Unity Connection 버전 10.5 SAML SSO 컨피그레이션 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[NTP(Network Time Protocol) 설정](#)
[DNS(Domain Name Server) 설정](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[네트워크 다이어그램](#)
[디렉터리 설정](#)
[SAML SSO 활성화](#)
[다음을 확인합니다.](#)
[문제 해결](#)

소개

이 문서에서는 UCXN(Cisco Unity Connection)용 SAML(Security Assertion Markup Language) SSO(Single Sign-on)를 구성하고 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

NTP(Network Time Protocol) 설정

SAML SSO가 작동하려면 올바른 NTP 설정을 설치하고 IdP(Identity Provider)와 Unified Communications 애플리케이션 간의 시간 차이가 3초를 초과하지 않는지 확인해야 합니다.클럭 동기화에 대한 자세한 내용은 Cisco Unified Communications Operating System Administration Guide의 NTP Settings 섹션을 참조하십시오.

DNS(Domain Name Server) 설정

Unified Communications 애플리케이션은 DNS를 사용하여 FQDN(정규화된 도메인 이름)을 IP 주소로 확인할 수 있습니다.서비스 공급자 및 IdP는 브라우저에서 확인할 수 있어야 합니다.

SAML 요청을 처리하려면 AD FS(Active Directory Federation Service) 버전 2.0을 설치하고 구성해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AD FS 버전 2.0을 IdP로 사용
- UCXN을 서비스 공급자로 사용
- Microsoft Internet Explorer 버전 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SAML은 데이터 교환을 위한 XML 기반의 개방형 표준 데이터 형식입니다.서비스 공급자가 사용자를 인증하기 위해 사용하는 인증 프로토콜입니다.보안 인증 정보는 IdP와 서비스 공급자 간에 전달됩니다.

SAML은 클라이언트가 클라이언트 플랫폼에 관계없이 SAML 지원 협업(또는 Unified Communication) 서비스에 대해 인증할 수 있도록 하는 개방형 표준입니다.

Cisco CUCM(Unified Communications Manager) 또는 UCXN과 같은 모든 Cisco Unified Communication 웹 인터페이스는 SAML SSO 기능에서 SAML Version 2.0 프로토콜을 사용합니다.LDAP(Lightweight Directory Access Protocol) 사용자를 인증하기 위해 UCXN은 IdP에 인증 요청을 위임합니다.UCXN에서 생성한 이 인증 요청은 SAML 요청입니다.IdP는 SAML Assertion을 인증하고 반환합니다.SAML Assertion에 Yes(authenticated) 또는 No(authentication failed)가 표시됩니다.

SAML SSO를 사용하면 LDAP 사용자가 IdP에서 인증하는 사용자 이름과 비밀번호를 사용하여 클라이언트 애플리케이션에 로그인할 수 있습니다.SAML SSO 기능을 활성화한 후 사용자가 Unified Communication 제품에서 지원되는 웹 애플리케이션에 로그인하면 CUCM 및 CUCM IM and Presence 외에도 UCXN에서 이러한 웹 애플리케이션에 액세스할 수 있습니다.

Unity Connection 사용자	웹 애플리케이션
관리자 권한이 있는 LDAP 사용자	• UCXN 관리 • Cisco UCXN 서비스 가용성 • Cisco Unified 서비스 가용성 • Cisco Personal Communications Assistant • 웹 받은 편지함 • 미니 웹 받은 편지함(데스크톱 버전)
관리자 권한이 없는 LDAP 사용자	• Cisco Personal Communications Assistant • 웹 받은 편지함 • 미니 웹 받은 편지함(데스크톱 버전) • Cisco Jabber 클라이언트

구성

네트워크 다이어그램

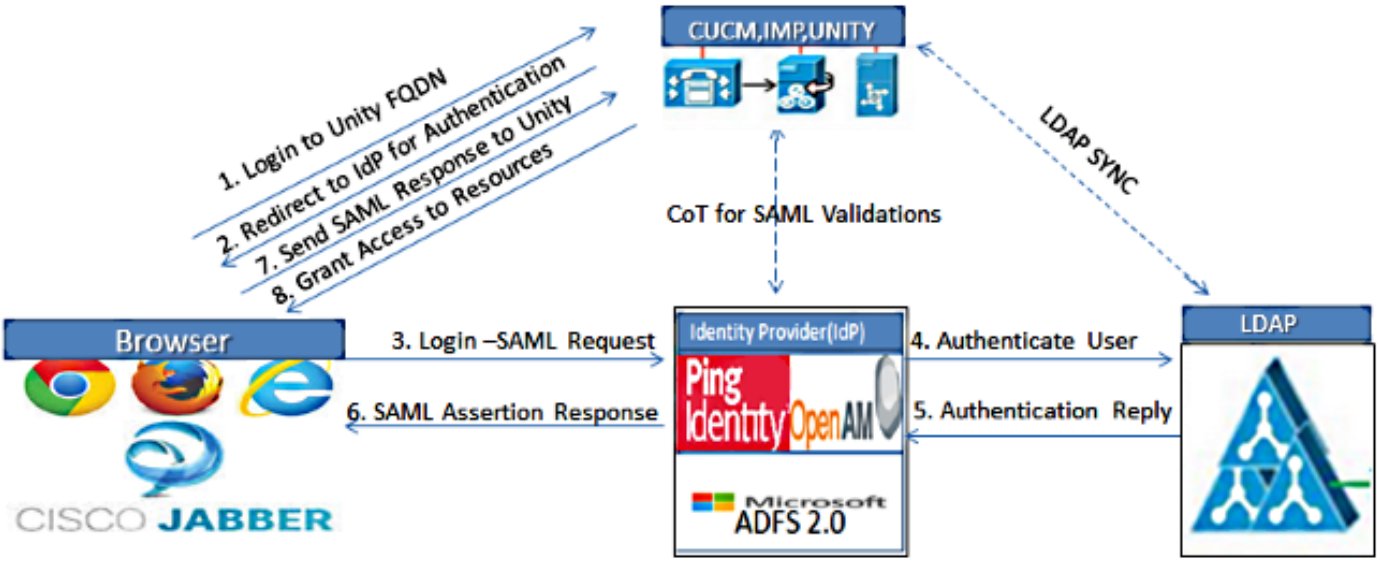
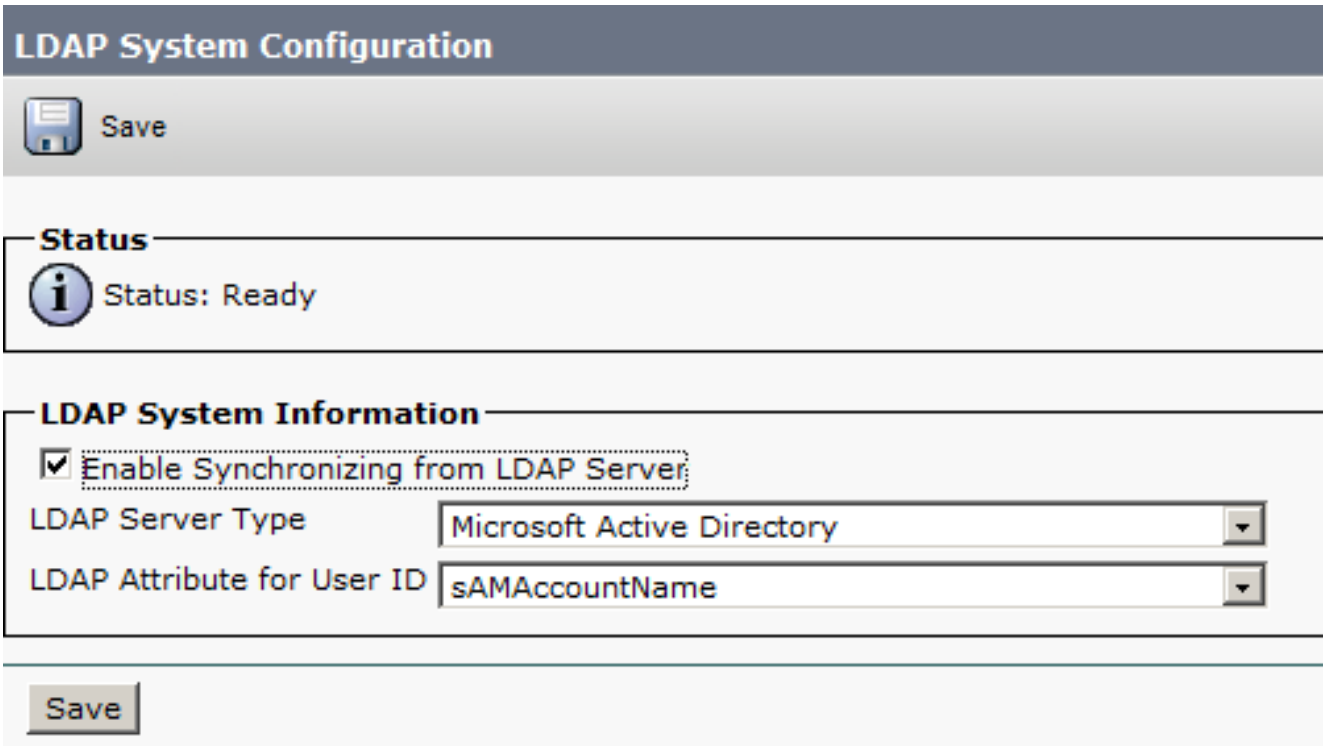


