# Configuración de SAML SSO con autenticación Kerberos

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Configurar AD FS Configurar explorador Microsoft Internet Explorer Mozilla FireFox Verificación Troubleshoot

## Introducción

Este documento describe cómo configurar Active Directory y Active Directory Federation Service (AD FS) versión 2.0 para permitirle utilizar la autenticación Kerberos por parte de los clientes Jabber (sólo Microsoft Windows), que permite a los usuarios iniciar sesión con su inicio de sesión de Microsoft Windows y no se les solicita las credenciales.

**Precaución:** Este documento se basa en un entorno de laboratorio y asume que es consciente del impacto de los cambios que realiza. Consulte la documentación del producto correspondiente para comprender el impacto de los cambios que realice.

# Prerequisites

#### Requirements

Cisco recomienda que tenga:

- AD FS versión 2.0 instalada y configurada con productos de Cisco Collaboration como confianza de terceros
- Productos de colaboración como Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN) y CUCM habilitados para utilizar el lenguaje de marcado de aserción de seguridad (SAML) Single Sign-on (SSO)

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Active Directory 2008 (Nombre de host: ADFS1.ciscolive.com)
- AD FS versión 2.0 (nombre de host: ADFS1.ciscolive.com)
- CUCM (Nombre de host: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versión 10
- Mozilla Firefox versión 34
- Telerik Fiddler Versión 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.

# Configurar

#### Configurar AD FS

1. Configure AD FS versión 2.0 con Service Principal Name (SPN) para habilitar el equipo cliente en el que Jabber está instalado para solicitar entradas, lo que a su vez permite que el equipo cliente se comunique con un servicio AD FS.



Consulte <u>AD FS 2.0: Cómo Configurar el SPN (servicePrincipalName) para la Cuenta de</u> <u>Servicio</u> para obtener más información.

 Asegúrese de que la configuración de autenticación predeterminada para el servicio AD FS (en C:\inetpub\adfs\ls\web.config) sea Autenticación integrada de Windows. Asegúrese de que no se haya cambiado a Autenticación basada en formulario.

<pre><microsoft.identityserver.web> <li><localauthenticationtypes></localauthenticationtypes></li></microsoft.identityserver.web></pre>
<pre><add name="Integrated" page="auth/integrated/"></add></pre>
<add name="Forms" page="FormsSignIn.aspx"></add>
<add name="TlsClient" page="auth/sslclient/"></add>
<add_name="basic" page="auth/basic/"></add_name="basic">
<commondomaincookie reader="" writer=""></commondomaincookie>
<context hidden="true"></context>
<pre><error page="Error.aspx"></error></pre>
<pre><acceptedfederationprotocols saml="true" wsfederation="true"></acceptedfederationprotocols></pre>
<homereaimdiscovery page="HomeReaImDiscovery.aspx"></homereaimdiscovery>
<pre><persistidentityproviderinformation enabled="true" lifetimeindays="30"></persistidentityproviderinformation></pre>
<pre><singlesignon enabled="true"></singlesignon></pre>

 Seleccione Autenticación de Windows y haga clic en Configuración avanzada en el panel derecho. En Advanced Settings, desmarque Enable Kernel-mode authentication, asegúrese de que Extended Protection esté Off y haga clic en OK.



4. Asegúrese de que AD FS versión 2.0 admita tanto el protocolo Kerberos como el protocolo NT LAN Manager (NTLM) porque todos los clientes que no son de Windows no pueden utilizar Kerberos y confían en NTLM.

En el panel derecho, seleccione **Proveedores** y asegúrese de que **Negociar** y **NTLM** estén presentes en Proveedores habilitados:



**Nota:** AD FS pasa el encabezado Negotiate security cuando se utiliza la autenticación integrada de Windows para autenticar las solicitudes del cliente. El encabezado de seguridad Negotiate permite a los clientes seleccionar entre la autenticación Kerberos y la autenticación NTLM. El proceso Negotiate selecciona la autenticación Kerberos a menos que una de estas condiciones sea verdadera:

- Uno de los sistemas involucrados en la autenticación no puede utilizar la autenticación Kerberos.

- La aplicación que llama no proporciona información suficiente para utilizar la autenticación Kerberos.

 Para habilitar el proceso Negotiate para seleccionar el protocolo Kerberos para la autenticación de red, la aplicación cliente debe proporcionar un SPN, un nombre de usuario principal (UPN) o un nombre de cuenta de Network Basic Input/Output System (NetBIOS) como nombre de destino. De lo contrario, el proceso Negotiate siempre selecciona el protocolo NTLM como el método de autenticación preferido.

#### Configurar explorador

#### **Microsoft Internet Explorer**

1. Asegúrese de que Internet Explorer > Advanced > Enable Integrated Windows

Authentication esté marcado.

