# Kerberos met ADFS 2.0 voor SAML van eindgebruiker voor Jabber Configuration Voorbeeld

### Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configuratie Verifiëren Problemen oplossen

# Inleiding

Dit document beschrijft hoe u Kerberos kunt configureren met ADFS (Active Directory Federation Services) 2.0.

## Voorwaarden

#### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

#### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### Achtergrondinformatie

Voor de configuratie van één enkel teken (End User Security Assessment Markup Language, SAML) moeten Kerberos (SSO) en de configuratie worden geconfigureerd zodat de end User SAML SIP voor Jabber kan werken met domeinverificatie. Wanneer SAML SSO met Kerberos wordt geïmplementeerd, verwerkt Lichtgewicht Directory Access Protocol (LDAP) alle autorisatieen gebruikerssynchronisatie, terwijl Kerberos de authenticatie beheert. Kerberos is een verificatieprotocol dat bedoeld is om te worden gebruikt in combinatie met een instantie die met de LDAP is ingeschakeld.

Op Microsoft Windows- en Macintosh-machines die worden aangesloten op een Active Directorydomein, kunnen gebruikers moeiteloos inloggen in Cisco Jabber zonder dat ze een gebruikersnaam of wachtwoord moeten invoeren en worden ze niet eens een inlogscherm weergegeven. Gebruikers die niet op hun computers zijn aangemeld, zien nog steeds een standaard inlogformulier.

Omdat de authenticatie één enkel token gebruikt dat van de besturingssystemen wordt doorgegeven, is geen omleiding vereist. De token is geverifieerd tegen de geconfigureerde Key Domain Controller (KDC) en als deze geldig is, is de gebruiker aangemeld.

# Configuratie

Hier is de procedure om Kerberos met ADFS 2.0 te configureren.

- 1. Installeer Microsoft Windows Server 2008 R2 op een machine.
- 2. Installeer Active Directory Domain Services (ADDS) en ADFS op dezelfde machine.
- 3. Installeer Internet Information Services (IS) op de Microsoft Windows Server 2008 R2geïnstalleerde machine.
- 4. Maak een zelf-ondertekend certificaat voor ISIS.
- 5. Importeer het zelf-ondertekende certificaat in IS en gebruik het als HTTPS servercertificaat.
- 6. Installeer Microsoft Windows7 op een andere machine en gebruik dit als een client.

Wijzig de Domain Name Server (DNS) in de machine waar u ADDS hebt geïnstalleerd.

Voeg deze machine toe aan het domein dat u met de installatie van ADDS hebt gemaakt.

Ga naar **Start**.Klik met de rechtermuisknop op **Computer**.Klik op **Eigenschappen**.Klik aan de rechterkant van het venster op **Instellingen wijzigen**.Klik op het **tabblad Computer Name**.Klik op **Wijzigen**.Voeg het domein toe dat u hebt gemaakt.

				rasnaikn Sca
ystem Properties	8	<ul> <li>User Management</li> </ul>	t 👻 Bulk Administration 👻 Hel	<del>ب</del> ط
Computer Name/Domain Changes	lote			
You can change the name and the membership of this computer. Changes might affect access to network resources.	mputer			
Computer name:	y/s	Security   System	•   • +   S	Search Control Panel
JabberPC1		ania information	about your computer	•
Full computer name: JabberPC1.mangolab.com		s edition	about your computer	
More Member of Domain: mangolab.com Workgroup:	t ID	Iows 7 Professional right © 2009 Microso ce Pack 1 nore features with a n	ft Corporation. All rights reserve ew edition of Windows 7	
OK Cancel		ig: essor: Iled memory (RAM):	System rating is not available Intel(R) Xeon(R) CPU E7- 2870 2.00 GB	@ 2.40GHz 2.40 GHz
UK Cancel	Врру	im type:	64-bit Operating System	
t Circo Unified Commun		and louch:	No Pen or Touch Input is availa	able for this Display
	Comp	uter name, domain, and	workgroup settings	
upport please visit our	Co	mputer name:	JabberPC1	😵 Change settings
	Fu	Il computer name:	JabberPC1.mangolab.com	
	Co	mputer description:	JabberPC1	
See also	Do	main:	mangolab.com	
Action Center	Windo	ws activation		
Windows Update	Wi	ndows is activated		
Performance Information ar Tools	nd Pro	oduct ID: 00371-221-876	7124-86146 Change product i	sy genuine Microsoft

