# Jabber のエンドユーザ SAML SSO 向け ADFS 2.0 での Kerberos 設定例

## 内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>コンフィギュレーション</u>
<u>確認</u>
トラブルシュート

### 概要

このドキュメントでは、Active Directory フェデレーション サービス(ADFS)2.0 で Kerberos を 設定する方法を説明します。

# 前提条件

#### 要件

このドキュメントに特有の要件はありません。

#### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

### 背景説明

End User Security Assertion Markup Language(SAML)シングル サインオン(SSO)を設定す

るには、Jabber がドメイン認証と連動できるよう End User SAML SSO を有効にするために、 Kerberos を設定する必要があります。Kerberos を使用して SAML SSO を実装すると、すべての アクセス許可とユーザ同期が Lightweight Directory Access Protocol(LDAP)で処理される一方 、認証は Kerberos で管理されるようになります。Kerberos は、LDAP 対応インスタンスと併せ て使用するよう意図された認証プロトコルです。

Active Directory ドメインに参加する Microsoft Windows および Macintosh マシン上では、ユーザ はユーザ名やパスワードを入力することなくシームレスに Cisco Jabber にログインすることがで き、ユーザにログイン画面が表示されることさえありません。コンピュータ上で Active Directory ドメインにログインしないユーザには、引き続き標準のログイン フォームが表示されます。

認証ではオペレーティング システムから渡される単一のトークンが使用されるため、リダイレク トの必要はありません。トークンは設定済みのキー ドメイン コントローラに照らし合わせて確認 され、トークンが有効であればユーザがログインされます。

# コンフィギュレーション

ADFS 2.0 で Kerberos を設定する手順は以下のとおりです。

- 1. マシンに Microsoft Windows Server 2008 R2 をインストールします。
- 2. Active Directory ドメイン サービス(ADDS)と ADFS を同じマシンにインストールします。
- 3. Microsoft Windows Server 2008 R2 がインストールされたマシンに、インターネット インフ ォメーション サービス(IIS)をインストールします。
- 4. IIS 用の自己署名証明書を作成します。
- 5. 自己署名証明書を IIS にインポートし、その自己署名証明書を HTTPS サーバ証明書として 使用します。
- 6. 別のマシンに Microsoft Windows 7 をインストールして、そのマシンをクライアントとして 使用します。

ドメイン ネーム サーバ(DNS)を変更し、ADDS がインストールされているマシンを DNS とします。

このマシンを、ADDS のインストール時に作成したドメインに追加します。

[Start]に移動します。[Computer]を右クリックします。[Properties] をクリックします。ウィンドウの右側にある [Change Settings]をクリックします。[Computer Name]タブをクリックします。[Change] をクリックします。作成したドメインを追加します。

				Contraction of the second second	rasnaikn	5
ystem Properties		8	User Management	t - Bulk Administration -	Help 💌	
Computer Name/Domain C	Changes 🗾	ote				
You can change the name an computer. Changes might affer More information	nd the membership of this act access to network resources.	omputer				<u>ع</u> اد
Computer name:		y/s	Security   System	- 47	Search Control Panel	-
JabberPC1			asis information	about your computer		e
Full computer name: JabberPC1.mangolab.com			s edition	about your computer	-	
Member of Domain: mangolab.com Workgroup:	More	<u>e ID</u>	right © 2009 Microso ce Pack 1 nore features with a n	ft Corporation. All rights rese ew edition of Windows 7	erved.	
	OK Cancel		ig: essor: lled memory (RAM):	System rating is not availab Intel(R) Xeon(R) CPU E7- 28 2.00 GB	ole 170 @ 2.40GHz 2.40 GHz	
	OK Cancel	Apply	em type:	64-bit Operating System		
Circo United Commun			and Touch:	No Pen or Touch Input is a	vailable for this Display	
caco official communications		Compu	uter name, domain, and	workgroup settings		
oport please visit our		Co	mputer name:	JabberPC1	😗 Change settin	gs
		Ful	l computer name:	JabberPC1.mangolab.com		
		Co	mputer description:	JabberPC1		
	See also	Do	main:	mangolab.com		
	Action Center	Windo	ws activation			
	Windows Update	Wir	ndows is activated		ask for .	2
	Performance Information and Tools	Pro	duct ID: 00371-221-876	7124-86146 Change produ	act key genuine Microsoft software	

7. Kerberos サービスが両方のマシンで生成されるかどうかを確認します。

管理者としてサーバ マシンにログインし、コマンド プロンプトを開きます。以下のコマン ドを実行します。

cd \windows\System32Klist tickets

C:\Users\Administrator.WIN2K8>cd \windows\System32				
C:\Windo	ows\System32>Klist tickets			
Current	LogonId is 0:0x3d6072			
Cached I	ickets: <1>			
#0>	Client: Administrator @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40e0000 -> 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			

