# Configuration de SAML SSO avec authentification Kerberos

### Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Configurer AD FS Configurer le navigateur Microsoft Internet Explorer Mozilla FireFox Vérification Dépannage

### Introduction

Ce document décrit comment configurer Active Directory et Active Directory Federation Service (AD FS) Version 2.0 afin de lui permettre d'utiliser l'authentification Kerberos par des clients Jabber (Microsoft Windows uniquement), qui permet aux utilisateurs de se connecter avec leur connexion Microsoft Windows et de ne pas être invités à entrer des informations d'identification.

Attention : Ce document est basé sur un environnement de travaux pratiques et suppose que vous connaissez l'impact des modifications que vous apportez. Reportez-vous à la documentation produit pertinente afin de comprendre l'impact des modifications que vous apportez.

### Conditions préalables

#### **Conditions requises**

Cisco recommande que vous ayez :

- AD FS version 2.0 installé et configuré avec les produits de collaboration Cisco en tant que confiance de la partie de confiance
- Produits de collaboration tels que la messagerie instantanée et la présence de Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN) et CUCM activés afin

d'utiliser le langage de balisage de sécurité (SAML) SSO (Single Sign-on)

### **Components Used**

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Active Directory 2008 (Nom d'hôte : ADFS1.ciscolive.com)
- AD FS version 2.0 (nom d'hôte : ADFS1.ciscolive.com)
- CUCM (nom d'hôte : CUCM1.ciscolive.com)
- Microsoft Internet Explorer version 10
- Mozilla Firefox version 34
- Telerik Fiddler Version 4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configuration

### **Configurer AD FS**

 Configurez AD FS version 2.0 avec le nom principal de service (SPN) afin d'activer l'ordinateur client sur lequel Jabber est installé pour demander des tickets, ce qui permet à son tour à l'ordinateur client de communiquer avec un service AD FS.



Reportez-vous à <u>AD FS 2.0 : Comment configurer le SPN (servicePrincipalName) pour le</u> <u>compte de service</u> pour plus d'informations.

 Assurez-vous que la configuration d'authentification par défaut pour le service AD FS (dans C:\inetpub\adfs\ls\web.config) est Authentification Windows intégrée. Assurez-vous qu'il n'a pas été modifié en Authentification basée sur les formulaires.

<pre><microsoft.identityserver.web>     <li><localauthenticationtypes>         <add name="Integrated" page="auth/integrated/"></add></localauthenticationtypes></li></microsoft.identityserver.web></pre>
<add name="Forms" page="Forms" signifi.aspx=""></add>
<add name="inscrient" page="auri/ssicrient/"></add>
<add_name=_basicpage=_autn _="" basic=""></add_name=_basicpage=_autn>
<commondomaincookie reader="" writer=""></commondomaincookie>
<context hidden="true"></context>
<error page="Error.aspx"></error>
<pre><acceptedfederationprotocols saml="true" wsfederation="true"></acceptedfederationprotocols></pre>
<pre><homerealmdiscovery page="HomeRealmDiscovery.aspx"></homerealmdiscovery></pre>
<pre><pre>consistIdentityProviderInformation enabled="true" lifetimeInDays="30" /&gt;</pre></pre>
<pre><singlesignon enabled="true"></singlesignon></pre>
y me over er wenere, ver rennev.

 Sélectionnez Authentification Windows et cliquez sur Paramètres avancés dans le volet de droite. Dans Paramètres avancés, décochez Activer l'authentification en mode noyau, assurez-vous que la protection étendue est désactivée, puis cliquez sur OK.



4. Assurez-vous qu'AD FS version 2.0 prend en charge le protocole Kerberos et le protocole NTLM (NT LAN Manager), car tous les clients non Windows ne peuvent pas utiliser Kerberos et utiliser NTLM.

Dans le volet de droite, sélectionnez **Fournisseurs** et assurez-vous que **Négocier** et **NTLM** sont présents sous Fournisseurs activés :



**Note**: AD FS transmet l'en-tête de sécurité Negotiate lorsque l'authentification Windows intégrée est utilisée afin d'authentifier les requêtes client. L'en-tête de sécurité Negotiate permet aux clients de sélectionner entre l'authentification Kerberos et l'authentification NTLM. Le processus de négociation sélectionne l'authentification Kerberos, sauf si l'une de ces conditions est vraie :

- Un des systèmes impliqués dans l'authentification ne peut pas utiliser l'authentification Kerberos.

- L'application appelante ne fournit pas suffisamment d'informations pour utiliser l'authentification Kerberos.

- Pour permettre au processus de négociation de sélectionner le protocole Kerberos pour l'authentification réseau, l'application cliente doit fournir un nom de compte SPN, un nom d'utilisateur principal (UPN) ou un nom de compte NetBIOS (Network Basic Input/Output System) comme nom cible. Sinon, le processus de négociation sélectionne toujours le protocole NTLM comme méthode d'authentification préférée.

#### Configurer le navigateur

#### **Microsoft Internet Explorer**

1. Assurez-vous que Internet Explorer > Advanced > Enable Integrated Windows Authentication

est coché.

