SAML SSO的AD FS 2.0版設定配置示例

目錄	
<u>必要條件</u>	
<u>採用元件</u>	
<u>設定</u>	
<u> </u>	
<u>下載合作伺服器(SP)後設資料</u>	
CUCM IM和線上狀態服務	
Unity Connection	
<u>Cisco Prime合作布建</u>	
<u>增加CUCM作為信賴方信任</u>	
增加CUCM IM和線上狀態作為信賴方信任	
<u>增加UCXN作為信賴方信任</u>	
<u>增加Cisco Prime合作調配作為信賴方信任</u>	
<u>驗證</u>	
<u>疑難排解</u>	

簡介

本文檔介紹如何配置Active Directory Federation Service (AD FS) 2.0版,以便為思科合作產品(如 Cisco Unified Communications Manager (CUCM)、Cisco Unity Connection (UCXN)、CUCM IM and Presence和Cisco Prime Collaboration) 啟用安全斷言標籤語言(SAML)單一登入(SSO)。

必要條件

需求

必須安裝並測試AD FS 2.0版。

⚠ 注意:本安裝指南基於實驗室設定,假設AD FS 2.0版僅用於帶有Cisco Collaboration產品的 SAML SSO。如果其他業務關鍵型應用程式使用它,則必須根據Microsoft官方文檔進行必要 的自定義。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- AD FS版本2.0
- Microsoft Internet Explorer 10

- CUCM版本10.5
- Cisco IM和狀態伺服器版本10.5
- UCXN版本10.5
- Cisco Prime合作布建10.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

下載AD FS 2.0版身份提供程式(IdP)後設資料

若要下載IdP中繼資料,請在瀏覽器上執行此連結:https://<ADFS的 FQDN>/FederationMetadata/2007-06/FederationMetadata.xml。

下載合作伺服器(SP)後設資料

CUCM IM和線上狀態服務

打開Web瀏覽器,以管理員身份登入CUCM,然後導航至系統> SAML單一登入。

Unity Connection

打開Web瀏覽器,以管理員身份登入UCXN,然後導航到系統設定> SAML單一登入。

Cisco Prime合作布建

打開Web瀏覽器,以globaladmin身份登入到Prime Collaboration Assurance,然後導航到 Administration > System Setup > Single Sign On。

增加CUCM作為信賴方信任

- 1. 登入AD FS伺服器,並從Microsoft Windows Programs功能表啟動AD FS 2.0版。
- 2. 選擇Add Reliing Party Trust。



3. 按一下Start。

Add Relying Party Trust	Wizard	×
Welcome		
Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.	
	< Previous Start Cancel Help	

4. 選擇從檔案導入有關信賴方的資料選項,選擇之前從CUCM下載的SPMetadata_CUCM.xml後 設資料檔案,然後按一下下一步。

🙀 Add Relying Party Trust W	fizard	×
Select Data Source		
Select Data Source Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Stutsers/Administrator/Desktop/SP/Metadata_CUCM.xm Browse C Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.]
	< Previous Next > Cancel Help	

5. 輸入Display name並按一下Next。

💱 Add Relying Party Trust V	Wizard	×
Specify Display Name		
Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	Type the display name and any optional notes for this relying party. Display name: CUCM Ngtes: Adding CUCM as Relaying Party to ADFS	A
	< Previous Next > Cancel H	elp

6. 選擇允許所有使用者訪問此信賴方並按一下下一步。

🙀 Add Relying Party Trust	Wizard	X
Choose Issuance Aut	horization Rules	
Choose Issuance Auth Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	Invitation Rules Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules. Image: Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. Image: Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.	
	< Previous Next > Cancel Help	

7. 選擇在嚮導關閉時打開信賴方信任的「編輯宣告規則」對話方塊,然後按一下關閉。

🙀 Add Relying Party Trus	t Wizard	×
Finish		
Finish Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snap-in. ✓ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
	Close	

8. 按一下Add Rule。

📬 Edit Claim Rules for CUCM	_ 🗆 🗙
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization	Rules
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	1
	1
	₽
Add Rule Edit Rule Remove Rule	
OK Cancel Apply	Help

9. 在預設宣告規則模板設定為Send LDAP Attributes as Claims的情況下,按一下Next。

🙀 Add Transform Claim Ruk	e Wizard	×
Select Rule Template		
Steps Choose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.	
Configure Claim Rule	Cain rule template: Send LDAP Attributes as Claims Cain rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute so using a sclaims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template. Tell me more about this rule template	
	< Previous Next > Cancel Help	

10. 在配置規則中,輸入宣告規則名稱,選擇Active Directory作為屬性儲存,配置LDAP屬性和傳 出宣告型別(如圖所示),然後按一下完成。

💊 附註:

