# AD FS バージョン 2.0 でクラスタごとに単一の SAML IdP 接続/アグリーメントを設定する

# 内容

概要
 前提条件
 要件
 使用するコンポーネント
 背景説明
 設定
 ステップ1:CUCMからSPメタデータをエクスポートする
 ステップ2:AD FSからIDPメタデータをダウンロードする
 ステップ3:IdPのプロビジョニング
 ステップ4:SAML SSOの有効化
 確認
 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(AD FS)を使用して、クラス タごとにシングルセキュリティアサーションマークアップ言語(SAML)アイデンティティプロバイ ダー(IdP)接続/アグリーメントを設定する方法について説明します。

# 前提条件

#### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager(CUCM)11.5以降
- Cisco Unified Communications Manager IM and Presenceバージョン11.5以降
- Active Directoryフェデレーションサービスバージョン2.0

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Active Directoryフェデレーションサービスバージョン2.0(IdP)
- Cisco Unified Communications Manager  $\mathcal{N} \mathcal{V} \exists \mathcal{V} 11.5$
- Cisco Unified Presence サーバ バージョン 11.5

# 背景説明

SAML SSOでは、サービスプロバイダー(SP)とIdPの間の信頼の輪である必要があります。 この 信頼は、信頼(メタデータ)が交換されるときに、SSOイネーブルメントの一部として作成され ます。 CUCMからメタデータをダウンロードしてIdPにアップロードします。同様に、IdPからメ タデータをダウンロードしてCUCMにアップロードします。

以前のCUCM 11.5では、発信元ノードがメタデータファイルを生成し、クラスタ内の他のノード からメタデータファイルを収集します。 すべてのメタデータファイルを1つのzipファイルに追加 し、管理者に提示します。管理者はこのファイルを解凍し、IdP上の各ファイルをプロビジョニン グする必要があります。たとえば、8ノードクラスタの8個のメタデータファイルです。

クラスタ機能ごとの単一SAML IdP接続/アグリーメントは、11.5から導入されました。この機能の一部として、CUCMは、クラスタ内のすべてのCUCMおよびIMPノードに対して単一のサービスプロバイダーメタデータファイルを生成します。メタデータファイルの新しい名前形式は<hostname>-single-agreement.xmlです

基本的に、1つのノードがメタデータを作成し、クラスタ内の他のSPノードにプッシュします。 これにより、プロビジョニング、メンテナンス、管理が容易になります。たとえば、8ノードクラ スタに対して1つのメタデータファイルがあります。

クラスタ全体のメタデータファイルは、クラスタ内のすべてのノードでキーペアが確実に使用さ れるマルチサーバtomcat証明書を使用します。メタデータファイルには、クラスタ内の各ノード のアサーションコンシューマサービス(ACS)URLのリストもあります。

CUCMおよびCisco IM and Presenceバージョン11.5クラスタ全体(クラスタごと**に1つのメタデ**ー タファイル)とノードごと(既存のモデル)の両方をサポートします。

このドキュメントでは、AD FS 2.0を使用してSAML SSOのクラスタ全体モードを設定する方法 について説明します。

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。

### 設定

#### ステップ1:CUCMからSPメタデータをエクスポートする

Webブラウザを開き、管理者としてCUCMにログインし、[**System**] > [**SAML Single Sign On]に移 動します。** 

デフォルトでは、[クラスタ**ワイド]**オプションボタンが選択されています。[すべてのメタデー**タをエクスポート]をクリックします。**管理者に<hostname>-single-agreement.xmlという名前で提示されるメタデー**タデータファイル** 



# ステップ2:AD FSからIDPメタデータをダウンロードする

IdPメタデータをダウンロードするには、リンク<u>https:// <FQDN of</u> <u>ADFS>/federationmetadata/2007-06/federationmetadata.xml</u>

# ステップ3:ldPのプロビジョニング

図に示すように、[AD FS 2.0 Management/Trust Relation Ships/Relying Party trust]に移動します。 [Add Relying Party Trust]をクリックします。

📬 AD F5 2.0			_ D X	
i File Action View Window Help			<u>_8×</u>	
🧇 🏟 🖄 🖬 🖬 🖬				
AD F5 2.0	Relying Party Trusts	Actions		
Service     Trust Relationships	Display Name	Relying Party Trusts	-	
Claims Provider Trusts		Add Relying Party Trust		
Relying Party Trusts		View New Window from Here	۲	
		G Refresh		
		Help		

図に示すように、[Add Relying Party Trust Wizard]が開き、[Start]をクリックします。

Madd Relying Party Trus	t Wizard	×
Welcome		
Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard           This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.           The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.	
	CPrevious Start Cancel Help	