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 involved of the signature is involved for publisher's certificate revocation</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 do</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable Integrated Windows Authentication*</li> <li>Takes effect after you restart Internet Explorer</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. Agregue AD FS URL bajo Security >Intranet zones > sites.

Internet Options	8
General Security Privacy Content Connections Programs Advar	iced
Calantin anna ta vísus as changes ann site antifana	
Select a zone to view or change security settings.	٦
Internet Local Intranet Trusted sites Restricted sites	
Local intranet This zone is for all websites that are found on your intranet. Sites	
Local intranet	x
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 Cance	
Local intranet	×
You can add and remove websites from this zone. All websites this zone will use the zone's security settings.	in
Add this website to the zone:	
Add	
Websites:	
Remove	

3. Agregue los nombres de host CUCM, IMP y Unity a **Security >Trusted sites**.

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 Restricter sites	d			
Trusted 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 this website to the zone:				
	Add			
Websites:				
cucm1.ciscolive.com	Remove			
imp1.ciscolive.com				
ucxn1.ciscolive.com				
Require server verification (https:) for all sites in this	zone			
	Close			

 Asegúrese de que Internet Exporer > security > Local Intranet > Security Settings > User Authentication - Logon esté configurado para utilizar las credenciales de inicio de sesión para los sitios de 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. Abra Firefox e introduzca **about:config** en la barra de direcciones.



2. Haga clic y tendré cuidado, ¡lo prometo!

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. Haga doble clic en el nombre de preferencia **network.negotiation-auth.allow-non-fqdn** para **true** y **network.negotiation-auth.trust-uris** para **ciscolive.com,adfs1.ciscolive.com** para modificarlo.

Search: 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. Cierre Firefox y vuelva a abrirlo.

### Verificación

Para verificar que los SPN para el servidor AD FS se han creado correctamente, ingrese el comando **setspan** y vea el resultado.



Verifique si los equipos cliente tienen entradas Kerberos:

ex. C:\Wine	idows\system32\cmd.exe	P 💌
C:\Users	Nuser1.CISCOLIVE>Klist tickets	<b>^</b>
Current	LogonId is 0:0xabc6d	
Cached T	lickets: <2>	
#0>	Client: user1 @ CISCOLIVE.COM Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40e0000 -> 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	Е
#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	<pre>s\user1.CISCOLIVE&gt;</pre>	

Complete estos pasos para verificar qué autenticación (autenticación Kerberos o NTLM) está en uso.

- 1. Descargue la herramienta Fiddler en su equipo cliente e instálela.
- 2. Cierre todas las ventanas de Microsoft Internet Explorer.
- 3. Ejecute la herramienta Fiddler y verifique que la opción **Capturar tráfico** esté habilitada en el menú Archivo. Fiddler funciona como proxy de paso entre la máquina cliente y el servidor y escucha todo el tráfico.
- 4. Abra Microsoft Internet Explorer, busque su CUCM y haga clic en algunos enlaces para generar tráfico.
- 5. Vuelva a la ventana principal de Fiddler y elija una de las tramas donde el resultado es **200** (correcto) y puede ver Kerberos como mecanismo de autenticación



6. Si el tipo de autenticación es NTLM, verá **Negotiate - NTLMSSP** al principio de la trama, como se muestra aquí.

🚸 Fiddl	er Web (	ebugger			
File Ed	it Rules	Tools Vie	ew Help GET/bo	ok 🔛 GeoEdge	
Q fy P	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 TextView WebForms HexView Auth Cookies Raw JSON XML
<b>≰</b> ≱2	200	HTTP	cucm.ciscolive	1	5, he from the basis of the day is seened
23	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	/ccmadmin/showHome.do	58 00 00 00 00 00 00 05 8 00 00 00 00 00 00 00 00 XX.
<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 XX.
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
58	302	HTTPS	cucm.ciscolive	/comadmin/showHome.do	78 AA CE A9 41 F3 D1 31 Xº18AÓÑ1
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	Cal Contractions Transformer Distances Traditions Instantions Middless
12 12	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	6, Get syntaxivew Transformer [Headers Textivew Imageview Hexivew 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 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	2,3 Date: Sat, 17 Jan 2015 20:05:06 GMT
19	200	HTTPS	cucm.ciscolive	/ciscologo.gif	Expires: -1
					Pragma: no-cache
•					Conkies / Lonin
[QuidEx	ec] ALT+C	) > type HB	LP		
Tie Capb	uring 1	Al Proce	sses	1 / 19 https://adfs1.ciscol	sive.com/adfs/(s/auth/integrated/?SAMLRequest=nVLLbtswELznKwjebYryIwphGX8sFDWQNErk9NDbil48CRSSVJp%28%

# Troubleshoot

Si todos los pasos de configuración y verificación se completan como se describe en este documento y aún tiene problemas de inicio de sesión, debe consultar a un administrador de Microsoft Windows Active Directory / AD FS.