Unity Connection版本10.5 SAML SSO配置示例

目录

简介

本文档介绍如何为Cisco Unity Connection(UCXN)配置和验证安全断言标记语言(SAML)单点登录(SSO)。

先决条件

要求

网络时间协议(NTP)设置

要使SAML SSO正常工作，必须安装正确的NTP设置，并确保身份提供程序(IdP)和统一通信应用之间的时间差不超过三秒。有关同步时钟的信息，请参阅《思科统一通信操作系统管理指南》中的“NTP设置”部分。

域名服务器(DNS)设置

统一通信应用可以使用DNS将完全限定域名(FQDN)解析为IP地址。服务提供商和IdP必须由浏览器解析。

必须安装并配置Active Directory联合身份验证服务(AD FS)版本2.0，才能处理SAML请求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- AD FS版本2.0作为IdP

- UCXN作为服务提供商
- Microsoft Internet Explorer版本10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

SAML是基于XML的开放标准数据格式，用于数据交换。它是服务提供商用于对用户进行身份验证的身份验证协议。安全身份验证信息在IdP和服务提供商之间传递。

SAML是一种开放标准，允许客户端根据任何支持SAML的协作（或统一通信）服务进行身份验证，而不管客户端平台如何。

所有思科统一通信Web接口(如思科统一通信管理器(CUCM)或UCXN)在SAML SSO功能中使用SAML 2.0版协议。为了对轻量级目录访问协议(LDAP)用户进行身份验证，UCXN将身份验证请求委托给IdP。UCXN生成的此身份验证请求是SAML请求。IdP验证并返回SAML断言。SAML断言显示是（已验证）或否（身份验证失败）。

SAML SSO允许LDAP用户使用在IdP上进行身份验证的用户名和密码登录客户端应用。在启用SAML SSO功能后，用户登录统一通信产品上支持的任何Web应用，也可以访问UCXN上的这些Web应用（除CUCM和CUCM IM and Presence外）：

Unity Connection用户	Web应用
具有管理员权限的LDAP用户	• UCXN管理 • Cisco UCXN适用性 • Cisco Unified 可维护性 • Cisco Personal Communications Assistant • Web收件箱 • 迷你Web收件箱（桌面版） • Cisco Personal Communications Assistant
无管理员权限的LDAP用户	• Web收件箱 • 迷你Web收件箱（桌面版） • Cisco Jabber客户端

配置

网络图

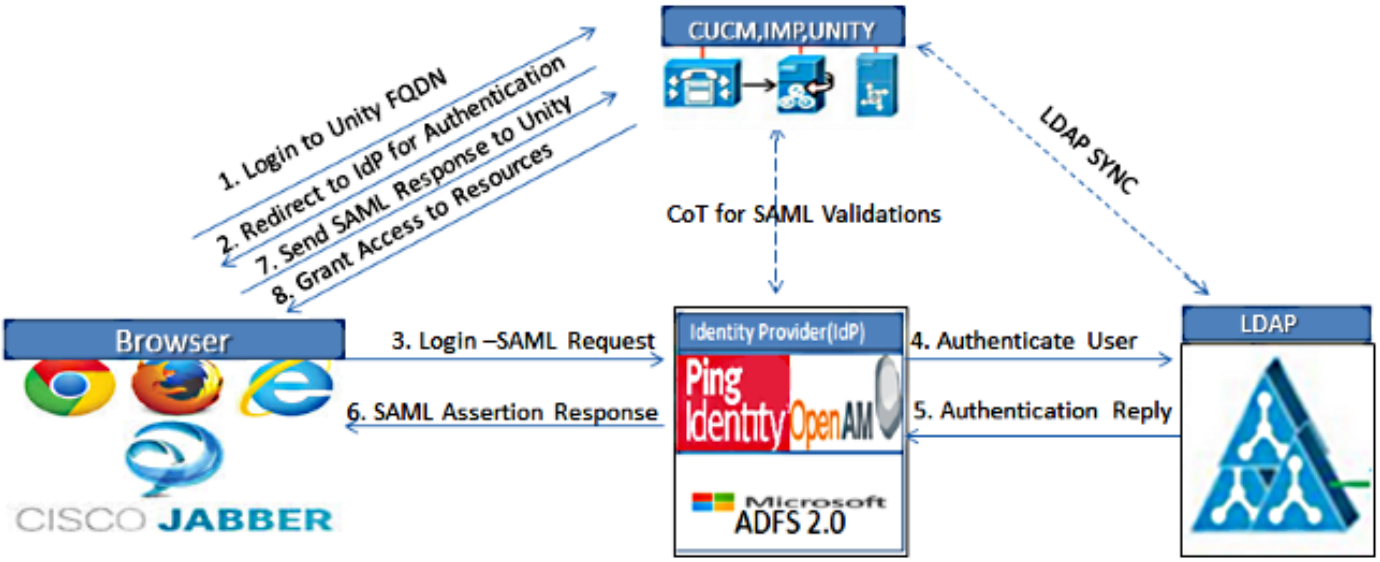
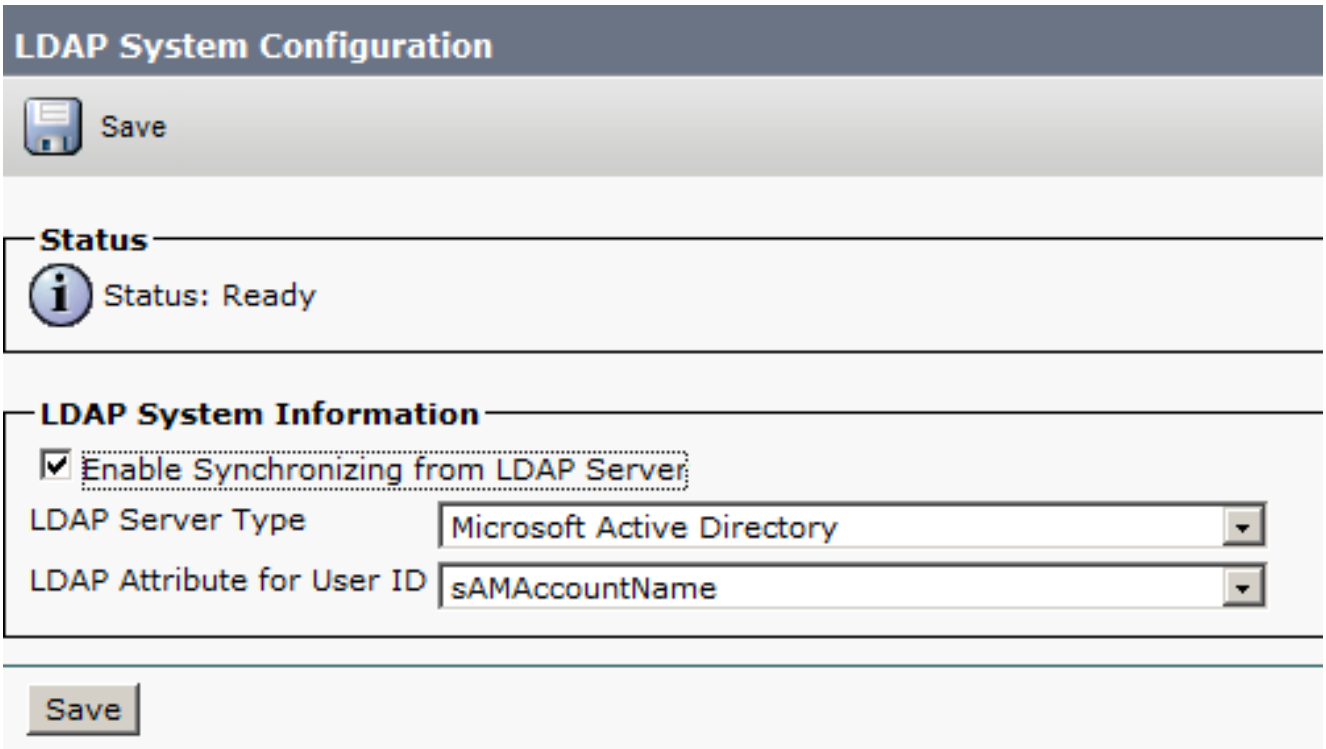