証明書利用者に関するインポートデータをファイルからクリックします。CUCM SAML SSO設定 ページからダウンロードしたSPメタデータを参照します。次に、図に示すように[**Next**]をクリッ クします。

Madd Relying Party True	st Wizard	×
Select Data Source		
Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party:  C Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.  Eederation metadata address (host name or URL):  Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file	
	Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.          Federation metadata file location:	
	< <u>Previous</u> <u>N</u> ext > Cancel <u>H</u> elp	

証明書利用者の[Display Name]とオプションのメモを入力します。図に示すように、[**Next**]をクリ ックします。

📬 Add Relying Party Trust	Wizard	×
Specify Display Nam	3	
Steps	Type the display name and any optional notes for this relying party.	
<ul> <li>Welcome</li> <li>Select Data Source</li> </ul>	Display name:	
Specify Display Name	CUCM_Cluster_Wide_Relying_Party_trust	
<ul> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	Notes:	
	< Previous Next > Can	cel Help

[Permit all users to access this relying party]**を選択して、すべてのユーザがこの証明書利用者にア クセスできるようにし**て、図に示すように[**Next**]をクリックします。

📬 Add Relying Party Trus	t Wizard
Choose Issuance Au	thorization Rules
Choose Issuance Au Steps • Welcome • Select Data Source • Specify Display Name • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	thorization Rules         Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.         Image: Comparison of the following options for the initial behavior of this relying party's issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.         Image: Comparison rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.         Image: Comparison rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< <u>Previous</u> <u>N</u> ext > Cancel <u>H</u> elp

[Ready to Add Trust] ページで、設定されている証明書利用者信頼の設定を確認できます。次に 、図に示すように**[Next]**をクリックします。

prehs	The relying party trust has been configured. Review the following settings, and then click Next to add the
Welcome	relying party trust to the AD FS configuration database.
<ul> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Issuance Authorization Bules</li> </ul>	Monitoring   Identifiers   Encryption   Signature   Accepted Claims   Organization   Endpoints   N.  Specify the monitoring settings for this relying party trust.
Ready to Add Trust	Relying party's federation metadata URL:
Frnish	<ul> <li>Monitor relying party</li> <li>Automatically update relying party</li> <li>This relying party's federation metadata data was last checked on:</li> <li>&lt; never &gt;</li> <li>This relying party was last updated from federation metadata on:</li> <li>&lt; never &gt;</li> </ul>

[完了]ページで、証明書利用者信頼がAD FS構成データベースに正常に追加されたことを確認しま す。図に示すように、[Box]のチェックマークを外**し、[Close]**をクリックします。

📬 Add Relying Party Trus	t Wizard	×
Finish		
Steps  Welcome  Select Data Source  Specify Display Name  Choose Issuance Authorization Rules  Ready to Add Trust  Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snapin.	
		]

# 図に示すように、[Relying Party Trusts]を右クリックして[Edit Claim Rules]をクリックします。

💱 AD FS 2.0			and a second		
🙀 File Action View Window	/ Help				<u>e</u> ×
AD FS 2.0	Relying Party Trusts			Actions	
E Service	Display Name 💌	Enabled	Identifier	Relying Party Trusts	•
Claims Provider Trusts	CUCM_Cluster_Wide_Relying_Party_trust	Yes	cucm1150 adis ucce.com	Add Relying Party Trust	-
Relying Party Trusts				View	•
	1			New Window from Here	
	1			G Refresh	
				👔 Help	
				CUCM_Cluster_Wide_Relying_Party_trust	
	1			Update from Federation Metadata	
	1			Edit Claim Rules	
	1			Disable	
	1			Properties	
	1			🔀 Delete	
	4			Help	-

次に、図に示すように[Add Rule]をクリックします。

Edit Claim Rules for CUCM_Cluster_Wide_Rely	ing_Party_trust	_ 🗆 🗙
Issuance Transform Rules Issuance Authorization Rul	es Delegation Authorization R	ules
The following transform rules specify the claims that w	ill be sent to the relying party.	
Order Rule Name	Issued Claims	
		-
Add Bule   Edit Bule   Bemove Bule	Í.	
	l	
ОКС	ancel Apply	Help

[Add Transform Claim Rule]**が開いた**ら、図に示すように、デフォルトのクレームルールテンプレ **ート[**Send LDAP Attributes as **Claims]をクリックします**。

📬 Add Transform Claim R	ule Wizard
Select Rule Templat	e
Steps	Select the template for the claim rule that you want to create from the following list. The description
Choose Rule Type	provides details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Send LDAP Attributes as Claims
	Claim rule template description:
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	< Previous Next > Cancel Help

