



# IM and Presence 서비스용 Cisco Unified Communications Manager 구성

- 통합 개요, 1 페이지
- Cisco Unified Communications Manager 통합 필수 조건, 1 페이지
- Cisco Unified Communications Manager에서 SIP 트렁크 구성, 3 페이지

## 통합 개요

이 섹션에서는 IM and Presence 서비스에 대한 구성을 완료하기 위해 Cisco Unified Communications Manager에서 완료해야 하는 작업에 대해 자세히 설명합니다.

## Cisco Unified Communications Manager 통합 필수 조건

Cisco Unified Communications Manager와 통합하기 위해 IM and Presence 서비스를 구성하기 전에 Cisco Unified Communications Manager에서 다음 일반 구성 작업을 완료해야 합니다. Cisco Unified Communications Manager 구성 방법에 대한 자세한 내용은 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

아래 표에는 IM and Presence 서비스 통합을 위한 필수 구성 작업이 나와 있습니다. 필드 및 해당 옵션에 대한 설명은 온라인 도움말을 참조하십시오.

표 1: Cisco Unified Communications Manager의 필수 구성

작업	설명
사용자 자격 증명 정책 수정	<p>사용자를 위한 자격 증명 정책에서 만료 날짜를 설정하는 것이 좋습니다. 자격 증명 만료 날짜가 필요하지 않은 유일한 사용자 유형은 애플리케이션 사용자입니다.</p> <p>LDAP 서버를 사용하여 Cisco Unified Communications Manager에서 사용자를 인증하는 경우, Cisco Unified Communications Manager는 자격 증명 정책을 사용하지 않습니다.</p> <p><b>Cisco Unified CM Administration</b> &gt; 사용자 관리 &gt; 사용자 설정 &gt; 인증서 정책 기본값</p>
전화기 디바이스를 구성하고, DN(디렉터리 번호)을 각 디바이스와 연결	<p>전화기와 클라이언트의 상호 운용을 허용하려면 CTI의 디바이스 제어 허용을 활성화합니다.</p> <p><b>Cisco Unified CM</b> 관리 &gt; 디바이스 &gt; 전화기</p>
사용자를 구성하고, 디바이스를 각 사용자와 연결	<p>사용자 ID 값이 각 사용자에 대해 고유한지 확인합니다.</p> <p><b>Cisco Unified CM</b> 관리 &gt; 사용자 관리 &gt; 최종 사용자</p>
사용자를 회선 표시와 연결	<p>자세한 내용은 다음 내용을 참조하십시오.</p> <p><b>Cisco Unified CM</b> 관리 &gt; 디바이스 &gt; 전화기</p>
CTI 활성화 사용자 그룹에 사용자 추가	<p>사무실 전화기 제어를 활성화하는 경우 CTI 활성화 사용자 그룹에 사용자를 추가해야 합니다.</p> <p><b>Cisco Unified CM</b> 관리 &gt; 사용자 관리 &gt; 사용자 그룹</p>
인증서 교환	<p>Cisco Unified Communications Manager와 IM and Presence 서비스 간의 인증서 교환은 설치 프로세스 중에 자동으로 처리됩니다. 그러나 문제가 발생하여 인증서 교환을 수동으로 완료해야 하는 경우 <a href="#">Cisco Unified Communications Manager와 인증서 교환</a>의 내용을 참조하십시오.</p>



**참고** IM and Presence 서비스에 업로드하는 Cisco Unified Communications Manager Tomcat 인증서에 SAN 필드에 호스트 이름이 포함되어 있는 경우 이 모든 인증서는 IM and Presence 서비스에서 확인할 수 있어야 합니다. IM and Presence 서비스가 DNS를 통해 호스트 이름을 확인할 수 있어야 합니다. 그렇지 않으면 Cisco 동기화 에이전트 서비스가 시작되지 않습니다. 이는 Cisco Unified Communications Manager 서버의 노드 이름에 대한 호스트 이름, IP 주소 또는 FQDN 사용 여부와 상관없이 적용됩니다.

