SIP OAuth 모드

- SIP OAuth 모드 개요, 1 페이지
- SIP OAuth 모드 사전 요건, 2 페이지
- SIP OAuth 모드 구성 작업 흐름, 2 페이지

SIP OAuth 모드 개요

Unified Communications Manager에 대한 보안 등록에는 CTL 파일 업데이트, 상호 인증서 신뢰 저장소 설정 등의 과정이 포함됩니다. 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 모든 디바이스 인증에 대한 OAuth 새로 고침 토큰을 사용할 수 있습니다. 이 기능은 Unified Communications Manager의 보안을 향상시킵니다.

Unified Communications Manager에서는 엔드포인트가 제공하는 토큰을 확인하고 구성 파일을 인증 전용으로 사용합니다. SIP 등록 중 OAuth 토큰 유효성 검사는 Unified Communications Manager 클러스터 및 다른 Cisco 디바이스에서 OAuth 기반 인증이 활성화될 때 완료됩니다.

SIP 등록에 대한 OAuth 지원은 다음에 대해 확장됩니다.

- Cisco Unified Communications Manager 12.5 릴리스의 Cisco Jabber 디바이스
- Cisco Unified Communications Manager 릴리스 14 이후의 SIP 전화기

참고 기본적으로 SIP OAUth가 활성화된 경우 TFTP는 SIP 전화기에 대해 안전합니다. TFTP 파일 다운로드는 보안 채널을 통해 인증된 전화기에 대해서만 발생합니다. SIP OAuth는 온-프레미스와 MRA를 통해 CAPF 온프레미스 없이 엔드 투 엔드 보안 신호 처리 및 미디어 암호화를 제공합니다.

다음은 OAuth에 대해 구성할 수 있는 전화기 보안 프로파일 유형입니다.

- 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
- Cisco 8811
- Cisco 8841
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 7811
- Cisco 7821
- Cisco 7841
- Cisco 7861
- Cisco 8845
- Cisco 8865
- Cisco 8865NR
- Cisco 7832
- Cisco 8832
- Cisco 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.
- 클라이언트 펌웨어가 SIP OAuth를 지원하는지 확인합니다.

SIP OAuth 모드 구성 작업 흐름

시스템에 대한 SIP OAuth를 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 1	전화기 엣지 신뢰에 CA 인증서 업로드	CA 인증서를 전화기 엣지 신뢰에 업로드하여 토큰을 가져옵니다. 이 단계는 Cisco Jabber 디바이스에는 해당되지 않습니다.
단계 2	디바이스에 대한 OAuth 액세스 토큰 활성화	중요 이 단계는 14 이후 릴리스부터 적용할 수 있습니다. Cisco IP 전화기 7800 및 8800 엔터프라이즈 시리즈에서 SIP 등록에 대해 OAuth를 활성화합니다. 이 단계는 Cisco Jabber 디바이스에는 해당되지 않습니다.
단계 3	새로 고침 로그인 구성, 5 페이지	SIP OAuth를 통해 디바이스를 등록하려면 Unified Communications Manager의 로그인 흐름 새로 고침을 사용하여 oauth를 활성화합니다.
단계 4	OAuth 포트 구성, 5 페이지	OAuth 등록이 있는 각 노드에 대해 OAuth에 대한 포트를 할당합니다.
단계 5	Expressway-C에 대한 OAuth 연결 구성, 6 페이지	Expressway-C에 상호 인증된 TLS 연결을 구성합니다.
단계 6	SIP OAuth 모드 활성화, 7 페이지	퍼블리셔 노드에서 CLI 명령을 사용하여 OAuth 서비스를 활성화합니다.
단계 7	Cisco CallManager 서비스 다시 시작, 7 페이지	OAuth 등록이 포함된 모든 노드에서 이 서비스를 다시 시작합니다.
단계 8	전화기 보안 프로파일에서 디바이스 보안 모드 구성	엔드포인트에 대한 암호화를 구축하는 경우 전화기 보안 프로파일 내에서 OAuth 지원을 구성합니다.
단계 9	(선택 사항) MRA 모드에 대해 SIP Oauth 등록 전화기 구성	중요 이 단계는 14 이후 릴리스부터 적용할 수 있습니다. MRA 모드에서 SIP OAuth 등록 전화기를 구성합니다. 이 단계는 Cisco Jabber 디바이스에는 해당되지 않습니다.

전화기 엣지 신뢰에 CA 인증서 업로드

이 절차를 사용하여 Tomcat 서명 인증서의 루트 인증서를 전화기 엣지 신뢰에 업로드합니다.

참고 이 절차는 Cisco 전화기에 대해서만 수행되며 Cisco Jabber에는 적용되지 않습니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서/인증서 체인 업로드 창의 인증서 용도 드롭다운 목록에서 전화기 엣지 신뢰를 선택합니다.
단계 **4** 파일 업로드 필드에서 찾아보기를 클릭하고 인증서를 업로드합니다.
단계 **5** 업로드를 클릭합니다.

디바이스에 대한 **OAuth** 액세스 토큰 활성화

중요 이 섹션은 14 이후 릴리스부터 적용할 수 있습니다.

