# Configurar Conexão/Contrato de IdP de SAML Única por Cluster com AD FS Versão 2.0

### Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar Etapa 1. Exportar metadados SP do CUCM Etapa 2. Transferir metadados IDP do AD FS Etapa 3. Provisionar IdP Etapa 4. Ativar SSO SAML Verificar Troubleshoot

### Introduction

Este documento descreve como configurar a conexão/o contrato do Provedor de Identidade (IdP) do SAML (Single Security Assertion Markup Language) por cluster com o AD FS (Ative Diretory Federation Service).

### Prerequisites

#### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM) 11.5 ou posterior
- Cisco Unified Communications Manager IM and Presence versão 11.5 ou posterior
- Ative Diretory Federation Service versão 2.0

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software:

- Ative Diretory Federation Service versão 2.0 como IdP
- Cisco Unified Communications Manager versão 11.5
- Cisco IM and Presence Server versão 11.5

## Informações de Apoio

Para o SSO SAML, precisa ser um círculo de confiança entre o provedor de serviços (SP) e o IdP. Essa confiança é criada como parte do SSO Enablement, quando a confiança (metadados) é trocada. Baixe os Metadados do CUCM e faça o upload para o IdP, faça o download dos metadados do IdP e faça o upload para o CUCM.

Antes do CUCM 11.5, o nó de origem gera o arquivo de metadados, além de coletar os arquivos de metadados de outros nós no cluster. Ele adiciona todos os arquivos de metadados a um único arquivo zip e apresenta ao administrador. O administrador precisa descompactar esse arquivo e provisionar cada arquivo no IdP. Por exemplo, 8 arquivos de metadados para um cluster de 8 nós.

Um único contrato/conexão de IdP SAML por recurso de cluster é apresentado a partir de 11.5. Como parte desse recurso, o CUCM gera um único arquivo de metadados do provedor de serviços para todos os nós CUCM e IMP no cluster. O novo formato de nome para o arquivo de metadados é **<hostname>-single-agreement.xml** 

Basicamente, um nó cria os Metadados e os envia para outros nós de SP no cluster. Isso facilita o provisionamento, a manutenção e o gerenciamento. Por exemplo, 1 arquivo de metadados para um cluster de 8 nós.

O arquivo de metadados do cluster wide usa o certificado de tomcat de multiservidor que garante que o par de chaves seja usado para todos os nós no cluster. O arquivo de metadados também tem uma lista de urls do Serviço de consumidor de asserção (ACS) para cada nó no cluster.

CUCM e Cisco IM and Presence versão 11.5 Suporta os Modos SSO, **em todo o cluster** (um arquivo de metadados por cluster) e por nó (modelo existente).

Este documento descreve como configurar o modo de cluster-wide do SSO SAML com AD FS 2.0.

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

#### Etapa 1. Exportar metadados SP do CUCM

Abra um navegador da Web, faça login no CUCM como administrador e navegue **paraSystem >** SAML Single Sign On (Sistema > Logon único SAML).

Por padrão, o botão de opção **Cluster Wide** está selecionado. Clique em **Exportar todos os metadados.** O arquivo de dados de metadados apresentado ao administrador no nome <hostname>-single-agreement.xml



#### Etapa 2. Transferir metadados IDP do AD FS

Para fazer o download dos metadados IdP, consulte o link <u>https:// <FQDN do</u> <u>ADFS>/federationmetadata/2007-06/federationmetadata.xml</u>

#### Etapa 3. Provisionar IdP

Como mostrado na imagem, navegue para Gerenciamento do AD FS 2.0 / Confiança de Confiança / Envio de Relação de Confiança do AD FS 2.0. Clique em Adicionar confiança de terceira parte confiável.

	_ # ×
Relying Party Trusts	Actions
Display Name	Relying Party Trusts
	Add Relying Party Trust
	View  New Window from Here
	G Refresh
*	Help
	Relying Party Trusts Display Name

O Assistente para Adicionar Confiança de Terceiros Confiantes é aberto conforme mostrado na imagem e, agora, clique em **Iniciar**.

