AS-SIP 엔드포인트 구성

AS-SIP 개요

AS-SIP(보증된 서비스 SIP) 엔드포인트는 MLPP, DSCP, TLS/SRTP 및 IPv6 요구 사항을 준수합니다. AS-SIP는 Unified Communications Manager에 여러 엔드포인트 인터페이스를 제공합니다.

대부분의 Cisco IP 전화기는 AS-SIP로 지원됩니다. 또한 타사 AS-SIP 엔드포인트 디바이스 유형을 사용하면 타사 AS-SIP 호환 엔드포인트를 구성하여 Cisco Unified Communications Manager에 사용할 수 있습니다. 또한 타사 AS-SIP 엔드포인트 디바이스 유형을 사용하면 타사 AS-SIP 호환 일반 엔드포인트를 구성하여 Cisco Unified Communications Manager에 사용할 수 있습니다.

AS-SIP 기능

다음과 같은 기능이 구현되거나 SIP 엔드포인트에 사용할 수 있게 됩니다.

- MLPP
- TLS
- SRTP
- 우선 수준을 위한 DSCP
- 오류 응답
- V.150.1 MER
- 컨퍼런스 팩토리 흐름 지원
- AS-SIP 회선 Early Offer

타사 **AS-SIP** 전화기

타사 전화기를 Cisco Unified Communications Manager에 제공하여 타사의 AS-SIP 엔드포인트 디바이스 유형을 사용할 수 있습니다.

AS-SIP를 실행 중인 타사 전화기는 Cisco Unified Communications Manager TFTP 서버를 통해 구성하지 않습니다. 고객은 기본 전화기 구성 메커니즘(일반적으로 웹 페이지 또는 TFTP 파일)을 사용하여 타사 전화기를 구성해야 합니다. 고객은 Cisco Unified Communications Manager 데이터베이스의 디바이스 및 회선 구성을 기본 전화기 구성과 동기화된 상태로 유지해야 합니다(예를 들면 전화기의 1002와 Cisco Unified Communications Manager의 1002). 또한, 회선의 디렉터리 번호를 변경하는 경우 고객은 Unified CM 관리와 기본 전화기 구성 메커니즘에서 모두 변경되도록 해야 합니다.

타사 전화기 식별

SIP를 실행 중인 타사 전화기는 MAC 주소를 전송하지 않으므로 사용자 이름을 사용하여 자체적으로 식별해야 합니다. REGISTER 메시지에는 다음 헤더가 포함됩니다.

```
Authorization: Digest
username="swhite",realm="ccmsipline",nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5",uri
="sip:172.18.197.224",
algorithm=MD5,response="126c0643a4923359ab59d4f53494552e"
```

사용자 이름인 **swhite**는 Cisco Unified CM 관리의 최종 사용자 구성 창에서 구성된 최종 사용자와 일치해야 합니다. 관리자는 전화기 구성 창의 다이제스트 사용자 필드에서 예를 들어 **swhite**라는 사용자를 사용하여 SIP 타사 전화기를 구성합니다.

참고 각 사용자 ID를 한 대의 타사 전화기에만 할당할 수 있습니다. 동일한 사용자 ID가 여러 전화기에 대해 다이제스트 사용자로 할당되는 경우 이러한 ID가 할당된 타사 전화기가 제대로 등록되지 않습니다.

타사 **AS-SIP** 전화기 및 **Cisco IP** 전화기 구성

다음 표에서는 Cisco Unified IP Phone과 AS-SIP를 실행하는 타사 전화기 사이의 구성 차이점을 간략히 비교하여 보여 줍니다.

표 ***1: Cisco IP*** 전화기와 타사 전화기 간의 구성 차이점 비교

AS-SIP를 실행하는 전화기	중앙 집중식 **TFTP**와 통합됨	**MAC** 주소 보내기	소프트키 파일 다운로드	다이얼 플랜 파일 다운로드	**Unified Communications Manager** 장애 조치 및 폴백 지원	재설정 및 재시작 지원
Cisco IP 전화기	예	예	예	예	예	예

AS-SIP를 실행하는 전화기	중앙 집중식 **TFTP**와 통합됨	**MAC** 주소 보내기	소프트키 파일 다운로드	다이얼 플랜 파일 다운로드	**Unified Communications Manager** 장애 조치 및 폴백 지원	재설정 및 재시작 지원
타사 AS-SIP 디바이스	아니요	아니요	아니요	아니요	아니요	아니요

참고 모든 Cisco IP 전화기가AS-SIP로 지원되지는 않습니다. 지원 정보는 전화기 모델의 전화기 관리 지침서를 참조하십시오.

