# 使用Kerberos身份驗證配置SAML SSO設定

### 目錄

<u>簡介</u> 必要條件 需求 採用元件 設定 配置AD FS 配置瀏覽器 Microsoft Internet Explorer Mozilla Firefox 驗證 疑難排解

# 簡介

本文檔介紹如何配置Active Directory和Active Directory聯合身份驗證服務(AD FS)版本2.0,以使其 能夠通過Jabber客戶端(僅限Microsoft Windows)使用Kerberos身份驗證,從而允許使用者使用其 Microsoft Windows Logon登入,而不提示輸入憑據。

**注意**:本文基於實驗室環境,並假設您已瞭解所做更改的影響。請參閱相關產品文檔以瞭解變 更的影響。

## 必要條件

#### 需求

思科建議您:

- 安裝AD FS 2.0版,並將思科合作產品配置為信賴方信任
- 合作產品(例如Cisco Unified Communications Manager(CUCM)IM and Presence、Cisco Unity Connection(UCXN)和CUCM),支援使用安全斷言標籤語言(SAML)單一登入(SSO)

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

• Active Directory 2008(主機名: ADFS1.ciscolive.com)

- AD FS 2.0版(主機名: ADFS1.ciscolive.com)
- CUCM(主機名: CUCM1.ciscolive.com)
- Microsoft Internet Explorer版本10
- Mozilla Firefox版本34
- Telerik Fiddler版本4

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

#### 配置AD FS

1. 使用服務主體名稱(SPN)配置AD FS版本2.0,以使安裝Jabber的客戶端電腦能夠請求票證,從 而使得客戶端電腦能夠與AD FS服務通訊。



請參閱AD FS 2.0:如何為服務帳戶配置SPN(servicePrincipalName)以瞭解詳細資訊。

 2. 確保AD FS服務的預設身份驗證配置(在C:\inetpub\adfs\ls\web.config中)為整合Windows身份 驗證。確保它未更改為基於表格的身份驗證。

 選擇Windows Authentication,然後按一下右窗格下的Advanced Settings。在「Advanced Settings」中,取消選中Enable Kernel-mode authentication,確保Extended Protection為 Off,然後按一下OK。

4. 確保AD FS版本2.0同時支援Kerberos協定和NT LAN Manager(NTLM)協定,因為所有非 Windows客戶端都不能使用Kerberos並依賴NTLM。

在右窗格中,選擇**Providers**,並確保**Negotiate**和**NTLM**位於Enabled Providers:



**附註**:使用整合Windows身份驗證對客戶端請求進行身份驗證時,AD FS會傳遞Negotiate安 全標頭。協商安全標頭允許客戶端在Kerberos身份驗證和NTLM身份驗證之間進行選擇。除非 以下條件之一為真,否則協商過程將選擇Kerberos身份驗證:

— 身份驗證中涉及的某個系統不能使用Kerberos身份驗證。

— 呼叫應用程式沒有提供足夠的資訊來使用Kerberos身份驗證。

 為了啟用協商過程以選擇用於網路身份驗證的Kerberos協定,客戶端應用程式必須提供 SPN、使用者主體名稱(UPN)或網路基本輸入/輸出系統(NetBIOS)帳戶名稱作為目標名稱。否 則,協商過程始終會選擇NTLM協定作為首選身份驗證方法。

#### 配置瀏覽器

**Microsoft Internet Explorer** 

1. 確保選中Internet Explorer > Advanced > Enable Integrated Windows Authentication。

Internet Options					
General Security Privacy Content Connections Programs Advanced					
Settings					
<ul> <li>Do not submit unknown addresses to your auto-search provide a Just display the results in the main window</li> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invited of the sinvited of the signature is invited of the signature is invite</li></ul>					
<ul> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable memory protection to help mitigate online attacks*</li> </ul>					
*Takes effect after you restart Internet Explorer					
Restore advanced settings					
Reset Internet Explorer settings					
Resets Internet Explorer's settings to their default Reset					
You should only use this if your browser is in an unusable state.					
OK Cancel Apply					

