SSO(Single Sign-On, 단일 인증) 구성

SAML SSO 솔루션 정보

중요 Cisco Jabber를 Cisco Webex Meeting 서버로 구축할 경우, Unified Communications Manager 및 Webex Meeting 서버는 같은 도메인에 있어야 합니다.

SAML은 관리자가 정의된 애플리케이션 중 하나에 로그인한 후에 해당 애플리케이션에 원활히 액세스하도록 해주는 XML 기반의 개방형 표준 데이터 형식입니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. 이것은 사용자를 인증하기 위해 서비스 제공자(예: Cisco Unified Communications Manager)가 사용하는 인증 프로토콜입니다. SAML은 IdP(Identity Provider)와 통신 사업자 간에 보안 인증 정보 교환을 가능하게 합니다.

SAML SSO는 SAML 2.0 프로토콜을 사용하여 Cisco 협업 솔루션에 대한 도메인 간 및 제품 간 SSO(Single Sign-On, 단일 인증)을 제공합니다. SAML 2.0을 사용하면 Cisco 애플리케이션에서 SSO를 활성화하고 Cisco 애플리케이션 및 IdP 간 페더레이션을 사용할 수 있습니다. SAML 2.0을 사용하면 Cisco 관리 사용자가 높은 보안 수준을 유지하면서 IdP 및 서비스 제공자 간에 보안 웹 도메인에 액세스하여 사용자 인증 및 인증 데이터를 교환할 수 있습니다. 기능은 다양한 애플리케이션 간에 일반 인증서 및 관련 정보를 사용하는 보안 메커니즘을 제공합니다.

SAML SSO 관리 액세스에 대한 인증은 Cisco 협업 애플리케이션에 로컬로 구성된 RBAC(역할 기반 액세스 제어)를 기반으로 합니다.

SAML SSO는 메타데이터 및 인증서를 프로비저닝 프로세스의 일부로 IdP와 서비스 제공업체 간에 교환하여 CoT(Circle of Trust)를 설정합니다. 서비스 제공자는 IdP의 사용자 정보를 신뢰하여 다양한 서비스 또는 애플리케이션에 대한 액세스를 제공합니다.

중요 서비스 제공자는 더 이상 인증과 관련되지 않습니다. SAML 2.0은 서비스 제공자와 IdP 사이의 인증을 대리합니다.

클라이언트가 IdP를 인증하고 IdP는 클라이언트에 어설션을 부여합니다. 클라이언트는 서비스 제공자에 어설션을 제공합니다. CoT가 설정되었으므로 서비스 제공자는 어설션을 신뢰하고 클라이언트에 대한 액세스를 부여합니다.

SAML SSO 구성 작업 플로우

이 작업을 완료하여 SAML SSO에 대한 Unified Communications Manager를 구성합니다.

시작하기 전에

SAML SSO 구성을 사용하려면 Unified Communications Manager를 구성하면서 동시에 ID 제공자(IdP)를 구성해야 합니다. IdP별 구성의 예는 다음을 참조하십시오.

- Active Directory Federation 서비스
- Okta
- Open Access Manager
- PingFederate

참고 위의 링크는 예로만 사용됩니다. 공식 설명서는 IdP 설명서를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 1	Cisco Unified Communications Manager에서 UC 메타데이터 내보내기, 3 페이지	신뢰 관계를 생성하려면 Unified Communications Manager와 IdP 간에 메타데이터 파일을 교환해야 합니다.
단계 2	ID 제공자(IdP)에 대한 SAML SSO 구성	다음 작업을 완료합니다. • CoT(Circle of Trust) 관계를 완료하기 위해 Unified Communications Manager에서 내보낸 UC 메타데이터 파일을 업로드합니다. • IdP에 대한 SAML SSO 구성 • IdP 메타데이터 파일을 내보냅니다. 이 파일을 Unified Communications Manager로 가져옵니다.

	명령 또는 동작	목적
단계 3	Cisco Unified Communications Manager에서 SAML SSO 활성화	IdP 메타데이터를 가져오고, Unified Communications Manager에서 SAML SSO를 활성화합니다.
단계 4	Cisco Tomcat 서비스 다시 시작, 6 페이지	SSO를 활성화하기 이전 및 이후에는 SSO가 활성화되어 있는 모든 클러스터 노드에서 Cisco Tomcat 서비스를 다시 시작해야 합니다.
단계 5	SAML SSO 구성 확인, 6 페이지	SAML SSO가 성공적으로 구성되었는지 확인하십시오.