Cisco Unified CM 관리를 사용하여 SIP를 실행하는 타사 전화기를 구성합니다. 자세한 내용은 *Cisco Unified Communications Manager*용 시스템 구성 설명서의 "SIP 프로파일 구성" 항목을 참조하십시오

. 관리자는 SIP를 실행하는 타사 전화기에서도 구성 단계를 수행해야 합니다. 다음 예를 참조하십시오.

- 전화기의 프록시 주소가 Cisco Unified Communications Manager의 IP 또는 FQDN(정규화된 도메인 이름)인지 확인합니다.
- 전화기의 디렉터리 번호가 Unified CM 관리에서 디바이스용으로 구성된 디렉터리 번호와 일치하는지 확인합니다.
- 전화기의 다이제스트 사용자 ID(인증 ID라고도 함)가 Cisco Unified CM 관리의 다이제스트 사용자 ID와 일치하는지 확인합니다.

자세한 내용은 타사 전화기와 함께 제공된 설명서를 참조하십시오.

AS-SIP 컨퍼런싱

기능 호출자(보류자, 호전환자 또는 전화회의 개시자)가 Cisco 전용 기능 신호 처리를 지원하는 경우 MOH가 대상(보류 상대방, 호전환 직전 피호전환자 또는 전화회의 참가 직전 회의 참가자)에 적용됩니다. 기능 호출자가 Cisco 전용 기능 신호 처리를 지원하지 않을 경우 MOH가 대상에 적용되지 않습니다. 또한, 엔드포인트가 컨퍼런스 믹서임을 명시적으로 알리는 경우 MOH가 대상에게 재생되지 않습니다. AS-SIP 컨퍼런싱에는 두 가지 형태가 있습니다.

- 로컬 믹싱
- 회의 팩터리

로컬 믹싱

Unified CM 측에서는 전화회의 개시자가 각각의 다른 전화회의 참석자마다 하나씩 단순히 활성 통화를 동시에 설정한 것처럼 보입니다. 이니시에이터는 로컬로 전화회의를 주최하며 이곳에서 음성이 믹싱됩니다. 컨퍼런스 주최자의 통화는 MOH 소스에 연결되지 않도록 하는 특수 신호 처리가 되어 있습니다.

회의 팩터리

컨퍼런스 주최자는 SIP 트렁크로부터 떨어져 있는 컨퍼런스 팩토리 서버에 전화를 겁니다. IVR 신호 처리를 통해 전화화의 개시자가 컨퍼런스 팩토리에 컨퍼런스 브리지를 예약하도록 지시합니다. 컨퍼런스 팩토리는 숫자 주소(전송 가능한 DN)를 전화화의 개시자에게 제공합니다. 그러면 전화화의 개시자는 브리지 가입을 설정하여 참가자를 추적할 전화화의 목록 정보를 수신합니다. 컨퍼런스 팩토리에서 MOH 소스에 연결되지 않도록 하는 특수 신호 처리를 전송합니다.

AS-SIP 사전 요건

충분한 디바이스 라이센스 단위를 사용할 수 있는지 확인합니다. 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "스마트 소프트웨어 라이센싱" 장을 참조하십시오.

AS-SIP 엔드포인트 구성 작업 흐름

감사 로깅을 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	다이제스트 사용자 구성, 5 페이지	SIP 요청에 대해 다이제스트 인증을 사용하도록 최종 사용자를 구성합니다.
단계 **2**	SIP 전화기 보안 포트 구성, 5 페이지	Cisco Unified Communications Manager는 이 포트를 사용하여 TLS를 통한 SIP 회선 등록을 위한 SIP 전화를 수신합니다.
단계 **3**	서비스 다시 시작, 6 페이지	보안 포트를 구성한 후 Cisco CallManager 및 Cisco CTL Provider 서비스를 다시 시작합니다.
단계 **4**	AS-SIP용 SIP 프로파일 구성, 6 페이지	AS-SIP 엔드포인트와 SIP 트렁크를 위한 SIP 설정을 사용하여 SIP 프로파일을 구성합니다. 참고 전화기 특정 매개 변수는 타사 AS-SIP 전화기에 다운로드되지 않으며, Cisco Unified Communications Manager에서만 사용됩니다. 타사 전화기에서는 동일한 설정을 로컬로 구성해야 합니다.
단계 **5**	AS-SIP에 대한 전화기 보안 프로파일 구성, 7 페이지	전화기 보안 프로파일을 사용하여 TLS, SRTP 및 다이제스트 인증과 같은 보안 설정을 할당할 수 있습니다.
단계 **6**	AS-SIP 엔드포인트 구성, 7 페이지	Cisco IP 전화기 또는 타사 엔드포인트 및 AS-SIP 지원을 구성 합니다.

