Kerberos 인증으로 SAML SSO 설정 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>구성</u> <u>AD FS 구성</u> <u>브라우저 구성</u> <u>Microsoft Internet Explorer</u> 모질라 파이어폭스 <u>다음을 확인합니다.</u> <u>문제 해결</u>

소개

이 문서에서는 Jabber 클라이언트에서 Kerberos 인증(Microsoft Windows만 해당)을 사용하도록 Active Directory 및 AD FS(Active Directory Federation Service) 버전 2.0을 구성하는 방법에 대해 설명합니다. 이 방법을 사용하면 사용자가 Microsoft Windows 로그온을 사용하여 로그인할 수 있으 며 자격 증명을 묻는 메시지가 표시되지 않습니다.

주의: 이 문서는 랩 환경을 기반으로 하며 변경 사항이 미치는 영향을 알고 있다고 가정합니다 . 변경 사항의 영향을 알아보려면 관련 제품 설명서를 참조하십시오.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 기능을 권장합니다.

- AD FS 버전 2.0이 Cisco Collaboration 제품을 Relying Party Trust로 설치 및 구성
- SAML(Security Assertion Markup Language) SSO(Single Sign-On)를 사용하기 위해 Cisco CUCM(Unified Communications Manager) IM and Presence, Cisco UCXN(Unity Connection) 및 CUCM과 같은 협업 제품

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Active Directory 2008(호스트 이름: ADFS1.ciscolive.com)
- AD FS 버전 2.0(호스트 이름: ADFS1.ciscolive.com)
- CUCM(호스트 이름: CUCM1.ciscolive.com)
- Microsoft Internet Explorer 버전 10
- Mozilla Firefox 버전 34
- Telerik Fiddler 버전 4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

AD FS 구성

1. Jabber가 설치된 클라이언트 컴퓨터가 티켓을 요청하도록 AD FS 버전 2.0을 SPN(서비스 사용자 이름)으로 구성하여 클라이언트 컴퓨터가 AD FS 서비스와 통신할 수 있게 합니다.



<u>AD FS 2.0</u>을 참조하십시오<u>. 자세한 내용을 보려면 서비스 계정에 대한</u> <u>SPN(servicePrincipalName)을 구성하는</u> 방법

 AD FS 서비스에 대한 기본 인증 컨피그레이션(C:\inetpub\adfs\ls\web.config에서)이 통합 Windows 인증인지 확인합니다. 양식 기반 인증으로 변경되지 않았는지 확인합니다.

 Windows 인증을 선택하고 오른쪽 창 아래에서 Advanced Settings를 클릭합니다. Advanced Settings(고급 설정)에서 Enable Kernel-mode authentication(커널 모드 인증 활성화)의 선택을 취소하고 Extended Protection(확장 보호)이 Off(꺼짐)인지 확인하고 OK(확인)를 클릭합니다.



4. 모든 비 Windows 클라이언트는 Kerberos를 사용할 수 없고 NTLM을 사용할 수 없으므로 AD FS 버전 2.0이 Kerberos 프로토콜과 NTLM(NT LAN Manager) 프로토콜을 모두 지원하는지 확인하십시오.

오른쪽 창에서 Providers(공급자)를 선택하고 Enabled Providers(활성화된 **공급자**) 아래에 **Negotiate(협상**) 및 **NTLM**이 있는지 확인합니다.



참고: AD FS는 클라이언트 요청을 인증하기 위해 통합 Windows 인증을 사용할 때 협상 보안 헤더를 전달합니다. Negotiate 보안 헤더를 사용하면 클라이언트가 Kerberos 인증과 NTLM 인 증 사이에서 선택할 수 있습니다. 협상 프로세스는 다음 조건 중 하나가 참인 경우를 제외하고 Kerberos 인증을 선택합니다.

- 인증과 관련된 시스템 중 하나가 Kerberos 인증을 사용할 수 없습니다.

- 발신 응용 프로그램이 Kerberos 인증을 사용할 수 있는 충분한 정보를 제공하지 않습니다.

- 협상 프로세스에서 네트워크 인증을 위해 Kerberos 프로토콜을 선택할 수 있도록 하려면 클 라이언트 응용 프로그램이 대상 이름으로 SPN, UPN(사용자 계정 이름) 또는 NetBIOS(Network Basic Input/Output System) 계정 이름을 제공해야 합니다. 그렇지 않으면 협상 프로세스는 항상 기본 인증 방법으로 NTLM 프로토콜을 선택합니다.