次の図に示**すように、[Configure Claim Rule]**をクリックします。LDAP属性は、CUCMのLDAPデ ィレクトリ設定のLDAP属性と一致している必要があります。送信要求の種類をuidとして**管理し** ます。図に示すように[Finish]をクリックします。

Add Transform Claim R	ule Wizard				×
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You o which issue Claim	an configure this rule to send the to extract LDAP attributes. Spe d from the rule. rule name: ID	e values of L cify how the	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will t	e
	Rule	template: Send LDAP Attributes a ute store:	as Claims		
	Mapp	e Directory ing of LDAP attributes to outgoin	ıg claim type		-
	•	SAM-Account-Name	*	uid	-
	*		-		-
			< <b>P</b> r	evious Finish Cancel Help	

証明書利用者のカスタムルールを追加します。[Add Rule] をクリックします。図に示すように、 **[カスタム規則を使用して要求を送**信]を選択**し、[次**へ]をクリックします。

🎁 Add Transform Claim Ru	le Wizard	×
Select Rule Template	3	
Steps	Select the template for the claim rule that you want to create from the following list. The description	
Choose Rule Type	provides details about each claim rule template.	
<ul> <li>Configure Claim Rule</li> </ul>	Claim rule template:	
	Send Claims Using a Custom Rule	
	Claim rule template description:	
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS 2.0 claim rule language. Capabilities that require custom rules include: <ul> <li>Sending claims from a SQL attribute store</li> <li>Sending claims from an LDAP attribute store using a custom LDAP filter</li> <li>Sending claims only when 2 or more incoming claims are present</li> <li>Sending claims only when an incoming claim value matches a complex pattern</li> <li>Sending claims for use only in later rules</li> </ul> Tell me more about this rule template	
	< Brevious Next > Cancel Help	

[要求ルールの構成]で、[要求ルール名]を入力し、ウィザードの[カスタムルール]フィールドに指 定された過去の要求ルールをコピーします。その後、要求ルールの名前修飾子とspname修飾子を 変更します。図に示すように[Finish]をクリックします。

#### クレームルール:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =</pre>
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =</pre>
"http:// <fqdn adfs="" of="">/adfs/com/adfs/services/trust",</fqdn>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =</pre>
" <entity id="" in="" metadata="" sp="" the="">");</entity>

Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's FQDN.

Configure Rule	
Steps Choose Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.
	Rule template: Send Claims Using a Custom Rule Cystom rule:
	<pre>ntname"] =&gt; issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier ", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "http://win- jd4ia7ugmrm.adfs.ucce.com/adfs/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "cucml150.adfs.ucce.com"); </pre>
	More about the claim rule language
	< <u>Previous</u> Finish Cancel <u>H</u> elp

図に示すように、[適用]をクリックし**て**、[**OK**]をクリ**ックします**。

l Nar 2 Clu	e Name melD ster_Side_Claim_	Rule	uid <see claim="" rule=""></see>	
	1		. 1	

# ステップ4:SAML SSOの有効化

Webブラウザを開き、管理者としてCUCMにログインし、[**System**] > [**SAML Single Sign On]に移動します**。

デフォルトでは、[クラスタ**ワイド]**オプションボタンが選択されています。図に示すように [Enable Saml SSO]をクリックします。



図に示すように、ポップアップはWebサーバの再起動に関する警告と、idpに応じてクラスタ全体 のSAML SSOまたはノードごとのSAML SSOを選択するための情報を通知します。[Continue] を クリックします。



クラスタ全体のSSOを有効にする基準は、マルチサーバのtomcat証明書がすでに配備されている 必要があることです。図に示すように、[Test for Multi-Server tomcat Certificate]をクリックしま す。

SAML Single Sign-On Configuration
Next
Status
(i) Status: Ready
• Test for Multi-Server tomcat certificate
The criteria for enabling dusterwide SSD is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:
1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR
3) Select Certificate Purpose as Tomcat
<ol> <li>Select Distribution as "Multi-Server"</li> </ol>
5) Click Generate
6) Download the CSR and get it signed from the CA of your choice
7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
8) Restart Tomcat service on all the nodes in the cluster
9) Restart TFTP service on all the TFTP nodes in the cluster
If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage
Test for Multi-Server tomcat certificate
Next Cancel

