Ejemplo de Configuración de AD FS Versión 2.0 para SSO de SAML

Contenido

ntroducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Descargar metadatos del proveedor de identidad (IdP) de AD FS versión 2.0
Descargar metadatos de Collaboration Server (SP)
CUCM IM and Presence Service
Unity Connection
Aprovisionamiento de Cisco Prime Collaboration
Agregar CUCM como confianza de usuario de confianza
Adición de CUCM IM y Presence como confianza de usuario de confianza
AddUCXN como confianza de usuario de confianza
Adición de Cisco Prime Collaboration Provisioning como elemento de confianza del usuario de confianza
<u>Verificación</u>
Troubleshoot

Introducción

Este documento describe cómo configurar el servicio de federación de Active Directory (AD FS) versión 2.0 para habilitar el inicio de sesión único (SSO) del lenguaje de marcado de aserción de seguridad (SAML) para productos de Cisco Collaboration como Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN), CUCM IM and Presence y Cisco Prime Collaboration.

Prerequisites

Requirements

AD FS versión 2.0 debe estar instalado y probado.

Precaución: esta guía de instalación se basa en una configuración de laboratorio y se supone que la versión 2.0 de AD FS se utiliza solo para SSO SAML con productos de Cisco Collaboration. En caso de que otras aplicaciones vitales para la empresa lo utilicen, la personalización necesaria debe realizarse según la documentación oficial de Microsoft.

Componentes Utilizados

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

- AD FS versión 2.0
- Microsoft Internet Explorer 10
- CUCM versión 10.5
- Cisco IM and Presence Server versión 10.5
- UCXN versión 10.5
- Cisco Prime Collaboration Provisioning 10.5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Descargar metadatos del proveedor de identidad (IdP) de AD FS versión 2.0

Para descargar metadatos IdP, ejecute este enlace en su navegador: https://<FQDN of ADFS>/FederationMetadata/2007-06/FederationMetadata.xml.

Descargar metadatos de Collaboration Server (SP)

CUCM IM and Presence Service

Abra un navegador web, inicie sesión en CUCM como administrador y navegue hasta Sistema > Inicio de sesión único SAML.

Unity Connection

Abra un navegador web, inicie sesión en UCXN como administrador y navegue hasta Configuración del sistema > Inicio de sesión único SAML.

Aprovisionamiento de Cisco Prime Collaboration

Abra un navegador web, inicie sesión en Prime Collaboration Assurance como globaladmin y vaya a Administration > System Setup > Single Sign On.

Agregar CUCM como confianza de usuario de confianza

1. Inicie sesión en el servidor de AD FS e inicie la versión 2.0 de AD FS desde el menú Programas de Microsoft Windows. 2. Seleccione Agregar confianza de usuario de confianza.



3. Haga clic en Start (Inicio).

Welcome 9 Welcome 9 Welcome 9 Select Data Source 9 Authorization Rules 9 Ready to Add Truat 9 Finish	http://www.commonscience.com	t Wizard	×
Steps Welcome • Welcome 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 Rules • Ready to Add Trust 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.	Welcome		
	Welcome 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		< Previous Start Cancel Help	1

4. Seleccione la opción Importar datos sobre el usuario de confianza desde un archivo, elija el archivo de metadatos SPMetadata_CUCM.xml que descargó de CUCM anteriormente y haga clic en Siguiente.

Add Relying Party Trust	Wizard	×
Select Data Source		
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:]
	< Previous Next > Cancel Help	

5. Ingrese Display name y haga clic en Next.

💱 Add Relying Party Trust V	Vizard	×
Specify Display Name		
Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	Type the display name and any optional notes for this relying party. Display name: CUCM Ngtes: Adding CUCM as Relaying Party to ADFS	
	<pre>c Previous</pre>	Heb 1
	< Previous Next > Cancel	Help

6. Elija Permitir a todos los usuarios acceder a este usuario de confianza y haga clic en Siguiente.

🙀 Add Relying Party Trust (Wizard X
Choose Issuance Auth	horization Rules
Steps	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party.
Welcome Select Data Several	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.
 Specify Display Name 	Permit all users to access this relying party
 Choose Issuance Authorization Rules 	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.
Ready to Add Trust	C Deny all users access to this relying party
 Finish 	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 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.
	< Previous Next > Cancel Help

7. Seleccione Abrir el cuadro de diálogo Editar reglas de reclamación para la confianza del usuario de confianza cuando se cierre el asistente y haga clic en Cerrar.

