# Kerberos mit ADFS 2.0 für Endbenutzer SAML SSO für Jabber - Konfigurationsbeispiel

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfiguration Überprüfen Fehlerbehebung

## Einführung

Dieses Dokument beschreibt, wie Kerberos mit Active Directory Federation Services (ADFS) 2.0 konfiguriert wird.

## Voraussetzungen

#### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

#### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Für die SSO-Konfiguration (Single Sign On) der Endbenutzer Security Assertion Markup Language (SAML) muss Kerberos konfiguriert werden, damit die Endbenutzer-SAML SSO für

Jabber mit der Domänenauthentifizierung arbeiten kann. Wenn SAML SSO mit Kerberos implementiert wird, übernimmt das Lightweight Directory Access Protocol (LDAP) die gesamte Autorisierung und Benutzersynchronisierung, während Kerberos die Authentifizierung übernimmt. Kerberos ist ein Authentifizierungsprotokoll, das in Verbindung mit einer LDAP-fähigen Instanz verwendet werden soll.

Bei Microsoft Windows- und Macintosh-Computern, die einer Active Directory-Domäne angehören, können sich Benutzer problemlos bei Cisco Jabber anmelden, ohne einen Benutzernamen oder ein Kennwort eingeben zu müssen. Es wird nicht einmal ein Anmeldebildschirm angezeigt. Benutzer, die nicht bei der Domäne auf ihrem Computer angemeldet sind, sehen immer noch ein Standard-Anmeldeformular.

Da bei der Authentifizierung ein einzelnes Token verwendet wird, das von den Betriebssystemen übergeben wird, ist keine Umleitung erforderlich. Das Token wird anhand des konfigurierten Key Domain Controller (KDC) überprüft. Wenn es gültig ist, ist der Benutzer angemeldet.

## Konfiguration

Hier ist die Prozedur zur Konfiguration von Kerberos mit ADFS 2.0.

- 1. Installieren Sie Microsoft Windows Server 2008 R2 auf einem Computer.
- 2. Installieren Sie Active Directory Domain Services (ADDS) und ADFS auf demselben Computer.
- 3. Installieren Sie Internetinformationsdienste (IIS) auf dem Computer, auf dem Microsoft Windows Server 2008 R2 installiert ist.
- 4. Erstellen Sie ein selbstsigniertes Zertifikat für IIS.
- 5. Importieren Sie das selbstsignierte Zertifikat in IIS, und verwenden Sie es als HTTPS-Serverzertifikat.
- 6. Installieren Sie Microsoft Windows7 auf einem anderen Computer, und verwenden Sie es als Client.

Ändern Sie den Domain Name Server (DNS) auf den Computer, auf dem ADDS installiert ist.

Fügen Sie diesen Computer der Domäne hinzu, die Sie bei der Installation von ADDS erstellt haben.

Klicken Sie auf **Start**.Klicken Sie mit der rechten Maustaste auf **Computer**.Klicken Sie auf **Eigenschaften**.Klicken Sie rechts im Fenster auf **Einstellungen ändern**.Klicken Sie auf die **Registerkarte Computername**.Klicken Sie auf **Ändern**.Fügen Sie die von Ihnen erstellte Domäne hinzu.

				and the second	In the second	rasnaikn S
ystem Properties		8	User Management	t 👻 Bulk Administration	Help	
Computer Name/Domain Changes		ote				
You can change the name and the membership of this computer. Onanges might affect access to network resources. More information						
Computer name:		y/s	Security   System	•	Search Control	Panel
JabberPC1						
Full computer name: JabberPC1 mangolab.com			s edition	about your compu	ter	
Member of Domain: mangolab.com Workgroup:	More	s ID	right © 2009 Microso ce Pack 1 nore features with a n	ft Corporation. All rights ew edition of Windows 7	reserved.	<b>*</b>
	OK Cancel	Apply	ıg: essor: lied memory (RAM): :m type:	System rating is not av Intel(R) Xeon(R) CPU E 2.00 GB 64-bit Operating Syster	ailable 7- 2870 @ 2.40GHz 2.	40 GHz
			and Touch:	No Pen or Touch Input	is available for this Dis	play
Cisco Unified Commun		Compu	uter name, domain, and	workproup settings		
upport please visit our ]		Co	mputer name:	JabberPC1		Change settings
1000		Ful	computer name:	JabberPC1.mangolab.c	om	• • • •
		Cor	mputer description:	JabberPC1		
See	also	Do	main:	mangolab.com		
Act	ion Center	Window	ws activation			
Wir	ndows Update	Wir	ndows is activated			ask for ,
Per Too	formance Information and ols	d Pro	duct ID: 00371-221-876	7124-86146 Change p	roduct key	genuine Microsoft software

7. Überprüfen Sie, ob der Kerberos-Dienst auf beiden Computern generiert wird.

