

Configurare una singola connessione/contratto IdP SAML per cluster con AD FS versione 2.0

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Esportare i metadati SP da CUCM](#)

[Passaggio 2. Scaricare i metadati IDP da ADFS](#)

[Passaggio 3. IdP provisioning](#)

[Passaggio 4. Abilitazione di SAML SSO](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare una connessione o un contratto Single Security Assertion Markup Language (SAML) Identity Provider (IdP) per cluster con Active Directory Federation Service (ADFS).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM) versione 11.5 o successive
- Cisco Unified Communications Manager IM e Presence versione 11.5 o successive
- Active Directory Federation Service versione 2.0

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Active Directory Federation Service versione 2.0 come IdP
- Cisco Unified Communications Manager versione 11.5
- Cisco IM e Presence Server versione 11.5

Premesse

Per l'SSO SAML, deve essere un circolo di fiducia tra il provider di servizi (SP) e l'IdP. Il trust viene creato come parte dell'abilitazione SSO, quando viene scambiato il trust (metadati).

Scaricare i metadati da CUCM e caricarli in IdP, analogamente scaricare i metadati da IdP e caricarli in CUCM.

Nelle versioni precedenti di CUCM 11.5, il nodo di origine genera il file di metadati e raccoglie i file di metadati dagli altri nodi del cluster. Tutti i file di metadati vengono aggiunti a un singolo file zip e quindi presentati all'amministratore. L'amministratore deve decomprimere questo file e effettuare il provisioning di ogni file nel provider di identità. Ad esempio, 8 file di metadati per un cluster a 8 nodi.

A partire dalla versione 11.5 è stata introdotta una singola connessione/accordo IdP SAML per ogni funzionalità cluster. Come parte di questa funzionalità, CUCM genera un singolo file di metadati Service Provider per tutti i nodi CUCM e IMP nel cluster. Il nuovo formato del nome per il file di metadati è **<hostname>-single-agreement.xml**

In pratica, un nodo crea i metadati e li invia ad altri nodi SP nel cluster. Ciò semplifica il provisioning, la manutenzione e la gestione. Ad esempio, 1 file di metadati per un cluster a 8 nodi.

Il file di metadati a livello di cluster utilizza il certificato multiserver tomcat che garantisce che la coppia di chiavi venga utilizzata sia uguale per tutti i nodi del cluster. Il file di metadati dispone inoltre di un elenco di URL di Assertion Consumer Service (ACS) per ogni nodo nel cluster.

CUCM e Cisco IM e Presence versione 11.5 Supportano sia le modalità SSO, a **livello di cluster** (un file di metadati per cluster) che per nodo (modello esistente).

In questo documento viene descritto come configurare la modalità estesa a tutto il cluster di SAML SSO con AD FS 2.0.

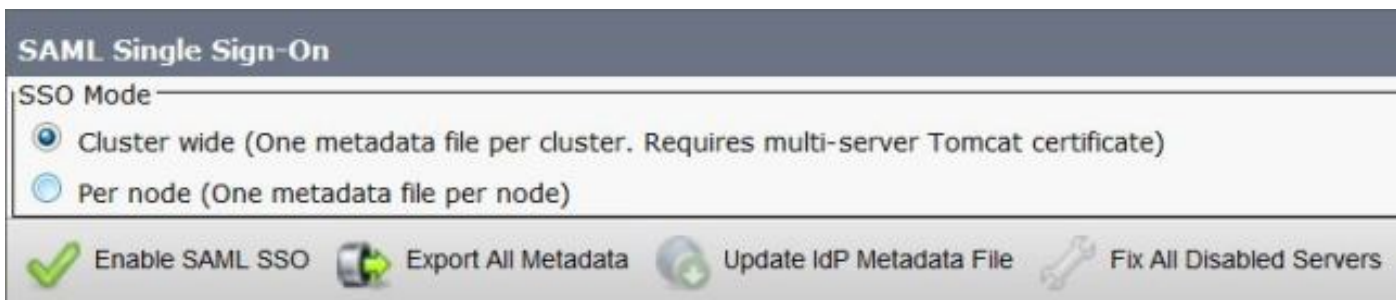
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

