# SIP OAuth 모드



## SIP OAuth 모드 개요

Unified Communications Manager에 대한 보안 등록에는 CTL 파일 업데이트, 상호 인증서 신뢰 저장소 설정 등의 과정이 포함됩니다. Cisco Jabber 디바이스가 온-프레미스와 오프-프레미스 사이에서 전환되는 경우, 보안 등록이 완료될 때마다 LSC를 업데이트하고 CAPF(Certificate Authority Proxy Function) 등록을 갱신하는 것은 어렵습니다.

SIP OAuth 모드를 사용하면 보안 환경에서 Cisco Jabber 인증에 대한 OAuth 새로 고침 토큰을 사용할 수 있습니다. Unified Communications Manager SIP 회선에서 OAuth를 지원하면 CAPF가 없는 보안 신호 처리 및 미디어를 사용할 수 있습니다. SIP 등록 중 OAuth 토큰 유효성 검사는 Unified Communications Manager 클러스터 및 Cisco Jabber 엔드포인트에서 OAuth 기반 인증이 활성화될 때 완료됩니다.

SIP 등록에 대한 OAuth 지원은 Cisco Unified Communications Manager 12.5 이후 릴리스에서 제공하는 Cisco Jabber 디바이스에 맞게 확장되었습니다.

다음은 OAuth에 대해 구성할 수 있는 전화기 보안 프로파일 유형입니다. 현재 이 기능은 Cisco Jabber에 대해서만 지원됩니다.

- iPhone용 Cisco 이중 모드(TCT 디바이스)
- Android용 Cisco 이중 모드(BOT 디바이스)
- Cisco Unified Client Service Framework(CSF 디바이스)
- 태블릿용 Cisco Jabber(TAB 디바이스)
- 범용 디바이스 템플릿

SIP 등록에 대한 OAuth 지원은 Cisco Unified Communications Manager 14.0 이후 릴리스에서 시작하여 다음 Cisco IP 전화기 시리즈 엔터프라이즈 모델로 확장되었습니다.

- 8811

- 8841
- 8851
- 8851NR
- 8861
- 7811
- 7821
- 7841
- 7861
- 8845
- 8865
- 8865NR
- 7832
- 8832
- 8832NR

# SIP OAuth 모드 사전 요건

이 기능은 사용자가 다음을 이미 완료했다고 가정합니다.

- 모바일 및 원격 액세스가 구성되고 Unified Communication Manager와 Expressway 사이에 연결이 설정되어 있는지 확인합니다.
- Unified Communications Manager가 내보내기 제어 허용 기능을 통해 스마트 또는 가상 어카운트에 등록되어 있는지 확인합니다.

# SIP OAuth 모드 구성 작업 흐름

시스템에 대한 SIP OAuth를 구성하려면 다음 작업을 완료하십시오.

프로시저

| | 명령 또는 동작 | 목적 |
|---|---|---|
| 단계 **1** | 디바이스에 대한 OAuth 액세스 토큰 활성화 | Cisco IP 전화기 7800 및 8800 엔터프라이즈 시리즈에서 SIP 등록에 대해 OAuth를 활성화 |

| | 명령 또는 동작 | 목적 |
|---|---|---|
| | | 합니다. 이 단계는 Cisco Jabber 디바이스에는 해당되지 않습니다. |
| 단계 2 | 새로 고침 로그인 구성, 4 페이지 | SIP OAuth를 통해 디바이스를 등록하려면 Unified Communications Manager의 로그인 흐름 새로 고침을 사용하여 oauth를 활성화합니다. |
| 단계 3 | OAuth 포트 구성, 4 페이지 | OAuth 등록이 있는 각 노드에 대해 OAuth에 대한 포트를 할당합니다. |
| 단계 4 | Expressway-C에 대한 OAuth 연결 구성, 5 페이지 | Expressway-C에 상호 인증된 TLS 연결을 구성합니다. |
| 단계 5 | SIP OAuth 모드 활성화, 6 페이지 | 퍼블리셔 노드에서 CLI 명령을 사용하여 OAuth 서비스를 활성화합니다. |
| 단계 6 | Cisco CallManager 서비스 다시 시작, 6 페이지 | OAuth 등록이 포함된 모든 노드에서 이 서비스를 다시 시작합니다. |
| 단계 7 | 보안 프로파일에서 OAuth 지원 구성, 6 페이지 | 엔드포인트에 대한 암호화를 구축하는 경우 전화기 보안 프로파일 내에서 OAuth 지원을 구성합니다. |

# 디바이스에 대한 OAuth 액세스 토큰 활성화

이 절차를 사용하여 전화기에 대한 OAuth 액세스 토큰을 활성화합니다.

참고 전화기의 SIP 등록에 대한 OAuth 지원에 대해서만 이 엔터프라이즈 매개 변수를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 2 **SSO** 및 **OAuth** 구성 섹션에서 디바이스에 대한 **OAuth** 액세스 토큰 값 드롭다운 목록이 암시적:이미 등록된 디바이스로 설정되어 있는지 확인합니다.

참고 디바이스에 대한 **OAuth** 액세스 토큰의 값을 명시적:활성화 코드 디바이스 온보딩 필요로 설정하여 전화기에 대한 SIP 등록을 위한 OAuth 지원을 비활성화합니다.

단계 3 저장을 클릭합니다.

# 새로 고침 로그인 구성

이 절차를 사용하여 Cisco Jabber 클라이언트에 대한 OAuth 액세스 토큰 및 새로 고침 토큰을 사용하여 새로 고침 로그인을 구성합니다.

프로시저

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

단계 **2** **SSO** 및 **OAuth** 구성 아래에서 새로 고침 로그인을 사용한 **OAuth** 매개 변수를 활성화됨으로 설정합니다.