Melden Sie sich als Administrator auf dem Servercomputer an, und öffnen Sie die Eingabeaufforderung. Führen Sie dann die folgenden Befehle aus:

cd \windows\System32Klist-Tickets



Melden Sie sich als Domänenbenutzer auf dem Client-Computer an, und führen Sie die gleichen Befehle aus.

:\Users\rashaikh>cd \windows\System32
::\Windows\System32>Klist tickets
Aurrent LogonId is 0:0x558ba
Cached Tickets: <5>
HD> Client: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbIicket Encryption Type: AES-256-CIS-HMAC-SHA1-96 Ticket Flags 0x60a00000 -> forwardable forwarded renewable pre_authent Start Time: 12/10/2014 18:35:23 (local> End Time: 12/11/2014 4:34:59 (local> Renew Time: 12/17/2014 18:34:59 (local> Session Key Type: AES-256-CIS-HMAC-SHA1-96
H)> Client: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40e00000 -> forwardable renewable initial pre_authent Start Time: 12/10/2014 18:34:59 (local> End Time: 12/11/2014 4:34:59 (local> Renew Time: 12/17/2014 18:34:59 (local> Session Key Type: AES-256-CTS-HMAC-SHA1-96
12> Client: rashaikh @ MANGOLAB.COM Server: LDAP/win2k8.mangolab.com/mangolab.com @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok as_dele
Start Time: 12/10/2014 19:05:15 (local) End Time: 12/11/2014 4:34:59 (local) Renew Time: 12/17/2014 18:34:59 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96
Client: rashaikh @ MANGOLAB.COM Server: HITP/win2k8.mangolab.com @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40a40000 -> forwardable renewable pre_authent ok_as_dele
Start Time: 12/10/2014 18:35:23 (local) End Time: 12/11/2014 4:34:59 (local) Renew Time: 12/17/2014 18:34:59 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96
14> Client: rashaikh @ MANGOLAB.COM Server: LDAP/win2k8.mangolab.com @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40a40000 -> forwardable renewable pre_authent ok_as_dele
Start Time: 12/10/2014 18:35:05 (local) End Time: 12/11/2014 4:34:59 (local) Renew Time: 12/17/2014 18:34:59 (local) Session Key Type: AES-256-CIS-HMAC-SHA1-96
C:\Windows\System32>

8. Erstellen Sie die ADFS Kerberos-Identität auf dem Computer, auf dem Sie ADDS installiert haben.

Der Microsoft Windows-Administrator, der sich bei der Microsoft Windows-Domäne angemeldet hat (z. B. als <Domänenname>\administrator), erstellt die ADFS Kerberos-Identität. Der ADFS-HTTP-Service muss eine Kerberos-Identität aufweisen, die als Service Principal Name (SPN) bezeichnet wird. Dieses Format hat folgende Eigenschaften: HTTP/DNS\_Name\_of\_ADFS\_Server. Dieser Name muss dem Active Directory-Benutzer zugeordnet werden, der die ADFS-HTTP-Serverinstanz darstellt. Verwenden Sie das Microsoft Windows **setspn**-Dienstprogramm, das standardmäßig auf einem Microsoft Windows 2008-Server verfügbar sein sollte.

Vorgehensweise Registrieren Sie die SPNs für den ADFS-Server. Führen Sie auf dem Active Directory-Domänencontroller den Befehl **setspn aus**.

Wenn beispielsweise der ADFS-Host **adfs01.us.renovations.com** ist und die Active Directory-Domäne **US.RENOVATIONS.COM** ist, lautet der Befehl:

```
setspn -a HTTP/adfs01.us.renovations.com
```

Der **HTTP**/Teil des SPN gilt, obwohl der Zugriff auf den ADFS-Server in der Regel über Secure Sockets Layer (SSL) erfolgt, d. h. HTTPS.