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 SIP OAuth 등록을 위한 수신 토큰을 암시적으로 비활성화하고 활성화 코드를 통한 수신 토큰만 지원합니다. 그런 다음 보안 프로파일에 표시된 경우 SIP OAuth 등록에 토큰을 사용할 수 있습니다.

릴리스 14 이후부터는 엔터프라이즈 매개변수 디바이스용 **OAuth** 액세스 토큰의 기본값은 암시적**:**이미 등록된 디바이스입니다.

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 다음 메뉴를 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 Cisco 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 Cisco Unified Communications Manager의 Tomcat-Trust 인증서 저장소에 업로드하기 위한 추가 단계를 수행해야 합니다.

- Expressway-C 인증서 및 Cisco Tomcat 인증서가 동일한 CA 인증서에 의해 서명되지 않았습니다.
- Unified CM Cisco 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 통합 커뮤니케이션 매니저 관리에 Expressway-C 연결을 추가합니다. SIP OAuth를 사용하는 모바일 및 원격 액세스 모드의 디바이스에 대해 이 구성이 필요합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 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.

시작하기 전에

14SU1 릴리스부터 프록시 TFTP가 활성화된 경우 오프 클러스터 Tomcat 인증서의 루트 CA 인증서를 프록시 전화기 엣지 신뢰로 복사해야 합니다.

프로시저

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

단계 **2** `utils sipOAuth-mode enable` CLI 명령을 실행합니다.
릴리스 14부터 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 통합 서비스 가용성에서 다음 메뉴를 선택합니다.도구 > 제어 센터 > 기능 서비스.

단계 **2** 서버 드롭다운 목록에서 서버를 선택합니다.

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

전화기 보안 프로파일에서 디바이스 보안 모드 구성

이 절차를 사용하여 전화기 보안 프로필에서 디바이스 보안 모드를 구성하고 해당 전화기의 전화기 보안 프로파일 내에서 디바이스 보안 모드를 암호화로 설정한 경우에만 필요합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 보안 > 전화기 보안 프로파일에 체크 표시합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 기존 전화기 보안 프로파일 검색

- 새로 추가를 클릭합니다.

단계 **3** 전화기 보안 프로파일 정보 섹션의 디바이스 보안 모드 드롭다운 목록에서 암호화를 선택합니다.

단계 **4** 전송 유형 드롭다운 목록에서 **TLS**를 선택합니다.

단계 **5** **OAuth** 인증 활성화 확인란을 선택합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** 전화기 보안 프로파일을 전화기에 연결합니다. 전화기 보안 프로파일을 적용하는 방법에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 보안 설명서의 "전화기에 보안 프로파일 적용" 섹션을 참조하십시오.

참고 변경 내용을 적용하려면 전화기를 재설정합니다,

참고 SIP OAuth 모드가 활성화되면 다이제스트 인증 활성화 및 **TFTP** 암호화 구성 옵션이 지원되지 않습니다. 전화기에서 **https(6971)**를 통해 TFTP 구성 파일을 안전하게 다운로드하고 토큰을 인증에 사용합니다.

MRA 모드에 대해 SIP Oauth 등록 전화기 구성

이 절차를 사용하여 SIP OAuth 등록 전화기를 MRA 모드로 구성합니다.

시작하기 전에

중요 이 섹션은 14 이후 릴리스부터 적용할 수 있습니다.

전화기가 활성화 코드를 사용하도록 구성되어 있는지 확인합니다. 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서에서 활성화 코드를 사용하도록 등록 방법 설정 섹션을 참조하십시오.

참고 MRA를 통한 SIP OAuth를 사용할 때 사용자는 로그인에 사용자 이름/암호를 사용할 수 없지만 활성화 코드 기반 온보딩을 사용해야 합니다.

프로시저

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

단계 **2** 찾기를 클릭하고 오프 프레미스 모드에 대해 구성하려는 디바이스를 선택합니다.

단계 **3** 디바이스 정보 섹션에서 다음을 수행합니다.

- **MRA**를 통한 활성화 코드 허용 확인란을 선택합니다.

- 활성화 코드 **MRA** 서비스 도메인 드롭다운 목록에서 필요한 MRA 서비스 도메인을 선택합니다. MRA 서비스 도메인을 구성하는 방법에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 *MRA* 서비스 도메인 구성 섹션을 참조하십시오.

참고 MRA를 통한 SIP OAuth 모드의 경우 활성화 코드만 사용하고 사용자 이름/암호 기반 로그인은 사용하지 마십시오.

단계 **4** 프로토콜 특정 정보 섹션의 장치 보안 프로파일 드롭다운 목록에서 OAuth 활성화된 SIP 프로파일을 선택합니다. 전화기가 OAuth 펌웨어를 지원하는지 확인합니다. 보안 프로파일을 만드는 방법에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 전화기 보안 프로파일 구성 섹션을 참조하십시오.

단계 **5** 저장을 클릭하고 구성 적용을 클릭합니다.

참고 전화기가 MRA 모드로 전환되고 Expressway와 통신을 시작합니다. 내부 네트워크가 온프레미스에서 Expressway와의 통신을 허용하지 않는 경우, 전화기는 등록되지 않지만 오프프레미스에 전원이 공급되면 Expressway에 연결될 수 있습니다.