Unity Connection版本10.5 SAML SSO配置示例

目录

<u>简介</u> 先决条件 要求 网络时间协议(NTP)设置 域名服务器(DNS)设置 使用的组件 背景信息 配置 网络图 目录设置 启用SAML SSO 验证 故障排除

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<u>理指南》中的</u> <u>"NTP设置"部分</u>。

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

- UCXN管理
- Cisco UCXN适用性
- Cisco Unified 可维护性

具有管理员权限的LDAP用户

- 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。

LDAP System Configurat	tion			
Save				
_				
-Status				
(i) Status: Ready				
о О				
—I DAP System Informati	ion			
Enable Synchronizing fr	om LDAP Server			
LDAP Server Type	Microsoft Active Directory			
LDAP Attribute for User ID	sAMAccountName			

Save

- 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<u>步的一般最佳实践的信</u>息,请参阅Cisco Unified Communications Manager SRND中的LDAP目录内容。

aluda Cisco Unity Conr	nection Administration	Navigation	Navigation Cisco Unity Connection Administration 💌 G		
For Cisco Unified Comm	unications Solutions	ucxnadmin	Search Documentation About Sign Ou		
 Cisco Unity Connection 	LDAP Directory Configuration	Find and List LDAP Directory Configurat	tions 🕨 LDAP Directory Configuration (LDAP)		
- Plugins	LDAP Directory Configuration R	efresh Help			
- fax Server					
EFLDAP	Save				
LDAP Setup					
LDAP Directory Configuration	Status				
	Status: Ready				
- DAR Custom Silter					
- SAMI Single Sign on	LDAP Directory Information				
- Cross-Origin Resource Sharing (C	LDAP Configuration Name*	LDAP			
E-SMTP Configuration	LDAP Manager Distinguished Nam	Pe [*] CN-Administrator CN-Users DC-sinceline D)C-00m		
E Advanced		CN-Administrator, CN-Osers, DC-Oscolive, D	-com		
Telephony Integrations	LDAP Password*	••••••			
- Phone System	Confirm Password*	••••••			
- Port Group	LDAP User Search Base*	CN=Users.DC=ciscolive.DC=com			
- Port	LDAP Custom Filter	< None >			
- Speech Connect Port					
Trunk					
Security	Berform Sync lust Once				
Tools	Perform Sync Just Once				
- Task Management	Perform a Re-sync Every*	7 DAY 💌			
- Bulk Administration Tool	Next Re-sync Time (YYYY-MM-DD	hh:mm)* 2015-01-18 00:00			
- Custom Keypad Mapping					
Higration Utilities	Chandraid Hone Stalida To Back	Survey and the second			
- Grammar Statistics	Cisco Unified Communications Ma	synchronized	Cisco Unified Communications Manager II		
-SMTP Address Search	User ID	sAMAccountName	First Name		
- Show Dependencies					

8. 单击"立即执行完全同步"。

I. IL	
LDAP Server Information	
Host Name or IP Address for Server ⁸	LDAP Port* Use SSL
adfs1.ciscolive.com	3268
Add Another Redundant LDAP Server	
Save Delete Copy Perform Full Sync Now Add New	

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。

alada Cisco Unity Connection Administration			Navigation Cisco Unity Connection Administration 💽 Go				
CISCO For Cisco Unified Co	ommur	nications So	lutions		ucxna	dmin Search Documen	tation About Sign Out
 Cisco Unity Connection 		Import Use	rs				Import Users
Users Users Import Users	1	Import Use	rs Refresh	Help			
Synch Users Class of Service Class of Service Class of Service Membership		Found	1 LDAP User(:	s)			
Templates User Templates Call Handler Templates Contact Templates Bit Notification Templates		Find End U Where Ali	sers In LDAi	P Directory 💌 Begins With 💌	Eind	1	
Contacts Contacts		Based on 1	Femplate adn	ninistratortemplate 💌			
Distribution Lists		Directory	Search Res	uits			
System Distribution Lists Call Management System Call Mandlers		Impor	t Selected	Import All 25 🔹	Rows Per Page		
Directory Handlers			Allas 🔺	First Name	Last Name	Phone Number	Extension
Interview Handlers Custom Recordings		Impor	t Selected	Saml	SSO		
E Message Storage							
Mailbox Stores Mailbox Stores Membership Mailbox Quotas							
Message Anion	<u>∎</u>						

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。

alialia Cisco Unity Conn	ection Ad	ministra	tion		Navig	ation Cisco Unity Co	nnection Administration 🚽 Go
CISCO For Cisco Unified Commu	nications Solu	tions			ucxnadmin	Search Docume	ntation About Sign Out
 Cisco Unity Connection 	SAML Single	Sign on					SAML Single Sign on
Plugins	SAML Single	Sign on Re	fresh Help				
-LDAP	SA Enable SA	WL SSO 🚷	Update IdP Netad	sta File 🚯 Export All	Netadata 🧷	Fix All Disabled Servers	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter SAM Simile Sign ad	Status SAML SS	50 disabled					
Cross-Origin Resource Sharing (C	SAML Sing	je Sign-On	(1 - 1 of 1)				Rows per Page 50 +
SMTP Configuration Advanced	Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
Telephony Integrations Phone System Port Group	UCXN1	Disabled	N/A	Never	🏄 file	Never	Never Run SSO Test
Port Speech Connect Port	Enable S	SAML SSO	Export Al	l Metadata			
B-Security	(🚺 *- indi	cates required	l item.				
I Tools							
Task Management							
Bulk Administration Tool							
Custom Keypad Mapping							
+-Migration Utilities							
Grammar Statistics							
-Show Dependencies	-						
	1						