# Cisco Unified Communications Manager에서 SIP 트렁크 구성

이러한 작업을 완료하여 Cisco Unified Communications Manager에 대한 SIP 트렁크 연결을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	<a href="#">SIP 트렁크 보안 프로파일 구성, 4 페이지</a>	Cisco Unified Communications Manager와 IM and Presence 서비스 간의 트렁크 연결을 위한 SIP 트렁크 보안 프로파일을 구성합니다.
단계 2	<a href="#">IM and Presence 서비스용 SIP 트렁크 구성, 4 페이지</a>	SIP 트렁크에 SIP 트렁크 보안 프로파일을 할당하고 Cisco Unified Communications Manager와 IM and Presence 서비스 간 트렁크 연결을 구성합니다.
단계 3	<a href="#">SRV 클러스터 이름 구성, 6 페이지</a>	(선택 사항) Cisco Unified Communications Manager와 IM and Presence 서비스 간의 SIP 트렁크에서 DNS SRV를 사용하고 IM and Presence 기본 도메인이 아닌 다른 SRV 주소를 사용하는 경우에만 이 절차를 완료하십시오. 이 경우, <b>SRV</b> 클러스터 이름 서비스 파라미터를 구성합니다. 그렇지 않은 경우 이 작업을 생략할 수 있습니다.
단계 4	<a href="#">Presence 게이트웨이 구성, 7 페이지</a>	IM and Presence 서비스에서 Cisco Unified Communications Manager를 프레즌스 게이트웨이로 할당하면 시스템이 프레즌스 정보를 교환할 수 있습니다.
단계 5	<a href="#">SIP 게시 트렁크 구성, 6 페이지</a>	(선택 사항) IM and Presence에 대한 SIP 게시 트렁크를 구성하려면 이 절차를 사용하십시오. 이 설정을 활성화하면 Cisco는 Cisco Unified Communications Manager에서 IM and Presence 서비스를 위해 Cisco Unified Communications Manager 사용이 허가된 사용자와 관련된 모든 회선 표시에 대해 전화기 프레즌스를 게시합니다.
단계 6	<a href="#">Cisco Unified Communications Manager에서 서비스 확인, 7 페이지</a>	Cisco Unified Communications Manager에서 필수 서비스가 실행 중인지 확인합니다.

	명령 또는 동작	목적
단계 7	클러스터 외부의 Cisco Unified Communications Manager에 대해 전화기 프레즌스 구성, 8 페이지	IM and Presence 서비스의 TLS 피어 주체로 Cisco Unified Communications Manager를 구성합니다. IM and Presence 서비스 클러스터 외부에 있는 Cisco Unified Communications Manager에서 전화기 프레즌스를 허용하려는 경우 TLS가 필요합니다.

## SIP 트렁크 보안 프로파일 구성

Cisco Unified Communications Manager에서 IM and Presence 서비스를 사용하여 트렁크 연결을 위한 SIP 트렁크 보안 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리 > 시스템 > 보안 > SIP 트렁크 보안 프로파일에서 찾기를 클릭합니다.

단계 2 비보안 SIP 트렁크 프로파일을 클릭합니다.

단계 3 복사를 클릭합니다.

단계 4 프로파일의 이름을 입력합니다. 예를 들어, IMP-SIP-Trunk-Profile.

단계 5 다음 설정을 완료하십시오.

- 디바이스 보안 모드 를 비보안으로 설정합니다.
- 수신 전송 유형을 TCP+UDP로 설정합니다.
- 발신 전송 유형을 TCP로 설정합니다.

단계 6 다음 확인란을 선택합니다.

- 프레즌스 가입 승인
- 대화 상자를 벗어난 REFER 승인
- 원하지 않는 통보 승인
- 대체 헤더 승인

단계 7 저장을 클릭합니다.

다음에 수행할 작업

[IM and Presence 서비스용 SIP 트렁크 구성, 4 페이지](#)

## IM and Presence 서비스용 SIP 트렁크 구성

Cisco Unified Communications Manager와 IM and Presence 서비스 클러스터간에 SIP 트렁크 연결을 설정합니다.