Überprüfen Sie, ob die SPNs für den ADFS-Server mit dem Befehl **setspn** korrekt erstellt wurden und zeigen Sie die Ausgabe an.

setspn -L



9. Konfigurieren Sie die Browsereinstellungen des Microsoft Windows-Clients.

Navigieren Sie zu **Extras > Internetoptionen > Erweitert**, um die integrierte Windows-Authentifizierung zu aktivieren.

Aktivieren Sie das Kontrollkästchen Integrierte Windows-Authentifizierung aktivieren:

Internet Options
General Security Privacy Content Connections Programs Advanced
Settings
<ul> <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 inv.</li> <li>Block unsecured images with other mixed content</li> <li>Check for publisher's certificate revocation</li> <li>Check for server certificate revocation*</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is ck</li> <li>Fnable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable native XMLHTTP support</li> <li>Enable SmartScreen Filter</li> <li>*Takes effect after you restart Interpet Evolorer</li> </ul>
Pactors advanced cettings
Reset Internet Explorer's settings to their default Reset
You should only use this if your browser is in an unusable state.
OK Cancel Apply

Navigieren Sie zu Extras > Internetoptionen > Sicherheit > Lokales Intranet > Benutzerdefiniert.. um die Option Automatische Anmeldung nur in der Intranetzone auszuwählen.

General       Security       Privacy       Connections       Programs       Advanced         Select a zone to view or change security settings.       Internet       Security is settings       Image: Security Setings       Image: Security Settings       Image:	Internet Options	- = ≥ C × 🗰 Cisco Unified Serviceability ×
OK Cancel Apply OK Cancel	General       Security       Privacy       Content       Connections       Programs       Advanced         Select a zone to view or change security settings.         Image: Security and the security settings.         Internet       Local intranet       Trusted sites       Restricted sites         Internet       Local intranet       Trusted sites       Restricted sites         Image: Content will be security level for this zone       Stes       Stes         Security level for this zone       Alowed levels for this zone       Stes         Alowed levels for this zone:       Alowed levels for this zone:       Stes         Security level for this zone       Alowed levels for this zone:       Stes         Image: Alowed levels for this zone:       Alowed levels for this zone:       Stes         Image: Alowed level for this zone:       Alowed levels for this zone:       Stes         Image: Alowed level for this zone:       Alowed level for this zone:       Stes         Image: Alowed level for this zone:       Alowed level for this zone:       Stes         Image: Alowed level for this zone:       Alowed level for this zone:       Alowed level for this zone:         Image: Alowed level for this zone:       Alowed level for this zone:       Alowed level for this zone:         Image: Alowed level for this zone:       S	Image: Cisco Unified Serviceability       X         Recurity Settings - Local Intranet Zone       Image: Cisco Unified Serviceability         Settings       Disable         Enable       Enable         Scripting of Java applets       Disable         Disable       Enable         Scripting of Java applets       Disable         Enable       Prompt         User Authentication       Logon         Automatic logon only in Intranet zone       Automatic logon with Current User name and password         Prompt for user name and password       Image: Cisco Unified Serviceability         *Takes effect after you restart Internet Explorer       Reset custom settings         Reset to:       Medum-low (default)       Reset         OK       Cancel

Navigieren Sie zu **Extras > Internetoptionen > Sicherheit > Lokales Intranet > Sites > Erweitert**, um die IDP-URL (Intrusion Detection & Prevention) zu lokalen Intranet-Sites hinzuzufügen.

**Hinweis**: Aktivieren Sie alle Kontrollkästchen im Dialogfeld Lokales Intranet, und klicken Sie auf die **Registerkarte Erweitert**.

Internet Options	► 🖴 🗟 Č 🗙 🛲 Cisco Unified Serviceability 🗙
General       Security       Privacy       Content       Connections       Programs       Advance         Select a zone to view or change security settings.       Image: Content image: C	Image: Contract intranet       Image: Contract intranet         Image: Contract intranet       Image: Contract intranet
Appropriate for websites on your local network     (Intranet)     Most content will be run without prompting you     Unsigned ActiveX controls will not be downloaded     Same as Medium level without prompts     Enable Protected Mode (requires restarting Internet Explorer)     Custom level     Default level     Reset all zones to default level     OK Cancel Apply	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: Websites: https:// <hostname idp="" of=""> Remove Remove Close</hostname>