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

디렉터리 설정

1. UCXN Administration(UCXN 관리) 페이지에 로그인하여 **LDAP**를 선택하고 LDAP Setup(**LDAP 설정)**을 클릭합니다.

2. Enable **Synchronizing from LDAP Server(LDAP 서버에서 동기화 활성화**)를 선택하고 Save(저장)를 **클릭합니다**.



3. LDAP를 **클릭합니다**.

4. LDAP **Directory Configuration을 클릭합니다**.

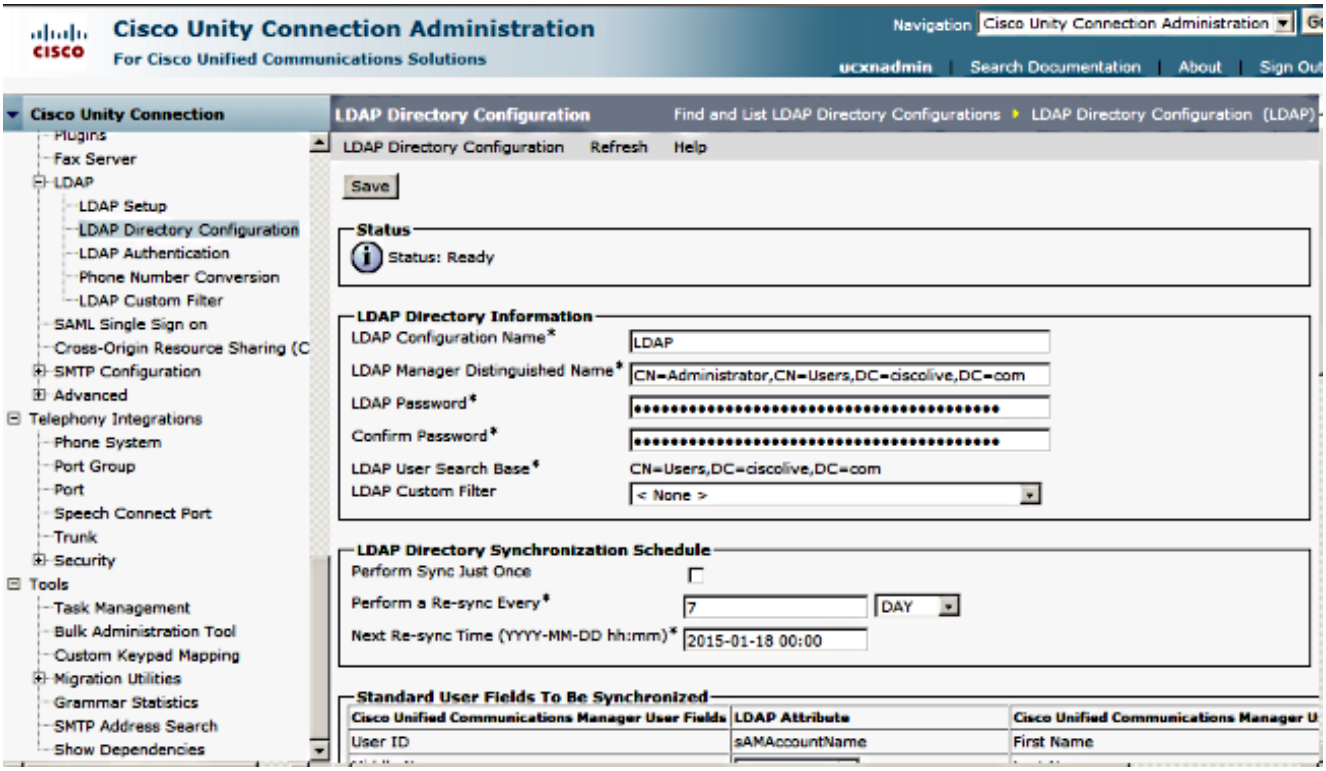
5. Add **New를 클릭합니다**.

6. 다음 항목을 구성합니다.