브라우저 구성

Microsoft Internet Explorer

1. Internet Explorer > Advanced > Enable Integrated Windows Authentication(통합 Windows 인 중 사용)이 선택되어 있는지 확인합니다.

Internet Options						
General Security Privacy Content Connections Programs Advanced						
Settings						
 Do not submit unknown addresses to your auto-search pro Just display the results in the main window Security Allow active content from CDs to run on My Computer* Allow active content to run in files on My Computer* Allow software to run or install even if the signature is invo Check for publisher's certificate revocation Check for server certificate revocation* Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is dc Enable DOM Storage Enable Integrated Windows Authentication* 						
Takes effect after you restart Internet Explorer						
Restore advanced 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. Security(보안) > Intranet zones(**인트라넷 영역) > sites(사이트**)에서 AD FS URL을 **추가합니** 다.

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.							
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 Remove							

3. CUCM, IMP 및 Unity 호스트 이름을 Security(보안) >Trusted sites(신뢰할 수 있는 사이트)에 추가합니다.

Internet Options	8 🕺						
General Security Privacy Content Connections Prog	rams Advanced						
Select a zone to view or change security settings.							
🛛 🔮 🔩 🗸 🚫							
Internet Local intranet Trusted sites Restricte sites	d						
Trusted sites	Sites						
Tructed 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.ciscolive.com							
Require server verification (https:) for all sites in this zone							
	Close						

4. Internet Explorer > **security > Local Intranet > Security Settings > User Authentication -**Logon이 인트라넷 사이트에 로그인된 자격 증명을 사용하도록 구성되어 있는지 확인합니다.

Internet Options	83
General Security Privacy Content Connection	s Programs Advanced
Í	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	Oisable
This zone is for all websites that are	Enable Scripting of Java applets
found on your intranet.	 Disable
	Enable
Security level for this zone	Prompt
Allowed levels for this zone: All	& Logon
- Medium-low	C Anonymous logon
 Appropriate for websites on your (intranet) 	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 offert after you contact Internet Evplorer
Custom level	Takes effect after you restart internet explorer
	Reset custom settings
Reset all zo	Reset to: Medium-low (default) Reset
	OK Cancel
OK	

모질라 파이어폭스

1. Firefox를 열고 주소 표시줄**에 about:config**를 입력합니다.



2. I'll be 주의, I promise!(주의하겠습니다, 약속합니다!)를 클릭합니다.

	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!

3. 기본 설정 이름 network.negotiate-auth.allow-non-fqdn을 true로 두 번 클릭하고 ciscolive.com,adfs1.ciscolive.com에 대한 network.negotiate-auth.trusted-uris를 클릭하여 수 정합니다.

Seech: 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. Firefox를 닫고 다시 엽니다.

다음을 확인합니다.

AD FS 서버의 SPN이 제대로 만들어졌는지 확인하려면 setspn 명령을 입력하고 출력을 봅니다.



클라이언트 컴퓨터에 Kerberos 티켓이 있는지 확인합니다.

C:\Windows\system32\cmd.exe	×
C:\Users\user1.CISCOLIUE>Klist tickets	-
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	ш
#1> Client: user1 @ CISCOLIVE.COM Server: host/pc1.ciscolive.com @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a00000 -> forwardable renewable 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	
C:\Users\user1.CISCOLIVE>	

사용 중인 인증(Kerberos 또는 NTLM 인증)을 확인하려면 다음 단계를 완료하십시오.

- 1. 클라이언트 컴퓨터에 Windows Installer 도구를 다운로드하여 설치합니다.
- 2. 모든 Microsoft Internet Explorer 창을 닫습니다.
- 3. File Tool을 실행하고 File 메뉴에서 Capture Traffic 옵션이 활성화되었는지 확인합니다. Fiddler는 클라이언트 시스템과 서버 간에 통과 프록시 역할을 하며 모든 트래픽을 수신합니다
- 4. Microsoft Internet Explorer를 열고 CUCM을 찾은 다음 일부 링크를 클릭하여 트래픽을 생성합니다.
- 5. Windows 주 창을 다시 참조하여 Frames(결과200(성공) 중 하나를 선택하고 Kerberos를 인증 메커니즘으로 볼 수 있습니다.