- 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"。

https://ucxn1.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitl D	< ^
Web server connections will be restarted Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.	
Click "Export All Metadata" button If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.	
Continue Cancel	1

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。

ahah. Cisco Unity Conr	nection Administration	Navigation Cisco Unity Connection Administration 💌 Go
CISCO For Cisco Unified Comm	unications Solutions	ucxnadmin Search Documentation About Sign Out
Cisco Unity Connection	SAML Single Sign on Configuration	SAML Single Sign on Configuration
Fax Server	SAML Single Sign on Configuration Refresh Help	
-LDAP	Next	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status Ready to import Identity Provider metadata trust	file to cluster servers
SAML Single Sign on Cross-Origin Resource Sharing (C SMTP Configuration Advanced	Import the IdP Metadata Trust File This step uploads the file acquired from the IdP in the 1)Select the IdP Metadata Trust file	previous manual step to the Collaboration servers.
Telephony Integrations Phone System	C:\Users\Administrator\Desktop\FederationMetadata.	arni Browse
Port Group Port	2)Import this file to the Collaboration servers	
Speech Connect Port Trunk	This action must be successful for at least the Publish Import IdP Metadata	ar before moving on to the next task in this wizard.
Security Tools	Next Cancel	
Task Management Bulk Administration Tool Custom Keynad Manning		
Migration Utilities Grammar Statistics		
	•	
<u> </u>		3 / Trusted attack Restanded Mades Off
lone		Trusted sites Protected Mode: Off

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。

alada Cisco Unity Con	nection Administration	Navigation Cisco Unity Connection Administration 🗾 Go
CISCO For Cisco Unified Comm	unications Solutions	ucxnadmin Search Documentation About Sign Out
 Cisco Unity Connection 	SAML Single Sign on Configuration	SAML Single Sign on Configuration
Fax Server	SAML Single Sign on Configuration Refresh Help	
E-LDAP	III Next	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status Import succeeded for all servers	
SAML Single Sign on Cross-Origin Resource Sharing (C B-SMTP Configuration B-Advanced	Timport the IdP Metadata Trust File This step uploads the file acquired from the IdP in the 1)Select the IdP Metadata Trust File	e previous manual step to the Collaboration servers.
Telephony Integrations Phone System	[Browse
Port Group	2)Import this file to the Collaboration servers	
Speech Connect Port	This action must be successful for at least the Publis	her before moving on to the next task in this wizard.
E-Security	Import IdP Hetadata	V Import succeeded for
E Tools		un activita
Bulk Administration Tool Custom Keypad Mapping	Next Cancel	
Migration Utilities		
Show Dependencies	-	
4 1		
Done		🛛 🎧 🗸 Trusted sites Protected Mode: Off 🛛 🍕 🔹 🔍 100% 🔹 🧷

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<u>添加UCXN作为中继方信任</u>。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。

alada Cisco Unity Conn	ection Administration	Navigation Cisco Unity Connection Administration 💌
CISCO For Cisco Unified Commu	nications Solutions	ucxnadmin Search Documentation About Sign (
Cisco Unity Connection	Heck Beck	
PluginsFax Server LDAPLDAP SetupLDAP Directory ConfigurationLDAP AuthenticationLDAP AuthenticationLDAP Custom FilterSAML Single Sign onCross-Origin Resource Sharing (CSAML Single Sign on	Status The server metadata file must be installed on Yest SSO Setup This test verifies that the metadata files are correct be run on any server for troubleshooting once SSO successful. 1)Pick a valid username to use for this test You must already know the password for the select This user must have administrator rights and also e Please use one of the Usernames shown below administrator lockout. Valid administrator Usernames sso	the IdP before this test is run. thy configured and will allow SSO to start up on the servers. This test can bas been enabled. SSO setup cannot be completed unless this test is ted username. exist in the IdP. w. Using any other Username to log into the IdP may result in
Tools Tools Tools Sulk Administration Tool Custom Keypad Mapping Migration Utilities Grammar Statistics SMTP Address Search Show Dependencies Tools	2)Launch SSO test page Run SSO Test Back Cancel	

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。

		<u> </u>
Windows Security	·	usted certifi
Connecting to AD	FS1.ciscolive.com.	ent website'
		ercept any c
	sso	
		e to this we
	Remember my credentials	
(
	OK Cancel	
		_
•		<u> </u>

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<u>,请参阅证书管</u>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。

https://ucxn1.ciscolive.com/?ssopage=true - Test SAML - Windows Internet Explorer	
SSO Test Succeeded!	*
Congratulations on a successful SAML SSO configuration test. Please close this window.	
Close	
Done	 0% → //

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。

🚱 🕞 💌 🛃 https://ucxn1.dscolive.com/	. م
👷 Favorites 🛛 🤧 🙋 Suggested Sites 🔹 🙋 Web Sice Galery 🔹	
🔠 🔹 🔿 Certificate Error: Navigation 🌾 https://ucxn1.ciscolive.c 🗙	🗈 📾 🔹 Page 🔹 Safety 🔹 Tools 🔹 😥 🔹
cisco	·
Installed Applications	
 Cisco Unity Connection Recovery URL to bypass Single Sign On (SSO) Cisco Prime License Manager Cisco Unified Serviceability 	
Platform Applications	
Disaster Recovery System Cisco Unified Communications OS Administration	

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<u>信息,请参阅对协作产品10.x的SAML SSO进行</u>故障排除。