SAML Single Sign-On 관리

SAML Single Sign-On 개요

SAML Single Sign-On(SSO)을 사용하여 이러한 애플리케이션 중 하나에 로그인한 후 Cisco 애플리케이션의 정의된 집합에서 액세스할 수 있습니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. 이것은 사용자를 인증하기 위해 서비스 제공자(예: Cisco Unified Communications Manager)에서 사용하는 인증 프로토콜입니다. SAML을 사용하여 IdP(ID 공급자)와 서비스 공급자 간에 보안 인증 정보가 교환됩니다. 기능은 다양한 애플리케이션 간에 일반 인증서 및 관련 정보를 사용하는 보안 메커니즘을 제공합니다.

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

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

iOS에서 Cisco Jabber용 인증서 기반 SSO 인증을 위한 옵트인 제어

Cisco Unified Communications Manager의 이 릴리스는 IdP(ID 공급자)를 사용하여 iOS SSO 로그인 동작에서 Cisco Jabber를 제어하기 위한 옵트인 구성 옵션을 소개합니다. 이 옵션을 사용하면 Cisco Jabber에서 제어되는 모바일 장치 관리(MDM) 배포에서 IdP를 사용하여 인증서 기반 인증을 수행할 수 있습니다.

Cisco Unified Communications Manager의 **iOS**용 **SSO** 로그인 동작 엔터프라이즈 매개 변수를 통해 옵트인 제어를 구성할 수 있습니다.

참고 이 매개 변수의 기본값을 변경하기 전에 http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html에서 Cisco Jabber 기능 지원 및 설명서를 참조하여 iOS의 Cisco Jabber가 SSO 로그인 동작 및 인증서 기반 인증을 지원하는지 확인하십시오.

이 기능을 활성화하려면 iOS에 Cisco Jabber용 SSO 로그인 동작 구성, 4 페이지 절차를 참조하십시오.

SAML Single Sign-On 필수 구성 요소

- Cisco Unified Communications Manager 클러스터를 위해 구성된 DNS
- IdP(ID 공급자) 서버
- IdP 서버에서 신뢰하고 시스템에서 지원하는 LDAP 서버

SAML 2.0을 사용하는 다음 IdP는 SAML SSO 기능에 대해 테스트됩니다.

- OpenAM 10.0.1
- Microsoft® Active Directory® 페더레이션 서비스 2.0(AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

타사 애플리케이션은 다음과 같은 구성 요구 사항을 충족해야 합니다.

- IdP에 필수 특성 “uid”를 구성해야 합니다. 이 특성은 Cisco Unified Communications Manager에서 LDAP 동기화된 사용자 ID로 사용되는 특성과 일치해야 합니다.
- SAML SSO에 참여하는 모든 엔티티의 시계를 동기화해야 합니다. 시계를 동기화하는 방법에 대한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html의 *Cisco Unified Communications Manager* 시스템 구성 설명서에서 “NTP 설정”을 참조하십시오.

SAML Single Sign-On 관리

SAML Single Sign-On 관리

SAML Single Sign-On 활성화

참고 동기화 에이전트 테스트 확인에 성공하기 전까지는 SAML SSO를 활성화할 수 없습니다.

시작하기 전에

- 사용자 데이터가 Cisco Unified Communications Manager 데이터베이스에 동기화되었는지 확인합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.
- Cisco Unified CM IM and Presence Service Cisco 동기화 에이전트 서비스에서 데이터 동기화를 성공적으로 완료했는지 확인합니다. **Cisco Unified CM IM and Presence** 관리 > 진단 > 시스템 문제 해결 도구를 선택하여 이 테스트의 상태를 확인합니다. “Sync Agent에서 관련 데이터(예: 장치, 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 CM 관리에 액세스할 수 있는지 확인합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.
- IdP와 서버 간 신뢰 관계를 구성하려면 먼저 IdP에서 신뢰 메타데이터 파일을 얻은 후 모든 서버로 가져와야 합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.
단계 **2** **SAML SSO** 활성화를 클릭합니다.
단계 **3** 모든 서버 연결이 다시 시작될 것임을 알려주는 경고 메시지가 표시되면 계속을 클릭합니다.
단계 **4** 찾아보기를 클릭하여 IdP 메타데이터를 찾고 업로드합니다.
단계 **5** **IdP** 메타데이터 가져오기를 클릭합니다.
단계 **6** 다음을 클릭합니다.
단계 **7** 신뢰 메타데이터 파일 집합 다운로드를 클릭하여 서버 메타데이터를 시스템으로 다운로드합니다.
단계 **8** IdP 서버에서 서버 메타데이터를 업로드합니다.
단계 **9** 다음을 클릭하여 작업을 계속합니다.