📬 Add Relying Party Trus	t Wizard	×
Finish		
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. ☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
	Close	

8. Haga clic en Agregar regla.

📬 Edit Claim Rules for CUCM				
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules				
The following transform rules specify the claims that will be sent to the relying party.				
Order Rule Name Issued Claims				
	T			
Add Rule Edit Kule Kemove Kule				
OK Cancel Apply	Help			

9. Haga clic en Siguiente con la plantilla de regla de reclamación predeterminada establecida para Enviar atributos LDAP como reclamaciones.

Mdd Transform Claim Rule	e Wizard	×
Select Rule Template		
Steps	Select the template for the claim rule that you want to create from the following list. The description	
Choose Hule 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	
	< Previous Next > Cancel Help	

10. En Configurar regla, ingrese el nombre de la regla de reclamación, seleccione Active Directory como el almacén de atributos, configure Atributo LDAP y el Tipo de reclamación saliente como se muestra en esta imagen, y haga clic en Finalizar.



- El atributo del protocolo ligero de acceso a directorios (LDAP) debe coincidir con el atributo de sincronización de directorios en CUCM.

- "uid" debe estar en minúsculas.

Configure Rule

Steps Choose Rule Type	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be
Configure Claim Rule	issued from the rule.
-	Claim rule name:
	Name ID
	Rule template: Send LDAP Attributes as Claims
	Attribute store:
	Active Directory
	Mapping of LDAP attributes to outgoing claim types:
	LDAP Attribute Outgoing Claim Type
	SAM-Account-Name
	*
	< Previous Finish Cancel Help

11. Haga clic en Agregar regla, seleccione Enviar reclamaciones usando una regla personalizada como plantilla de regla de reclamación y haga clic en Siguiente.

Edit Claim Rules for CUCM	_ 🗆 ×
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization	Rules
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
1 Name ID uid	
	₽
Add Rule Edit Rule Remove Rule	
OK Cancel Apply	Help

Select Rule Template

iteps	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	Qlaim 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: Sending claims from a SQL attribute store Sending claims from an LDAP attribute store using a custom LDAP filter Sending claims from a custom attribute store Sending claims only when 2 or more incoming claims are present Sending claims only when 2 or more incoming claims are present
	Sending claims only when an incoming claim value matches a complex pattern Sending claims with complex changes to an incoming claim value
	Tell me more about this rule template

12. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

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

(NOTA: Si copia y pega el texto de estos ejemplos, tenga en cuenta que algún software de procesamiento de texto sustituirá las comillas ASCII (") por las versiones UNICODE (""). Las versiones UNICODE provocarán un error en la regla de notificación.)

X

Add Transform Claim Ru	e Wizard	×
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. Qaim rule name: Call Manager Claim Rule Rule template: Send Claims Using a Custom Rule Custom rule: Thttp://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou Antname"]=> issue (Type = "http://schemas.milsoap.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://ADFS1.CISCOLIVE.COM/com/adfs/services/trust", 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://ADFS1.CISCOLIVE.COM/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna megualifier"] = "CUCM.CISCOLIVE.COM"); More about the claim rule language	
	< <u>Previous</u> Finish Cancel Help	

Nota:

- El nombre de dominio completo (FQDN) de CUCM y ADFS se rellena automáticamente con el laboratorio CUCM y AD FS en este ejemplo y se debe modificar para que coincida con su entorno.

