# SAML SFS-instellingen configureren met Kerberos-verificatie

### Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren AD FS configureren browser configureren Microsoft Internet Explorer Mozilla FireFox Verifiëren Problemen oplossen

### Inleiding

In dit document wordt beschreven hoe u Active Directory en Active Directory Federation Service (AD FS) versie 2.0 kunt configureren om Kerberos-verificatie door Jabber Clients (alleen Microsoft Windows) te kunnen gebruiken, waardoor gebruikers inloggen met hun Microsoft Windows-inlognaam en niet worden gevraagd naar aanmeldingsgegevens.

**Voorzichtig:** Dit document is gebaseerd op een labomgeving en gaat ervan uit dat u zich bewust bent van de impact van veranderingen die u maakt. Raadpleeg de relevante productdocumentatie om het effect van veranderingen te begrijpen.

## Voorwaarden

### Vereisten

Cisco raadt u aan:

- AD FS versie 2.0 geïnstalleerd en geconfigureerd met Cisco Collaboration-producten als Relay Party Trust
- Collaboration-producten zoals Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN) en CUCM-enabled voor het gebruik van Security Association Markup Language (SAML) met één aanmelding (SSO)

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Active Directory 2008 (Hostname: ADFS1.ciscolive.com)
- AD FS versie 2.0 (Hostname: ADFS1.ciscolive.com)
- CUCM (Hostname: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versie 1.0
- Mozilla Firefox versie 3.4
- Telerik Fidler versie 4

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.

## Configureren

### AD FS configureren

1. Configureer AD FS versie 2.0 met Service Principal Name (SPN) om de clientcomputer waarop Jabber is geïnstalleerd in staat te stellen om tickets te vragen, zodat de clientcomputer op zijn beurt kan communiceren met een AD FS-dienst.



Raadpleeg <u>AD FS 2.0: Het configureren van de SPN (servicePrincipalName) voor de</u> <u>servicekaccount</u> voor meer informatie.

 Zorg ervoor dat de standaardverificatieconformatie voor de AD FS-service (C:\inetpub\adfs\ls\web.config) Geïntegreerde Windows-verificatie is. Zorg ervoor dat deze niet is gewijzigd in Formulier-gebaseerde verificatie.

<microsoft.identityserver.web></microsoft.identityserver.web>
<localauthenticationtypes></localauthenticationtypes>
<add name="Integrated" page="auth/integrated/"></add>
<pre><add name="Forms" page="FormsSignIn.aspx"></add></pre>
<add name="TlsClient" page="auth/sslclient/"></add>
<add name="Basic" page="auth/basic/"></add>
<commondomaincookie reader="" writer=""></commondomaincookie>
<context hidden="true"></context>
<pror page="Error.aspx"></pror>
<pre><acceptedfederationprotocols saml="true" wsfederation="true"></acceptedfederationprotocols></pre>
<pre><homerealmdiscovery page="HomeRealmDiscovery.aspx"></homerealmdiscovery></pre>
<pre><persistidentityproviderinformation enabled="true" lifetimeindays="30"></persistidentityproviderinformation></pre>
<singlesignon_enabled="true"></singlesignon_enabled="true">

 Selecteer Windows-verificatie en klik op Geavanceerde instellingen onder het rechter deelvenster. Schakel in het geval van geavanceerde instellingen de optie Kernel-modeverificatie uit, zorg ervoor dat de uitgebreide bescherming uit is en klik op OK.



4. Zorg ervoor dat AD FS versie 2.0 zowel het Kerberos-protocol als het NTLM-protocol (NT LAN Manager) ondersteunt omdat alle niet-Windows-clients Kerberos niet kunnen gebruiken en niet op NTLM kunnen vertrouwen.

Selecteer in het rechter deelvenster de optie **Leveranciers** en zorg ervoor dat **onderhandeling** en **NTLM** aanwezig zijn onder Ingeschakelde providers:



**Opmerking:** AD FS geeft de onderhandelingstafel over wanneer de Geïntegreerde Windowsauthenticatie wordt gebruikt om clientverzoeken te authentiseren. De onderhandelingshoofdlijst laat klanten tussen Kerberos authenticatie en NTLM authenticatie selecteren. In het onderhandelingsproces wordt Kerberos-verificatie geselecteerd, tenzij een van deze voorwaarden waar is:

- Een van de systemen die bij de authenticatie betrokken is, kan geen Kerberos-authenticatie gebruiken.

- De oproepende toepassing verschaft niet voldoende informatie om Kerberos-authenticatie te gebruiken.

- Om het onderhandelingsproces in staat te stellen het Kerberos-protocol voor netwerkverificatie te selecteren, moet de clienttoepassing een SPN-, een User Principal Name (UPN) of een Network Basic I/O System (Netopgemerkt)-naam als doelnaam bieden. Anders selecteert het onderhandelingsproces altijd het NTLM-protocol als de meest geprefereerde authenticatiemethode.