Passaggio 1. Esportare i metadati SP da CUCM

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

Per impostazione predefinita, è selezionato il pulsante di opzione **Cluster Wide**. Fare clic su **Esporta tutti i metadati**. Il file di dati dei metadati presentato all'amministratore nel nome **<hostname>-single-agreement.xml**

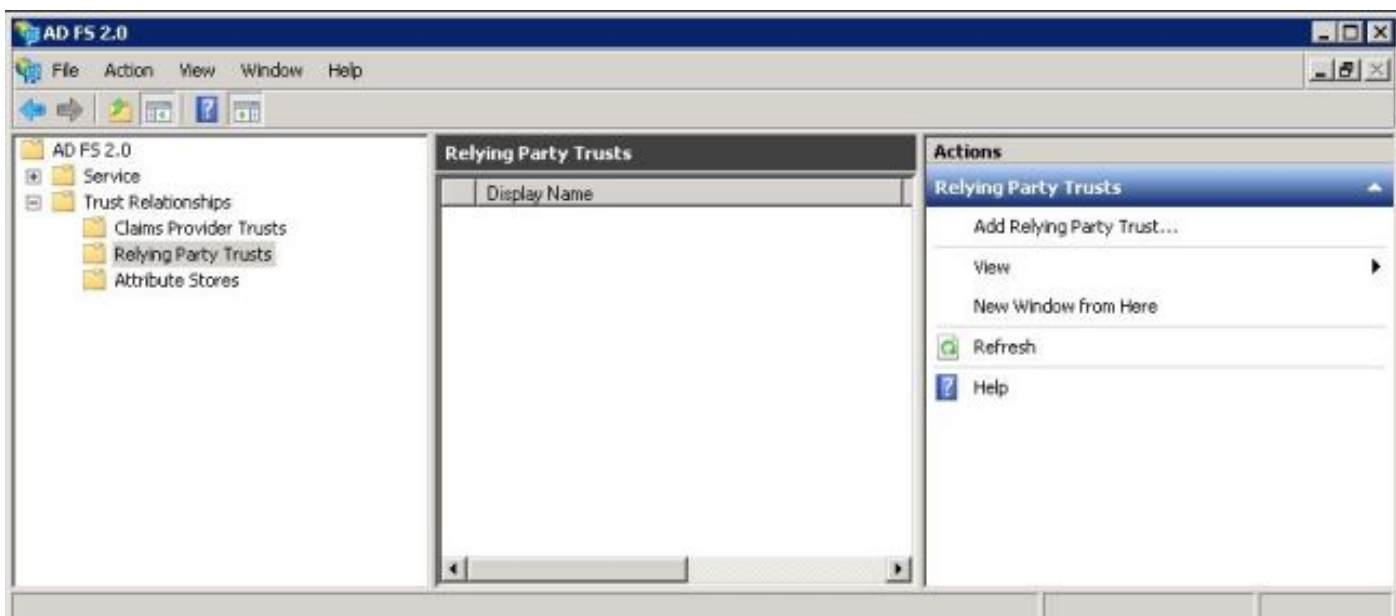


Passaggio 2. Scaricare i metadati IDP da ADFS

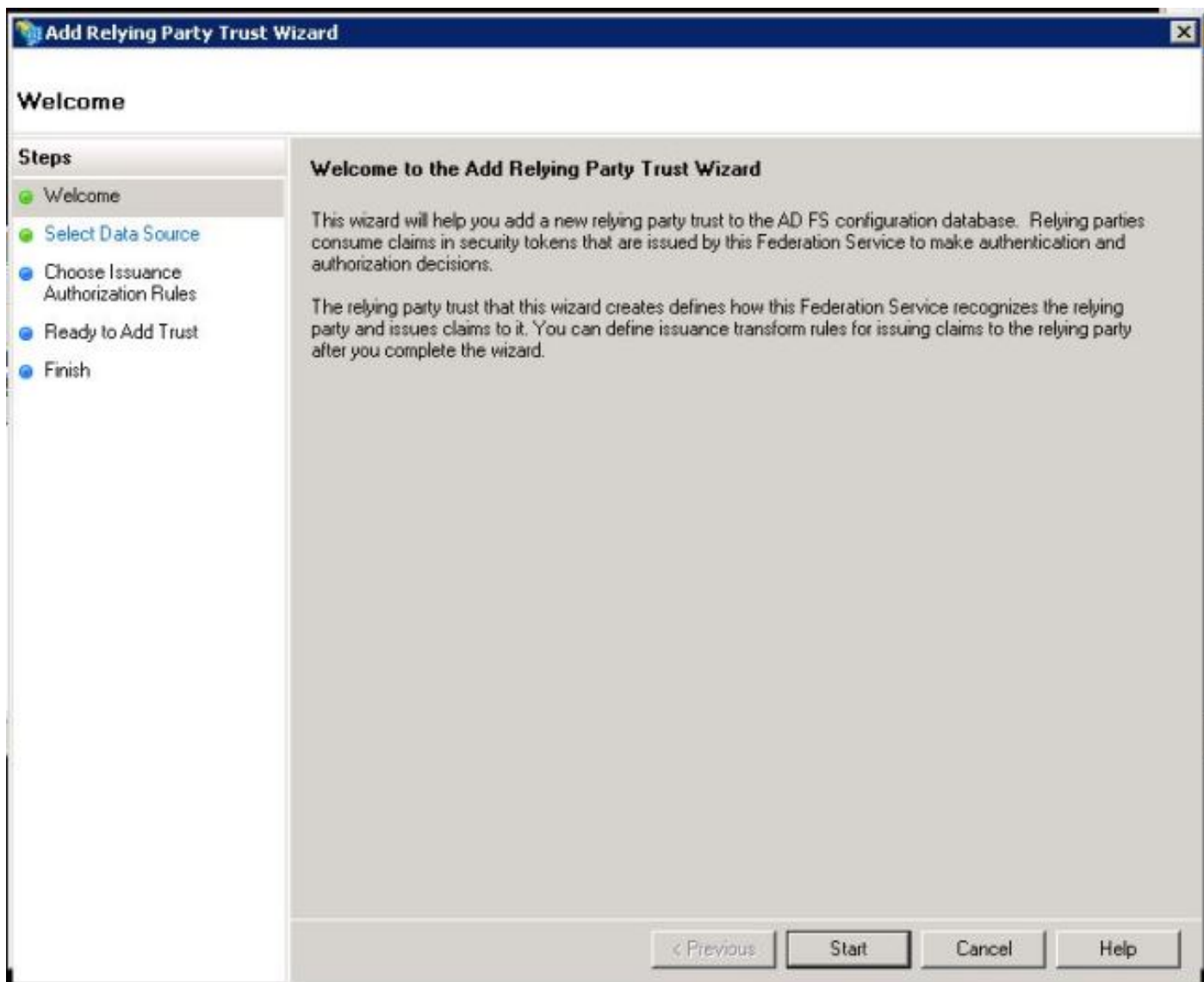
Per scaricare i metadati IdP, fare riferimento al collegamento [https:// <FQDN di ADFS>/federationmetadata/2007-06/federationmetadata.xml](https://<FQDN di ADFS>/federationmetadata/2007-06/federationmetadata.xml)