7. Controleer of de Kerberos-service op beide machines genereert.

Meld u aan als beheerder in de servermachine en open de opdrachtmelding. Voert vervolgens deze opdrachten uit:

cd \windows\System32Klist tickets

C:\Users	s\Administrator.WIN2K8>cd \windows\System32
C:∖Windo	ows\System32>Klist tickets
Current	LogonId is 0:0x3d6072
Cached I	lickets: <1>
#0>	Client: Administrator @ 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 18:06:04 (local) End Time: 12/11/2014 4:06:04 (local) Renew Time: 12/17/2014 18:06:04 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96

Log in als domeingebruiker op de client en voer dezelfde opdrachten uit.

C:\Users\rashaikh>cd \windows\System32
C:\Windows\System32>Klist tickets
Current LogonId is 0:0x558ba
Cached Tickets: <5>
#0> 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</local></local></local>
11> Client: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40e00000 -> 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
#2> 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
Ate 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
43> 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
Ate 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
44> 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
te 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-CTS-HMAC-SHA1-96
C:\Windows\System32>

8. Maak de ADFS Kerberos-identiteit op de machine waar u ADDS installeerde.

De Microsoft Windows-beheerder inlogt in het Microsoft Windows-domein (als <naam>\beheerder), bijvoorbeeld in de Microsoft Windows-domeincontroller, maakt de ADFS Kerberos-identiteit aan. De ADFS HTTP-service moet een Kerberos-identiteit hebben, die een Service Principal Name (SPN) wordt genoemd in deze indeling: HTTP/DNS\_name\_of\_ADFS\_server.

Deze naam moet in kaart worden gebracht aan de Active Directory-gebruiker die de ADFS

HTTP-serverinstantie vertegenwoordigt. Gebruik het Microsoft Windows **software**hulpprogramma dat standaard beschikbaar zou moeten zijn op een Microsoft Windows 2008server.

Procedure Registreer de SPN's voor de ADFS-server. Draai de **ingestelde** opdracht op de Active Directory-controller.

Bijvoorbeeld, wanneer de ADFS-host **adfs01.us.renovations.com** is en het Active Directorydomein **US.RENOVATIONS.COM** is, is de opdracht:

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

Het **HTTP**/gedeelte van de SPN is van toepassing, ook al heeft de ADFS-server doorgaans toegang tot Secure Socket Layer (SSL), wat HTTPS is.

Controleer of de SPN's voor de ADFS-server goed met de **ingestelde** spn-opdracht zijn gemaakt en bekijk de uitvoer.

setspn -L



9. Configureer de instellingen van de Microsoft Windows-client.

Navigeer naar **Gereedschappen > Internet-opties > Geavanceerd** om geïntegreerde Windows-verificatie in te schakelen.

Controleer het vakje Geïntegreerde Windows-verificatie inschakelen:

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 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>Enable DON Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable networy protection to help mitigate online attacks*</li> <li>Enable native XMLHTTP support</li> <li>Enable SmartScreen Filter</li> <li>Takes effect after you restart Internet Evelorer</li> </ul>
Parters effect after you restart internet Explorer
Restore advanced settings
Reset Internet Explorer settings Resets Internet Explorer's settings to their default condition. You should only use this if your browser is in an unusable state.
OK Cancel Apply

Navigeer naar Gereedschappen > Internet-opties > Beveiliging > Lokaal intranet > Aangepast niveau... om alleen de optie Automatisch aanmelden in Intranet zone te selecteren.