단계 **10** 유효한 관리자 ID 목록에서 관리자 권한이 있는 LDAP 동기화된 사용자를 선택합니다.

단계 **11** 테스트 실행을 클릭합니다.

단계 **12** 유효한 사용자 이름과 암호를 입력합니다.

단계 **13** 성공 메시지가 표시되면 브라우저 창을 닫습니다.

단계 **14** 완료를 클릭하고 웹 애플리케이션이 다시 시작될 때까지 1 ~ 2분 기다립니다.

iOS에 Cisco Jabber용 SSO 로그인 동작 구성

프로시저

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

단계 **2** 옵트인 제어를 구성하려면 SSO 구성 섹션에서 **iOS**에 대한 **SSO** 로그인 동작 매개 변수에 대해 기본 브라우저 사용 옵션을 선택합니다.

참고 **iOS**에 대한 **SSO** 로그인 동작 매개 변수는 다음 옵션을 포함합니다.

- 포함된 브라우저 사용—이 옵션을 활성화하면 Cisco Jabber는 SSO 인증을 위해 포함된 브라우저를 사용합니다. 이 옵션을 사용하여 기본 Apple Safari 브라우저로 교차 실행하지 않고 버전 9 이전의 iOS 장치에서 SSO를 사용할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- 기본 브라우저 사용—이 옵션을 활성화하면 Cisco Jabber는 iOS 장치의 Apple Safari 프레임워크를 사용하여 MDM 배포에서 IdP(Identity Provider)를 사용하여 인증서 기반 인증을 수행합니다.

  참고 기본 브라우저 사용은 포함된 브라우저 사용만큼 안전하지 않으므로 제어된 MDM 배포를 제외하고 이 옵션을 구성하는 것이 좋습니다.

단계 **3** 저장을 클릭합니다.

업그레이드한 후 WebDialer에서 SAML Single Sign-on 활성화

업그레이드 후에 Cisco WebDialer에서 SAML Single Sign-On을 다시 활성화하려면 이 작업을 수행합니다. SAML Single Sign-On을 활성화하기 전에 Cisco WebDialer가 활성화된 경우 Cisco WebDialer에서 기본적으로 SAML Single Sign-On이 활성화되지 않습니다.

프로시저

	명령 또는 동작	목적
단계 1	Cisco WebDialer 서비스 비활성화, 5 페이지	Cisco WebDialer 웹 서비스가 이미 활성화되어 있는 경우 비활성화합니다.
단계 2	SAML Single Sign-On 비활성화, 5 페이지	SAML Single Sign-on이 이미 활성화 되어 있는 경우 비활성화합니다.
단계 3	Cisco WebDialer 서비스 활성화, 6 페이지	
단계 4	SAML Single Sign-On 활성화, 3 페이지	

Cisco WebDialer 서비스 비활성화

Cisco WebDialer 웹 서비스가 이미 활성화되어 있는 경우 비활성화합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.
단계 2 서버 드롭다운 목록에서 나열된 Cisco Unified Communications Manager 서버를 선택합니다.
단계 3 **CTI** 서비스에서 **Cisco WebDialer** 웹 서비스 확인란을 선택 취소합니다.
단계 4 저장을 클릭합니다.

다음에 수행할 작업

SAML Single Sign-On 비활성화, 5 페이지

SAML Single Sign-On 비활성화

SAML Single Sign-on이 이미 활성화 되어 있는 경우 비활성화합니다.

시작하기 전에

Cisco WebDialer 서비스 비활성화, 5 페이지

프로시저

CLI에서 명령 **utils sso disable**을 실행합니다.

다음에 수행할 작업

Cisco WebDialer 서비스 활성화, 6 페이지

Cisco WebDialer 서비스 활성화

시작하기 전에

SAML Single Sign-On 비활성화, 5 페이지

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 다음을 선택합니다 도구 > 서비스 활성화.

단계 **2** 서버 드롭다운 목록에서 나열된 Unified Communications Manager 서버를 선택합니다.

단계 **3** **CTI** 서비스에서 **Cisco WebDialer** 웹 서비스 확인란을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** Cisco 통합 서비스 가용성에서 다음을 선택합니다 도구 > 제어 센터 - 기능 서비스를 선택하여 CTI 관리자 서비스가 활성 상태이며 시작 모드인지 확인합니다.

Webdialer가 제대로 작동하려면 CTI 관리자 서비스를 활성화하고 시작 모드에 있어야합니다.

다음에 수행할 작업

SAML Single Sign-On 활성화, 3 페이지

복구 URL에 액세스

복구 URL을 사용하면 문제 해결을 위해 SAML Single Sign-On을 우회하여 Cisco Unified Communications Manager 관리 및 Cisco Unified CM IM and Presence Service 인터페이스에 로그인할 수 있습니다. 예를 들어, 서버의 도메인 또는 호스트 이름을 변경하기 전에 복구 URL을 활성화합니다. 복구 URL에 로그인하여 서버 메타데이터를 손쉽게 업데이트할 수 있습니다.