Passaggio 3. IdP provisioning

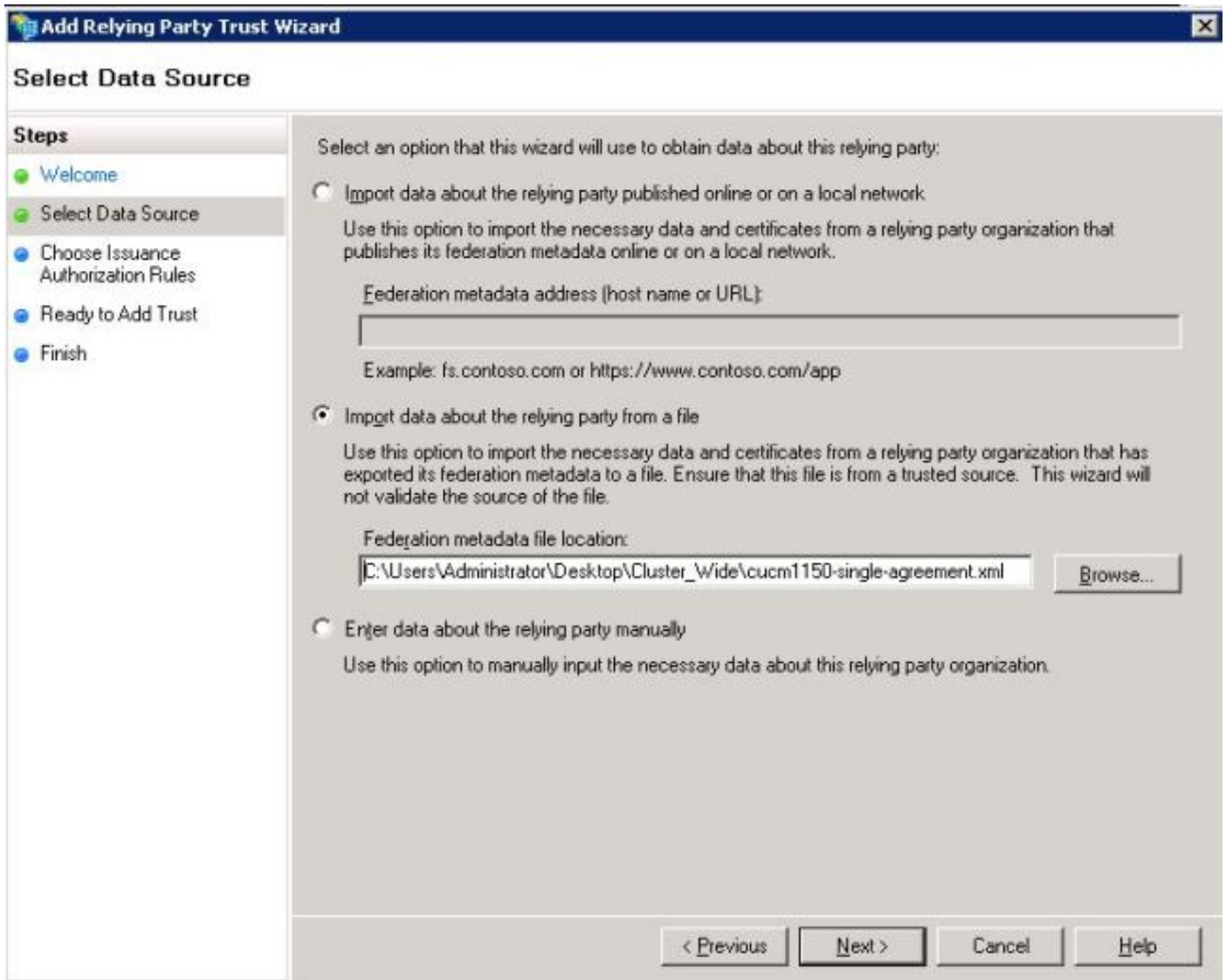
Come illustrato nell'immagine, passare a **Gestione AD FS 2.0/relazione di trust Spedizioni/attendibilità componente attendibilità**. Fare clic su **Aggiungi attendibilità componente**.



