Esempio di installazione di AD FS versione 2.0 per la configurazione di SAML SSO

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Configurazione
Scarica metadati provider di identità (IdP) versione 2.0 di AD FS
Scarica metadati di Collaboration Server (SP)
Servizio CUCM IM e presenza
Unity Connection
Cisco Prime Collaboration Provisioning
Aggiungi CUCM come attendibilità componente
Aggiungi messaggistica immediata CUCM e presenza come attendibilità componente
Aggiungi UCXN come attendibilità componente
Aggiungi Cisco Prime Collaboration Provisioning come attendibilità componente
<u>Verifica</u>
Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare Active Directory Federation Service (ADFS) versione 2.0 per abilitare Security Assertion Markup Language (SAML) Single Sign-On (SSO) per i prodotti Cisco Collaboration quali Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN), CUCM IM e Presence e Cisco Prime Collaboration.

Prerequisiti

Requisiti

È necessario installare e testare AD FS versione 2.0.

Attenzione: questa guida all'installazione si basa su un'installazione lab e si presume che ADFS versione 2.0 venga utilizzato solo per SAML SSO con i prodotti Cisco Collaboration. Se viene utilizzato da altre applicazioni business-critical, è necessario eseguire la personalizzazione necessaria in base alla Documentazione Microsoft ufficiale.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Scarica metadati provider di identità (IdP) versione 2.0 di AD FS

Per scaricare i metadati IdP, eseguire questo collegamento nel browser: https://<FQDN di ADFS>/FederationMetadata/2007-06/FederationMetadata.xml.

Scarica metadati di Collaboration Server (SP)

Servizio CUCM IM e presenza

Aprire un browser Web, accedere a CUCM come amministratore e selezionare Sistema > Single Sign-On SAML.

Unity Connection

Aprire un browser Web, accedere a UCXN come amministratore e selezionare Impostazioni di sistema > SAML Single Sign-On.

Cisco Prime Collaboration Provisioning

Aprire un browser Web, accedere a Prime Collaboration Assurance come globaladmin e selezionare Amministrazione > Configurazione del sistema > Single Sign-On.

Aggiungi CUCM come attendibilità componente

- 1. Accedere al server AD FS e avviare AD FS versione 2.0 dal menu Programmi di Microsoft Windows.
- 2. Selezionare Aggiungi attendibilità componente.



3. Fare clic su Start.

http://www.commonscience.com	Wizard	×
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	

4. Selezionare l'opzione Importa dati sul componente da un file, scegliere il file di metadati SPMetadata_CUCM.xml scaricato in precedenza da CUCM e fare clic su Avanti.

Add Relying Party Trust	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: 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. Federation 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: C. Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.]
	< Previous Next > Cancel Help	

5. Immettere il nome visualizzato e fare clic su Avanti.

🙀 Add Relying Party Trust W	/izard	×
Specify Display Name		
Steps Welcome Select Data Source	Type the display name and any optional notes for this relying party.	
Specify Display Name	СОСМ	
Choose Issuance Authorization Rules Ready to Add Trust	Ngtes: Adding CUCM as Relaying Party to ADFS	-
Finish		Y
	< Previous Next > Cancel	Help

6. Scegliere Consenti a tutti gli utenti di accedere a questo componente e fare clic su Avanti.

🙀 Add Relying Party Trust V	Nizard	(
Choose Issuance Auth	norization 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. Selezionare Apri la finestra di dialogo Modifica regole attestazione per l'attendibilità del componente alla chiusura della procedura guidata e fare clic su Chiudi.

🙀 Add Relying Party Trust	Wizard	X
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	
	Oose	

8. Fare clic su Aggiungi regola.

📬 Edit Claim Rules for CUCM			
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules			
The following transform rules specify the claims that w	ill be sent to the relying party.		
Order Rule Name	Issued Claims		
	•		
Add Rule Edit Rule Remove Rule			
ОК Са	ancel Apply Help		

9. Fare clic su Avanti con il modello di regola Attestazione predefinito impostato su Invia attributi LDAP come attestazioni.

🙀 Add Transform Claim Ruk	e Wizard	×
Select Rule Template		
Steps Choose Rule Type	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 LDAP Attributes as Claims Caim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute south 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. In Configura regola, immettere il nome della regola di attestazione, selezionare Active Directory come archivio attributi, configurare Attributo LDAP e Tipo di attestazione in uscita come mostrato in questa immagine e fare clic su Fine.



- L'attributo LDAP (Lightweight Directory Access Protocol) deve corrispondere all'attributo Sincronizzazione directory in CUCM.

- "uid" deve essere in lettere minuscole.