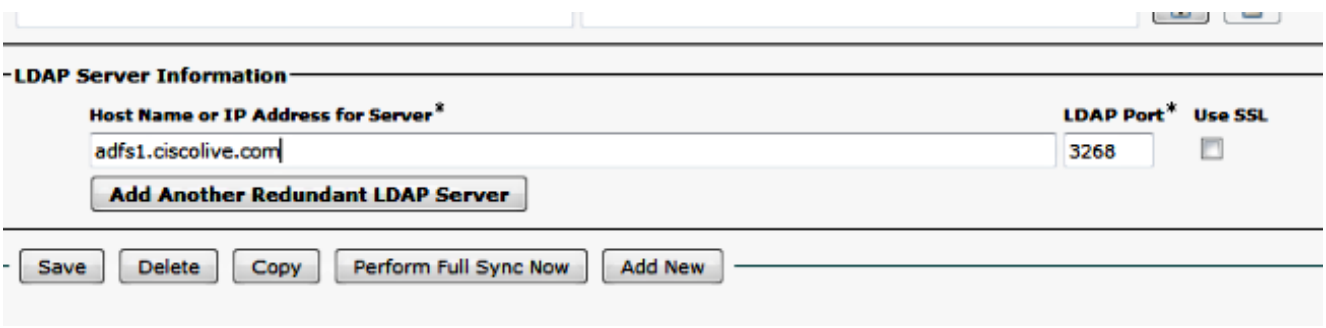
   LDAP 디렉터리 계정 설정동기화할 사용자 특성동기화 일정LDAP 서버 호스트 이름 또는 IP 주소 및 포트 번호

7. LDAP 디렉토리와 통신하기 위해 SSL(Secure Socket Layer)을 사용하려면 Use SSL(SSL 사용)을 선택합니다.

   팁:SSL을 통해 LDAP를 구성하는 경우 LDAP 디렉토리 인증서를 CUCM에 업로드합니다.특정 LDAP 제품의 계정 동기화 메커니즘 및 LDAP 동기화에 대한 일반 모범 사례에 대한 자세한 내용은 Cisco Unified Communications Manager SRND의 LDAP 디렉토리 콘텐츠를 참조하십시오.



8. Perform **Full Sync Now(지금 전체 동기화 수행)를 클릭합니다**.



참고:Save(저장)**를 클릭하기** 전에 서비스 가용성 웹 페이지에서 Cisco DirSync 서비스가 활성화되어 있는지 확인합니다.

9. Users(**사용자**)를 확장하고 **Import Users(사용자 가져오기)를 선택합니다**.

10. Find **Unified Communications Manager End Users(Unified Communications Manager 최종 사용자 찾기)** 목록에서 LDAP **Directory(LDAP 디렉토리)를** 선택합니다.

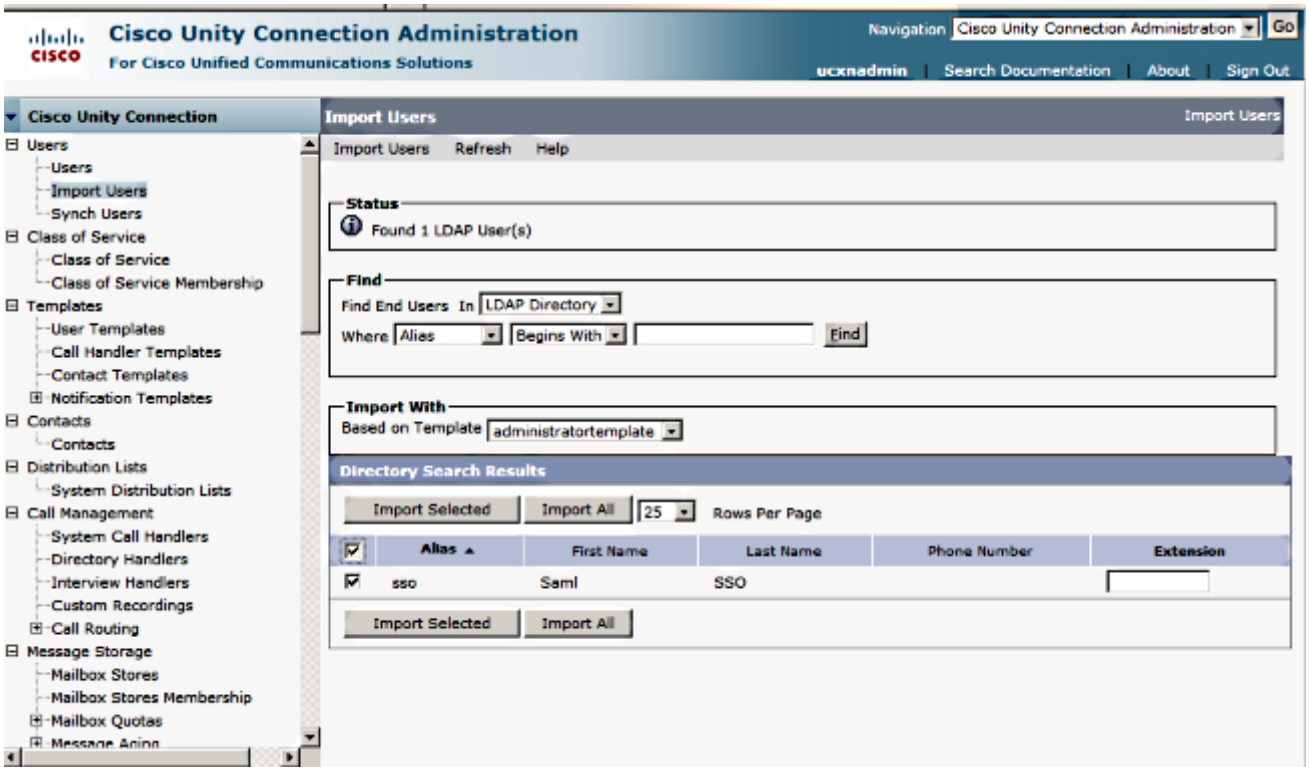
11. UCXN을 통합한 LDAP 디렉토리의 사용자 하위 집합만 가져오려면 검색 필드에 해당 사양을 입력합니다.

12. 찾기를 **선택합니다**.

13. Based on Template(템플릿 기반) 목록에서 선택한 사용자를 생성할 때 UCXN에서 사용할 **Administrator 템플릿**을 선택합니다.

    주의:관리자 템플릿을 지정하면 사용자에게 사서함이 없습니다.