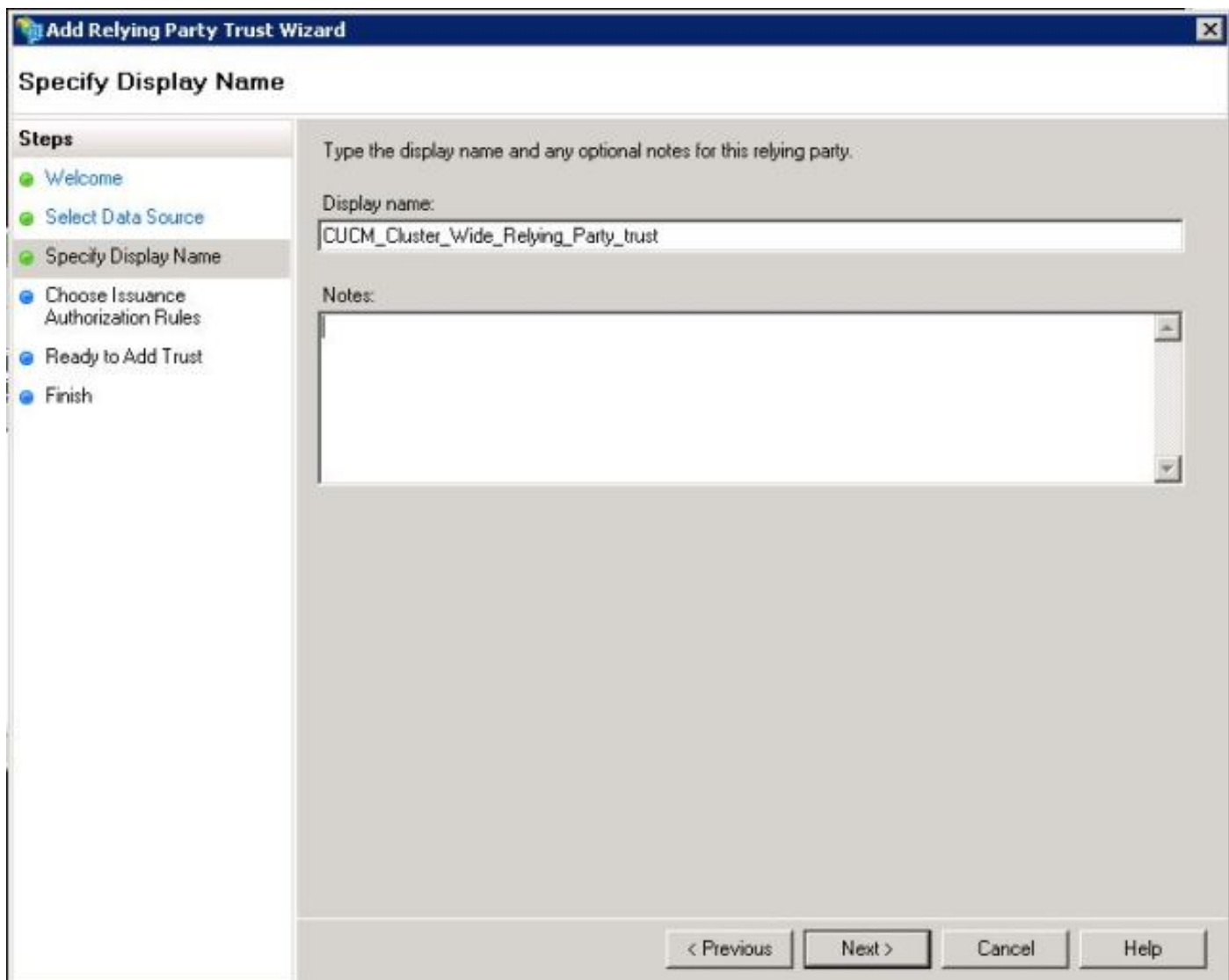
Verrà aperta l'Aggiunta guidata attendibilità componente come illustrato nell'immagine. Fare clic su **Start**.