Cisco Unified Communications Manager에서 UC 메타데이터 내보내기

이 절차를 사용하여 서비스 공급자(Unified Communications Manager)에서 UC 메타데이터 파일을 내보냅니다. CoT(Circle of Trust) 관계를 구축하기 위해 메타데이터 파일을 ID 제공자(IdP)로 가져옵니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **SAML SSO(Single Sign-On,** 단일 인증**)**을 선택합니다.

단계 2 **SAML SSO(Single Sign-On,** 단일 인증**)** 창에서 **SSO** 모드 필드에 대한 옵션 중 하나를 선택합니다.

- 클러스터 수준—클러스터에 대한 단일 SAML 규약입니다.

  참고 이 옵션을 선택하는 경우 클러스터의 모든 노드에 대한 Tomcat 서버에 동일한 인증서(다중 서버 SAN 인증서)가 있는지 확인합니다.

- 노드 당—각 노드에는 별도의 SAML 계약이 있습니다.

단계 3 **SAML SSO(Single Sign-On,** 단일 인증**)** 창에서 인증서 필드에 대한 옵션 중 하나를 선택합니다.

- 시스템에서 생성한 자체 서명 인증서 사용
- **Tomcat** 인증서 사용

단계 4 메타데이터 파일을 내보내려면 모든 메타데이터 내보내기를 클릭합니다.

참고 3단계에서 클러스터 수준 옵션을 선택하는 경우, 다운로드를 위해 클러스터에 대해 단일 메타데이터 XML 파일이 표시됩니다. 그러나 노드 당 옵션을 선택하는 경우, 다운로드를 위해 클러스터의 각 노드에 대해 하나의 메타데이터 XML 파일이 표시됩니다.

다음에 수행할 작업

IdP에 대한 다음 작업을 완료해야 합니다.

- Unified Communications Manager에서 내보낸 UC 메타데이터 파일 업로드
- IdP에 대한 SAML SSO 구성
- IdP 메타데이터 파일을 내보냅니다. 이 파일은 CoT(Circle of Trust) 관계를 완료하기 위해 Unified Communications Manager로 가져옵니다.

Cisco Unified Communications Manager에서 SAML SSO 활성화

이 절차를 사용하여 서비스 제공자(Unified Communications Manager)에서 SAML SSO를 활성화합니다. 이 프로세스에는 IdP 메타데이터를 Unified Communications Manager 서버로 가져오는 작업이 포함됩니다.

중요 SAML SSO를 활성화 또는 비활성화한 후에 Cisco Tomcat 서비스를 다시 시작하는 것이 좋습니다.

참고 SAML SSO를 활성화 또는 비활성화하면 Cisco CallManager 관리, Cisco Unified CM IM and Presence 관리, Cisco CallManager Serviceability 및 Unified IM and Presence Serviceability 서비스가 다시 시작됩니다.

시작하기 전에

이 절차를 완료하기 전에 다음을 확인하십시오.

- IdP에서 내보낸 메타데이터 파일이 필요합니다.
- 엔드 유저 데이터가 Cisco Unified Communications Manager 데이터베이스에 동기화되었는지 확인하십시오.
- Cisco Unified CM IM and Presence Cisco Sync Agent 서비스에서 데이터 동기화를 성공적으로 완료했는지 확인하십시오. 진단 > 시스템 문제해결 도구를 선택하여 **Cisco** 통합 **CM IM** 및 프레즌스 관리에서 이 테스트의 상태를 확인하십시오. "Sync Agent에서 관련 데이터(예: 디바이스, 사용자, 라이센싱 정보)를 동기화함" 테스트에서는 데이터 동기화가 성공적으로 완료된 경우 "테스트 통과" 결과를 표시합니다.
- 하나 이상의 LDAP 동기화된 사용자가 표준 CCM 수퍼 사용자 그룹에 추가되어 Cisco Unified 관리에 액세스할 수 있는지 확인합니다. 엔드 유저 데이터를 동기화하고 LDAP 동기화된 사용자를 그룹에 추가하는 것에 대한 자세한 내용은, Cisco Unified Communications Manager 관리 설명서의 "시스템 설정"과 "엔드 유저 설정" 섹션을 참조하십시오.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.

단계 **2** **SAML SSO** 활성화를 클릭한 다음 계속을 클릭합니다.

모든 서버 연결이 다시 시작된다는 경고 메시지가 통지됩니다.