Navigieren Sie zu Extras > Sicherheit > Vertrauenswürdige Sites > Sites, um die CUCM-

Hostnamen vertrauenswürdigen Sites hinzuzufügen:

Internet Options	- = ≥ C × O sso-44.com ×
General Security Privacy Content Connections Programs Advanced	
Select a zone to view or change security settings.	Trusted sites
Internet Local intranet Trusted sites Restricted sites	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Trusted sites	Add this website to the zone:
This zone contains websites that you trust not to damage your computer or	Add
your files.	Websites:
Tou nave websites in this zone.	https:// CUCM1.domainname.com Remove
Allowed levels for this zone All	https:// CUCM2.domainname.com
- I - Medium	2.5
<ul> <li>Prompts before downloading potentially unsafe</li> </ul>	
Content     Unsigned ActiveX controls will not be downloaded	Require server verification (https:) for all sites in this zone
Enable Protected Mode (requires restarting Internet Explorer)	Close
Custom level Default level	
	and local country laws governing import, export, transfer and use. De with U.S. and local country laws. By using this product you agree to co
Reset all zones to default level	und at our Export Compliance Product Rep
	ur <u>Unified Communications System Docum</u> Loading, please
OK Cancel Apply	

# Überprüfen

In diesem Abschnitt wird erläutert, wie Sie überprüfen, welche Authentifizierung (Kerberos- oder NT LAN Manager-(NTLM-)Authentifizierung) verwendet wird.

- 1. Laden Sie das <u>Tool</u> "<u>Ordner</u>" auf Ihren Client-Computer herunter und installieren Sie es.
- 2. Schließen Sie alle Internet Explorer-Fenster.
- 3. Führen Sie das Tool Ordner aus, und überprüfen Sie, ob die Option **Datenverkehr erfassen** im Menü Datei aktiviert ist.

Fiddler agiert als Pass-Through-Proxy zwischen dem Client-Computer und dem Server und überwacht den gesamten Datenverkehr, der Ihre Internet Explorer-Einstellungen vorübergehend wie folgt festlegt:

Local Area	Network (LA	AN) Settings	-	23
Automa Automa use of r Auto Use Add	tic configuration tic configuration manual setting omatically deter automatic con	ion ion may override manual settings. To gs, disable automatic configuration. ect settings nfiguration script	ensu	re the
Proxy s Use dial-	erver a proxy serve up or VPN cor ings	er for your LAN (These settings will no nnections).	t app	ly to
Servers	Type HTTP: Secure: FTP: Socks:	Proxy address to use          127.0.0.1         127.0.0.1         same proxy server for all protocols		Port 8888 8888
Exception	Do not use p <-loopback	proxy server for addresses beginning k> ons (; ) to separate entries.	with:	*

- 4. Öffnen Sie Internet Explorer, rufen Sie die URL des CRM-Servers (Customer Relationship Management) auf, und klicken Sie auf einige Links, um Datenverkehr zu generieren.
- 5. Rufen Sie das Hauptfenster der Ordner auf, und wählen Sie eines der Frames aus, in dem das Ergebnis 200 (Erfolg) lautet:

O Fid	dler Web I	Debugger				x
E21a	Edia Dud	Teels	Mana Hala OFT 6	and Placetain		
rite	cont Man	65 10005	view nep or se	Bull Geoenge		
Q +9	Replay 2	X - 🕨 Go	🗣 Stream 🌆 Deci	ode 🔰 Keep: All sessions 👻 🕀 Any Proce	is 🌺 Find 🔣 Save 🔢 🔞 🏈 🏉 Browse 🔹 🛠 Clear Cache 🎢 TextWizard 🕼 Tearoff 🛛 MSDN Search	E.
	Result	Protocol	Host	URL ^	🕐 Statistics 👫 Inspectors 🛫 AutoResponder 🎯 Composer 🔽 Pitters 🗉 Log 🚍 Timeline	
0	200	HTTP	save defenitureer	244 with 260 and with 000 the part of the second states 1 202	Headers TectWess WebForms HexWess Auth Cookies Raw JSON XNL	
632	200	HTTP	www.default-searc	Reid=176baid=1009itype=r6yer=1307;	Ka Provu-Authorization Header is present	
(f) 3	200	HTTP	Tunnel to	vos-cm35.sso-44.com/443	No Prosy-Adenor Falleron Header To present.	A .
634	200	HTTPS	vos-cm35.ssp-44.com	1	Authorization Header (Negotiate) appears to contain a Kerberos tickets	
55	302	HTTPS	vos-cm35.sso-44.com	(conadmin/showHome.do	30 82 06 03 A0 30 30 2E 06 09 2A 86 48 82 F7 12 0 00* H +.	
56	302	HTTPS	vos-cm35.sso-44.com	/ssosp/samillogin?relayurl=%2Fccmadmir	28 06 01 04 01 82 37 02 02 1E 06 0A 28 06 01 04 + 7	
曲7	200	HTTP	Tunnel to	vos-cm44.sso-44.com/443	01 02 37 02 02 0A A2 02 05 CD 04 02 05 C9 60 02 . 74 .1E	
58	302	HTTPS	vos-cm44.sso-44.com	/ad/s/is/PSAMLRequest=nVLLbtswELznKv	82 05 84 30 82 05 80 A0 03 02 01 05 A1 03 02 01 . '0 . '	
2 9	401	HTTPS	vos-m44.ssp-44.com	ladisikia thintercated PSAM Beruester	0E A2 07 03 05 00 20 00 00 00 A3 82 04 3E 61 82	
10	200	HTTPS	vos-cm44.sso-44.com	/adfs/ls/auth/integrated/?SAMLRequestr	53 4F 20 34 34 2E 43 4F 40 A2 26 30 24 A0 03 02 50-44.COM4605	
(f) 11	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	73 20 63 60 34 34 26 73 73 6F 20 34 34 26 63 6F s-cm44.sso-44.co	
212	302	HTTPS	vos-cm35.sso-44.c	/ssosp/sami/S50/alias/vos-cm35.sso-44.c	60 A3 92 03 F7 30 92 03 F3 A0 03 02 01 17 A1 03 md .+0 .0	
5 13	302	HTTPS	vos-cm35.sso-44.c	/ssospirelay	aa 17 na ad 20 9a ne E7 ee de Ee no e7 en ne et 3 1 5 46 ha	-
<b>\$\$14</b>	200	HTTPS	vos-cm35.sso-44.c	(conadmin/showhtome.do	Get SyntaxWew Transformer Headers TextWew InageWew HexWew WebWew Auth Cach	ing
凸 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Contine Day ISON XM	- 1
16	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443		-
曲 17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Response Headers (How) Header Octivito	
m 18	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	HTTP/1.1 200 UK	
<u>m</u> 19	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Cache	-
<u>m</u> 20	200	HTTP	Tunnel to	vos-cm35.sso-44.com/0443	Cache-Control: no-cache	UU .
m 21	200	HTTP	Tunnel to	vos-cm35.sso-94.com/8443	Evolution of	
4		- In the	Ti post so	100 CH IS COL 01 CONVOLD?	Drama: nurarhe	•
DUGE	xec] ALT+0	2 > type HEI	JP		۲	
Hit Car	hains 1	al Descen	110	himmilium and an 44 confactories	i Ak bekara dari 1904 M Damarkardi i Maradi mela Tadiasi AD 475 M di SAD 2016 - 2015 M S 400 M A 400 M A 400 M A	
and Cab	caring	T A Proce	1/3	notes//vos-cinn4.sso-44.com/ad/s/s/ar	kriginke grade oprisering nederation in de tradingere zoone diveziet zoona diveziet and a second second second	294 J

Wenn der Authentifizierungstyp NTLM ist, sehen Sie am Anfang des Frames **Negotiate - NTLMSSP**, wie hier gezeigt:

🕅 Statistics 🔛 Inspectors 🚿 AutoResponder 🗳 Request Builder 🔲 Filters 🗉 Log 🚍 Timeline
Headers TextView WebForms HexView Auth Raw XML
No Proxy-Authorization Header is present.
Authorization Header is present: Negotiate
4E 54 4C 4D 53 53 50 00 03 00 00 00 18 00 18 00 NTLMSSP
48 00 00 00 10 00 10 00 58 00 00 00 10 00 10 00 HX
68 00 00 00 00 00 00 A8 00 00 05 82 88 A2 h
05 01 28 0A 00 00 0F 49 00 4E 00 54 00 57 00(I.N.T.W.

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.