### 確認が完了したら、すべてのノードにマルチサーバ証明書が表示され、[すべてのノードにマルチ サーバ証明書が**あります]と表示さ**れ、[次へ]**をクリック**します(図を参照)。

SAML Single Sign-On Configuration
Next 1
_ Status
i Status: Ready
All nodes have Multi Server Certificate
Test for Multi-Server tomcat certificate
The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:
1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR
3) Select Certificate Purpose as Tomcat
4) Select Distribution as "Multi-Server"
5) Click Generate
6) Download the CSR and get it signed from the CA of your choice
7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
B) Restart Tomcat service on all the nodes in the duster
9) Restart TFTP service on all the TFTP nodes in the cluster
If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage
Test for Multi-Server tomcat certificate
Next Cancel

# 図に示すように、[次へ]をクリ**ックします**。

SAML Single Sign-On Configuration
Next
Status
(i) Status: Ready
Download Identity provider(IdP) Metadata Trust File
To configure the trust relationship between the IdP and your devices, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP before you can upload it to your Collaboration servers.
This is a manual step!
1)Log in to your IdP and download the metadata trust file to your local server.
2)Click Next once you have this file available locally.
Next Cancel

#### ダウンロードしたIdPメタデータを参照して選択します。図に示すように[Import IdP Metadata]を クリックします。

SAML Single Sign-On Configuration
Next
Status
i Status: Ready
Ready to import Identity Provider metadata trust file to cluster servers
_ Import the IdP Metadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1)Select the IdP Metadata Trust File
Browse federationmetadata.xml
2)Import this file to the Collaboration servers
This action must be successful for at least the Publisher before moving on to the next task in this wizard.
Import IdP Metadata
Next Cancel

次の図に示すように、ページで[Import succeeded for all servers]が確認さ**れ**、[**Next**]をクリックし ます。

SAML Single Sign-On Configuration
Next
Status
(i) Status: Ready
Import succeeded for all servers
Import the IdP Metadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1)Select the IdP Metadata Trust File
Browse, No file selected.
2)Import this file to the Collaboration servers
This action must be successful for at least the Publisher before moving on to the next task in this wizard.
Import IdP Metadata Vinceeded for all servers
Next Cancel

#### 図に示すように、[Next] をクリックします。これは、初期SAML SSO設定ページからSPメタデー タがすでにエクスポートされているためです。

SAML Single Sign-On Configuration
Back Next
Status
i Status: Ready
If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP
IdP Metadata has been imported to servers in this cluster
Download Server Metadata and install on the IdP
Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup.
1)Download the server metadata trust files to local storage
Download Trust Metadata File
This is a manual step!
2)Log in to your IdP and upload the server metadata trust file.
3)Click Next once you have installed the server metadata on the IdP.
Back Next Cancel

CUCMはLDAPディレクトリと同期している必要があります。ウィザードには、LDAPディレクト リで設定されている有効な管理者ユーザが表示されます。図に示すように、ユーザを選択し、 [Run SSO Test]をクリックします。

AML Single Sign-On Config	juration
Back	
Status The server metadata file	must be installed on the IdP before this test is run.
Fest SSO Setup	
This test verifies that the met oun on any server for troubles successful.	adata files are correctly configured and will allow SSO to start up on the servers. This test can be shooting once SSO has been enabled. SSO setup cannot be completed unless this test is
1)Pick a valid username to use	e for this test
You must already know the pa This user must have administr Please use one of the Us	assword for the selected username. rator rights and also exist in the IdP. rernames shown below. Using any other Username to log into the IdP may result in administrator
IOCKOUL.	
samluser	
2)Launch SSO test page	

図に示すように、プロンプトが表示されたら、ユーザIDとそれぞれのパスワードを入力します。

8	Enter username and password for https://win-jd4ia7ugmrm.adfs.ucce.com			
User Name:	samluser			
Password:	••••••			

図に示すように、ポップアップはテストが成功したことを示します。



図に示すように、[Finish]をクリックして、SSOを有効にするための設定を完了します。

System 💌	Call Routing 💌	Media Resources 💌	Advanced Features 💌	Device 💌	Application •	User Management	<ul> <li>Bulk Administra</li> </ul>
SAML Sing	jle Sign-On Co	onfiguration					
Back	Finish						
Chattan							
Status-							
🖌 sso i	SSO Metadata Test Successful						
⊂ Ready to Enable SSO							
Clicking "Fit	nieh" will comple	ate enabling SSO on a	all the servers in this d	uster Then	a will he a chort	t delay while the anr	lications are
being upda	ited.	ete enability SSO on a	all the servers in this t	uster. men	e will be a short	t delay while the app	hicacions are
To verify th	o SSO status	of each server check	the main SSO Configu	ration nade			
Additional testing and manual unloads may be performed from the main nage if percessary							
Additional costing and manual aploads may be performed from the main page in neccessary.							
Back	Finish Can	icel					

図に示すページは、すべてのサーバでSAML SSOの有効化プロセスが開始されていることを示しています。

SAML Single Sign-On Configuration

- Status-

SAML SSO enablement process initiated on all servers. There will be a short delay while the applications are being updated on each server. To verify the SSO status of each server, check the main SSO Configuration page.