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 invo</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>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable Integrated Windows Authentication*</li> </ul>		
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. Ajoutez l'URL AD FS sous **Sécurité >Zones Intranet > Sites**.

Internet Options			
General Security Privacy Content Connections Pro	ograms Advanced		
Select a zone to view or change security settings.			
🧶 👒 🗸 🚫			
Internet Local intranet Trusted sites Restrict sites	ed		
Local intranet	<b>C</b> 't		
This zone is for all websites that are	Sites		
Local intranet	23		
Use the settings below to define which websites as 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			
You can add and remove websites from this zor	ne. All websites in		
this zone will use the zone's security settings.	]		
Add this website to the zone:	Add		
Websitzer			
adfs1.ciscolive.com	Remove		

3. Ajoutez les noms d'hôte CUCM, IMP et Unity à Security >Trusted Sites.

Internet Options		
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	
Trusted sites		
You can add and remove websites from this zon 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		
ucxn1.ciscolive.com		
Require server verification (https:) for all sites in this	zone	
	Close	

4. Assurez-vous que Internet Explorer > security > Local Intranet > Security Settings > User Authentication - Logon est configuré afin d'utiliser les informations d'identification de connexion pour les sites intranet.

Internet Options	83
General Security Privacy Content Connections	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 This zone is for all websites that are found on your intranet.	Disable     Disable     Enable     Scripting of Java applets     Disable
Security level for this zone Allowed levels for this zone: All - Allowed levels for this zone: All - Appropriate for websites on your (intranet) - Most content will be run without pro- - Unsigned ActiveX controls will not - Same as Medium level without pro-	Disable     Prompt     Pi     Disable     Pi     Pi     Disable     Pi     Disable     Pi     Pi     Disable     Pi     Pi
Enable Protected Mode (requires restartin	*Takes effect after you restart Internet Explorer
Reset all zo	Reset custom settings Reset to: Medium-low (default)   Reset
ОК	OK Cancel

#### Mozilla FireFox

1. Ouvrez Firefox et entrez **about:config** dans la barre d'adresse.



2. Cliquez sur Je serai prudent, je vous le promets !

1	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. Double-cliquez sur le nom de préférence **network.negotiation-auth.allow-non-fqdn** pour **true** et **network.negotiation-auth.trust-uris** pour **ciscolive.com**, **adfs1.ciscolive.com** afin de modifier.

Status	Туре	Value
default	boolean	false
default	boolean	true
user set	boolean	true
default	boolean	true
default	string	
default	string	
user set	string	adfs1.adfs1.ciscolive.com.ciscolive.com
default	boolean	true
default	boolean	false
	Status default	Status Type     default boolean     default boolean     default boolean     default boolean     default string     default string     user set string     default boolean     default boolean

4. Fermez Firefox et rouvrez-vous.

### Vérification

I

Afin de vérifier que les SPN du serveur AD FS sont correctement créés, entrez la commande **setspn** et affichez le résultat.

```
Administrator: Command Prompt

Microsoft Windows [Version 6.1.7601]

Copyright (c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -L sso

Registered ServicePrincipalNames for CN=Saml SSO, CN=Users, DC=ciscolive, DC=com:

HITP/adfs1

C:\Users\Administrator>_
```

Vérifiez si les ordinateurs clients ont des tickets Kerberos :

```
C:\Windows\system32\cmd.exe
C:\Users\user1.ClSCOLIUE>Klist tickets
Current LogonId is 0:0xabc6d
Cached Tickets: 
Client: user1 @ ClSCOLIUE.COM
Server: krbtgt/ClSCOLIUE.COM @ ClSCOLIUE.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)
Renew Time: 1/24/2015 6:52:47 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start Time: 1/17/2015 20:52:47 (local)
Renew Time: 1/24/2015 20:52:47 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start Time: 1/17/2015 20:52:47 (local)
Renew Time: 1/18/2015 6:52:47 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start 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.CISCOLIUE>_
```

Complétez ces étapes afin de vérifier quelle authentification (authentification Kerberos ou NTLM) est utilisée.

- 1. Téléchargez l'outil Fiddler sur votre ordinateur client et installez-le.
- 2. Fermez toutes les fenêtres de Microsoft Internet Explorer.
- 3. Exécutez l'outil Fiddler et vérifiez que l'option **Capture Traffic** est activée dans le menu Fichier. Fiddler fonctionne comme un proxy de transfert entre la machine cliente et le serveur et écoute tout le trafic.
- 4. Ouvrez Microsoft Internet Explorer, accédez à CUCM et cliquez sur quelques liens pour générer du trafic.
- 5. Reportez-vous à la fenêtre principale de Fiddler et choisissez l'une des trames où le résultat est **200** (réussite) et vous pouvez voir Kerberos comme mécanisme d'authentification



6. Si le type d'authentification est NTLM, vous voyez **Negotiate - NTLMSSP** au début de la trame, comme indiqué ici.

🚸 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
5 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>Z</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%

# Dépannage

Si toutes les étapes de configuration et de vérification sont effectuées comme décrit dans ce document et que vous avez toujours des problèmes de connexion, vous devez consulter un administrateur Microsoft Windows Active Directory / AD FS.