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

目录设置

1. 登录UCXN Administration页面，选择LDAP，然后单击**LDAP Setup**。

2. 选中**启用从LDAP服务器同步**并单击**保存**。



3. 单击**LDAP**。

4. 单击“**LDAP Directory Configuration**”。

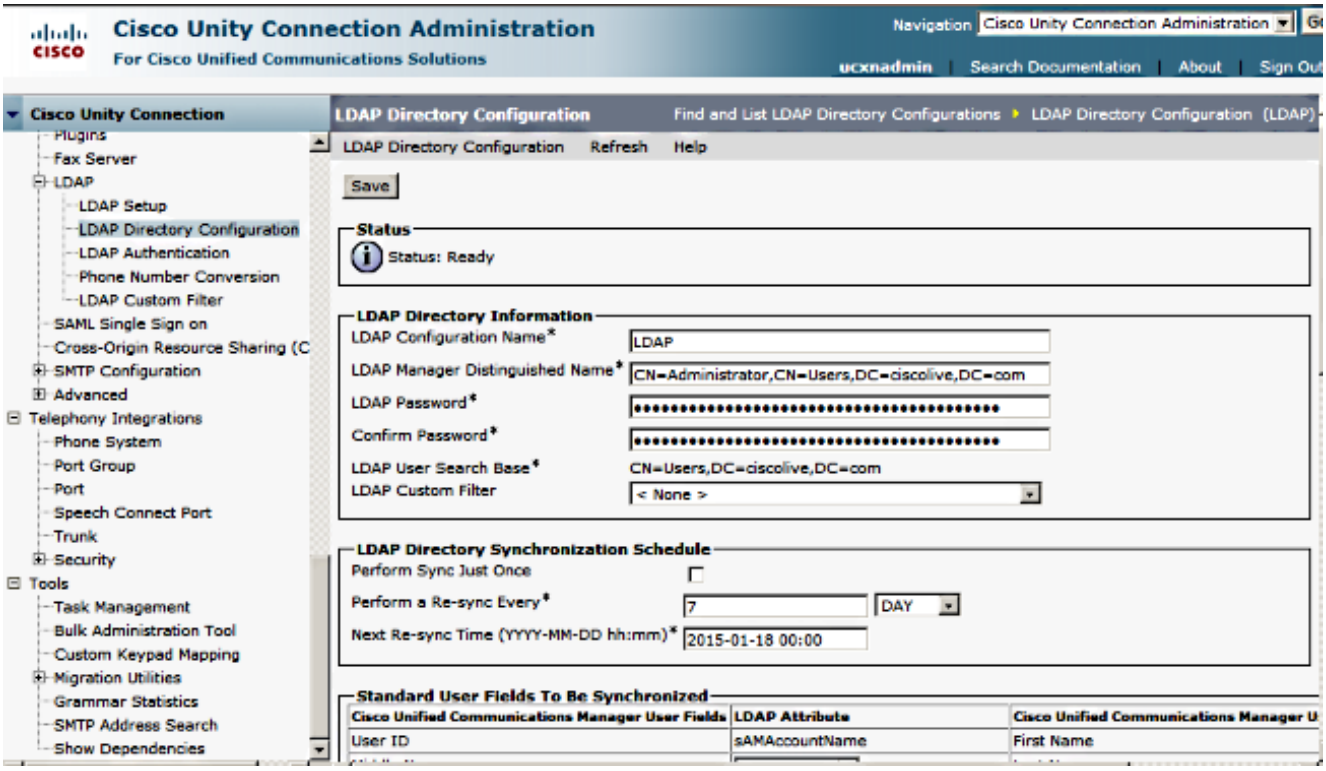
5. 单击新增。

6. 配置以下项目：

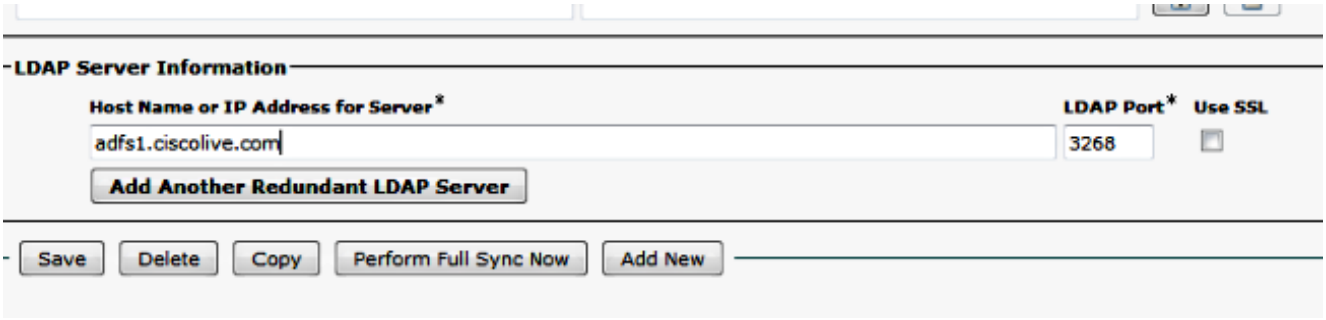
   LDAP目录帐户设置要同步的用户属性同步计划LDAP服务器主机名或IP地址和端口号