	명령 또는 동작	목적
단계 **7**	디바이스를 최종 사용자에 연결, 8 페이지	엔드포인트를 사용자와 연결합니다.
단계 **8**	AS-SIP에 대한 SIP 트렁크 보안 프로파일 구성, 9 페이지	SIP 트렁크 보안 프로파일을 사용하여 TLS 또는 다이제스트 인증과 같은 보안 기능을 SIP 트렁크에 할당할 수 있습니다.
단계 **9**	AS-SIP에 대한 SIP 트렁크 구성, 9 페이지	AS-SIP 지원을 사용하여 SIP 트렁크를 구성합니다.
단계 **10**	AS-SIP 기능 구성, 10 페이지	MLPP, TLS, V.150 및 IPv6과 같은 추가 AS-SIP 기능을 구성합니다.

다이제스트 사용자 구성

이 절차를 사용하여 최종 사용자를 다이제스트 인증을 사용하는 다이제스트 사용자로 구성합니다. 사용자와 연결된 디바이스는 사용자의 다이제스트 인증서를 통해 인증됩니다.

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 사용자를 생성하려면 새로 추가를 클릭합니다.
- 찾기를 클릭하고 기존 사용자를 선택합니다.

단계 **3** 다음 필수 필드가 완료되었는지 확인합니다.

- 사용자 ID
- 성

단계 **4** 다이제스트 인증서 필드에 암호를 입력합니다. 최종 사용자는 엔드포인트를 사용할 때 이 암호를 통해 자신을 인증해야 합니다.

단계 **5** 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

SIP 전화기 보안 포트 구성

다음 단계를 수행하여 SIP 전화기 보안 포트를 구성합니다. Cisco Unified Communications Manager는 이 포트를 사용하여 TLS를 통한 SIP 회선 등록을 위한 SIP 전화를 수신합니다.

단계 **1** Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM**을 선택합니다.

단계 **2** 이 서버에 대한 **Cisco Unified Communications Manager TCP** 포트 설정 섹션에서 **SIP** 전화기 보안 포트 필드에 포트 번호를 지정하거나 기본값으로 설정된 필드를 그대로 둡니다. 기본값은 5061입니다.

단계 **3** 저장을 클릭합니다.

단계 **4** 구성 적용을 클릭합니다.

단계 **5** 확인을 클릭합니다.

서비스 다시 시작

다음 단계에 따라 Cisco CallManager 및 Cisco CTL Provider 서비스를 다시 시작합니다.

단계 **1** Cisco Unified Serviceability 인터페이스에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 Cisco Unified Communications Manager 서버를 선택합니다.
CM 서비스 영역에서 Cisco CallManager가 서비스 이름 열에 표시됩니다.

단계 **3** Cisco CallManager 서비스에 해당하는 라디오 버튼을 클릭합니다.

단계 **4** 재시작을 클릭합니다.
서비스가 다시 시작되고 서비스가 다시 시작되었습니다라는 메시지가 표시됩니다.

단계 **5** 3단계와 4단계를 반복하여 Cisco CTL Provider 서비스를 다시 시작합니다.

AS-SIP용 SIP 프로파일 구성

이 절차를 사용하여 AS-SIP 엔드포인트와 SIP 트렁크를 위한 SIP 설정을 사용하여 SIP 프로파일을 구성합니다.

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 SIP 프로파일을 만듭니다.
- 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.

단계 **3** SIP 프로파일의 이름과 설명을 입력합니다.

단계 **4** 보증된 서비스 **SIP** 일치 확인란을 선택합니다.

참고 SIP 트렁크 및 타사 AS-SIP 전화기의 경우 이 확인란을 선택해야 합니다. AS-SIP을 지원하는 Cisco IP 전화기의 경우 필수 사항은 아닙니다.

단계 **5** 전화기에 사용된 매개 변수] 섹션에서 예상하는 통화 유형에 대한 DSCP 우선 순위 값을 구성합니다.

참고 클러스터 수준 서비스 매개 변수를 통해 DSCP 값을 구성할 수도 있습니다. 그러나 SIP 프로파일 내의 DSCP 값은 SIP 프로파일을 사용하는 모든 디바이스에 대한 클러스터 수준 설정을 무시합니다.