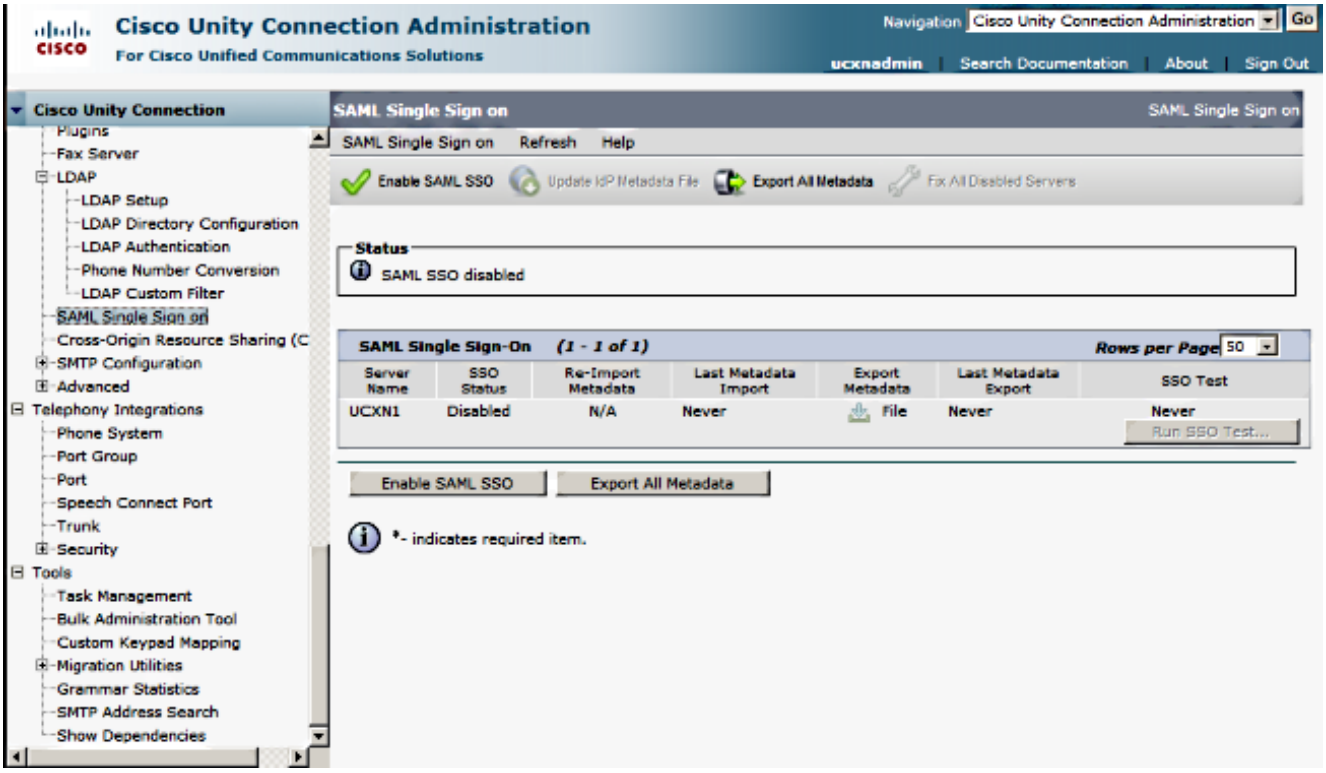
14. UCXN 사용자를 생성하려는 LDAP 사용자의 확인란을 선택하고 Import Selected를 **클릭합니다**.



SAML SSO 활성화

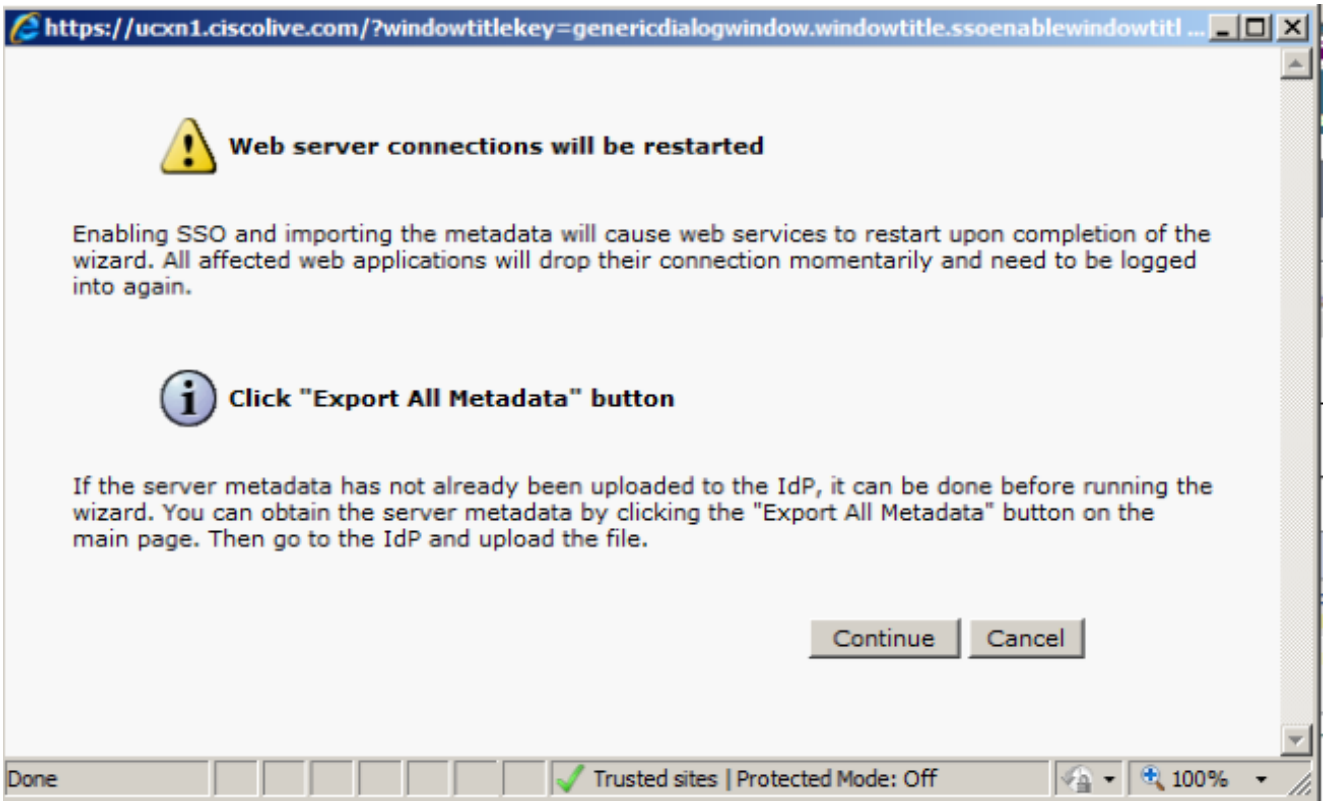
1. UCXN 관리 사용자 인터페이스에 로그인합니다.