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

Navigeer naar Gereedschappen > Internet-opties > Beveiliging > Lokaal intranet > Sites > Geavanceerd om de URL van inbraakdetectie en -preventie (IDP) aan lokale intranet toe te voegen.

**Opmerking:** Controleer alle vinkjes in het dialoogvenster Local Intranet en klik op het **tabblad Advanced**.

Internet Options           General         Security         Privacy         Content         Connections         Programs         Advance	23 → A R C × dtb Cisco Unified Serviceability ×
Select a zone to view or change security settings.	Local intranet S
Security level for this zone Allowed levels for this zone: All - Alpropriate for websites on your local network - (ntranet) - Nost 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)	What are intranet settings?       Advanced       OK       Cancel         Local intranet       Image: Comparison of the comparison of th
Custom level Default level Reset all zones to default level OK Cancel Apply	Add () Websites: https:// <hostname idp="" of=""> Remove</hostname>
	Close

Navigeer naar Gereedschappen > Beveiliging > Vertrouwde sites > Plaatsen om de CUCM-

hostnamen aan Trusted-sites toe te voegen:

	_
Internet Options	
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 Stes	Add
<ul> <li>trust not to damage your computer or your files.</li> <li>You have websites in this more</li> </ul>	Webstes:
	https:// CUCM1.domainname.com Remove
Security level for this zone	https:// CUCM2.domainname.com
Allowed levels for this zone: All	2.5
- Medium	
Prompts before downloading potentially unsafe     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 Deraut level	and local country laws governing import, export, transfer and use. De
Reset all zones to default level	with U.S. and local country laws. By using this product you agree to co
robes di serier se del due lever	und at our Export Compliance Product Rep
	ur <u>Unified Communications System Docum</u> Loading, please
OK Cancel Apply	

## Verifiëren

In deze sectie wordt uitgelegd hoe u controleert welke verificatie (Kerberos of NT LAN Manager (NTLM) wordt gebruikt.

- 1. Download het Verkenner gereedschap naar uw clientmachine en installeer het.
- 2. Sluit alle Internet Explorer-vensters.
- 3. Draai het gereedschap Fuzler en controleer of de optie **Opname verkeer** is ingeschakeld onder het menu Bestand.

Fiddler werkt als een passthrough-proxy tussen de client en de server en luistert naar al het verkeer, waarbij tijdelijk de instellingen van Internet Explorer op deze manier worden ingesteld:

Local Area	Network (LA	N) Settings	-	23
Automa Automa use of r Auto Use Add	tic configuration nanual setting matically detenation automatic con	on on may override manual settings. To s, disable automatic configuration. ect settings figuration script	ensu	re the
Proxy setting	a proxy serve up or VPN con ings	r for your LAN (These settings will not nections).	app	ly to
Servers	Type HTTP: Secure: FTP: Socks:	Proxy address to use           127.0.0.1           127.0.0.1           ame proxy server for all protocols	; ] : [ ] : [ ] : [	Port 8888 8888
Exception	Do not use p <-loopback Use semicolo	roxy server for addresses beginning v	with:	*

- 4. Open Internet Explorer, blader in de URL van de CRM-server (Customer Relation Management) en klik op een paar koppelingen om verkeer te genereren.
- 5. Raadpleeg het hoofdvenster van Fidler en kies een van de frames waarin het resultaat 200 is (succes):

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 m6 .+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 Oetrito	
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: nucarhe	•
DUGE	xec] ALT+0	2 > type HEI	JP		۲	
Hit Car	hains 1	al Descen	110	himmilium and an 44 contations	i Ak bekara da 1920an Damarkani i Maradi weka Tadiwi K.D. 27-240 da 200 2014 wekati kiti katake 2014 K.D. 1920 K.D.	
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 zonwab gree Babies verwet Babies werden gg	294 J

Als het verificatietype NTLM is, dan ziet u **Negotiate - NTLMSSP** in het begin van het frame zoals hier wordt getoond:

🕅 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.

### Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.