7. 如果要使用安全套接字层(SSL)以与LDAP目录通信，请选中**使用SSL**。

   提示：如果配置LDAP over SSL，请将LDAP目录证书上传到CUCM。有关特定LDAP产品的帐户同步机制和LDAP同步的一般最佳实践的信息，请参阅Cisco Unified Communications Manager SRND中的LDAP目录内容。



8. 单击“**立即执行完全同步**”。



   注意：在单击“**保存**”之前，请确保在“可维护性”网页中启用了Cisco DirSync服务。

9. 展开**用户**并选择**导入用户**。

10. 在“查找**Unified Communications Manager最终用户**”列表中，选择**LDAP目录**。

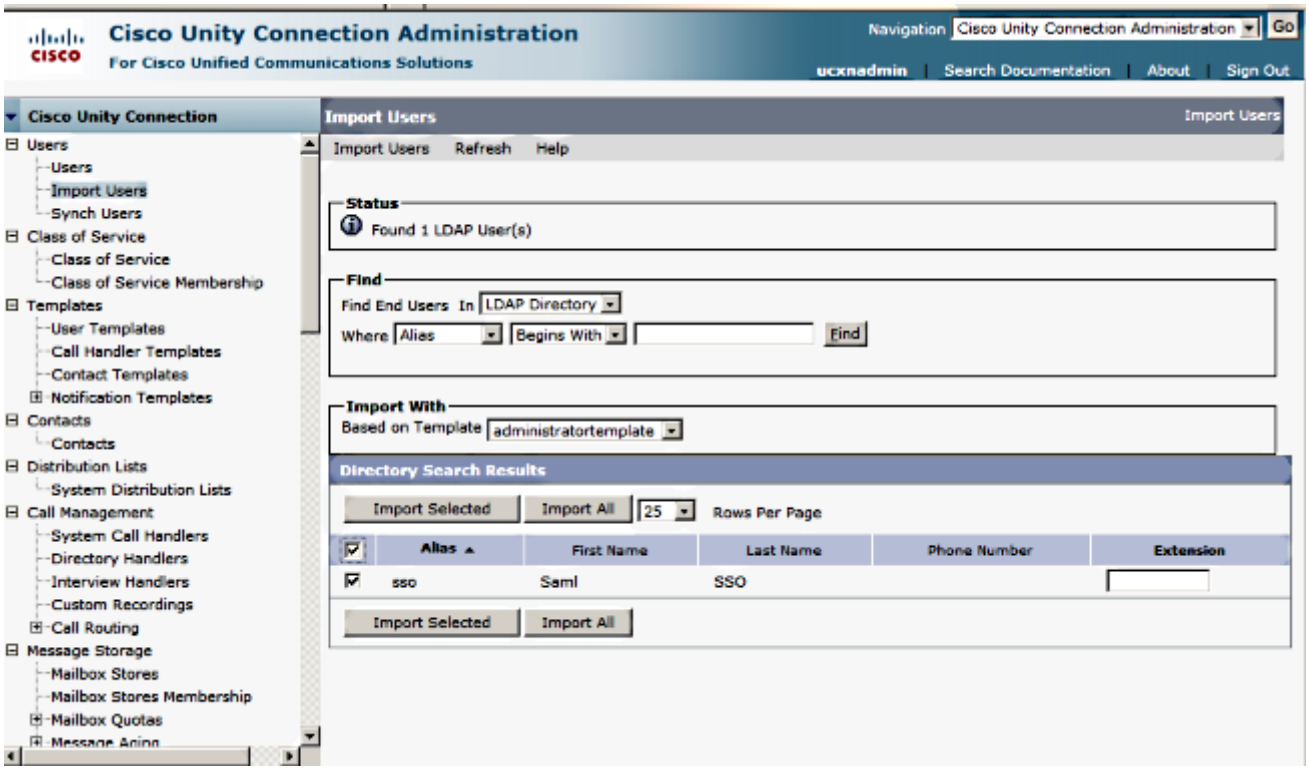
11. 如果只想在集成了UCXN的LDAP目录中导入用户的子集，请在搜索字段中输入适用的规范。