ドメイン ユーザとしてクライアント マシンにログインし、同じコマンドを実行します。

::\Users\rashaikh>cd \windows\System32				
::\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				
t1> 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_del				
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_del				
te 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				
t4> 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_del				
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-CIS-HMAC-SHA1-96				
C:\Windows\System32>				

8. ADDS がインストールされているマシンで、ADFS Kerberos ID を作成します。

Microsoft Windows ドメインにログインしている Microsoft Windows 管理者(たとえば、 Microsoft Windows ドメイン コントローラに <domainname>\administrator としてログイン しているユーザ)が ADFS Kerberos ID を作成します。ADFS HTTP サービスには、サービ スプリンシパル名(SPN)と呼ばれる Kerberos ID がHTTP/DNS\_name\_of\_ADFS\_server 形式で設定されてるはずです。

この名前を、ADFS HTTP サーバ インスタンスを表す Active Directory ユーザにマッピング

する必要があります。それには、Microsoft Windows の setspn ユーティリティを使用します 。このユーティリティはデフォルトで Microsoft Windows 2008 Server で使用可能になって いるはずです。

手順 ADFS サーバの SPN を登録します。Active Directory ドメイン コントローラで、 setspn コマンドを実行します。

たとえば、ADFS ホストが adfs01.us.renovations.com で、Active Directory ドメインが US.RENOVATIONS.COM の場合、以下のコマンドを実行します。

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

ADFS サーバに通常はセキュア ソケット レイヤ(SSL)(つまり、HTTPS)でアクセスす るとしても、SPN の **HTTP/の部分は適用されます。** 

ADFS サーバの SPN が正しく作成されたことを確認するために、setspn コマンドを入力し、出力を表示します。

setspn -L



9. Microsoft Windows クライアントのブラウザ設定を構成します。

統合 Windows 認証を有効にするために、[Tools] > [Internet Options] > [Advanced]に移動し ます。

[Enable Integrated Windows Authentication]チェックボックスをオンにします。

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>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable native XMLHTTP support</li> <li>Enable SmartScreen Filter</li> <li>Table SmartScreen Filter</li> </ul>					
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					

[Tools] > [Internet Options] > [Security] > [Local intranet] > [Custom level...] に移動して、 [Automatic logon only in Intranet zone] をオンにします。

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:       Alowed level         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:       Image: Alowed level for this zone:       Stes         Image: Alowed level for this zone:       Cot contr	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

[Tools] > [Internet Options] > [Security] > [Local intranet] > [Sites] > [Advanced]に移動して、 Intrusion Detection & Prevention (IDP) URL をローカル イントラネット サイトに追加しま す。

**注**: [Local intranet] ダイアログボックスのすべてのチェックボックスをオンにして、 [Advanced]タブをクリックします。

Internet Options	- 🖴 🗟 C 🗙 🎎 Cisco Unified Serviceability 🗙
General       Security       Privacy       Content       Connections       Programs       Advance         Select a zone to view or change security settings.       Image: Content internet       Image: C	Local intranet Serviceability × Local intranet Use the settings below to define which websites are included in the local intranet zone.    Local intranet     Local intranet      Local intranet
Security level for this zone Allowed levels for this zone: All Medium-low 	What are intranet settings?       Advanced       OK       Cancel         Local intranet       Image: Concel       Ima
OK Cancel Apply	Require server verification (https:) for all sites in this zone

[Tools] > [Security] > [Trusted sites] > [Sites]に移動して、CUCM ホスト名を [Trusted sites]

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	Add
your files.	Webstes:
You have websites in this zone.	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
	Chree
Enable Protected Mode (requires restarting Internet Explorer)	CKME
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	

# 確認

このセクションでは、使用されている認証(Kerberos 認証または NT LAN Manager(NTLM)認 証)を確認する方法を説明します。

- 1. クライアント マシンに Fiddler ツールをダウンロードしてインストールします。
- 2. すべての Internet Explorer ウィンドウを閉じます。
- 3. Fiddler ツールを実行し、[File] メニューの [Capture Traffic] オプションが有効であることを 確認します。

Fiddler は、クライアント マシンとサーバ間のパススルー プロキシとして機能し、すべての トラフィックをリッスンします。Fiddler により、Internet Explorer 設定は一時的に以下のよ うに変更されます。

Local Area	Network (L	AN) Settings	in and	23	
Automa Automa use of r Auto Use	Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration. Automatically detect settings Use automatic configuration script				
Proxy s Use dial-	a proxy serv up or VPN co	er for your LAN (These settings will n nnections).	not app	ly to	
		the second second			
Servers	Туре	Proxy address to use	F	Port	
	HTTP:	127.0.0.1	:	8888	
	Secure:	127.0.0.1	:	8888	
	FTP:		:		
	Socks:		:		
	🔲 Use the	same proxy server for all protocols			
Exception	ons				
5	Do not use	proxy server for addresses beginnin	g with:		
	<-loopbac	k>		<u>^</u>	
	Use semicol	ons (;) to separate entries.			