시작하기 전에

[SIP 트렁크 보안 프로파일 구성, 4 페이지](#)

프로시저

- 단계 1 **Cisco Unified CM** 관리에서 디바이스 > 트렁크를 선택합니다.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 트렁크 유형 드롭다운 목록 상자에서 **SIP** 트렁크를 선택합니다.
- 단계 4 디바이스 프로토콜 드롭다운 목록 상자에서 **SIP**을 선택합니다.
- 단계 5 트렁크 서비스 유형 드롭다운 목록 상자에서 **없음**을 선택합니다.
- 단계 6 다음을 클릭합니다.
- 단계 7 디바이스 이름 필드에 트렁크 이름을 입력합니다. 예를 들어, `IMP-SIP-Trunk`.
- 단계 8 드롭다운 목록 상자에서 디바이스 풀을 선택합니다.
- 단계 9 **SIP** 정보 섹션에서 IM and Presence 클러스터에 대한 주소 정보를 입력하여 IM and Presence 서비스에 트렁크를 할당합니다.

- IM and Presence 서비스에 대해 DNS SRV 레코드를 사용하는 경우 대상 주소가 **SRV** 확인란을 선택하고 대상 주소 필드에 SRV를 입력합니다.
- 그렇지 않으면 대상 주소 필드에 IM and Presence 게시자 노드의 IP 주소 또는 FQDN을 입력합니다. (+) 버튼을 클릭하여 노드를 더 추가합니다. 최대 16개 노드를 입력할 수 있습니다.

- a) 대상 주소 필드에 IM and Presence의 IP 주소, FQDN 또는 DNS SRV를 입력합니다.
- b) 다중 노드 구축을 구성 중인 경우 대상 주소가 **SRV**를 선택합니다.

이 시나리오에서 Cisco Unified Communications Manager는 DNS SRV 레코드 쿼리를 수행하여 이름을 확인합니다(예: `_sip._tcp.hostname.tld_sip._tcp.hostname.tld`). 단일 노드 구축을 구성 중인 경우 이 확인란을 선택하지 않으면 Cisco Unified Communications Manager에서는 DNS A 레코드 쿼리를 수행하여 이름을 확인합니다(예: `hostname.tld`).

DNS SRV 레코드의 대상 주소로 IM and Presence 서비스 기본 도메인을 사용하는 것이 좋습니다.

**참고** DNS SRV 레코드의 대상 주소로 원하는 도메인 값을 지정할 수 있습니다. 지정된 도메인에 사용자를 할당할 필요가 없습니다. IM and Presence 서비스 기본 도메인과 다른 도메인 값을 입력하는 경우, SRV 클러스터 이름(SRV Cluster Name)이라는 IM and Presence 서비스의 SIP 프록시 서비스 파라미터가 DNS SRV 레코드에서 지정한 도메인 값과 일치해야 합니다. 기본 도메인을 사용하는 경우 SRV 클러스터 이름(SRV Cluster Name) 파라미터를 변경할 필요가 없습니다.

두 시나리오 모두에서 Cisco Unified Communications SIP 트렁크 대상 주소는 DNS로 확인 가능해야 하며 IM and Presence 노드에 구성된 SRV 클러스터 이름(SRV Cluster Name)과 일치해야 합니다.

- 단계 10 대상 포트에 **5060**을 입력합니다.
- 단계 11 **SIP** 트렁크 보안 프로파일 드롭다운 목록 상자에서 이전 작업에서 만든 SIP 트렁크 보안 프로파일을 선택합니다.

단계 12 **SIP** 프로파일 드롭다운 목록 상자에서 프로파일을 선택합니다(예: 표준 **SIP** 프로파일).

단계 13 저장을 클릭합니다.

다음에 수행할 작업

Cisco Unified Communications Manager와 IM and Presence 서비스 간의 SIP 트렁크에서 DNS SRV를 사용하고 IM and Presence 기본 도메인이 아닌 다른 SRV 주소를 사용하는 경우에만 [SRV 클러스터 이름 구성, 6 페이지](#).