2. System(**시스템**) > **SAML Single Sign-on**을 선택하면 SAML SSO Configuration(SAML SSO 컨피그레이션) 창이 열립니다.

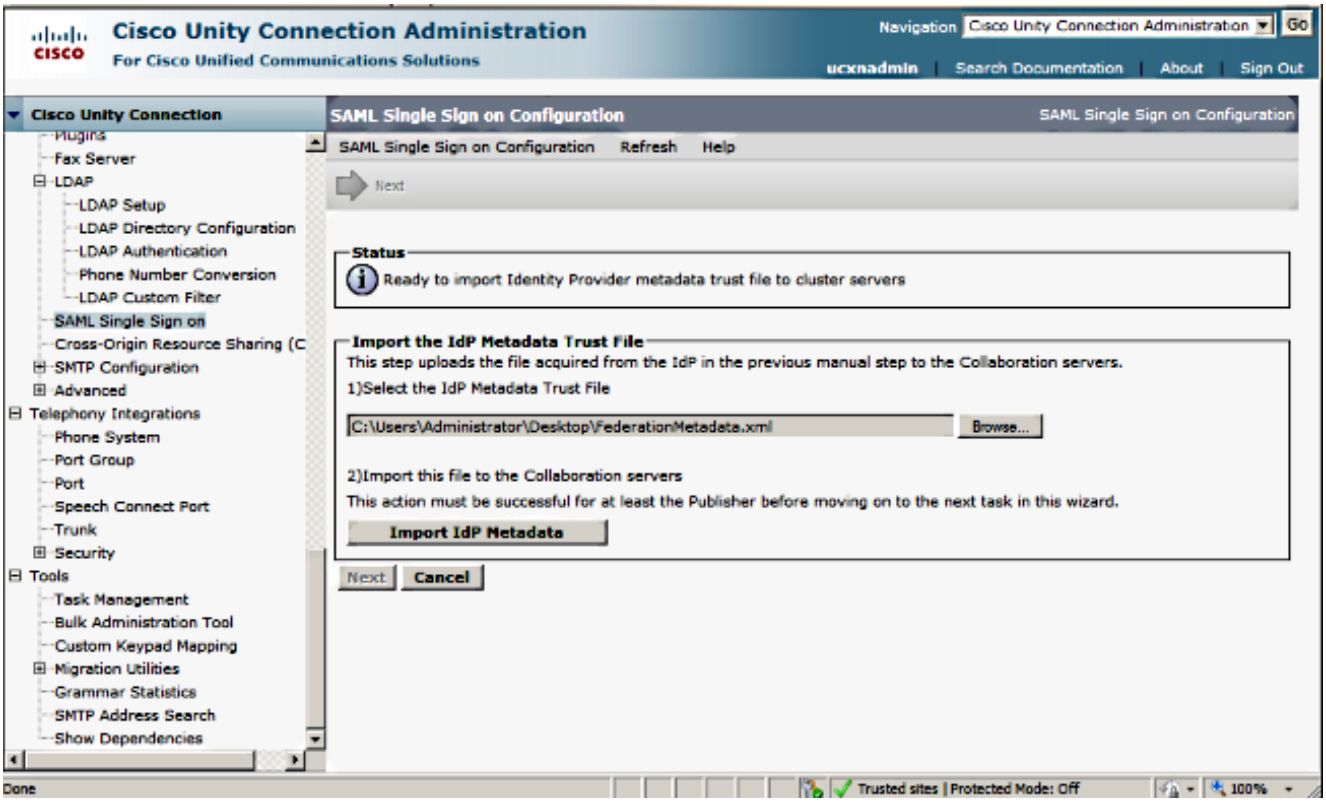


3. 클러스터에서 SAML SSO를 활성화하려면 Enable SAML **SSO**를 클릭합니다.

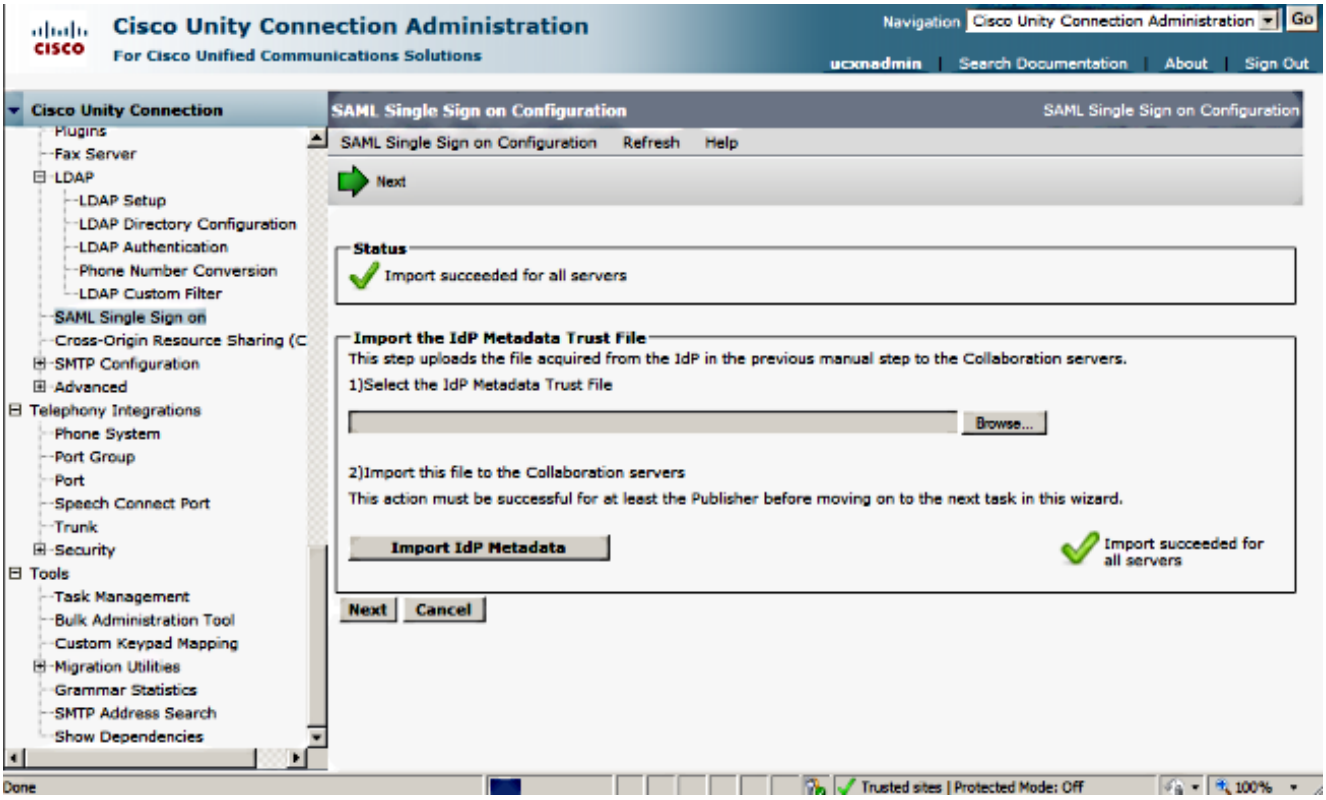
4. Reset Warning(경고 재설정) 창에서 Continue(**계속**)를 클릭합니다.