단계 **3** (선택 사항) **SSO** 및 **OAuth** 구성 섹션에서 다른 매개 변수를 설정합니다. 매개변수 설명이 필요한 경우, 매개변수 이름을 클릭합니다.

단계 **4** 저장을 클릭합니다.

# OAuth 포트 구성

이 절차를 사용하여 SIP OAuth에 사용되는 포트를 할당합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다., 시스템 > **Cisco Unified CM**.

단계 **2** SIP OAuth를 사용하는 각 서버에 대해 다음을 수행합니다.

단계 **3** 서버를 선택합니다.

단계 **4** Cisco Unified Communications Manager **TCP** 포트 설정 아래에서 다음 필드에 대한 포트 값을 설정합니다.

- SIP 전화기 OAuth 포트

  기본값은 5090입니다. 허용 가능한 구성 가능 범위는 1024 ~ 49151입니다.

- SIP 모바일 및 원격 액세스 포트

  기본값은 5091입니다. 허용 가능한 구성 가능 범위는 1024 ~ 49151입니다.

참고 Cisco Unified Communications Manager는 SIP 전화기 OAuth 포트(5090)를 사용하여 TLS를 통해 Jabber 온프레미스 디바이스에서 SIP 회선 등록을 수신 대기합니다. 그러나 Unified CM은 SIP 모바일 원격 액세스 포트(기본값 5091)를 사용하여 mLTS를 통해 Expressway의 Jabber에서 SIP 회선 등록을 수신 대기합니다.

두 포트 모두 수신 TLS/mTLS 연결에 대해 Tomcat 인증서 및 Tomcat-trust를 사용합니다. Tomcat-trust 저장소에서 모바일 및 원격 액세스가 정확하게 작동하려면 SIP OAuth 모드에 대한 Expressway-C 인증서를 확인할 수 있어야 합니다.

다음의 경우에는 Expressway-C 인증서를 Unified Communications Manager의 Tomcat 인증서에 업로드하기 위한 추가 단계를 수행해야 합니다.

- Expressway-C 인증서 및 Tomcat 인증서가 동일한 CA 인증서에 의해 서명 지 않았습니다.
- Unified CM Tomcat 인증서는 CA에 서명이 되어 있지 않습니다.

단계 **5** 저장을 클릭합니다.

단계 **6** SIP OAuth를 사용하는 각 서버에 대해 이 절차를 반복합니다.

# Expressway-C에 대한 OAuth 연결 구성

이 절차를 사용하여 Cisco Unified Communications Manager Administration에 Expressway-C 연결을 추가합니다. SIP OAuth를 사용하는 모바일 및 원격 액세스 모드의 디바이스에 대해 이 구성이 필요합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다. 디바이스 > **Expressway-C** .

단계 **2** (선택 사항) **Expressway-C** 찾기 및 나열 창에서 찾기를 클릭하여 Expressway-C에서 Unified Communications Manager(으)로 푸시된 X.509 주체 이름/주체 대체 이름을 확인합니다.

참고 필요한 경우 값을 수정할 수 있습니다. 또는 항목이 누락된 경우 Expressway-C 정보를 추가합니다.

Expressway-C가 Unified Communications Manager와 다른 도메인에 있는 경우 관리자가 Cisco Unified CM 관리 사용자 인터페이스에 액세스하고 Unified CM 구성에서 Expressway C에 도메인을 추가해야 합니다.

단계 **3** 새로 추가를 클릭합니다.

단계 **4** Expressway-C의 IP 주소, 호스트 이름 또는 정규화된 도메인 이름을 입력합니다.

단계 **5** 설명을 입력합니다.

단계 **6** Expressway-C 인증서에서 Expressway-C의 X.509 주체 이름/주체 대체 이름을 입력합니다.

단계 **7** 저장을 클릭합니다.

# SIP OAuth 모드 활성화

명령줄 인터페이스를 사용하여 SIP OAuth 모드를 활성화합니다. 퍼블리셔 노드에서 이 기능을 활성화하면 모든 클러스터 노드의 기능도 활성화됩니다.

프로시저

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

단계 **2** `utils sipOAuth-mode enable` CLI 명령을 실행합니다.
읽기 전용 클러스터 **SIPOAuth** 모드 엔터프라이즈 매개 변수가 활성화됨으로 업데이트됩니다.

# Cisco CallManager 서비스 다시 시작

CLI를 통해 SIP OAuth를 활성화한 후 엔드포인트가 SIP OAuth를 통해 등록되는 모든 노드에서 Cisco CallManager 서비스를 다시 시작합니다.

프로시저

단계 **1** Cisco Unified Serviceability에서 다음을 선택합니다. 도구 > 제어 센터 > 기능 서비스.

단계 **2** 서버 드롭다운 목록에서 서버를 선택합니다.

단계 **3** **Cisco CallManager** 서비스를 선택하고 다시 시작을 클릭합니다.

# 보안 프로파일에서 OAuth 지원 구성

SIP OAuth 등록을 지원하는 암호화된 엔드포인트를 구축하는 경우 이 절차를 사용하여 OAuth 인증을 구성합니다.

프로시저

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

단계 **2** 찾기를 클릭하고 전화기에서 사용하는 보안 프로파일을 선택합니다.

단계 **3** 디바이스 보안 모드가 암호화됨이고 전송 유형이 **TLS**인지 확인합니다

단계 **4** **OAuth** 인증 활성화 확인란을 선택합니다.

단계 **5** 저장을 클릭합니다.

참고 SIP OAuth 모드가 활성화되면 다이제스트 인증 활성화 및 **TFTP** 암호화 구성 옵션이 지원되지 않습니다.