Unity Connection版本10.5 SAML SSO配置示例

文档ID118772

已更新：简21， 2015

贡献由A.M.Mahesh Babu， Cisco TAC工程师。

下载 pdf文档
打印
Feedback

相关产品

- Cisco Unity Connection
- Cisco Unified Communications Manager (CallManager)

目录

简介

本文描述如何配置和验证安全断言标记语言(SAML)单一登录(SSO) Cisco Unity Connection的(UCXN)。

先决条件

要求

网络时间协议(NTP)设置

为了使工作SAML的SSO，您必须安装设置的正确NTP和确保，标识供应商(IdP)之间的时差，并且统一通信应用程序不超出三秒。关于同步时钟的信息，请参阅在Cisco Unified通信操作系统管理指南的NTP设置部分。

(DNS)设置的域名服务器

统一通信应用程序能使用DNS为了解决完全合格的域名(FQDN)到IP地址。服务提供商和IdP一定是可解决由浏览器。

活动目录联邦必须安装和配置服务(AD FS)版本2.0为了处理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
- 微软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基于XML的，数据交换的开放标准数据格式。它是服务提供商用于的认证协议为了验证用户。安全认证信息通过在IdP和服务提供商之间。

SAML是使客户端验证所有SAML启用的协作的开放标准(或Unified通信)不管客户端平台，服务。

所有Cisco Unified Communications Web接口，例如Cisco Unified Communications Manager (CUCM)或UCXN，使用SAML在SAML SSO功能的版本2.0协议。为了验证轻量级目录访问协议(LDAP)用户， UCXN委派认证请求对IdP。UCXN生成的此认证请求是SAML请求。IdP验证并且返回SAML断言。SAML断言显示或者是(验证)或没有(验证失败)。

SAML SSO允许LDAP用户登录与在IdP验证的用户名和密码的客户端应用。对的用户签到任何在Unified统一的通信产品的支持的Web应用程序，在您启用SAML SSO功能后，也获得访问到在UCXN的这些Web应用程序(除CUCM外和CUCM IM和在线状态) ：

Unity Connection用户	Web应用程序
有管理员权利的LDAP用户	• UCXN管理 • 思科UCXN维护性 • Cisco Unified 可维护性

没有管理员权利的LDAP用户	• Cisco Personal Communications Assistant • Web收件箱 • 微型Web收件箱(桌面版本) • Cisco Personal Communications Assistant • Web收件箱 • 微型Web收件箱(桌面版本) • 思科Jabber客户端

配置

网络图

目录设置

1. 签字到UCXN管理页面和挑选**LDAP**并且点击**LDAP设置**。
2. 检查**同步从LDAP服务器的Enable (event)**并且点击**"Save"**。
3. 点击**LDAP**。
4. 点击**LDAP目录配置**。
5. 单击新增。
6. 配置这些项目：

   LDAP目录帐户设置将同步的用户属性同步日程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为了与LDAP目录，联络请检查**使用SSL**。

   提示：如果配置在SSL的LDAP，请上传在CUCM上的LDAP目录证书。参考在Cisco Unified Communications Manager SRND的LDAP目录内容关于特定LDAP产品和一般最佳实践的帐户同步机制的信息LDAP同步的。
8. 单击**当前执行全双工同步**。

Note:在您点击“Save”前，请确保**思科DirSync**服务启用在维护性网页。

9. 展开**用户**并且选择**导入用户**。

10. 在**最终用户**列出的**查找统一通信管理器**，选择**LDAP目录**。

11. 如果要导入用户的仅一子集您集成UCXN的LDAP目录的，请在搜索字段输入可适用的规格。

12. 选择**查找**。

13. 在根据模板列表的，请选择**管理员模板**您希望UCXN使用，当创建所选的用户时。

    Caution:如果指定管理员模板，用户不会有邮箱。

14. 检查复选框您要创建UCXN用户并且点击**选择的导入的**LDAP用户。

启用SAML SSO

1. 登录UCXN管理用户界面。

2. 选择**系统> SAML单一登录，**并且SAML SSO配置窗口打开。

3. 为了启用在集群的SAML SSO，请点击**Enable (event) SAML SSO**。

4. 在重置警告窗口，请单击**继续。**

5. 在SSO屏幕，请单击**浏览**为了导入有DownloadIdp**元数据步骤的FederationMetadata.xml元数据**XML文件。

6. 一旦元数据文件上传，请点击**导入IdP元数据**为了导入IdP信息到UCXN。确认导入是成功的并且单击**在旁边**继续。

7. 请点击**下载托拉斯元数据文件集**(请执行此，只有当未配置ADFS已经与UCXN元数据)为了保存UCXN元数据到一个本地文件夹和去添加UCXN，当中继Party托拉斯。一旦AD FS配置完成，请继续对步骤8。

8. 选择**SSO**作为管理用户并且点击**运行SSO测验**。

9. 忽略证书警告并且将来发生。当提示对于凭证时，请输入用户SSO的用户名和密码并且点击OK键。

Note:此配置示例根据UCXN和AD FS自签名证书。万一使用Certificate Authority (CA)证书，在AD FS和UCXN必须安装适当的证书。参考的证书管理和验证欲知更多信息。

10. 在所有步骤完成后，您接收成功的“SSO测验!”消息。点击**Close**并且**完成**为了继续。

您顺利地当前完成配置任务启用在UCXN的SSO与AD FS。

必须注意：如果它是集群为了启用SAML SSO，请运行UCXN用户的SSO测验。必须为所有UCXN节点配置AD FS在集群的。

提示：如果配置所有节点的在IdP的元数据XML文件，并且开始启用在一个节点的SSO操作，则SAML SSO在所有将自动地启用在集群的节点。

如果要使用SAML SSO思科Jabber客户端和给一真的SSO体验对最终用户，您能也配置CUCM和SAML SSO的CUCM IM和在线状态。

验证

打开Web浏览器并且输入UCXN FQDN，并且您看到新选项在呼叫**Recovery的**已安装应用程序下**URL绕过单一登录(SSO)**。一旦点击**Cisco Unity Connection**链路，提示对于凭证由AD FS。在您输入用户SSO的凭证后，您将是顺利地登录的Unity管理页面， Unified维护性页。

Note:SAML SSO不启用对这些页的访问：
-最初许可授权的管理器
- OS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。

参考故障排除协作产品的10.x SAML SSO欲知更多信息。

本文档是否是有用？有 没有

感谢您的反馈。

打开支持案例（需要思科服务合同。）

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：简21， 2015
文档ID118772