2. 在**Security > Intranet zones > sites**下新增AD FS URL。

Internet Options					
General Security Privacy Content Connections Programs Advanced					
Select a zone to view or change security settings.					
Internet Local intranet Trusted sites Restricted sites					
Local intranet This zone is for all websites that are found on your intranet. Sites					
Local intranet 🛛 🕅					
Use the settings below to define which websites are included in the local intranet zone.					
Automatically detect intranet network					
Include all local (intranet) sites not listed in other zones					
Include all sites that bypass the proxy server					
Include all network paths (UNCs)					
What are intranet settings? Advanced OK Cancel					
Local intranet 💽					
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.					
Add this website to the zone:					
Add					
Websites:					
adfs1.ciscolive.com					

3. 將CUCM、IMP和Unity主機名新增到Security >Trusted sites。

Internet Options				
General Security Privacy Content Connections Pro	grams Advanced			
Select a zone to view or change security settings.				
🥥 🔩 🗸 🚫				
Internet Local intranet Trusted sites Restricter sites	ed			
Trusted sites	Sites			
Trusted sites	×			
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.				
	Add			
Websites:				
cucm1.ciscolive.com	Remove			
imp1.ciscolive.com				
ucxn1.clscolive.com				
Require server verification (https:) for all sites in this	zone			
	Close			

4. 確保已配置Internet Explorer > **security** > **Local Intranet** > **Security Settings** > **User Authentication - Logon**,以便使用Intranet站點的登入憑據。

Internet Options	83
General Security Privacy Content Connection	s Programs Advanced
	Security Settings - Local Intranet Zone
Select a zone to view or change security settings.	Settings
🔮 👒 🗸	O Disable
Internet Local intranet Trusted sites	Enable     Enable XSS filter
Local intranet	Disable
This zone is for all websites that are	Enable     Scripting of Java applets
found on your intranet.	<ul> <li>Disable</li> </ul>
	Enable
Security level for this zone	Prompt
Allowed levels for this zone: All	& Logon
- Medium-low	Anonymous logon
<ul> <li>Appropriate for websites on your (intranet)</li> </ul>	Automatic logon only in Intranet zone
- Most content will be run without p	Automatic logon with current user name and password     Prompt for user name and password
- Same as Medium level without pro	· · · · · · · · · · · · · · · · · · ·
Enable Protected Mode (requires restartin	*Takes effect after you restart Internet Evilorer
Custom level	Takes effect and you restart internet explorer
	Reset custom settings
Reset all zo	Reset to: Medium-low (default)   Reset
	OK Cancel
OK	

#### Mozilla Firefox

1. 開啟Firefox,在位址列中輸入**about:config**。



2. 單擊「我會小心的,我保證!」

	Here be dragons!	
	Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.	
	Show this warning next time	
	I'll be careful, I promise!	

 按兩下偏好設定network.negotiate-auth.allow-non-fqdn至true,按兩下偏好設定 network.negotiate-auth.trusted-uris至ciscolive.com,adfs1.ciscolive.com以進行修改。

Search: network.n							
Preference Name	Status	Туре	Value				
network.negotiate-auth.allow-insecure-ntlm-v1	default	boolean	false				
network.negotiate-auth.allow-insecure-ntlm-v1-https	default	boolean	true				
network.negotiate-auth.allow-non-fqdn	user set	boolean	true				
network.negotiate-auth.allow-proxies	default	boolean	true				
network negotiate-auth delegation-uris	default	string					
network.negotiate-auth.gsslib	default	string					
network.negotiate-auth.trusted-uris	user set	string	adfs1.adfs1.ciscolive.com.ciscolive.com				
network.negotiate-auth.using-native-gsslib	default	boolean	true				
network.ntlm.send-lm-response	default	boolean	false				

4. 關閉Firefox並重新開啟。

### 驗證

若要檢查AD FS伺服器的SPN是否正確建立,請輸入setspn命令並檢視輸出。



檢查客戶端電腦是否具有Kerberos票證:

C:\Windows\system32\cmd.exe	X
C:\Users\user1.CISCOLIVE>Klist tickets	<b>^</b>
Current LogonId is 0:0xabc6d	
Cached Tickets: <2>	
#0> Client: user1 @ CISCOLIVE.COM Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent Start Time: 1/17/2015 20:52:47 (local) End Time: 1/18/2015 6:52:47 (local) Renew Time: 1/24/2015 20:52:47 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96	Е
<pre>#1&gt; Client: user1 @ CISCOLIVE.COM Server: host/pc1.ciscolive.com @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a00000 -&gt; forwardable renewable pre_authent Start Time: 1/17/2015 20:52:47 (local&gt; End Time: 1/18/2015 6:52:47 (local&gt; Renew Time: 1/24/2015 20:52:47 (local&gt; Session Key Type: AES-256-CTS-HMAC-SHA1-96</pre>	
C:\Users\user1.CI\$COLIVE>	

完成以下步驟以驗證正在使用哪些身份驗證(Kerberos或NTLM身份驗證)。

- 1. 將Fiddler工具下載到您的客戶端電腦並進行安裝。
- 2. 關閉所有Microsoft Internet Explorer視窗。
- 3. 運行Fiddler Tool並檢查File選單下的**Capture Traffic**選項是否已啟用。Fiddler充當客戶端電腦 和伺服器之間的傳遞代理,並偵聽所有流量。
- 4. 開啟Microsoft Internet Explorer,瀏覽到您的CUCM,然後按一下某些連結以生成流量。
- 5. 返回到Fiddler主視窗,並選擇結果為200(成功)的其中一個幀,您可以看到Kerberos作為身 份驗證機制

📀 Fide	dier Web I	Debugger	w Help CIT ha	nk 🔛 Geolidae		
Q 49	Replay >	<- > Go	Stream 👑	Decode Keep: All sessions -	- 🕀 Any Process 🏦 Find 🔜 Save   🞼 🕐 🎓 Browse - 🕀 Clear Cache 🎢 TextWizard   🛃 Tearoff	
	Result	Protocol	Host	URL	🔺 🔿 Statistics 🚟 Inspectors 🖉 AutoResponder 📝 Composer 🔲 Filters 🗈 Log 🚍 Timeline	
2	200	HTTP	cucm.ciscolive	/ciscologo.gif	Headers TextView WebForms HexView Auth Cookies Raw JSON XML	
E 3	200	HTTP	cucm.ciscolive	/favicon.ico		
54	302	HTTP	cucm.ciscolive	/ccmadmin/showHome.do	No Proxy-Authorization Header is present.	
🖄 5	200	HTTP	Tunnel to	cucm.ciscolive.com:443	Authorization Header (Negotiate) appears to contain a Kerberos ticket:	
<b>b</b> 6	302	HTTPS	cucm.ciscolive	/ccmadmin/showHome.do	4D 53 53 50 00 03 00 00 00 00 00 00 58 00 00 MSSPX	
57	302	HTTPS	cucm.ciscolive	/ssosp/sami/login?relayurl	00 00 00 00 58 00 00 00 00 00 00 00 58 00 00XX	
6 8	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	00 00 00 00 00 58 00 00 00 15 C2 88 E2 06 01 B1X	
59	302	HTTPS	adfs1.ciscoliv	/adfs/ls/75AMLRequest=n	1D 00 00 00 0F 7E AF 60 90 3B D7 F3 E2 F4 5E 84~ ;xôâô^	
2 10	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	E 50 2D 22 9A 84 00 00 00 00 PS 17 A7 2.C -L	
2 11	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?		
<\$¥12	200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	Californiation Transformer Handers Tradition Insection Heating Highlight	
Ø 13	502	HTTP	www.downloa	/msdownload/update/v3/s	Get Syntaxview Transformer Headers Textview Imageview Hexview Webview	
14	401	HTTPS	adfs1.ciscoliv	/favicon.ico	E Auth Caching Cookies Raw JSON XML	
15	200	HTTP	Tunnel to	cucm.ciscolive.com:8443	No Proxy-Authenticate Header is present.	
3 16	302	HTTPS	cucm.ciscolive	/ssoep/sami/SSO/alias/CU	WWW-Authenticate Header (Neontiate) appears to be a Kerbergs reply:	
2 17	403	HTTPS	cucm.ciscolive	/ssosp/relay	A1 18 30 19 A0 03 0A 01 00 A3 12 04 10 01 00 00 i.0f	
18	200	HTTPS	cucm.ciscolive	/ciscologo.gif	00 43 87 E0 88 C1 36 E3 A9 00 00 00 00 .C a A6ab	
Ø 19	502	HTTP	www.downloa	/msdownload/update/v3/s		
Ø 20	502	HTTP	www.downloa	/msdownload/update/v3/s		
					<u>고</u>	
<b>.</b>						
[QuickE)	(QuideExec) ALT+Q > type HELP					
Capturing 👻 All Processes 1 / 20 Download Progress: 0 bytes. Ht F5 to refresh.						