$_{igodoldelta}$ Fi	iddler Web I)ebugger				
Fie	Edit Rules	Tools Vie	ew Help GET /bo	ok 🔛 GeoEdge		
Q •	Replay >	<- 🕨 Go	🕸 Stream 腸	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
3	200	HTTP	cucm.ciscolive	/favicon.ico	1	No Promy-Authorization Header is present
54	302	HTTP	cucm.ciscolive	/ccmadmin/showHome.do		No Proxy-Aution 22cton neader 15 present.
🖺 5	200	HTTP	Tunnel to	cucm.ciscolive.com:443		Authorization Header (Negotiate) appears to contain a Kerberos ticket:
16	302	HTTPS	cucm.ciscolive	/ccmadmin/showHome.do		4D 53 53 50 00 03 00 00 00 00 00 00 00 58 00 00 MSSPX.
57	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl		
1 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		10 00 00 0F 7E AF 60 90 3B D7 F3 E2 F4 5E 84~ ;x0a0^
21	0 401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	- e -	50 2D 22 9A 84 00 00 00 00 P-"
21	1 401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	- 2	
431	2 200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?		California Transformer Handers Tradition Interations Heating Highlight
01	3 502	HTTP	www.downloa	/msdownload/update/v3/s		dec syntaxiew in a slot men i neadels i fexchew anageview i nextiew vieuview
1 1	4 401	HTTPS	adfs1.ciscoliv	/favicon.ico	e	Auth Caching Cookies Raw JSON XML
台 1	5 200	HTTP	Tunnel to	cucm.ciscolive.com:8443		No Proxy-Authenticate Header is present.
🔂 1	6 302	HTTPS	cucm.ciscolive	/seesp/sami/SSO/alias/CU		WWW-Authenticate Header (Neoptiate) appears to be a Kerberos reply:
1 1	7 403	HTTPS	cucm.ciscolive	/ssosp/relay	- 2	A1 18 30 19 A0 03 0A 01 00 A3 12 04 10 01 00 00 i.0
1	8 200	HTTPS	cuam.ciscolive	/ciscologo.gif		00 43 87 E0 88 C1 36 E3 A9 00 00 00 00 .C a A6a8
01	9 502	HTTP	www.downloa	/msdownload/update/v3/s		
02	0 502	HTTP	www.downloa	/msdownload/update/v3/s	_	
					. .	
1					<u> </u>	
[Quid	(Exec] ALT+0	2 > type HE	LP			P
iii c	apturing	+ All Proce	5905	1 / 20 Download Progress	: 0 bytes	s. Hit F5 to refresh.

6. 인증 유형이 NTLM이면 프레임 시작에 협상 - NTLMSSP가 표시됩니다(아래 참조).

🚸 Fidd	er Web C	ebugger				<u>lo ×</u>
File Ed	it Rules	Tools Vie	ew Help GET /bo	ook 🔛 GeoEdge		
Q 🐓	Replay >	<- 🕨 Go	🔹 Stream 👹	Decode Keep: All sessions *	🕀 Any Process 🏦 Find 🔜 Save 🛛 🎼 🥎 🏈 Browse 🔹 🅀 Clear Cache 🎢 TextWizard 🛛 🖉 Tearoff	=
	Result	Protocol	Host	URL	🕒 🕅 Statistics 🞇 Inspectors 🖉 AutoResponder 🛛 🛪 Composer 🗍 🗖 Fiters 🕒 Log 🚍 Tim	eline
Ø 1	502	HTTP	www.bing.com	/favicon.ico	Headers TextVew WebForms HexView Auth Cookies Raw JSON XML	
≪≯2	200	HTTP	cucm.ciscolive	1	5, he from bother in the local of the second s	<u> </u>
23	200	HTTP	cucm.ciscolive	/ciscologo.gif	NO Proxy-Authorization Header is present.	-
Ξ4	200	HTTP	cucm.ciscolive	/favicon.ico	1, Authorization Header is present: NTLM	
N 5	302	HTTP	cucm.ciscolive	/ccmadmin/showHome.do	4E 54 4C 4D 53 53 50 00 03 00 00 00 00 00 00 00 00 00 NTLMSSPX.	_
<u>6</u> 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 8	302	HTTPS	cucm.ciscolive	/comadmin/showHome.do	78 AA CE A9 41 F3 D1 31 X°18AÓÑ1	
59	302	HTTPS	cucm.ciscolive	/ssosp/sami/login?relayurl		
10	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	-[NTLM Type3: Authentication]	-
5 11	302	HTTPS	adfs1.ciscoliv	/adfs/ls/75AMLRequest=n	Coloursteen Transformer Distance Transition Institute Making	
12	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	6, Get Syntaxivew Transformer [Headers Textview Imageview Hexview Webview]	
1 13	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	7, Auth Caching Cookies Raw JSON XML	
14	200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	9/ Response Headers [Raw] Header Definit	ionsl
15	401	HTTPS	adfs1.ciscoliv	/favicon.ico	6, HTTP/1.1 200 OK	_
16	200	HTTP	Tunnel to	cucm.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	2,1 Date: Sat, 17 Jan 2015 20:05:06 GMT	
2 19	200	HTTPS	cucm.ciscolive	/ciscologo.gif	Expires: -1	
					Pragma: no-cache	
•					Conkies / Lonin	_ <u>–</u>
[QuidEx	ec] ALT+C) > type HB	LP			<u> </u>
Tie Capt	uring	Al Proce	sses	1 / 19 https://adfs1.ciscol	sive.com/adfs/ls/auth/integrated/75AMLRequest=nVLLbtswELznKw/ebYryIwphGX8sFDWQNErk9NDbi48CR55V3p%	28%2

문제 해결

이 문서에 설명된 대로 모든 컨피그레이션 및 확인 단계가 완료되었지만 로그인 문제가 있는 경우 Microsoft Windows Active Directory/AD FS 관리자에게 문의해야 합니다.