12. 选择“**查找**”。

13. 在“基于模板”(Based on Template)列表中，选**择希望**UCXN在创建选定用户时使用的管理员模板。

    警告：如果指定管理员模板，用户将没有邮箱。

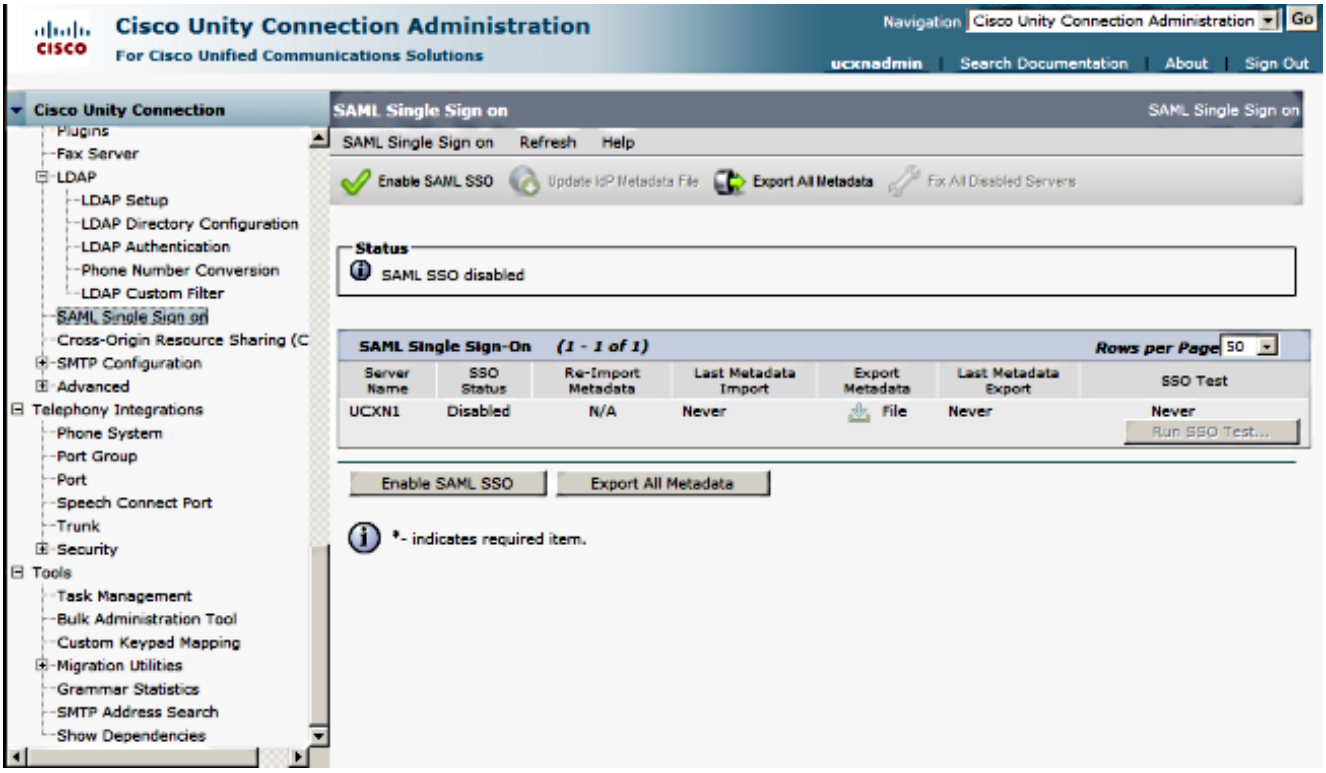
14. 选中要为其创建UCXN用户的LDAP用户的复选框，然后点击导**入选定**。