단계 **3** 클러스터 수준 SSO 모드를 구성한 경우, 다중 서버 **tomcat** 인증서 테스트 버튼을 클릭합니다. 그렇지 않으면 이 단계를 생략할 수 있습니다.

단계 **4** 다음을 클릭합니다.

IdP 메타데이터를 가져올 수 있는 대화 상자가 표시됩니다. IdP와 서버 간 신뢰 관계를 구성하려면 먼저 IdP에서 신뢰 메타데이터 파일을 얻은 후 모든 서버로 가져와야 합니다.

단계 **5** IdP에서 내보낸 메타데이터 파일을 가져옵니다.

a) 브라우징을 통해 내보낸 IdP 메타데이터 파일을 찾아 선택합니다.
b) **IdP** 메타데이터 가져오기를 클릭합니다.
c) 다음을 클릭합니다.
d) 서버 메타데이터 다운로드 및 **IdP**에서 설치 화면에서 다음을 클릭합니다.

참고 클러스터의 노드 하나 이상에서 IdP 메타데이터 파일을 성공적으로 가져온 경우에만 다음 버튼이 활성화됩니다.

단계 **6** 다음과 같이 연결을 테스트하고 구성을 완료합니다.

a) 최종 사용자 설정 창에서 LDAP 동기화되었으며 권한 정보 목록 표에서 "표준 CCM 슈퍼 사용자"로서 권한을 갖는 사용자를 선택합니다.
b) 테스트 실행을 클릭합니다.

IdP 로그인 창이 표시됩니다.

참고 테스트가 성공하기 전까지는 SAML SSO를 활성화할 수 없습니다.

c) 유효한 사용자 이름과 암호를 입력합니다.

인증에 성공하면 다음 메시지가 표시됩니다:

`SSO 테스트가 성공했습니다.`

이 메시지가 표시되면 브라우저 창을 닫습니다.

인증이 실패하거나 인증에 60초 이상 걸리는 경우, [IdP 로그인] 창에 "로그인 실패" 메시지가 표시됩니다. [SAML Single Sign-On] 창에 다음 메시지가 표시됩니다.

`SSO 메타데이터 테스트 시간이 초과되었습니다.`

IdP에 다시 로그인을 시도하려면, 다른 사용자를 선택하고 다른 테스트를 실행합니다.

d) 마침을 클릭하여 SAML SSO 설정을 완료합니다.

SAML SSO가 활성화되고 SAML SSO에 참여하는 웹 애플리케이션이 모두 다시 시작됩니다. 웹 애플리케이션이 다시 시작되는 데 1~2분 걸릴 수 있습니다.

Cisco Tomcat 서비스 다시 시작

SAML 싱글 사인-온을 활성화 또는 비활성화하기 이전과 이후에, 싱글 사인-온을 실행 중인 모든 통합 CM 및 IM과 프레즌스 서비스 클러스터 노드에서 Cisco Tomcat 서비스를 다시 시작합니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** `utils service restart Cisco Tomcat` CLI 명령을 실행합니다.

단계 **3** SSO(Single Sign-On, 단일 인증)가 활성화된 모든 클러스터 노드에서 이 절차를 반복합니다.

SAML SSO 구성 확인

두 서비스 제공자(Unified Communications Manager) 및 IdP 모두에서 SAML SSO를 구성한 후에는 Unified Communications Manager에서 이 절차를 사용하여 구성이 작동하는지 확인합니다.

시작하기 전에

다음을 확인하십시오.

- Unified CM 관리의 **SAML Single Sign-on** 구성 창에 **IdP** 메타데이터 신뢰 파일을 성공적으로 가져왔다고 표시됩니다.
- 서비스 제공자 메타데이터 파일은 IdP에 설치됩니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **SAML SSO(Single Sign-On,** 단일 인증**)**을 선택하고 **SAML Single Sign-on** 구성 창이 열리면 다음을 클릭합니다.

단계 **2** 유효한 관리자 사용자 이름 영역에서 관리 사용자를 선택하고 **SSO** 테스트 실행 **...** 버튼을 클릭합니다.

참고 테스트 사용자가 관리자 권한을 보유해야만 하며, IdP 서버에서 사용자로 추가되어 있어야만 합니다. [유효한 관리자 사용자 이름] 영역에 테스트를 실행하기 위해 가져올 수 있는 사용자 목록이 표시됩니다.

테스트에 성공하면 SAML SSO가 성공적으로 구성됩니다.