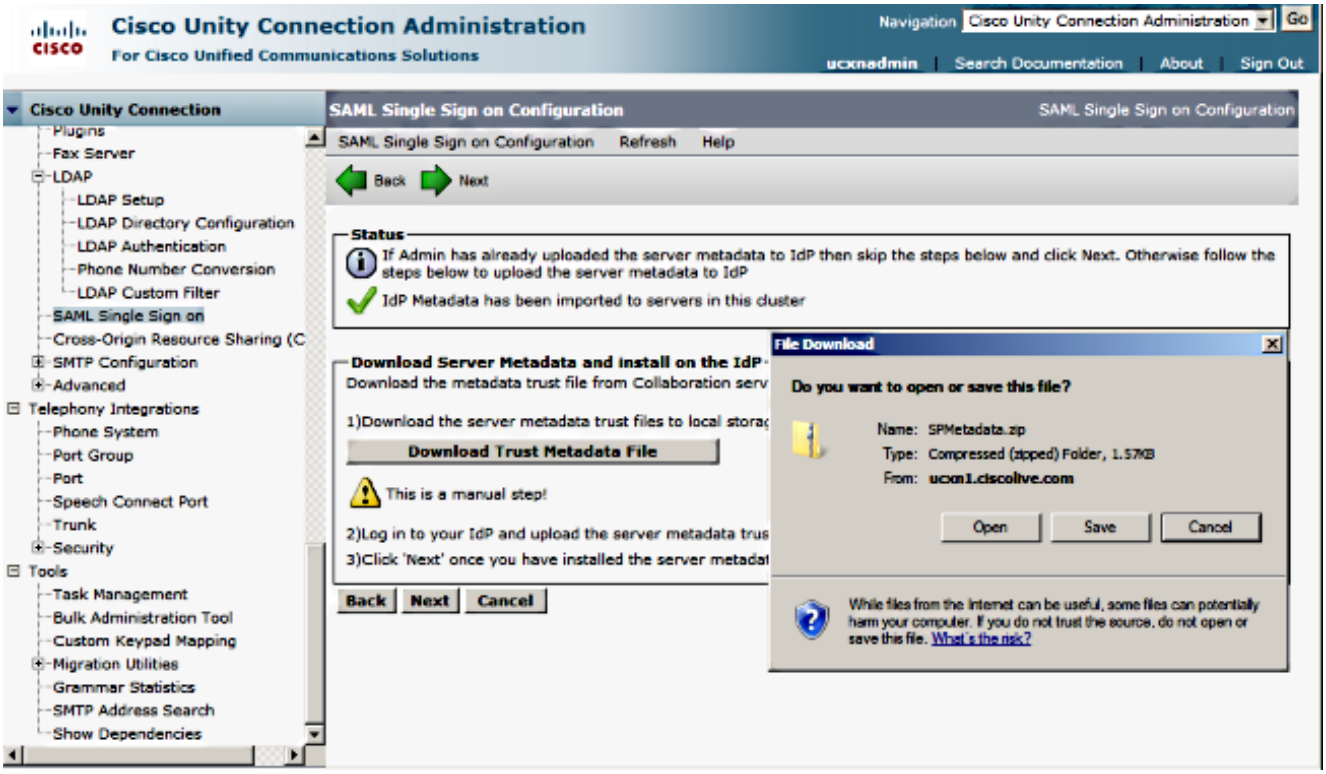
5. SSO 화면에서 **찾아보기**를 클릭하여 **FederationMetadata.xml** 메타데이터 XML 파일을 Download Idp Metadata 단계로 **가져옵니다**.



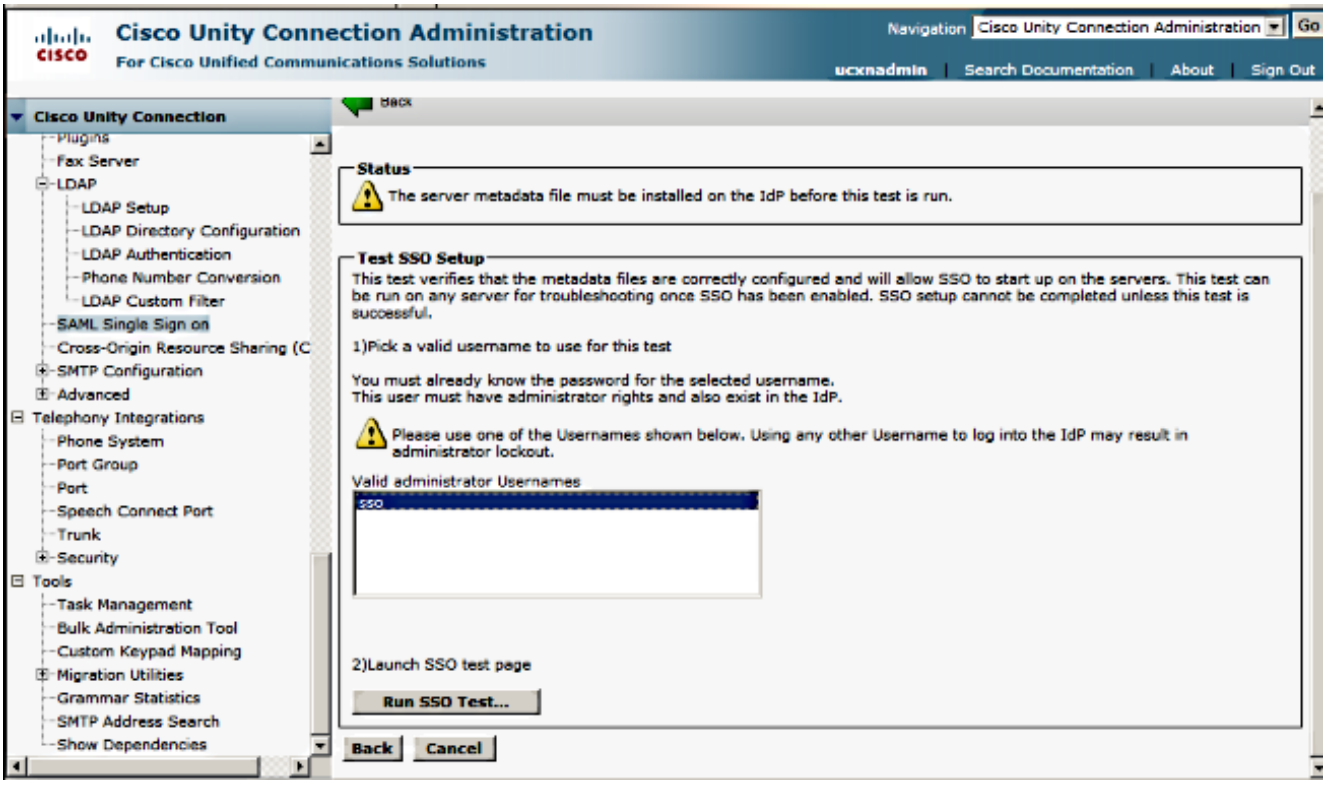
6. 메타데이터 파일이 업로드되면 **Import IdP Metadata(IdP 메타데이터 가져오기)**를 클릭하여 IdP 정보를 UCXN으로 가져옵니다.가져오기에 성공했는지 확인하고 **Next(다음)**를 클릭하여 계속합니다.



