화기에 LSC가 설치될 때까지 전화기는 기본 Unified Communications Manager에 등록되지 않습니다. 세션이 종료되면, 전화기가 등록되고, 즉시 인증됨 또는 암호화됨 모드로 실행됩니다.

이 예에서 인증 문자열 사용을 구성할 수 없습니다. 그 이유는 전화기가 CAPF 서버에 자동으로 연결되지 않아, 전화기에 유효한 LSC가 없는 경우 등록이 실패하기 때문입니다.

IPv6 주소 지정과의 CAPF 상호 작용

CAPF는 IPv4, IPv6 또는 두 가지 유형의 주소를 모두 사용하는 전화기로 인증서를 발급하고 업그레이드할 수 있습니다. IPv6 주소를 사용하는 SCCP를 실행 중인 전화기에 대한 인증서를 발급하거나 업그레이드하려면, Unified Communications Manager 관리에서 IPv6 활성화 서비스 매개변수를 참으로 설정해야 합니다.

전화기가 CAPF에 연결되어 인증서를 가져올 때 CAPF는 [IPv6 활성화] 엔터프라이즈 매개변수에서 구성을 사용하여 전화기에 인증서를 발급 또는 업그레이드할지 여부를 결정합니다. 엔터프라이즈 매개변수가 거짓으로 설정된 경우, CAPF는 IPv6 주소를 사용하는 전화기에서 연결을 무시하거나 거부하며 전화기는 인증서를 수신하지 않습니다.

다음 표에서는 IPv4, IPv6 또는 두 유형의 주소가 있는 전화기가 CAPF에 연결되는 방식에 대해 설명합니다.

표 2: IPv6 또는 IPv4 전화기가 CAPF에 연결되는 방법

전화기의 IP 모드	전화기의 IP 주소	CAPF IP 주소	전화기가 CAPF에 연결되는 방법
두 개의 스택	IPv4 및 IPv6 사용 가능	IPv4, IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다. 즉, 전화기를 IPv6 주소를 통해 연결할 수 없는 경우, 전화기에서는 IPv4 주소를 사용하여 연결을 시도합니다.
두 개의 스택	IPv4	IPv4, IPv6	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
두 개의 스택	IPv6	IPv4, IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다. 시도가 실패하면 전화기에서 IPv4 주소를 사용하여 CAPF에 연결합니다.
두 개의 스택	IPv4	IPv4	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
두 개의 스택	IPv4 및 IPv6 사용 가능	IPv6	전화기가 IPv6 주소를 사용하여 CAPF에 연결됩니다.
두 개의 스택	IPv4 및 IPv6 사용 가능	IPv4	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
두 개의 스택	IPv4	IPv6	전화기가 CAPF에 연결될 수 없습니다.
두 개의 스택	IPv6	IPv4	전화기가 CAPF에 연결될 수 없습니다.
두 개의 스택	IPv6	IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다.
IPv4 스택	IPv4	IPv4, IPv6	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
IPv6 스택	IPv6	IPv4, IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다.
IPv4 스택	IPv4	IPv4	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
IPv4 스택	IPv4	IPv6	전화기가 CAPF에 연결될 수 없습니다.
IPv6 스택	IPv6	IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다.
IPv6 스택	IPv6	IPv4	전화기가 CAPF에 연결될 수 없습니다.