그렇지 않으면, [SIP 게시 트렁크 구성, 6 페이지](#).

## SRV 클러스터 이름 구성

Cisco Unified Communications Manager와 IM and Presence 서비스 간의 SIP 트렁크에서 DNS SRV를 사용하고 IM and Presence 기본 도메인이 아닌 다른 SRV 주소를 사용하는 경우에만 **SRV** 클러스터 이름 서비스 파라미터를 구성합니다. 그렇지 않은 경우 이 작업을 생략할 수 있습니다.

프로시저

단계 1 Cisco Unified CM IM and Presence 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 2 서버 드롭다운 메뉴에서 IM and Presence 게시자 노드를 선택하고 이동을 클릭합니다.

단계 3 서비스 드롭다운에서 **Cisco SIP Proxy** 서비스를 선택합니다.

단계 4 **SRV** 클러스터 이름 필드에 SRV 주소를 입력합니다.

단계 5 저장을 클릭합니다.

## SIP 게시 트렁크 구성

IM and Presence에 대한 SIP 게시 트렁크를 구성하려면 이 선택적 절차를 사용하십시오. 이 설정을 활성화하면 Cisco는 Cisco Unified Communications Manager에서 IM and Presence 서비스를 위해 Cisco Unified Communications Manager 사용이 허가된 사용자와 관련된 모든 회선 표시에 대해 전화기 프레즌스를 게시합니다.

프로시저

단계 1 Cisco Unified CM IM and Presence 관리에서 프레즌스 > 설정 > 표준 구성을 선택합니다.

단계 2 **CUCM IM** 및 프레즌스 게시 트렁크 드롭다운 목록에서 Cisco Unified Communications Manager에서 IM and Presence 서비스에 대해 구성한 SIP 트렁크를 선택합니다.

단계 3 저장을 클릭합니다.

참고 이 새 설정을 저장하면 Cisco Unified Communications Manager의 **IM and Presence** 게시 트렁크 서비스 파라미터도 이 새 설정으로 업데이트됩니다.

다음에 수행할 작업

[Cisco Unified Communications Manager에서 서비스 확인, 7 페이지](#)

## Presence 게이트웨이 구성

IM and Presence 서비스에서 이 절차를 사용하여 Cisco Unified Communications Manager를 프레즌스 게이트웨이로 할당합니다. 이 구성을 통해 Cisco Unified Communications Manager와 IM and Presence 서비스 간의 프레즌스 정보 교환이 가능합니다.

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리프레즌스 > 게이트웨이에서

단계 2 새로 추가를 클릭합니다.

단계 3 프레즌스 게이트웨이 드롭다운 목록 상자에서 **CUCM**을 선택합니다.

단계 4 설명을 입력합니다.

단계 5 프레즌스 게이트웨이 필드에 다음 옵션 중 하나를 입력합니다.

- Cisco Unified Communications Manager 게시자 노드의 IP 주소 또는 FQDN
- Cisco Unified Communications Manager 가입자 노드로 확인되는 DNS SRV

단계 6 저장을 클릭합니다.

다음에 수행할 작업

[SIP 게시 트렁크 구성, 6 페이지](#)

## Cisco Unified Communications Manager에서 서비스 확인

이 절차를 사용하여 Cisco Unified Communications Manager 노드에서 필수 서비스가 실행 중인지 확인합니다.

프로시저

단계 1 Cisco Unified Serviceability에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 2 서버 메뉴에서 Cisco Unified Communications Manager 클러스터 노드를 선택하고 이동을 클릭합니다.

단계 3 다음 서비스가 실행 중인지 확인합니다. 실행되지 않고 있는 경우 시작하십시오.

- Cisco CallManager
- Cisco TFTP
- Cisco CTIManager
- Cisco AXL Web 서비스(IM and Presence 및 Cisco Unified Communications Manager 간 데이터 동기화를 위해)

단계 4 위의 서비스 중 하나라도 실행 중이 아니면 서비스를 선택하고 시작을 클릭합니다.