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 incred from the add.		
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. Fare clic su Aggiungi regola, selezionare Invia attestazioni utilizzando una regola personalizzata come modello di regola attestazione e fare clic su Avanti.

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

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	Qaim 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 an incoming claim value matches a complex pattern Sending claims for use only in later rules Tell me more about this rule template
	< Previous Next > Cancel Help

12. Immettere un nome per il nome della regola attestazione e copiare questa sintassi nello spazio indicato in Regola personalizzata:

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

(NOTA: se si copia e si incolla il testo da questi esempi, tenere presente che alcuni programmi di elaborazione testi sostituiranno le virgolette ASCII (") con le versioni UNICODE (""). Le versioni UNICODE impediranno il corretto funzionamento della regola attestazione.)

X

Add Transform Claim Rul	e Wizard	×
Configure Rule		
Steps Choose Rule Type	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 Rule	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: "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou 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/pname qualifier"] = "CUCM.CISCOLIVE.COM");	
	< Previous Finish Cancel Help	

Nota:

- Il nome di dominio completo (FQDN) CUCM e ADFS è precompilato con il nome di dominio completo (CUCM) e ADFS lab in questo esempio e deve essere modificato in base all'ambiente.

- Il nome di dominio completo (FQDN) di CUCM/ADFS fa distinzione tra maiuscole e minuscole e deve corrispondere ai file di metadati.

- 13. Fare clic su Finish (Fine).
- 14. Fare clic su Apply (Applica), quindi su OK.
- 15. Riavviare il servizio AD FS versione 2.0 da Services.msc.

Aggiungi messaggistica immediata CUCM e presenza come attendibilità componente

- 1. Ripetere i passi da 1 a 11 come descritto per Aggiungi CUCM come attendibilità componente e andare al passo 2.
- 2. Immettere un nome per il nome della regola attestazione e copiare questa sintassi nello spazio indicato in Regola personalizzata:

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

🙀 Add Transform Claim Ri	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:
	Custom Rule for IMP
	Rule template: Send Claims Using a Custom Rule
	Custom rule:
	<pre>"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou 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"] = "IMP.ciscolive.com");</pre>
	< Previous Finish Cancel Help

Si noti che l'FQDN di messaggistica immediata e presenza e ADFS è precompilato con l'IM lab e la Presenza e ADFS in questo esempio e deve essere modificato in base all'ambiente.

3. Fare clic su Finish (Fine).

- 4. Fare clic su Apply (Applica), quindi su OK.
- 5. Riavviare il servizio AD FS versione 2.0 da Services.msc.

Aggiungi UCXN come attendibilità componente

- 1. Ripetere i passi da 1 a 12 come descritto per Aggiungi CUCM come attendibilità componente e andare al passo 2.
- 2. Immettere un nome per il nome della regola attestazione e copiare questa sintassi nello spazio specificato in Regola personalizzata:

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

🙀 Add Transform Claim Ru	le 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 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

Si noti che l'FQDN di UCXN e ADFS è precompilato con l'UCXN e l'ADFS lab in questo esempio e deve essere modificato in base all'ambiente.

- 3. Fare clic su Finish (Fine).
- 4. Fare clic su Apply (Applica), quindi su OK.
- 5. Riavviare il servizio AD FS versione 2.0 da Services.msc.

Aggiungi Cisco Prime Collaboration Provisioning come attendibilità componente

- 1. Ripetere i passi da 1 a 12 come descritto per Aggiungi CUCM come attendibilità componente e andare al passo 2.
- 2. Immettere un nome per il nome della regola attestazione e copiare questa sintassi nello spazio specificato in Regola personalizzata:

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

🙀 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/name qualifier"] = "http:///ADFS1.ciscolive.com/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "PCP.ciscolive.com"; More about the claim rule language	
	< Previous Finish Cancel Help	

Si noti che Prime Provisioning e FQDN di AD FS sono precompilati con PCP (Prime Collaboration Provisioning) e AD FS di questo esempio e devono essere modificati in base all'ambiente.

- 3. Fare clic su Finish (Fine).
- 4. Fare clic su Apply (Applica), quindi su OK.
- 5. Riavviare il servizio AD FS versione 2.0 da Services.msc.

Dopo aver configurato ADFS versione 2.0, procedere all'abilitazione di SAML SSO sui prodotti Cisco Collaboration.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

ADFS registra i dati di diagnostica nel registro eventi di sistema. Da Server Manager sul server AD FS aprire Diagnostica -> Visualizzatore eventi -> Applicazioni e servizi -> AD FS 2.0 -> Amministrazione

Cerca errori registrati per l'attività ADFS



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).