启用SAML SSO

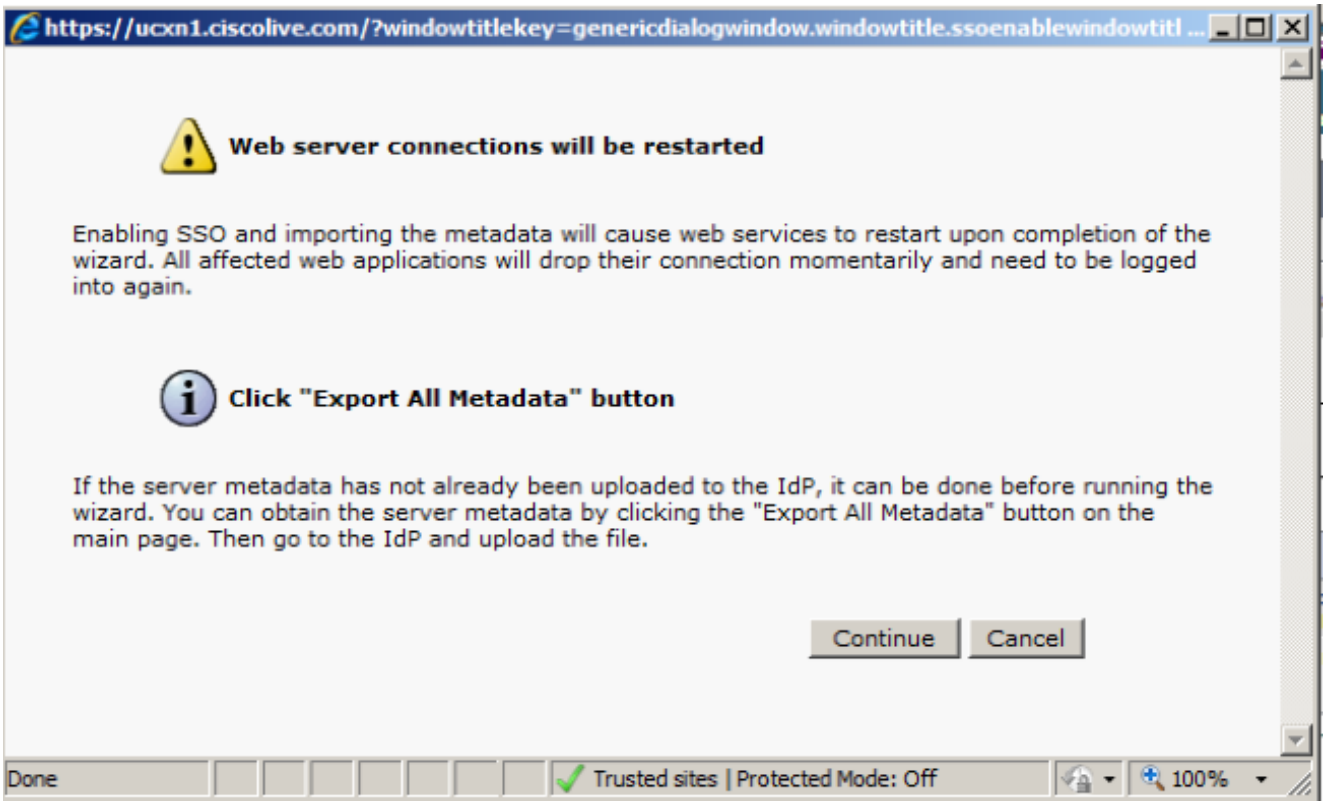
1. 登录UCXN管理用户界面。

2. 选择**System > SAML Single Sign-on**,SAML SSO Configuration窗口打开。

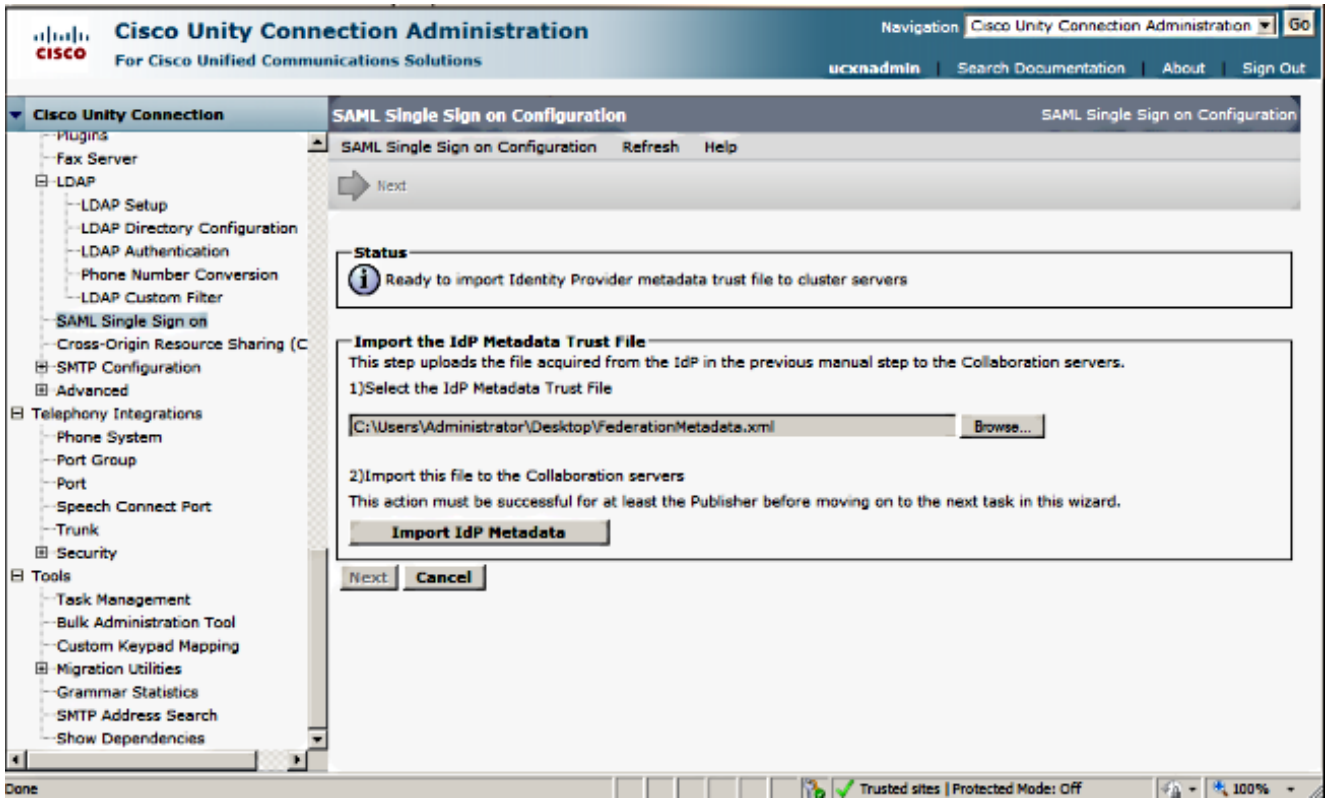


3. 要在集群上启用SAML SSO，请单击**Enable SAML SSO**。

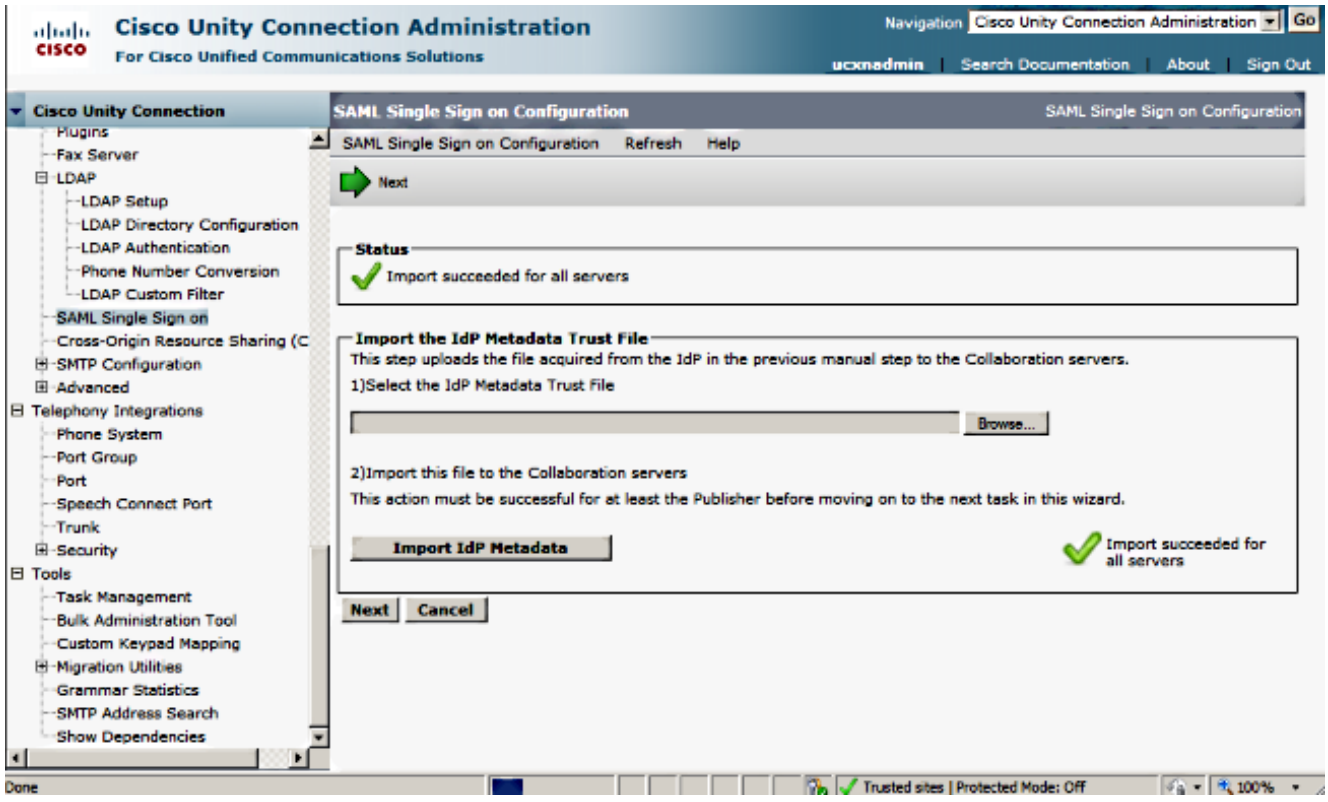