## 클러스터 외부의 Cisco Unified Communications Manager에 대해 전화기 프레즌스 구성

IM and Presence 서비스 클러스터 외부에 있는 Cisco Unified Communications Manager에서 전화기 프레즌스를 허용할 수 있습니다. 그러나 IM and Presence 서비스가 클러스터 외부에 있는 Cisco Unified Communications Manager에서 SIP 계시를 수락하려면 Cisco Unified Communications Manager가 IM and Presence의 TLS에서 신뢰하는 피어로 나열되어야 합니다.

프로시저

	명령 또는 동작	목적
단계 1	<a href="#">Cisco Unified Communications Manager를 TLS 피어로 추가, 8 페이지</a>	IM and Presence 서비스의 TLS 피어로 Cisco Unified Communications Manager를 추가합니다.
단계 2	<a href="#">Unified Communications Manager에 대한 TLS 컨텍스트 구성, 9 페이지</a>	Cisco Unified Communications Manager TLS 피어 추가

### Cisco Unified Communications Manager를 TLS 피어로 추가

IM and Presence 서비스가 클러스터 외부에 있는 Cisco Unified Communications Manager에서 SIP 계시를 수락하려면 Cisco Unified Communications Manager가 IM and Presence 서비스의 TLS에서 신뢰하는 피어로 나열되어야 합니다.

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리 > 시스템 > 보안 > **TLS** 피어 주체에서 새로 추가를 클릭합니다.

단계 2 피어 주체 이름 필드에 외부 Cisco Unified Communications Manager의 IP 주소를 입력합니다.

단계 3 설명 필드에 노드의 이름을 입력합니다.

단계 4 저장을 클릭합니다.



다음에 수행할 작업

[TLS 컨텍스트 구성](#)

## Unified Communications Manager에 대한 TLS 컨텍스트 구성

다음 절차에 따라 이전 작업에서 구성한 Cisco Unified Communications Manager TLS 피어를 선택된 TLS 피어에 추가합니다.

시작하기 전에

[Cisco Unified Communications Manager를 TLS 피어로 추가, 8 페이지](#)

프로시저

- 
- 단계 1 **Cisco Unified CM IM and Presence** 관리 > 시스템 > 보안 > **TLS** 컨텍스트 구성에서 찾기를 클릭합니다.
  - 단계 2 **Default\_Cisco\_UP\_SIP\_Proxy\_Peer\_Auth\_TLS\_Context**를 클릭합니다.
  - 단계 3 사용 가능한 TLS 피어 주체의 목록에서 Cisco Unified Communications Manager에 대해 자신이 구성한 TLS 피어 주체를 선택합니다.
  - 단계 4 이 TLS 피어 주체를 선택한 TLS 피어 주체로 이동합니다.
  - 단계 5 저장을 클릭합니다.
  - 단계 6 모든 클러스터 노드에서 Cisco OAMAgent를 다시 시작합니다.
    - a) Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
    - b) 서버 드롭다운 목록 상자에서 IM and Presence 서버를 선택하고 이동을 클릭합니다.
    - c) **IM and Presence** 서비스 아래에서 **Cisco OAMAgent**를 선택하고 다시 시작을 클릭합니다.
    - d) 모든 클러스터 노드에서 서비스를 다시 시작합니다.
  - 단계 7 OAM 에이전트가 다시 시작된 후 Cisco Presence 엔진을 다시 시작합니다.
    - a) 도구 > 제어 센터 - 기능 서비스를 선택합니다.
    - b) 서버 드롭다운 목록 상자에서 IM and Presence 노드를 선택하고 이동을 클릭합니다.
    - c) **IM and Presence** 서비스 아래에서 **Cisco Presence** 엔진을 선택하고 다시 시작을 클릭합니다.
    - d) 모든 클러스터 노드에서 서비스를 다시 시작합니다.
- 

다음에 수행할 작업

[Cisco Unified Communications Manager에서 서비스 확인, 7 페이지](#)



## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.