Madd Relying Party True	st 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.
	< Previous Start Cancel Help

Clique nos dados de importação sobre a terceira parte confiável de um arquivo. Navegue pelos metadados SP baixados da página de configuração SSO do CUCM SAML. Em seguida, clique em **Avançar**, conforme mostrado na imagem:

http://www.commonscience.com	st Wizard	×
Select Data Source		
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	Select an option that this wizard will use to obtain data about this relying party: <ul> <li>Ignout data about the relying party published online or on a local network</li> <li>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.</li> <li>Eederation metadata address (host name or URL): <ul> <li>Example: fs.contoso.com or https://www.contoso.com/app</li> </ul> </li> <li>Impgt data about the relying party from a file</li> <li>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.</li> <li>Federation metadata file location: <ul> <li>EvusersVadministrator/Desktop/Cluster_Wide\cucm1150-single-agreement.xml</li> <li>Browse</li> </ul> </li> <li>C Enter data about the relying party manually</li> <li>Use this option to manually input the necessary data about this relying party organization.</li> </ul>	
	< <u>Previous</u> <u>Next</u> > Cancel <u>H</u> elp	

Digite o nome de exibição e todas as notas opcionais para a terceira parte confiável. Clique em **Avançar**, conforme mostrado na imagem:

📬 Add Relying Party Trust	Wizard	×
Specify Display Nam	e	
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 > C	ancel Help

Selecione **Permitir que todos os usuários acessem esta terceira parte confiável** para permitir que todos os usuários acessem esta terceira parte confiável e clique em **Avançar**, como mostrado na imagem:

Add Relying Party Trust	Wizard
Choose Issuance Au	thorization Rules
Steps Velcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	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. • Permit gli users to access this relying party The 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. • Deny all users access to this relying party The issuance authorization 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 to enable any users to access this relying party. You can change the 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

Na página **Pronto para adicionar confiança**, você pode revisar as configurações para a Confiança da terceira parte confiável, que foi configurada. Agora clique em **Next**, como mostrado na imagem:

Steps	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.
Select Data Source     Specify Display Name     Choose Issuance     Authorization Bulas	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N.
Readu to Add Taret	Relying party's federation metadata URL:
Finish	<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>

A página Concluir confirma que a confiança da terceira parte confiável foi adicionada com êxito ao banco de dados de configuração do AD FS. Desmarque a caixa e clique em **Fechar**, como mostrado na imagem:

📬 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 snap-in.	

Clique com o botão direito do mouse em **Confianças de terceira parte** e clique em **Editar regras de reivindicação**, conforme mostrado na imagem:

1 AD FS 2.0	Net stall			×
File Action View Window	i Help			×
AD PS 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.adfs.ucce.com	Add Relying Party Trust
Relying Party Trusts				View
withbute stores	1			New Window from Here
	1			G Refresh
				1 Help
				CUCM_Cluster_Wide_Relying_Party_trust
	1			Update from Federation Metadata
	1			Edit Claim Rules
	1			Disable
	1			Properties
	1			🗙 Delete
	4			🛛 Help
	1-1			

Agora clique em Add Rule., como mostrado na imagem:

Edit Claim Rules for CUCM_Cluster_Wide_ Issuance Transform Rules Issuance Authorizatio	Relying_Party_trust
The following transform rules specify the claims t Order Rule Name	hat will be sent to the relying party.
	1
Add Rule Edit Rule Remove Ru	le
ОК	Cancel Apply Help

Quando a **opção Add Transform Claim Rule** for aberta, clique em **Next** com o modelo de regra de reivindicação padrão **Send LDAP Attributes as Claims**, como mostrado na imagem:

teps	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.		
Choose Rule Type			
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. Tell me more about this rule template		

Clique em **Configure Claim Rule** conforme mostrado nesta imagem. O atributo LDAP deve corresponder ao atributo LDAP na configuração do diretório LDAP no CUCM. Gerenciar o tipo de declaração de saída como **uid**. Clique em **Concluir**, conforme mostrado na imagem:

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:	e values of L cify how the	DAP attributes as claims. Select an attribute store attributes will map to the outgoing claim types that	from t will be
	Name Rule Attrib	HD template: Send LDAP Attributes : ute store:	as Claims		
	Activ	e Directory ing of LDAP attributes to outgoin	ng claim type	• •	
		LDAP Attribute		Outgoing Claim Type	-
	*		-		-
			< Pre	evious Finish Cancel	Help

Adicione a regra personalizada para a terceira parte confiável. Clique em Adicionar regra. Selecione Enviar reivindicações usando uma regra personalizada e clique em Avançar, conforme mostrado na imagem:

🍿 Add Transform Claim Ru	ile Wizard
Select Rule Template	3
Steps	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Configure Claim Rule	Claim rule template: Send Claims Using a Custom Rule
	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 with complex changes to an incoming claim value</li> <li>Creating claims for use only in later rules</li> </ul> Tell me more about this rule template
	< Previous Next > Cancel Help

Em Configurar regra de Reivindicação, digite um Nome da regra de Reivindicação e, em seguida, Copie a regra de reivindicação fornecida e passada no campo Regra personalizada do assistente que modifica o qualificador de nome e qualificador de nome de nome na regra de Reivindicação. Clique em **Concluir**, conforme mostrado na imagem:

#### Regra de solicitação:

```
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,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<FQDN of ADFS>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<Entity ID in the SP Metadata>");
```

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

🖥 Add Transform Claim R	ule Wizard				
Configure Rule					
Steps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts				
Choose Rule Type	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.				
Configure Claim Rule	Claim rule name:				
	Cluster_Side_Claim_Rule				
	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/spna mequalifier"] = "cucml150.adfs.ucce.com"); </pre>				
	More about the claim rule language				
	< <u>Previous</u> Finish Cancel <u>H</u> elp				

Como mostrado na imagem, clique em Apply e em OK.

Drder Ru 1 Na 2 Clu	le Name melD ister_Side_Claim_	Rule	lissued Claim uid <see claim="" r<="" th=""><th>s ule&gt;</th></see>	s ule>
				4
	1 5051		. 1	

#### Etapa 4. Ativar SSO SAML

Abra um navegador da Web, faça login no CUCM como administrador e navegue **paraSystem** >SAML Single Sign On.

Por padrão, o botão de opção **Cluster Wide** está selecionado. Clique em **Enable Saml SSO**, conforme mostrado na imagem:



Como mostrado na imagem, o pop-up notifica o aviso de reinicialização do servidor Web e as informações para escolher o SAML SSO ou o SSO SAML por nó de todo o cluster de acordo com o idp. Clique em **Continuar**.



O critério para ativar o SSO em todo o cluster é que você deve ter um certificado tomcat multiservidor já implantado. Clique em **Test for Multi-Server tomcat Certificate**, conforme mostrado na imagem:

AML Single Sign-On Configuration
Net
Status
3 Status: Ready
Test for Multi-Server tomcat certificate
The criteria for enabling dusterwide SSD is that you must have a multiserver torncat 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
8) Restart Tomcat service on all the nodes in the cluster
9) Restart TFTP service on all the TFTP nodes in the duster
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

Depois de confirmado, todos os nós têm o Certificado de servidor múltiplo exibido e **Todos os nós** têm o Certificado de servidor múltiplo e, em seguida, clique em Avançar, conforme mostrado na imagem:

SAML Single Sign-On Configuration
Next 1
r Status
Status: Ready
V 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
8) 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

Como mostrado na imagem, clique em Avançar.

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

Navegue e selecione os metadados IdP baixados. Clique em **Importar Metadados do IdP**, como mostrado na imagem:

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

A página confirma a Importação bem-sucedida para todos os servidores e clique em **Avançar**, como mostrado na imagem:

SAML Single Sign-On Configuration
Next
Status
(j) 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 VIII Import succeeded for all servers
Next Cancel

Como mostrado na imagem, clique em **Avançar**, pois já exportou os metadados SP da página de configuração inicial do SSO SAML.