4. 在“重置警告”窗口中，单击“**继续**”。



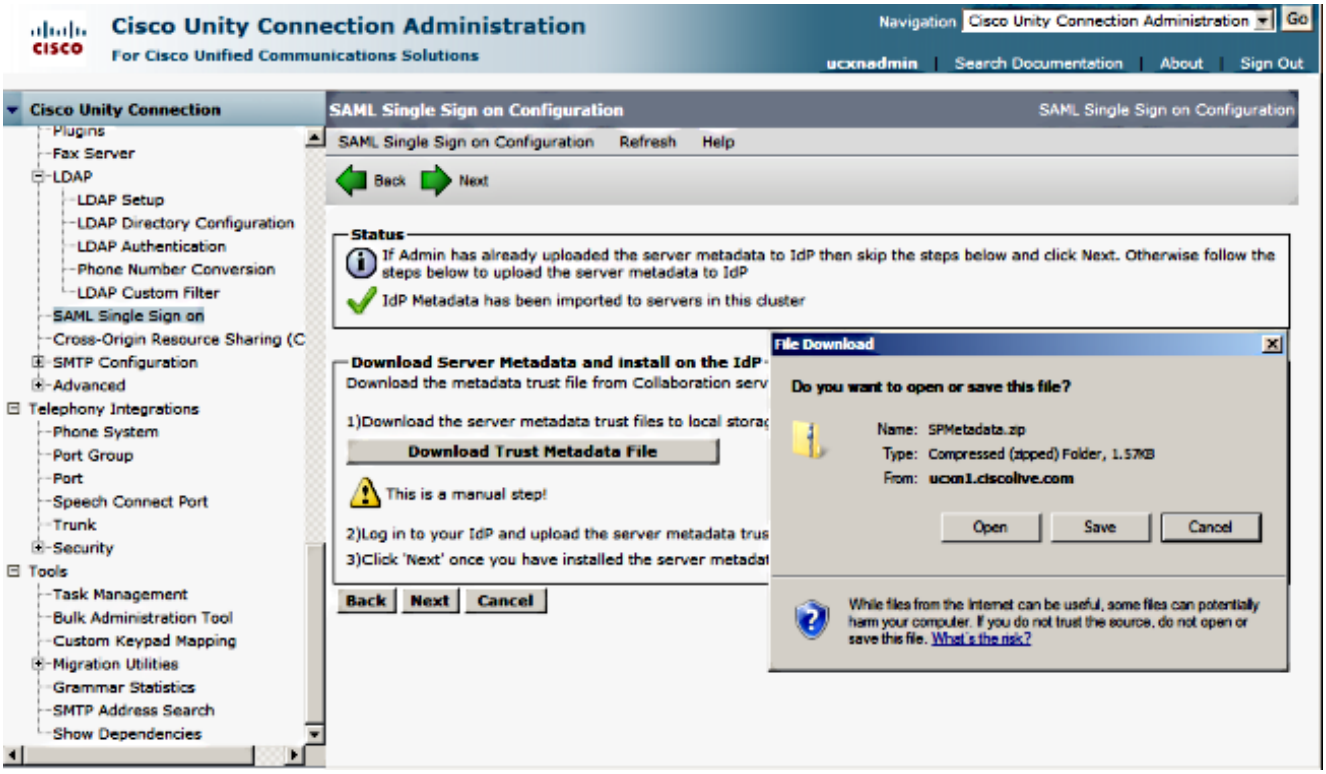
5. 在SSO屏幕上，单击**Browse**以使用“下载Idp元数据”**步骤导**入FederationMetadata.xml元**数据XML**文件。



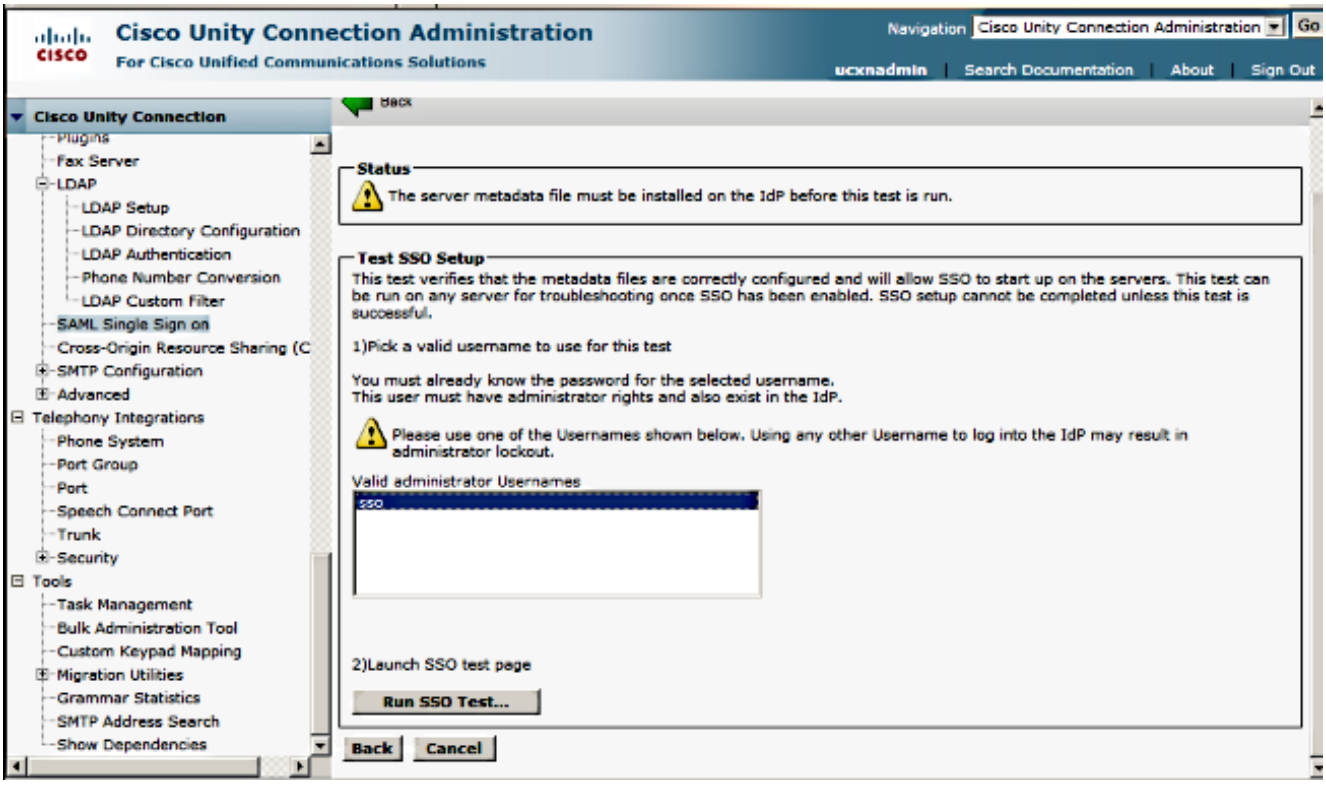
6. 上载元数据文件后，单击**Import IdP Metadata**以将IdP信息导入UCXN。确认导入成功，然后单击“下**一步”**继续。