ログアウトし、SAML SSOクレデンシャルを使用してCUCMに再度ログインします。[システム (System)] > [SAMLシングルサインオン(SAML Single Sign On)]に移動します。図に示すように、 クラスタ内の他のノードに対して[SSOテストの実行(Run SSO Test)]をクリックします。

SAML Single Sign-On							
SSO Mode Cluster wide (One metadal Per node (One metadata fi	ta file per cluster le per node)	. Requires n	nulti-server Tomcat certificate)	)			
🗙 Disable SAML SSO 👔	Export All Metadat	a 🔞 Upd	ale kdP Metadata File 🧳 Fix.	All Disabled Sen	vers		
RTMT is enabled for SSC     SAML SSO enabled     SAML Single Sign-On	). You can chang I - 3 of 3)	e SSO for R	ITMT <u>here.</u>			Row	s per Page 50 🔻
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	S90 Test	
cucm1150.adfs.ucce.com	SAML	N/A	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Passed - June 21, 2016 9:29:14 PM IST	Run SSO Test
cucm1150sub.adfs.ucce.com	SAML	🔶 IdP	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Never	Run SSO Test
imp115.adfs.ucce.com	SAML	🔶 IdP	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Never	Run SSO Test

# 確認

#### ここでは、設定が正常に機能しているかどうかを確認します。

SAML SSOが有効になっているノードのSSOテストが成功したことを確認します。[System] > [SAML Single Sign On]に移動します。成功したSSOテストのステータスは[Passed]です。

SAML Single Sign-On SSO Mode							
<ul> <li>Cluster wide (One metadat</li> <li>Per node (One metadata fi</li> </ul>	ta file per clu: le per node)	ster. Requires m	nulti-server Tomcat certificate)	)			
🗙 Disable SAML SSO 👔	Export All Meta	data 🔞 Upda	ate IdP Metadata File 🧳 Fix /	All Disabled Ser	vers		
Status (i) RTMT is enabled for SSO (i) SAML SSO enabled SAML Single Sign-On (2)	). You can ch I - 3 of 3)	ange SSO for R	TMT <u>here.</u>			Rows	s per Page 50 🔻
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucm1150.adfs.ucce.com	SAML	N/A	June 20, 2016 9:57:30 AM IST	📥 File	June 20, 2016 10:06:27 PM IST	Passed - June 20, 2016 9:59:02 PM IST	Run SSO Test
cucm1150sub.adfs.ucce.com	SAML	star 💠	June 20, 2016 10:15:46 PM IST	🎂 File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:11:39 PM IST	Run SSO Test
imp115.adfs.ucce.com	SAML	star 💠	June 20, 2016 10:15:46 PM IST	🎂 File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:12:40 PM IST	Run SSO Test
Disable SAML SSO Exp	ort All Metad	ata Update	IdP Metadata File	Disabled Serve	rs		

SAML SSOがアクティブになると、次の図に示すように、CUCMログインページの[Installed Applications]および[Platform Applications]が表示されます。

# Installed Applications

- Cisco Unified Communications Manager
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Communications Self Care Portal
- Cisco Prime License Manager
- Cisco Unified Reporting
- Cisco Unified Serviceability

**Platform Applications** 

- Disaster Recovery System
- Cisco Unified Communications OS Administration

SAML SSOがアクティブになると、次の図に示すように、IM and Presenceログインページの [Installed Applications and Platform Applications]がリストされます。

Installed Applications

- Cisco Unified Communications Manager IM and Presence
   Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Reporting
- Cisco Unified Serviceability

# Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

デバッグするSSOログを設定するには、コマンドset samitrace level DEBUGを使用します

RTMTを使用するか、CLIを使用してactivelog /tomcat/logs/ssosp/log4j/\*.logの場所からSSOログ を収集します。

SSOログの例は、生成されたメタデータと他のノードへの送信を示します

2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET API to generate Clusterwide SP Metadata in the Local node. 2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to post the generated SP Metadata to other nodes 2016-05-28 14:59:47,185 INFO [http-bio-443-exec-297] cluster.SAMLSSOClusterManager -Begin:postClusterWideSPMetaData 2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes [cucm1150, cucm1150sub.adfs.ucce.com] 2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150 2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150 2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150