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 IdD-
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

O CUCM deve estar em sincronia com o diretório LDAP. O assistente mostra os usuários administradores válidos configurados no diretório LDAP. Selecione o usuário e clique em **Executar teste SSO**, conforme mostrado na imagem:

AML Single Sign-On Configur	ration
Back	
Status The server metadata file mu	st be installed on the IdP before this test is run.
Fest SSO Setup	
This test verifies that the metada run on any server for troublesho successful.	ata files are correctly configured and will allow SSO to start up on the servers. This test can be oting once SSO has been enabled. SSO setup cannot be completed unless this test is
1)Pick a valid username to use fo	or this test
You must already know the pass This user must have administrate Please use one of the Userr lockout.	word for the selected username. or rights and also exist in the IdP. names shown below. Using any other Username to log into the IdP may result in administrator
Valid administrator Usernames	
samluser	*
2)Launch SSO test page Run SSO Test	

Como mostrado na imagem, digite a ID de usuário e a respectiva senha assim que ela solicitar.

Authentication	Required				
?	Enter username and password for https://win-jd4ia7ugmrm.adfs.ucce.com				
User Name:	samluser				
Password:	••••••				
	OK Cancel				

O pop-up, como mostrado na imagem, confirma que o teste foi bem-sucedido.



Como mostrado na imagem, clique em Concluir para concluir a configuração para ativar SSO.

System 💌	Call Routing 💌	Media Resources 💌	Advanced Features 💌	Device 💌	Application •	User Management	Bulk Administra
SAML Sing	jle Sign-On Co	onfiguration					
Back	Finish						
- Status-							
sso i	Metadata Test S	Successful					
Ready to	Enable SSO						
Clicking "Fir being upda	nish" will comple ited.	ete enabling SSO on a	all the servers in this d	uster. There	e will be a short	delay while the app	lications are
To verify th Additional t	ne SSO status o testing and mar	of each server, check nual uploads may be p	the main SSO Configur performed from the ma	ration page. in page if ne	eccessary.		
Back	Finish Can	cel					

A página mostrada na imagem confirma que o processo de ativação de SSO SAML é iniciado em todos os servidores.



Faça logoff e logon novamente no CUCM usando as credenciais de SSO SAML. Navegue até **Sistema >Logon único SAML**. Clique em **Executar Teste SSO** para outros nós no cluster, conforme mostrado na imagem:

SAML Single Sign-On							
SSO Mode Cluster wide (One metadat Per node (One metadata fi	ta file per cluste le per node)	r. Requires n	nulti-server Tomcat certificate)	)			
🗙 Disable SAML SSO 👔	Export All Metadat	a 🔞 Upd	ale kdP Metadata File 🥜 Fix.	All Disabled Ser	vers		
ATMS     ATMT is enabled for SSO     SAML SSO enabled     SAML Single Sign-On (1)	). You can chang 1 - 3 of 3)	je SSO for R	.TMT <u>here.</u>			Row	s per Page 50 🔻
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	550 Te	est
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

### Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Confirme se o Teste SSO foi bem-sucedido para os nós que estão ativados para SSO SAML. Navegue até **Sistema >Logon único SAML**. Testes SSO bem-sucedidos mostram o status Passado.

SAML Single Sign-On							
SSO Mode Cluster wide (One metadai Per node (One metadata fi	ta file per clu: le per node)	ster. Requires n	nulti-server Tomcat certificate)	)			
🗙 Disable SAML SSO 👔	Export All Meta	idata 👩 Upd	late IdP Metadata File 🧳 Fix.	All Disabled Ser	vers		
Status	). You can ch	ange SSO for R	(TMT <u>here.</u>			Row	s per Dage SD V
Server Name	SSO Status	Re-Import Netadata	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	🔶 IdP	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 Fix All I	Disabled Serve	rs		

Quando o SSO SAML é ativado, os aplicativos instalados e os aplicativos de plataforma são listados para a página de login do CUCM, como mostrado nesta imagem.

### 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

Quando o SSO SAML é ativado, os aplicativos instalados e os aplicativos de plataforma são listados para a página de login IM e Presence, como mostrado nesta imagem:

#### 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

### Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para definir os logs SSO como debug, use o comando set samitrace level DEBUG

Colete os registros SSO usando RTMT ou do **ativelog /tomcat/logs/ssosp/log4j/\*.log** local usando CLI.

Exemplo de logs SSO mostra os metadados gerados e enviados a outros nós

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