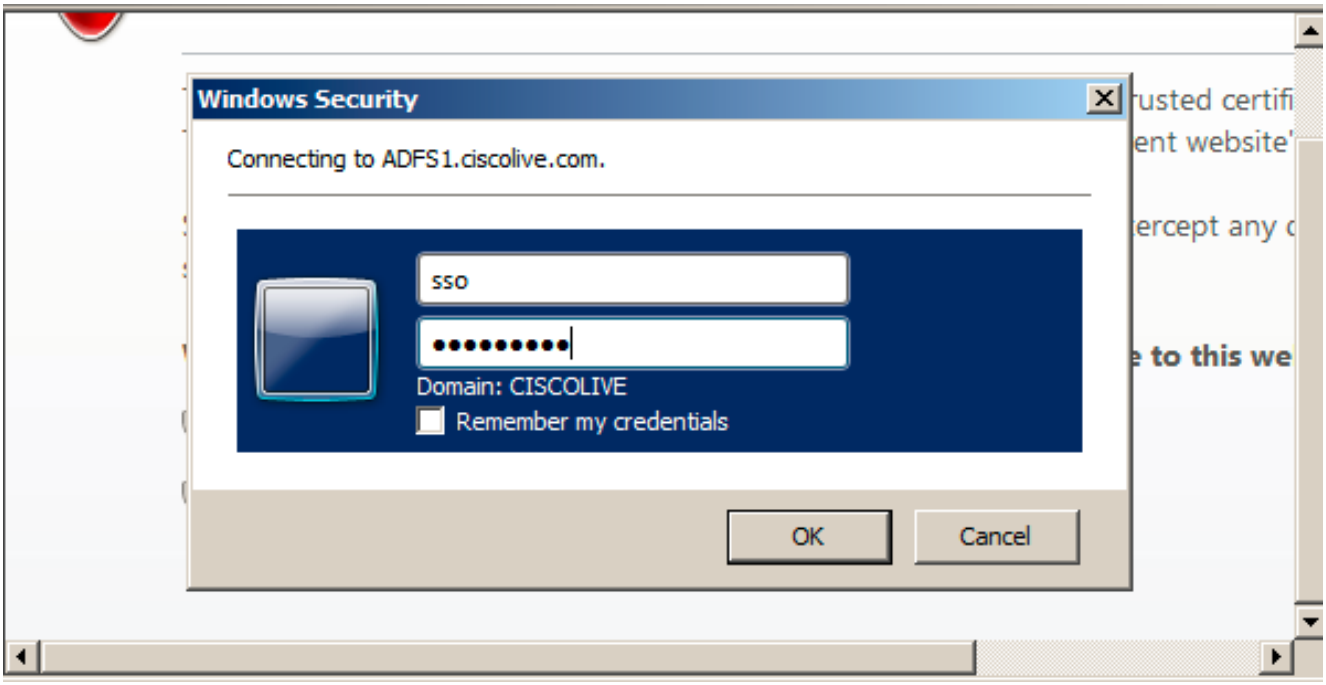
7. 单击**下载信任元数据文件集**（仅当尚未使用UCXN元数据配置ADFS时执行此操作），以便将UCXN元数据保存到本地文件夹，然后转到[添加UCXN作为中继方信任](#)。完成AD FS配置后，继续执行步骤8。