단계 **6** 음성 및 영상 통화에 **Early Offer** 지원 드롭다운 목록에서 다음 옵션 중 하나를 선택하여 이 프로파일을 사용하는 SIP 트렁크에 대한 얼리 오퍼 지원을 구성합니다.

- 비활성화됨

- Best Effort(삽입된 MTP 없음)
- 필수(필요한 경우 MTP 삽입)

단계 **7** **SIP** 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

AS-SIP에 대한 전화기 보안 프로파일 구성

이 절차를 사용하여 AS-SIP 엔드포인트에 대한 전화기 보안 프로파일을 구성합니다. 보안 프로파일을 사용하여 TLS 및 SRTP와 같은 보안 설정을 할당할 수 있습니다.

단계 **1** Cisco Unified CM 관리에서 시스템 > 보안 > 전화기 보안 프로파일을 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 전화기 보안 프로파일을 만듭니다.
- 찾기를 클릭하여 기존 프로파일을 선택합니다.

단계 **3** 새 프로파일의 경우 전화기 보안 프로파일 드롭다운에서 옵션을 선택하고 전화기 모델 타사 **AS-SIP** 엔드포인트를 선택하고 다음을 클릭합니다.

- Cisco IP 전화기의 경우 전화기 모델을 선택하고 다음을 클릭합니다.
- 타사의 AS-SIP 엔드포인트인 경우 타사 **AS-SIP** 엔드포인트를 선택하고 다음을 클릭합니다.

단계 **4** 프로토콜의 경우 **SIP**을 선택하고 다음을 클릭합니다.

단계 **5** 프로토콜의 이름과 설명을 입력합니다.

단계 **6** 다음 설정 중 하나에 디바이스 보안 모드를 할당합니다.

- 인증됨 - Cisco Unified Communications Manager에서 TLS 설정을 사용하여 전화기에 대해 무결성 및 인증을 제공합니다.
- 암호화됨 - Cisco Unified Communications Manager에서 TLS 신호 처리를 사용하여 전화기에 대해 무결성 및 인증을 제공합니다. 또한 SRTP는 미디어 스트림을 암호화합니다.

단계 **7** 다이제스트 인증 활성화 확인란을 선택합니다.

단계 **8** 전화기 보안 프로파일 구성 창에서 남아 있는 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **9** 저장을 클릭합니다.

AS-SIP 엔드포인트 구성

이 절차를 사용하여 AS-SIP 엔드포인트를 구성합니다. 대부분의 Cisco IP 전화기는 AS-SIP를 지원합니다. 또한 타사 엔드포인트에 대해 SIP로 구성할 수 있습니다.

단계 **1** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화기 유형 드롭다운 목록에서 AS-SIP를 지원하는 Cisco IP 전화기를 선택합니다. 그렇지 않은 경우에는 타사 **AS-SIP** 엔드포인트를 선택합니다.

단계 **4** 다음을 클릭합니다.

단계 **5** 다음 필수 필드를 구성합니다.필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

- 디바이스 신뢰 모드 — 타사의 AS-SIP 엔드포인트에만 해당됩니다. 신뢰 또는 신뢰 안 함을 선택합니다.
- MAC 주소
- 디바이스 풀
- 전화기 버튼 템플릿
- 소유자 사용자 ID
- 디바이스 보안 프로파일 - AS-SIP로 설정된 전화기 보안 프로파일을 선택합니다.
- SIP 프로파일 - 사용자가 구성하는 AS-SIP 사용 가능 SIP 프로파일을 선택합니다.
- 다이제스트 사용자 - 다이제스트 사용자로 구성하는 사용자 ID를 선택합니다. 다이제스트 인증을 위해 사용자를 활성화해야 합니다.
- DTMF 수신 필요 - 엔드포인트에서 DTMF 숫자를 수락하도록 허용하려면 이 확인란을 선택합니다.
- 음성 및 영상 통화에 대한 Early Offer 지원 - Early Offer 지원을 활성화하려면 이 확인란을 선택합니다. 이 필드는 타사 전화기에 대해서만 표시됩니다.

단계 **6** **MLPP** 및 기밀 액세스 수준 정보 섹션에서 필드를 구성합니다.

단계 **7** 저장을 클릭합니다.