- 輕型目錄訪問協定(LDAP)屬性應與CUCM上的目錄同步屬性匹配。

- 「uid」應使用小寫。

Configure Rule

Steps Choose Rule Type	You c which	an configure this rule to send the to extract LDAP attributes. Spe	e values of L cify how the	LDAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be
Configure Claim Rule	issued	from the rule.		
	Claim	rule name:		
	Name	ID		
	Rule t	emplate: Send LDAP Attributes	as Claims	
	Attribu	te store:		
	Active	e Directory		•
	Марр	ing of LDAP attributes to outgoin	ng claim type	85:
		LDAP Attribute		Outgoing Claim Type
	•	SAM-Account-Name	-	uid 🗾
	*		-	
	_			
			< Pre	revious Finish Cancel Help

11. 點選增加規則,選擇使用自定義規則傳送宣告作為宣告規則模板,然後點選下一步。

Edit Claim Rules for CUCM	_ 🗆 ×
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization	Rules
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
1 Name ID uid	
	₽
Add Rule Edit Rule Remove Rule	
OK Cancel Apply	Help

Select Rule Template

Steps	Select the template for the claim rule that you want to create from the following list. The description
Choose Rule Type	provides details about each claim rule template.
Configure Claim Rule	Qaim rule template:
	Send Claims Using a Custom Rule
	Send Claims Using a Custom Rule ✓ ✓ Claim rule template description: Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS 2.0 claim rule language. Capabilities that require custom rules include: 9. Sending claims from a SQL attribute store 9. Sending claims from a LDAP attribute store using a custom LDAP filter. 9. Sending claims only when 2 or more incoming claims are present. 9. Sending claims only when an incoming claim value matches a complex pattern. 9. Sending claims for use only in later rules Tell me more about this rule template
	< <u>Previous</u> Cancel <u>H</u> elp

12. 輸入宣告規則名稱的名稱,並在自訂規則下指定的空格中複製此語法:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(]

(注意:如果您複製並貼上這些範例中的文字,請注意某些文書處理軟體會以UNICODE版本

(「」)取代ASCII引號(「)。UNICODE版本會導致宣告規則失敗。)

X

Add Transform Claim Ru	le Wizard	×
Configure Rule		
Steps Choose Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language. Qaim rule name: Call Manager Claim Rule Rule template: Send Claims Using a Custom Rule Custom rule: Thttp://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou ntname"]=> issue (Type = "http://schemas.milsoap.org/ws/2005/05/identity/claims/nameidentifier ", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "http://ADFS1.CISCOLIVE.COM/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "CUCM.CISCOLIVE.COM"); More about the claim rule language	
	< <u>Previous</u> Finish Cancel <u>H</u> elp	

💊 附註:

- 在本示例中,CUCM和ADFS完全限定域名(FQDN)預填充了實驗CUCM和AD FS,必 須對其進行修改以符合您的環境。

- CUCM/ADFS的FQDN區分大小寫,必須與後設資料檔案匹配。

- 13. 按一下「Finish」(結束)。
- 14. 按一下Apply,然後按一下OK。
- 15. 從Services.msc重新啟動AD FS版本2.0服務。

增加CUCM IM和線上狀態作為信賴方信任

- 1. 重複增加CUCM為信賴方信任所述的步驟1到11,然後繼續步驟2。
- 2. 輸入宣告規則名稱的名稱, 並在自訂規則下指定的空格中複製此語法:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(1

📬 Add Transform Claim Ru	ule Wizard							
Configure Rule								
Steps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts							
Choose Rule Type	claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and issuance statement using the AD FS 2.0 claim rule language.							
Configure Claim Rule	Claim rule name:							
	Custom Rule for IMP							
	Rule template: Send Claims Using a Custom Rule							
	Custom nile:							
	"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou							
	ntname"]=> issue (Type =							
	"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier							
	c.Value, ValueType = c.ValueType, Properties							
	<pre>["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties</pre>							
	["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name							
	<pre>qualifier"] = "http:///ADFS1.ciscolive.com/com/adfs/services/trust", Properties</pre>							
	["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna							
	<pre>mequalifier"] = "IMP.ciscolive.com");</pre>							
	More about the claim rule language							
	< Previous Finish Cancel Help							

請注意,在本例中,IM and Presence和AD FS FQDN預填充了實驗室IM and Presence和AD FS,必須對其進行修改以符合您的環境。

- 3. 按一下「Finish」(結束)。
- 4. 按一下Apply,然後按一下OK。
- 5. 從Services.msc重新啟動AD FS版本2.0服務。

增加UCXN作為信賴方信任

- 1. 重複增加CUCM為信賴方信任所述的步驟1到步驟12, 然後繼續步驟2。
- 2. 輸入宣告規則名稱的名稱, 並在自訂規則下的空白處複製此語法:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(]