8. 选择SSO作为管理用户，然后单击Run SSO Test。

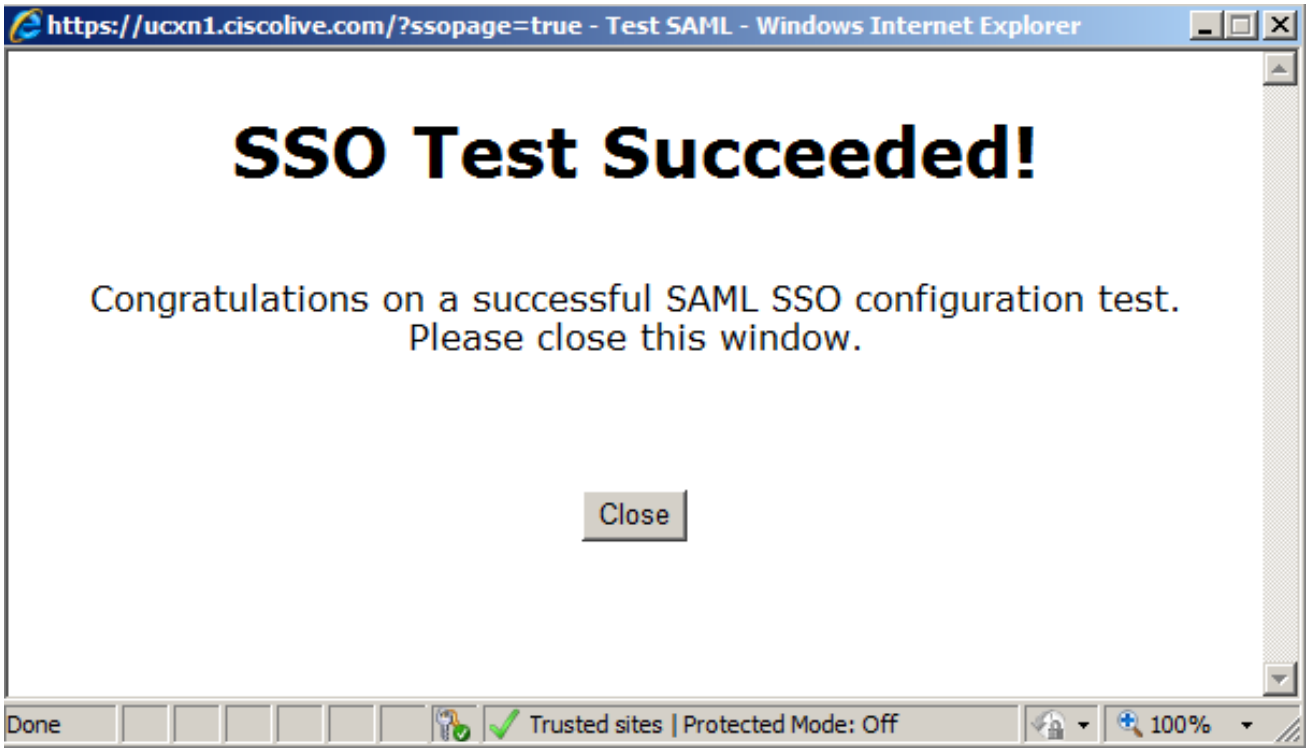


9. 忽略证书警告并继续。当系统提示您输入凭证时，输入用户SSO的用户名和密码，然后单击OK。



注意：此配置示例基于UCXN和AD FS自签名证书。如果您使用证书颁发机构(CA)证书，则必须在AD FS和UCXN上安装适当的证书。有关详细信息，请参阅证书管理和验证。

10. 完成所有步骤后，您将收到“SSO测试成功！”邮件.单击**关闭**和**完成**以继续。



您现在已成功完成配置任务，以在UCXN上启用SSO和AD FS。

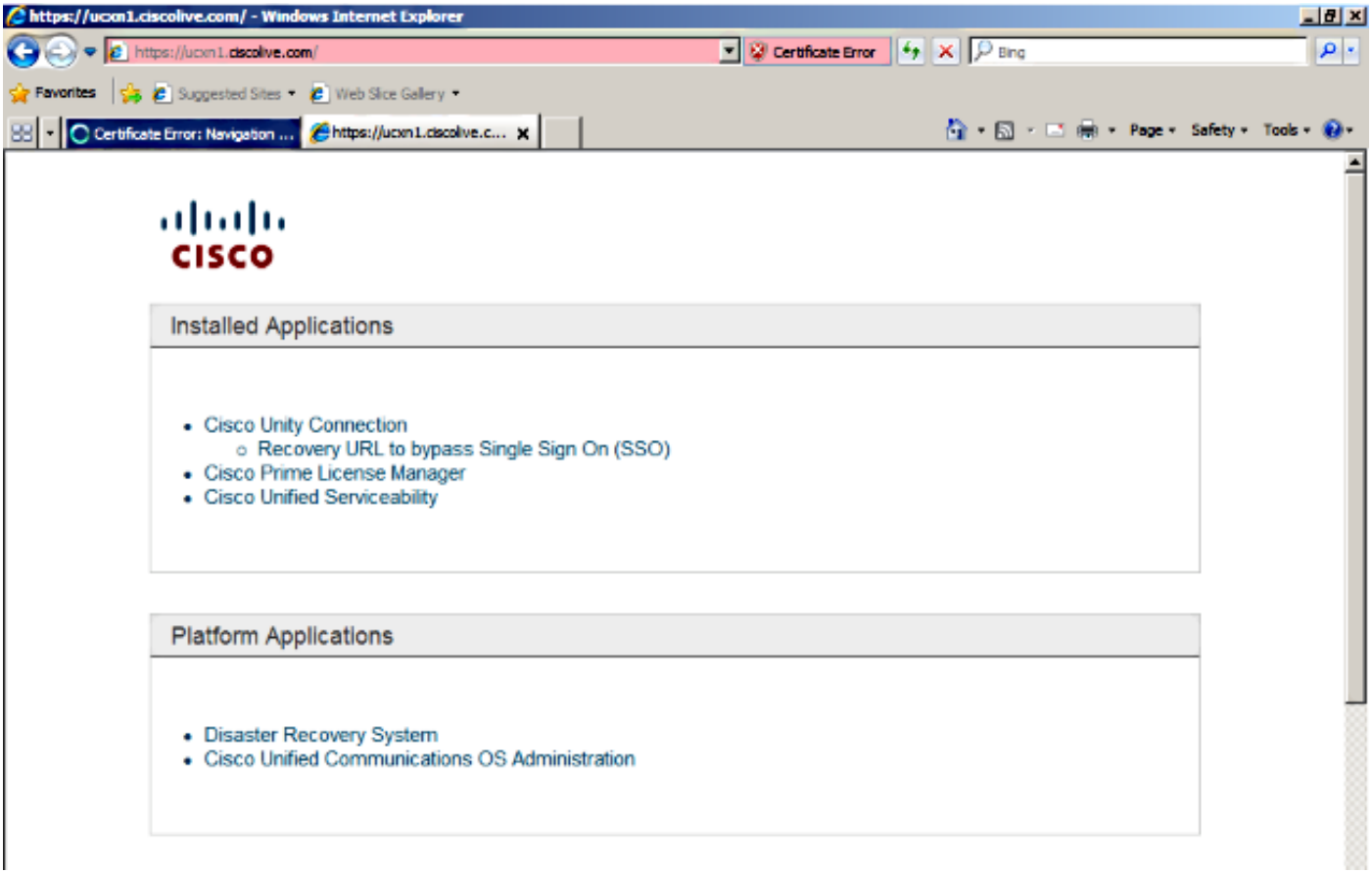
必填注:如果UCXN订用服务器是集群，则运行SSO测试以启用SAML SSO。必须为集群中UCXN的所有节点配置AD FS。

提示：如果在IdP上配置所有节点的元数据XML文件，并且开始在一个节点上启用SSO操作，则会自动在集群中的所有节点上启用SAML SSO。

如果要将SAML SSO用于Cisco Jabber客户端，并为最终用户提供真正的SSO体验，您还可以为SAML SSO配置CUCM和CUCM IM and Presence。

验证

打开Web浏览器并输入UCXN的FQDN，在“已安装的应用”(Installed Applications)下，您会看到一个名为“恢复URL”(**Recovery URL)的新选项，以绕过单点登录(SSO)**。 单击Cisco Unity Connection**链接**后，AD FS会提示您输入凭证。输入用户SSO的凭证后，您将成功登录Unity Administration页面，即Unified Serviceability页面。



注意：SAML SSO不启用对以下页面的访问：
- Prime许可管理器
— 操作系统管理
-灾难恢复系统

故障排除

目前没有针对此配置的故障排除信息。

有关详细信息，请参阅对协作产品10.x的SAML SSO进行故障排除。