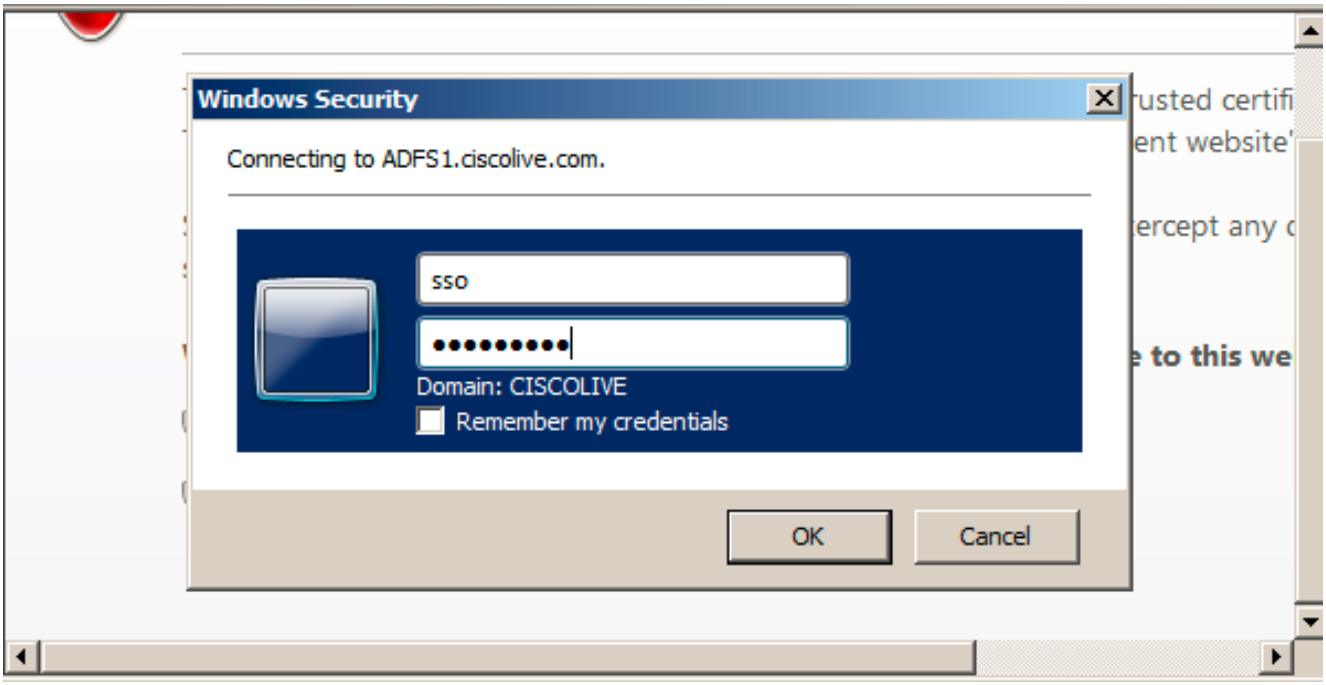
7. UCXN 메타데이터를 로컬 폴더에 저장하고 Add UCXN as Relaing Party Trust로 이동하려면 **Download Trust Metadata Fileset**(UCXN 메타데이터로 이미 ADFS를 구성하지 않은 경우에만 해당)을 클릭합니다.AD FS 컨피그레이션이 완료되면 8단계로 진행합니다.



8. 관리 사용자로 SSO를 선택하고 Run **SSO Test(SSO 테스트 실행)를 클릭합니다**.

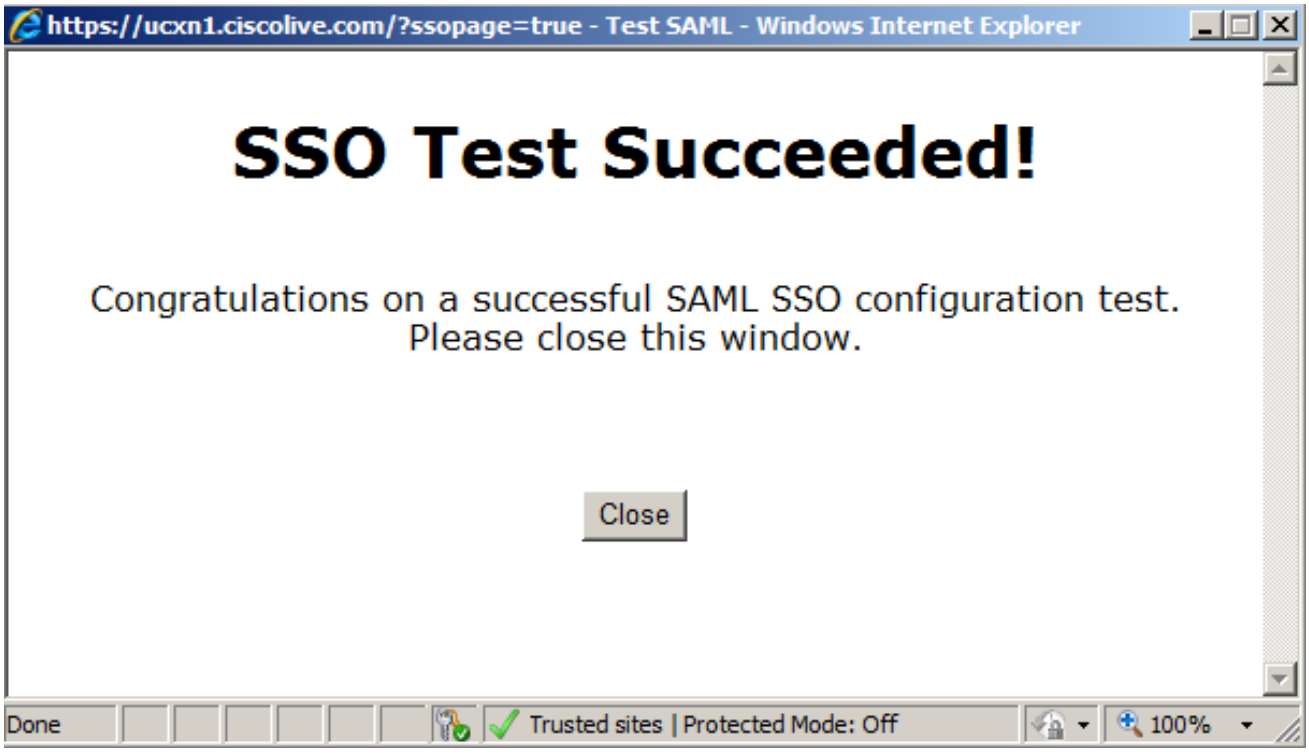


9. 인증서 경고를 무시하고 계속 진행합니다.자격 증명을 입력하라는 메시지가 표시되면 사용자 SSO의 사용자 이름과 비밀번호를 입력하고 **OK**를 클릭합니다.