#### browser configureren

#### **Microsoft Internet Explorer**

1. Zorg ervoor dat Internet Explorer > Geavanceerd > Geïntegreerde Windows-verificatie

inschakelen is ingeschakeld.

Internet Options						
General Security Privacy Content Connections Programs Advanced						
Settings						
<ul> <li>Do not submit unknown addresses to your auto-search pro</li> <li>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 invi</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 clc</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable Integrated Windows Authentication*</li> </ul>						
*Takes effect after you restart Internet Explorer						
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						

2. Voeg AD FS URL toe onder **Security >Intranet zones > sites**.

Internet Options	8 23					
General Security Privacy Content Connections Pro	ograms Advanced					
Select a zone to view or change security settings.						
🤮 👒 🗸 🕓						
Internet Local intranet Trusted sites Restrict sites	ted					
Local intranet This zone is for all websites that are found on your intranet.	Sites					
Local intranet	23					
Use the settings below to define which websites at the local intranet zone.	re included in					
Automatically detect intranet network						
Include all local (intranet) sites not listed in	other zones					
Include all sites that bypass the proxy serv	er					
Include all network paths (UNCs)						
What are intranet settings? Advanced OK	Cancel					
Local intranet	<b>—</b>					
You can add and remove websites from this zor this zone will use the zone's security settings.	ne. All websites in					
Add this website to the zone:						
Add						
Websites:						
adfs1.ciscolive.com	Remove					

3. Voeg de CUCM, IMP, en Unity hostname toe aan **Security >Trusted sites**.

Internet Options	8 8				
General Security Privacy Content Connections Prog	rams Advanced				
Select a zone to view or change security settings.					
🥥 🔩 🗸 🚫					
Internet Local intranet Trusted sites Restricted sites	d				
Trusted sites	Sites				
Trusted sites					
You can add and remove websites from this zone this zone will use the zone's security settings. Add this website to the zone:	e. All websites in				
Websites:					
cucm1.ciscolive.com	Remove				
imp1.ciscolive.com					
Require server verification (https:) for all sites in this zone					
	Close				

4. Zorg ervoor dat Internet-exporteur > beveiliging > Lokaal intranet > Beveiligingsinstellingen > Gebruikersverificatie - Aanmelden is ingesteld om intranetsites te kunnen gebruiken.

Internet Options	
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	S Enable XSS filter
Local intranet	Oisable     Enable
This zone is for all websites that are found on your intranet	Scripting of Java applets
	Disable     Enable
<ul> <li>Security level for this zone</li> </ul>	O Prompt
Allowed levels for this zone: All	St. Logon
- Medium-low	Anonymous logon
(intranet)	Automatic logon only in Intranet zone     Automatic logon with current user name and password
- Unsigned ActiveX controls will not	Prompt for user name and password
Enable Protected Mode (requires restartin	< <u> </u>
Custom level	*Takes effect after you restart Internet Explorer
	Reset custom settings
Reset all zo	Reset to: Medium-low (default)   Reset
ОК	OK Cancel

#### Mozilla FireFox

1. Open Firefox en voer **over:fig** in de adresbalk in.



2. Klik ik zal voorzichtig zijn.

	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!
l	

3. Dubbelklik op de **naam** Preferentie **network.onderhandelingen-auth.allow-non-fqdn** om **waar** te zijn en **network.onderhandelingen-auth.vertrouwde-uris** naar **ciscolive.com**, **adfs1.ciscolive.com** om te wijzigen.

Seegch: network.n			
Preference Name	<ul> <li>Status</li> </ul>	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-Im-response	default	boolean	false

4. Sluit Firefox en open deze opnieuw.

### Verifiëren

Om te controleren of de SPN's voor de AD FS-server goed zijn gemaakt, voert u de **ingestelde** spn-opdracht in en geeft u de uitvoer weer.



Controleer of de clientmachines Kerberos-tickets hebben:

C:\Windows\system32\cmd.exe	x
C:\Users\user1.CISCOLIVE>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>	

Voltooi deze stappen om te verifiëren welke verificatie (Kerberos of NTLM-verificatie) in gebruik is.

- 1. Download het gereedschap van de Fidler aan uw clientmachine en installeer het.
- 2. Sluit alle Microsoft Internet Explorer-vensters.
- 3. Start het bestandsindeling en controleer of de optie **Opname verkeer** is ingeschakeld in het menu Bestand. Fiddler werkt als een passthrough-proxy tussen de client en de server en luistert naar al het verkeer.
- 4. Open Microsoft Internet Explorer, blader in de CUCM en klik op bepaalde koppelingen om verkeer te genereren.
- 5. Raadpleeg het hoofdvenster van FormFiller en kies een van de frames waarin het resultaat **200** is (succes) en u kunt Kerberos als verificatiemechanisme zien