시작하기 전에

- 관리 권한이 있는 애플리케이션 사용자만 복구 URL에 액세스할 수 있습니다.
- SAML SSO가 활성화된 경우, 복구 URL은 기본적으로 활성화됩니다. CLI에서 복구 URL을 활성화하거나 비활성화할 수 있습니다. 복구 URL을 활성화 및 비활성화하기 위한 CLI 명령에 대한 자세한 내용은 *Command Line Interface Guide for Cisco Unified Communications Solutions*를 참조하십시오.

프로시저

브라우저에 `https://hostname:8443/ssosp/local/login`을 입력합니다.

도메인 또는 호스트 이름 변경 후 서버 메타데이터 업데이트

도메인 또는 호스트 이름을 변경한 후 이 절차를 수행할 때까지 SAML Single Sign-On이 작동하지 않습니다.

참고 이 절차를 수행한 후에도 **SAML Single Sign-On** 창에 액세스할 수 없는 경우에는 브라우저 캐시를 지우고 다시 로그인해 보십시오.

시작하기 전에

복구 URL이 비활성화된 경우 Single Sign-On 링크를 우회할 URL이 나타나지 않습니다. 복구 URL을 활성화하려면 CLI에 로그인하고 **utils sso recovery-url enable**명령을 실행합니다.

프로시저

단계 **1** 웹 브라우저의 주소 표시줄에 다음 URL을 입력합니다.

`https://<Unified CM-server-name>`

여기서 `<Unified CM-server-name>`은 서버의 IP 주소 또는 호스트 이름입니다.

단계 **2** **Single Sign On(SSO)**를 우회할 복구 **URL**을 클릭합니다.

단계 **3** 관리자 역할을 가진 애플리케이션 사용자의 자격 증명을 입력하고 로그인을 클릭합니다.

단계 **4** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.

단계 **5** 메타데이터 내보내기를 클릭하여 서버 메타데이터를 다운로드합니다.

단계 **6** 서버 메타데이터 파일을 IdP에 업로드합니다.

단계 **7** 테스트 실행을 클릭합니다.

단계 **8** 올바른 사용자 ID 및 암호를 입력합니다.

단계 **9** 성공 메시지가 표시되면 브라우저 창을 닫습니다.

서버를 삭제한 후 서버 메타데이터 업데이트

클러스터에서 서버를 삭제한 후 Unified CM 메타데이터를 내보내는 경우 IdP에서 이 파일을 가져와서 인덱스 값이 서로 일치하는지 확인하는 것이 좋습니다.

시작하기 전에

참고 복구 URL이 비활성화된 경우 Single Sign-On 링크를 우회할 URL이 나타나지 않습니다. 복구 URL을 활성화하려면 CLI에 로그인하고 **utils sso recovery-url enable**명령을 실행합니다.

프로시저

단계 **1** 웹 브라우저의 주소 표시줄에 다음 URL을 입력합니다.

`https://<Unified CM-server-name>`

여기서 `<Unified CM-server-name>`은 서버의 IP 주소 또는 호스트 이름입니다.

단계 **2** **Single Sign On(SSO)**를 우회할 복구 **URL**을 클릭합니다.

단계 **3** 관리자 역할을 가진 애플리케이션 사용자의 자격 증명을 입력하고 로그인을 클릭합니다.

단계 **4** Cisco Unified CM 관리에서 시스템 > **SAML** 싱글 사인-온을 선택합니다.

단계 **5** 메타데이터 내보내기를 클릭하여 서버 메타데이터를 다운로드합니다.

단계 **6** 서버 메타데이터 파일을 IdP에 업로드합니다.

단계 **7** 테스트 실행을 클릭합니다.

단계 **8** 올바른 사용자 ID 및 암호를 입력합니다.

단계 **9** 성공 메시지가 표시되면 브라우저 창을 닫습니다.

서버 메타데이터 수동 프로비저닝

여러 개의 UC 애플리케이션에 대한 ID 공급자에서 단일 연결을 설정하려면 ID 공급자 및 서비스 공급업체 사이에 신뢰할 수 있는 범위를 구성하는 한편, 서버 메타데이터를 수동으로 설정해야 합니다. 신뢰할 수 있는 범위를 구성하는 방법에 대한 자세한 내용은 IdP 제품 설명서를 참조하십시오.

일반적인 URL 구문은 다음과 같습니다.

`https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>`

프로시저

서버 메타데이터를 수동으로 설정하려면 ACS(Assertion Customer Service) URL을 사용합니다.

예제:

샘플 ACS URL: `<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com" index="0"/>`