- El FQDN de CUCM/ADFS distingue entre mayúsculas y minúsculas y debe coincidir con los archivos de metadatos.

- 13. Haga clic en Finish (Finalizar).
- 14. Haga clic en Aplicar y luego en Aceptar.
- 15. Reinicie el servicio AD FS versión 2.0 desde Services.msc.

Adición de CUCM IM y Presence como confianza de usuario de confianza

1. Repita los pasos del 1 al 11 tal y como se describe en Agregar CUCM como confianza de

usuario de confianza y vaya al paso 2.

2. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(1

🙀 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 claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an
Configure Claim Bule	issuance statement using the AD FS 2.0 claim rule language.
o on inguiro orann rhaio	Claim rule name:
	Custom Rule for IMP
	Rule template; Send Claims Using a Custom Rule
	Custom nie:
	<pre>ntname"]=> 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:///ADFS1.ciscolive.com/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "IMF.ciscolive.com"); </pre>
	More about the claim rule language
	< Previous Finish Cancel Help

Observe que el FQDN de IM and Presence y AD FS se rellena automáticamente con el laboratorio de IM and Presence y AD FS en este ejemplo y se debe modificar para que coincida con su entorno.

3. Haga clic en Finish (Finalizar).

- 4. Haga clic en Aplicar y luego en Aceptar.
- 5. Reinicie el servicio AD FS versión 2.0 desde Services.msc.

Agregar UCXN como confianza de usuario de confianza

- 1. Repita los pasos del 1 al 12 tal y como se describe en Agregar CUCM como confianza de usuario de confianza y vaya al paso 2.
- 2. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(1

💱 Add Transform Claim Rul	e Wizard	X
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 a issuance statement using the AD FS 2.0 claim rule language.	
Configure Claim Rule	Claim rule name:	
	Custom Rule for UCXN	
	Rule template: Send Claims Using a Custom Rule	
	Custom rule:	
	<pre>>> 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:///ADFS1.ciscolive.com/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "UCXN1.ciscolive.com"); </pre>	
	More about the claim rule language	
	< Previous Finish Cancel Help	

Observe que el FQDN de UCXN y AD FS se rellena automáticamente con el UCXN y ADFS de laboratorio en este ejemplo y se debe modificar para que coincida con su entorno.

- 3. Haga clic en Finish (Finalizar).
- 4. Haga clic en Aplicar y luego en Aceptar.
- 5. Reinicie el servicio AD FS versión 2.0 desde Services.msc.

Adición de Cisco Prime Collaboration Provisioning como elemento de confianza del usuario de confianza

- 1. Repita los pasos del 1 al 12 tal y como se describe en Agregar CUCM como confianza de usuario de confianza y vaya al paso 2.
- 2. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

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

🙀 Add Transform Claim Rule	Wizard	×
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. Claim rule name: Custom Rule for PCP Rule template: Send Claims Using a Custom Rule Custom rule: ntname"] => 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/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form qualifier"] = "http://ADFS1.ciscolive.com/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname qualifier"] = "PCP.ciscolive.com"; More about the claim rule language	
	< Previous Finish Cancel Help	

Observe que el FQDN de Prime Provisioning y AD FS se rellena automáticamente con el aprovisionamiento de colaboración de Prime (PCP) y AD FS de este ejemplo y se debe modificar para que coincida con su entorno.

- 3. Haga clic en Finish (Finalizar).
- 4. Haga clic en Aplicar y luego en Aceptar.
- 5. Reinicie el servicio AD FS versión 2.0 desde Services.msc.

Una vez configurada la versión 2.0 de AD FS, continúe para habilitar SSO de SAML en los productos de Cisco Collaboration.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

AD FS registra los datos de diagnóstico en el Registro de eventos del sistema. Desde el Administrador del servidor en el servidor AD FS, abra Diagnóstico -> Visor de eventos -> Aplicaciones y servicios -> AD FS 2.0 -> Administrador



Buscar errores registrados para actividad de AD FS

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).