단계 **8** 새 디렉터리 번호 추가:

a) 왼쪽 탐색 모음에서 새 **DN** 추가를 클릭합니다. 디렉터리 번호 구성 창이 열립니다.
b) 디렉터리 번호를 추가합니다.
c) 디렉터리 번호 구성 창의 나머지 필드를 완료합니다.
d) 저장을 클릭합니다.

단계 **9** 관련 링크 필드에서 디바이스 구성을 선택하고 이동을 클릭합니다.

단계 **10** 구성 적용을 클릭합니다.

디바이스를 최종 사용자에 연결

이 절차를 사용하여 최종 사용자를 AS-SIP 엔드포인트에 연결합니다.

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다 사용자 관리 > 최종 사용자

단계 **2** 찾기를 클릭하고 디바이스에 연결할 사용자를 선택합니다.

단계 **3** 디바이스 정보 영역에서 디바이스 연결을 클릭합니다.
[사용자 디바이스 연결] 창이 나타납니다.

단계 4 사용 가능한 디바이스 목록을 보려면 찾기를 클릭합니다.

단계 5 연결할 디바이스를 선택하고 선택 항목/변경 사항 저장을 클릭합니다.

단계 6 관련 링크에서 사용자로 돌아가기를 선택한 다음 이동을 클릭합니다.
최종 사용자 구성 창이 나타나고 선택한 연결 디바이스가 제어된 이바이스 창에 표시됩니다.

AS-SIP에 대한 SIP 트렁크 보안 프로파일 구성

이 절차를 사용하여 AS-SIP를 지원하는 SIP 트렁크에 대한 보안 프로파일을 구성합니다.

단계 1 Cisco Unified CM 관리에서 시스템 > 보안 > **SIP** 트렁크 보안 프로파일을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 보안 프로파일의 이름을 입력합니다.

단계 4 디바이스 보안 모드 드롭다운 목록에서 인증됨 또는 암호화됨을 선택합니다.

단계 5 수신 전송 유형 및 발신 전송 유형 필드가 자동으로 **TLS**로 변경됩니다.

단계 6 다이제스트 인증 활성화 확인란을 선택합니다.

단계 7 V. 150을 구축하는 경우에는 **SIP V.150** 아웃바운드 **SDP** 제공 필터링 드롭다운 목록에 대한 값을 구성합니다.

단계 8 **SIP** 트렁크 보안 프로파일 구성 창에서 나머지 필드를 완료합니다.필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 9 저장을 클릭합니다.

AS-SIP에 대한 SIP 트렁크 구성

이 절차를 사용하여 AS-SIP를 지원하는 SIP 트렁크를 설정합니다.

단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 트렁크를 선택합니다.
- 새로 추가를 클릭하여 새 트렁크를 만듭니다.

단계 3 새 트렁크 유형의 경우 트렁크 유형 드롭다운 목록에서 **SIP** 트렁크를 선택합니다.

단계 4 트렁크 서비스 유형 드롭다운 목록에서 없음**(**기본값**)**을 선택하고 다음을 클릭합니다.

단계 5 트렁크에 대한 디바이스 이름을 입력합니다.

단계 6 디바이스 풀 드롭다운 목록에서 디바이스 풀을 선택합니다.

단계 7 대상 주소 필드에 트렁크를 연결하는 서버의 주소를 입력합니다.

단계 8 **SIP** 트렁크 보안 프로파일 드롭다운 목록에서 AS-SIP로 생성한 프로파일을 선택합니다.

단계 9 **SIP** 프로파일 드롭다운 목록에서 AS-SIP에 대해 설정된 SIP 프로파일을 선택합니다.

단계 **10** 트렁크 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **11** 저장을 클릭합니다.

AS-SIP 기능 구성

이전 작업 흐름의 절차에서는 엔드포인트 및 트렁크에서 AS-SIP 지원을 구성하는 방법에 대해 설명합니다. 다음 표에서는 구축할 수 있는 AS-SIP 기능을 개략적으로 설명하고 각각에 대한 구성 참조를 제공합니다.