- 4. Internet Explorer を開いて顧客関係管理(CRM)サーバの URL を参照し、いくつかのリン クをクリックしてトラフィックを生成します。
- 5. Fiddler のメイン ウィンドウに戻り、結果が 200(成功)となっているフレームのいずれか を選択します。

Ó Ed	dier Web I	lehunger				
E21.	Edia Dud	Teels	Mana Hala OFT 6	and Plantan		-
File	East Mult	es 10015	view Help OET/D	book Buil Geoedge		
Q +9	Replay 2	X - 🕨 Go	🗣 Stream 🌆 Deci	ode 🔰 Keep: All sessions 🝷 🕀 Any Proces	is 👬 Find 🔣 Save 📙 🕐 🏉 Browse 🔹 🕀 Clear Cache 🥂 TextWizard 🛛 🔛 Tearoff 🛛 MSDN Search	
	Result	Protocol	Host	URL *	🕐 Statistics 👬 Inspectors 🗲 AutoResponder 🎯 Composer 🔲 Filters 📋 Log 🚍 Timeline	
01	200	HTTP	www.default-searc	Paid=476baid=1000cvps=c6war=1307;	Headers TextWew WebForms HexWew Auth Cookies Raw 350N XNL	
432	200	HTTP	www.default-searc	/rsid=4768aid=1008itype=n6ver=1307:	No Proxy-Authorization Header is present.	
(ff) 3	200	HTTP	Tunnel to	vos-cm35.sso-44.com:443		ŝ.
434	200	HTTPS	vos-cm35.sso-44.com	1	Authorization Header (Regotiate) appears to contain a Kerberos ticketi	
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/sami/login?relayurl=%2Fccmadmir	28 06 01 04 01 82 37 02 02 1E 06 0A 28 06 01 04 t 7t	
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 .IE	
58	302	HTTPS	vos-cm44.sso-44.com	/adfs/is/?SAMLRequest=nVLLbtswELznKv	82 05 84 30 82 05 80 A0 03 02 01 05 A1 03 02 01 . 0 .*	
29	401	HTTPS	Vos-m44.ssp-44.com	ladisikia thintenatedi?SAM Request-	04 3A 30 92 04 36 A0 03 02 01 05 A1 0C 18 0A 57 .:0 .6	
\$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 90-44.COM4605	
(f) 11	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	73 20 63 60 34 34 2E 73 73 6F 20 34 34 2E 63 6F s-cm44.sso-44.co	
2 12	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 mf .+0 .0	
5 13	302	HTTPS	vos-cm35.sso-44.c	(ssosp(relay	da 13 nd ad 20 9a na 63 88 dd 68 n3 87 dn na d1 3 11 8 76 "Na	•
<b>\$\$14</b>	200	HTTPS	vos-cm35.sso-44.c	/conadmin/showttome.do	Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Cachin-	
曲 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Contine Daw 1900 XM	1
16	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443		- I
曲 17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Response Headers (How) Header Detroitons	40
m 18	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	HTTP/1.1 200 0K	
m 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	
m 21	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Date: Fil, 25 Jul 2014 13:07:58 GMI	
Translation use on 26 con 64 c					•	
DudiEnci AUT+O > type +EIP						
HECH	📲 Cardwine 💌 Al Decreases 1130 https://www.faite.com/ad-com/ad-faite/sub-thio/security/2004 Base ad-wei/1160-05 wei/sub-2/2004/BaSe 2004/BaSe 2004/Ba					
sta cat	comig	T A Proce	ses 1/30	notestives-cirea.sec.ad.com/adis/s/ad	and the second	* .A

認証タイプが NTLM の場合、以下のようにフレームの先頭に [Negotiate - NTLMSSP] と表示されます。

🕑 Statistics 🔛 Inspectors 🖌 AutoResponder 🗳 Req	uest 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
78 00 00 00 18 00 18 00 90 00 00 00 10 00 10	00 x
48 00 00 00 10 00 10 00 58 00 00 00 10 00 10	00 HX
68 00 00 00 00 00 00 00 A8 00 00 05 82 88	A2 h c
05 01 28 0A 00 00 00 0F 49 00 4E 00 54 00 57	00(I.N.T.W.

# トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。