🚸 Fid	dler Web I	Debugger				× D
File E	dit Rules	Tools Vi	ew Help GET /bo	ook 🔝 GeoEdge		
9	Replay 🕻	K - 🕨 Go	🗣 Stream 👸	Decode Keep: All sessions *	Any Any	y 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	- 22	Headers TextWew WebForms HexView Auth Cookies Raw JSON XML
= 3	200	HTTP	cucm.ciscolive	/favicon.ico	1	No Provy-Authorization Header is present.
54	302	HTTP	cucm.ciscolive	/ccmadmin/showHome.do		
1 5	200	HTTP	Tunnel to	cucm.ciscolive.com:443		Authorization Header (Negotiate) appears to contain a Kerberos ticket:
<b>5</b> 6	302	HTTPS	cucm.ciscolive	/comadmin/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		
<u> </u>	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 00 0F 7E AF 60 90 38 D7 F3 E2 F4 5E 84~ ;XOMO^ E6 0F 74 85 2D A3 12 04 10 01 00 00 00 F5 17 A7 z.t -f
10	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	€	50 2D 22 9A 84 00 00 00 00 P-"
8 11	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	- 2	J 🗵
<> <u>12</u>	200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?		Get Syntaxiliew Transformer Headers TextView ImageView Herview WebView
Ø 13	502	HTTP	www.downioa	/msdownload/update/v3/s		
14	401	HTTPS	adfs1.ciscoliv	/favicon.ico	e	Auth Cadning Cookies Raw JSON XML
首 15	200	HTTP	Tunnel to	cucm.ciscolive.com:8443		No Proxy-Authenticate Header is present.
5 16	302	HTTPS	cucm.ciscolive	/ssosp/sami/SSO/alias/CU		WWW-Authenticate Header (Negotiate) appears to be a Kerberos reply:
<b>F</b> 17	403	HTTPS	cucm.ciscolive	/ssosp/relay	- 1	A1 18 30 19 A0 03 0A 01 00 A3 12 04 10 01 00 00 i.0
18	200	HTTPS	cucm.ciscolive	/ciscologo.gif		
Ø 19	502	HTTP	www.downioa	/msdownload/update/v3/s		
Ø 20	502	HTTP	www.downioa	/msdownload/update/v3/s	_	
					. Č	
		_			<u> </u>	
Quide	IQUIXEExecj ALT+Q > type HELP					
👯 Cap	oturing	👻 All Proce	19905	1 / 20 Download Progress	0 byter	s. Hit F5 to refresh.

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

🚸 Fidd	ler Web (	)ebugger			
File Ed	it Rules	Tools Vie	ew Help GET /bo	ok 🔛 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 🗍 🗖 Filters 🕒 Log 🚍 Timeline
<b>Ø</b> 1	502	HTTP	www.bing.com	/favicon.ico	Headers TextVew WebForms HexVew Auth Cookies Raw JSON XML
≪≱2	200	HTTP	cucm.ciscolive	1	S, he forest to be been and the second s
2 3	200	HTTP	cucm.ciscolive	/ciscologo.gif	NO Proxy-Authorization Header is present.
= 4	200	HTTP	cucm.ciscolive	/favicon.ico	1, Authorization Header is present: NTLM
N 5	302	HTTP	cucm.ciscolive	/comadmin/showHome.do	58 00 00 00 00 00 00 05 8 00 00 00 00 00 00 00 00 00 7
<u>6</u> 6	200	HTTP	Tunnel to	cucm.ciscolive.com:443	58 00 00 00 00 00 00 05 58 00 00 00 00 00 00 00 XXX.
07	502	нттр	www.downloa	/msdownload/update/v3/s	06 01 81 1D 00 00 00 0F 4E 84 C3 AA 0D D1 81 34
58	302	HTTPS	cucm.ciscolive	/comadmin/showHome.do	78 AA CE A9 41 F3 D1 31 Xº18AÓÑ1
59	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl	
10	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	-[NTLM Type3: Authentication]
5 11	302	HTTPS	adfs1.ciscoliv	/adfs/ls/75AMLRequest=n	California Transformer 2000000 Tealiton Investigation Under
12 12	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	6, Get Syntaxivew Transformer THeaders Textivew Imageview Hexivew Webview
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 [Rew] [Header Definitions
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, Date: Sat, 17 Jan 2015 20:05:06 GMT
<b>2</b> 19	200	HTTPS	cucm.ciscolive	/ciscologo.gif	Expires: -1
					Pragma: no-cache
•					Cookies / Login
[QuidEx	ec] ALT+C	) > type HE	LP		
Tie Capt	uring	Al Proce	sses	1 / 19 https://adfs1.ciscol	olive.com/adfs/ls/auth/integrated/?SAMLRequest=nVLLbtswELznKwjebYryIwphGX8sFDWQNErk9NDbl48CRS5VJp%28%

# Problemen oplossen

Als alle configuratie- en verificatiestappen zijn voltooid zoals in dit document wordt beschreven en u nog steeds inlogproblemen hebt, moet u een Microsoft Windows Active Directory / AD FS-beheerder raadplegen.