AS-SIP 기능	**Configuration Description(**컨피그레이션 설명**)**
Early Offer	SIP Early Offer 기능을 사용하면 엔드포인트에서 INVITE 요청 중에 미디어를 협상하고 200OK 응답을 받을 수 있습니다. Early Offer에는 두 가지 모드가 있습니다. • Best Effort Early Offer(삽입된 MTP 없음) • Mandatory Early Offer(필요한 경우 MTP 삽입) 다음 구성 창의 필드를 통해 Early Offer 지원을 구성합니다. 자세한 필드 설명은 온라인 도움말을 참조하십시오. **SIP** 프로파일 구성 창 • 음성 및 영상 통화에 대한 Early Offer 지원 - 이 필드를 구성하여 SIP 트렁크에서 Early Offer 지원을 활성화합니다. • Early Offer 및 Re-invite를 위한 SDP 세션 수준 대역폭 한정자 • 통화 중 INVITE에 전송-수신 SDP 전송 전화기 구성 창(타사 AS-SIP 단말 디바이스 유형이 사용되는 경우에만) • 음성 및 영상 통화에 대한 Early Offer 지원 - Early Offer 지원을 활성화하려면 이 확인란을 선택합니다.

AS-SIP 기능	Configuration Description(컨피그레이션 설명)
회의 팩터리	IMS 클라이언트에서 전화회의를 설정하는 데 사용하는 URI를 지정합니다. 1. Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택합니다. 2. 서버 드롭다운 목록에서 Cisco Unified Communications Manager 서버를 선택합니다. 3. 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다. 4. 클러스터 수준 매개 변수(기능 - 전화회의)에서 **IMS** 전화회의 팩토리 **URI**를 할당합니다. 5. 저장을 클릭합니다.
DSCP 표시	DSCP 설정을 사용하여 네트워크 내에서 QoS 및 대역폭을 관리할 수 있습니다. DSCP 설정은 통화별로 통화에 우선 순위가 지정된 트래픽 클래스 레이블을 할당하는 데 사용됩니다. 서비스 매개 변수를 통해 클러스터 수준 DSCP 설정을 구성할 수 있으며 SIP 프로파일을 사용하여 해당 프로파일을 사용하는 사용자에 대해 사용자 정의된 QoS 정책을 할당할 수 있습니다. 예를 들어, 임원(예: CEO) 또는 판매 팀의 통화에 더 높은 우선 순위를 할당하여 네트워크 대역폭 문제가 발생하는 경우 통화가 손실되지 않도록 할 수 있습니다. DSCP를 구성하려면 DSCP 설정 구성 작업 흐름의 내용을 참조하십시오.
IPv6	기본값으로 Cisco Unified Communications Manager는 IPv4 주소 지정을 사용하도록 구성되어 있습니다. 하지만 시스템을 구성하여 IPv6 stack을 지원하여 IPv6 전용 엔드포인트로 SIP 네트워크를 구축할 수 있습니다. IPv6 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "듀얼 스택 IPv6 구성 작업 흐름" 장을 참조하십시오.
MLPP(Multilevel Precedence and Preemption)	MLPP(Multilevel Precedence and Preemption) 서비스를 사용하여 우선 통화를 연결할 수 있습니다. 이 기능으로 국가 비상 사태 또는 네트워크 성능 저하 상황과 같은 네트워크 스트레스 상황 동안 주요 담당자는 중요한 조직 및 개인에 대한 통신을 보장할 수 있습니다. MLPP를 구성하려면 MLPP(Multilevel Precedence and Preemption) 작업 흐름의 내용을 참조하십시오.
SRTP(Secure Real-Time Transport Protocol)	보안 실시간 전송 프로토콜(SRTP)을 사용하여 통화의 미디어 스트림에 암호화 및 인증을 제공할 수 있습니다. 전화기에서 사용하는 전화기 보안 프로파일 구성 내에서 전화기에 대해 SRTP를 구성할 수 있습니다. 디바이스 보안 모드 필드를 암호화됨으로 설정해야 합니다.

AS-SIP 기능	**Configuration Description(**컨피그레이션 설명**)**
TLS(전송 레이어 신호 처리)	TLS(전송 레이어 보안)는 보안 포트 및 인증서 교환을 사용하여 두 시스템 또는 디바이스 간에 안전하고 신뢰할 수 있는 신호 처리 및 데이터 전송을 제공합니다. TLS를 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager*에 대한 보안 설명서의 "TLS 설정" 장을 참조하십시오.
V.150	V.150 최소 필수 요구 사항 기능을 사용하면 IP 네트워크를 통한 모뎀에서 보안 전화를 걸 수 있습니다. 이 기능은 기존 PSTN(공중 전화 교환망)에서 작동하는 모뎀 및 전화 통신 디바이스의 대규모 설치 기반으로 전화 접속 모뎀을 사용합니다. V.150을 구성하는 자세한 내용은 *Cisco Unified Communications Manager*에 대한 보안 설명서의 "Cisco V. 150 최소 필수 요구 사항(MER)" 장을 참조하십시오.