참고:이 컨피그레이션 예는 UCXN 및 AD FS 자체 서명 인증서를 기반으로 합니다 .CA(Certificate Authority) 인증서를 사용하는 경우 AD FS와 UCXN에 모두 적절한 인증서를 설치해야 합니다.자세한 내용은 인증서 관리 및 검증을 참조하십시오.

10. 모든 단계가 완료되면 "SSO 테스트 성공!"이 표시됩니다. 메시지.계속하려면 **닫기** 및 **마침**을 클릭합니다.



이제 AD FS를 사용하여 UCXN에서 SSO를 활성화하는 구성 작업을 완료했습니다.

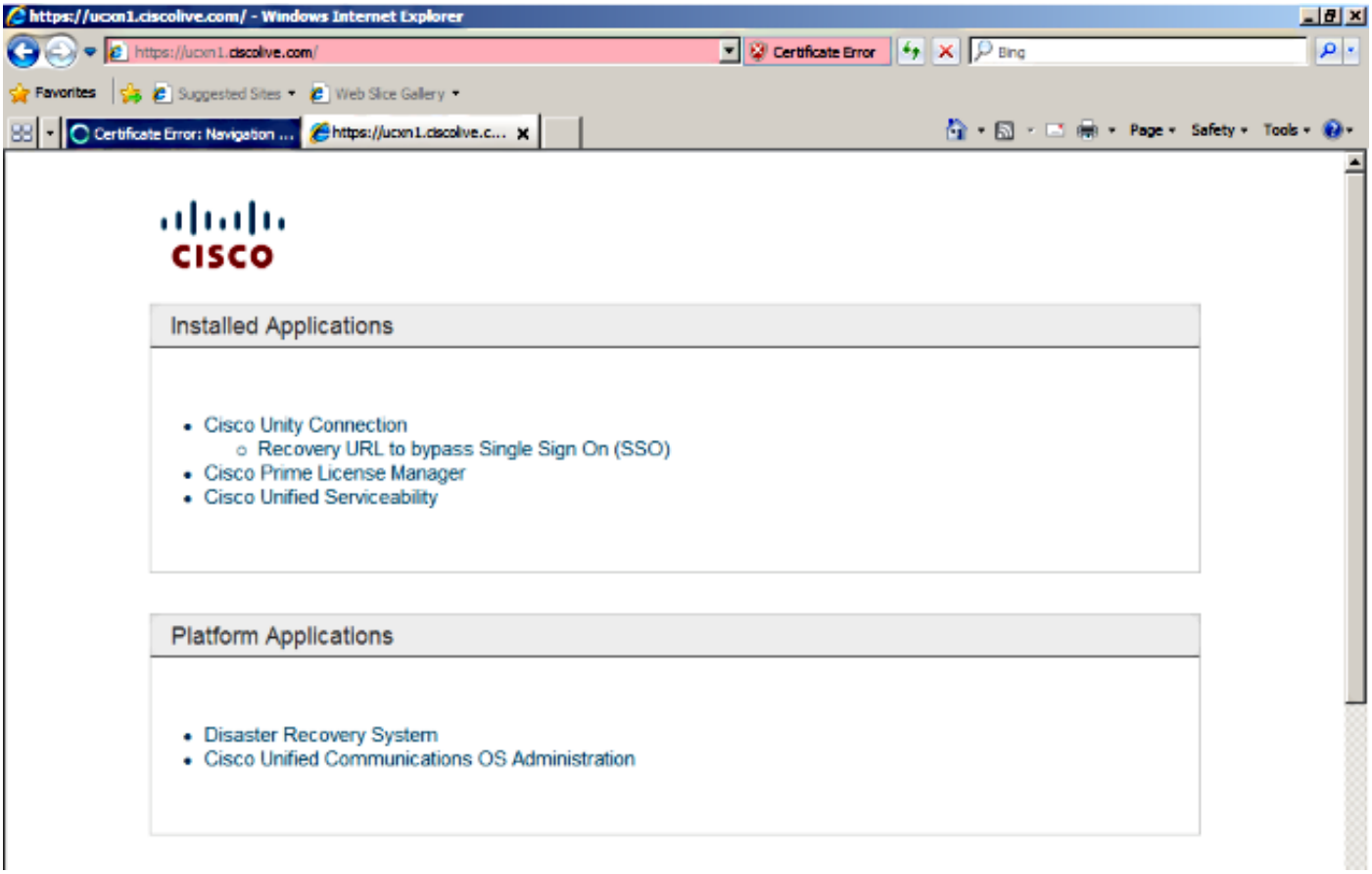
필수 참고:SAML SSO를 활성화하려면 UCXN 가입자에 대한 SSO 테스트를 클러스터인 경우 실행합니다.클러스터에 있는 UCXN의 모든 노드에 대해 AD FS를 구성해야 합니다.

팁:IdP에서 모든 노드의 메타데이터 XML 파일을 구성하고 한 노드에서 SSO 작업을 활성화하기 시작하면 클러스터의 모든 노드에서 SAML SSO가 자동으로 활성화됩니다.

Cisco Jabber 클라이언트에 SAML SSO를 사용하고 최종 사용자에게 진정한 SSO 환경을 제공하려는 경우 SAML SSO에 대해 CUCM 및 CUCM IM and Presence를 구성할 수도 있습니다.

다음을 확인합니다.

웹 브라우저를 열고 UCXN의 FQDN을 입력하면 Installed Applications(**SSO(Single Sign-on)를 우회하기 위해 Recovery URL(복구 URL)**이라는 새 옵션이 표시됩니다. **Cisco Unity Connection** 링크를 클릭하면 AD FS에서 자격 증명을 입력하라는 프롬프트가 표시됩니다.사용자 SSO의 자격 증명을 입력하면 Unity Administration(Unity 관리) 페이지의 Unified Serviceability(Unified 서비스 가용성) 페이지에 성공적으로 로그인됩니다.



참고:SAML SSO는 다음 페이지에 대한 액세스를 활성화하지 않습니다.
- Prime Licensing Manager
- OS 관리
- 재해 복구 시스템

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

자세한 내용은 Collaboration 제품 10.x용 SAML SSO 문제 해결을 참조하십시오.