💱 Add Transform Claim Rule	Wizard	×					
Configure Rule							
Steps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts						
Choose Rule Type	issuance statement using the AD FS 2.0 claim rule language.						
Configure Claim Rule	Claim rule name:						
	Custom Rule for UCXN						
	Rule template: Send Claims Using a Custom Rule						
	Custom rule:						
	<pre>=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier ", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "http://ADFS1.ciscolive.com/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "UCXN1.ciscolive.com"); </pre>						
	More about the claim rule language						
	< Previous Finish Cancel Help						

請注意,在本例中,UCXN和AD FS FQDN預填充了實驗UCXN和ADFS,必須對其進行修改 以符合您的環境。

- 3. 按一下「Finish」(結束)。
- 4. 按一下Apply,然後按一下OK。
- 5. 從Services.msc重新啟動AD FS版本2.0服務。

增加Cisco Prime合作調配作為信賴方信任

- 1. 重複增加CUCM為信賴方信任所述的步驟1到步驟12, 然後繼續步驟2。
- 2. 輸入宣告規則名稱的名稱, 並在自訂規則下的空白處複製此語法:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(]

🏘 Add Transform Claim Ru	e Wizard	×					
Configure Rule							
Steps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts						
Choose Rule Type	claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.						
Configure Claim Rule	Claim rule name:						
	Custom Rule for PCP						
	Rule template: Send Claims Using a Custom Rule						
	Custom rule:						
	ntname"]						
	<pre>>> issue(lype = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier ", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "http://ADFS1.ciscolive.com/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "PCP.ciscolive.com"); More about the claim rule language</pre>						
	< Previous Finish Cancel Help						

請注意,本示例中的Prime調配和AD FS FQDN預填充了實驗Prime合作調配(PCP)和AD FS,必須對其進行修改以符合您的環境。

- 3. 按一下「Finish」(結束)。
- 4. 按一下Apply,然後按一下OK。

5. 從Services.msc重新啟動AD FS版本2.0服務。

設定AD FS版本2.0後,繼續啟用思科合作產品上的SAML SSO。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

AD FS將診斷資料記錄到系統事件日誌。 從AD FS伺服器上的伺服器管理器打開Diagnostics -> Event Viewer -> Applications and Services -> AD FS 2.0 -> Admin

查詢為AD FS活動記錄的錯誤

📕 Server Manager														
File Action View Help														
(= =) 🖄 🖬 🛛 🖬														
Server Manager (CUC-ADFS)	Server Manager (CUC-ADFS) Admin Number of events: 211													
🗈 🔁 Roles		Data and Tax		Carrow	Event ID	Tech Coloran								
Features	Level	Date and time	2.414	Source	Event ID	Task Category								
Diagnostics	Information	6/26/2016 11:18:1	ZAM	AD FS 2.0	337	None	_							
Event Viewer	Information	6/28/2016 11:18:1	ZAM	AD FS 2.0	336	None								
E Custom Views	Information	6/28/2016 11:17:1	ZAM	AD FS 2.0	390	None								
Windows Logs	Information	6/28/2016 11:17:1	ZAM	AD FS 2.0	385	None								
	Information	6/28/2016 11:17:1	ZAM	AD FS 2.0	399	None								
Admin	Information	6/28/2016 11:17:1	ZAM	AD FS 2.0	15/	None								
Hardware Events	Information	6/28/2016 11:17:1	ZAM	AD FS 2.0	150	None								
Internet Explorer	Information	6/27/2016 11:18:0	2 PM	AD F5 2.0	33/	None								
Key Management S	Information	6/2//2016 11:18:0	2 PM	AD FS 2.0	336	None								
🖅 🧮 Microsoft	Information	6/27/2016 8:12:59	PM	AD FS 2.0	388	None								
Windows PowerShe	Error	6/27/2016 8:12:11	PM	AD FS 2.0	364	None								
Subscriptions	Error	6/27/2016 8:12:11	PM	AD FS 2.0	321	None								
Performance	Information	6/27/2016 8:12:10	PM	AD FS 2.0 2		None								
Bevice Manager	Information	6/27/2016 8:11:59	PM	AD FS 2.0	100	None	-							
Configuration	Event 221 AD ES 2.0						×							
🗉 📇 Storage	Event 521, AD F5 2.0													
	General Details													
	Decision						1							
	The SAML with	entiration request had a Nam	ID Doliou that could	I not be estimated										
	Requestor cisco	uc-105-imps1 ciscouc ora	el Policy that could	not be satisfied.		Ē								
	Name identifier	format: urn:oasis:names:tc:S	ML:2.0:nameid-for	mattransient		-								
	Log Name:	AD FS 2.0/Admin												
	Source:	AD FS 2.0	Logged:	6/27/2016 8:12:11 PM										
	Event ID:	321	Task Category:	None			-							
•														

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。