6. 如果身份驗證型別為NTLM,則會在幀的開頭看到協商 — NTLMSSP,如下所示。

🚸 Fide	🕑 Fiddler Web Debugger					
File E	File Edit Rules Tools View Help GET book 50 GeoEdge					
Q 4g	🔍 🍫 Replay 🗙 + 🕨 Go 🔹 Stream 🛗 Decode 🛛 Knep: Al sessions + 🕀 Any Process 🌺 Find 😡 Save 📲 🔞 🔗 🔗 Browse - 🏈 Clear Cache 🎢 TextWizard 🕼 Tearoff					
	Result	Protocol	Host	URL	B (2) Statistics 🗱 Inspectors 🖉 AutoResponder 🖉 Composer 📄 Filters 🕒 Log 🚍 Timeline	
<b>Ø</b> 1	502	HTTP	www.bing.com	/favicon.ico	Headers TextView WebForms HexView Auth Cookies Raw JSON XML	
≪≯2	200	HTTP	cucm.ciscolive	1	5, No Prove Authorization Hander is present	
23	200	HTTP	cucm.ciscolive	/ciscologo.gif	No Proxy-Authorization Header is present.	
E 4	200	HTTP	cucm.dscolive	/favicon.ico	1, Authorization Header 15 present: NTLM	
5 5	302	HTTP	cucm.ciscolive	/comadmin/showHome.do	58 00 00 00 00 00 00 58 00 00 00 00 00 00 00 XX.	
i 🛗 6	200	HTTP	Tunnel to	cucm.ciscolive.com:443	58 00 00 00 00 00 00 58 00 00 00 00 00 00 00 XXX	
07	502	HTTP	www.downloa	/msdownload/update/v3/s	06 01 81 1D 00 00 00 0F 4E 84 C3 AA 0D D1 81 34 N Å*.N 4	
58	302	HTTPS	cucm.ciscolive	/comadmin/showHome.do	78 AA CE A9 41 F3 D1 31 X°IBAON1	
59	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl	(ITH Tests betweet estimates)	
10 🗂	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	-[NTLM Type3: Authentication]	
5 11	302	HTTPS	adfs1.ciscoliv	/adfs/ls/?SAMLRequest=n	Cet Syntaxiliew Transformer Headers TextView ImageView HexView WebView	
12	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	6, but solve solve solve sources the second	
13 13	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	7, Auth Cadhing Cookies Raw JSON XML	
<≯14	200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	9, Response Headers [Raw] [Header Definitions]	
7 15	401	HTTPS	adfs1.ciscoliv	/favicon.ico	6, HTTP/1.1 200 OK	
16 🗂	200	HTTP	Tunnel to	cuam.ciscolive.com:8443	Cache	
17	302	HTTPS	cucm.ciscolive	/ssosp/sami/SSO/alias/CU	Cache-Control: no-cache	
18	403	HTTPS	cucm.ciscolive	/ssosp/relay	2,: Date: Sat, 17 Jan 2015 20:05:06 GMT	
<b>Z</b> 19	200	HTTPS	cucm.ciscolive	/ciscologo.gif	Expires: -1	
			12		Pragma: no-cache	
		_			Cookies / Login	
QuidExec(ALT+Q > type HELP						
🗱 Capturing 👻 All Processes 1 / 19 https://adfs1.dscolive.com/adfs/s/auth/integrated/75AMLRequest=nVLbtswELznKwjebYrytwphGXBsFDWQNErk9NDbHBCR55V1p%2B%2						

# 疑難排解

如果所有配置和驗證步驟均按本文檔所述完成,並且您仍存在登入問題,則必須諮詢Microsoft Windows Active Directory/AD FS管理員。