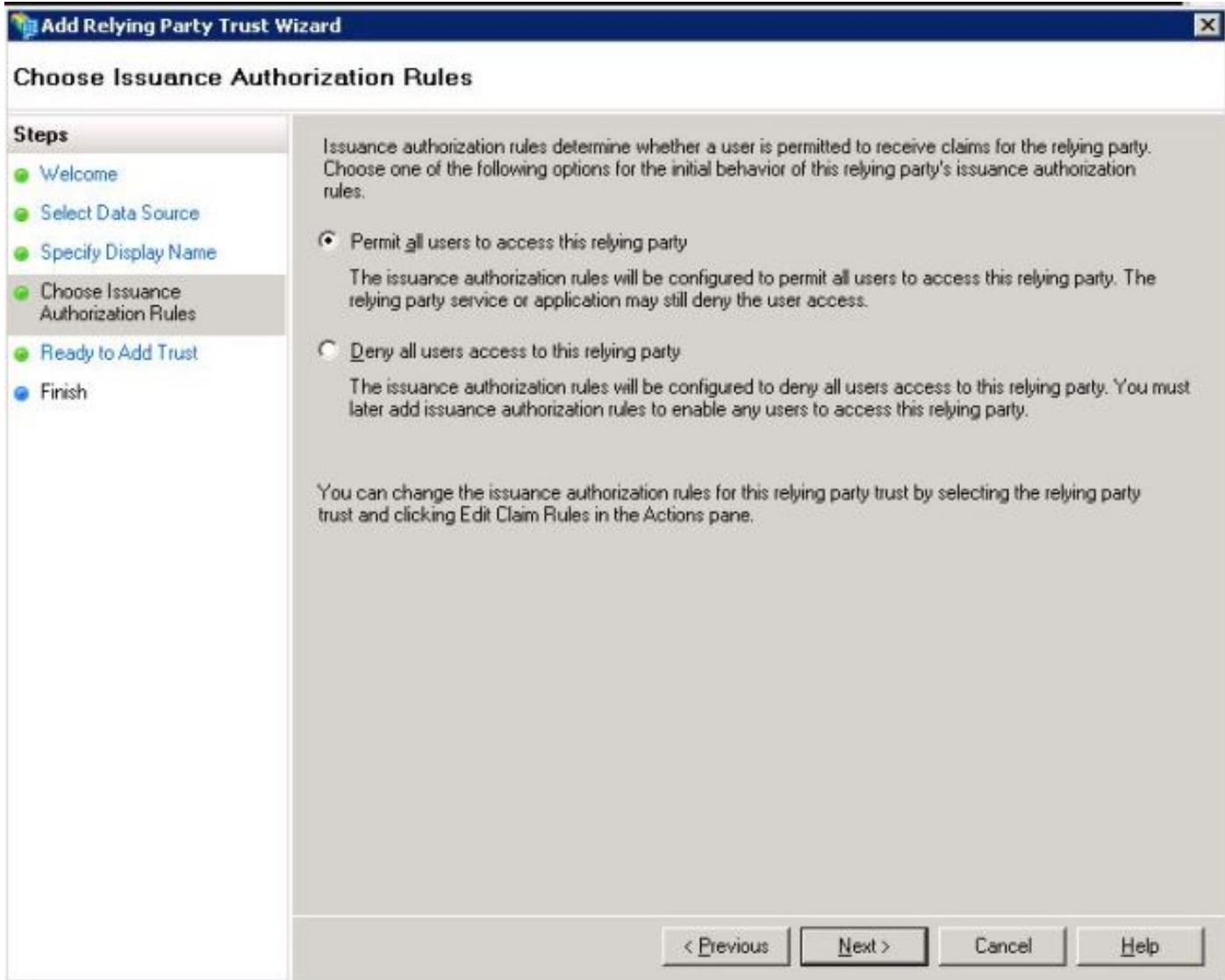
Fare clic sui dati di importazione relativi al componente da un file. Sfoglia i metadati SP scaricati dalla pagina Configurazione SAML SSO CUCM. Fare quindi clic su **Next** (Avanti), come mostrato nell'immagine:



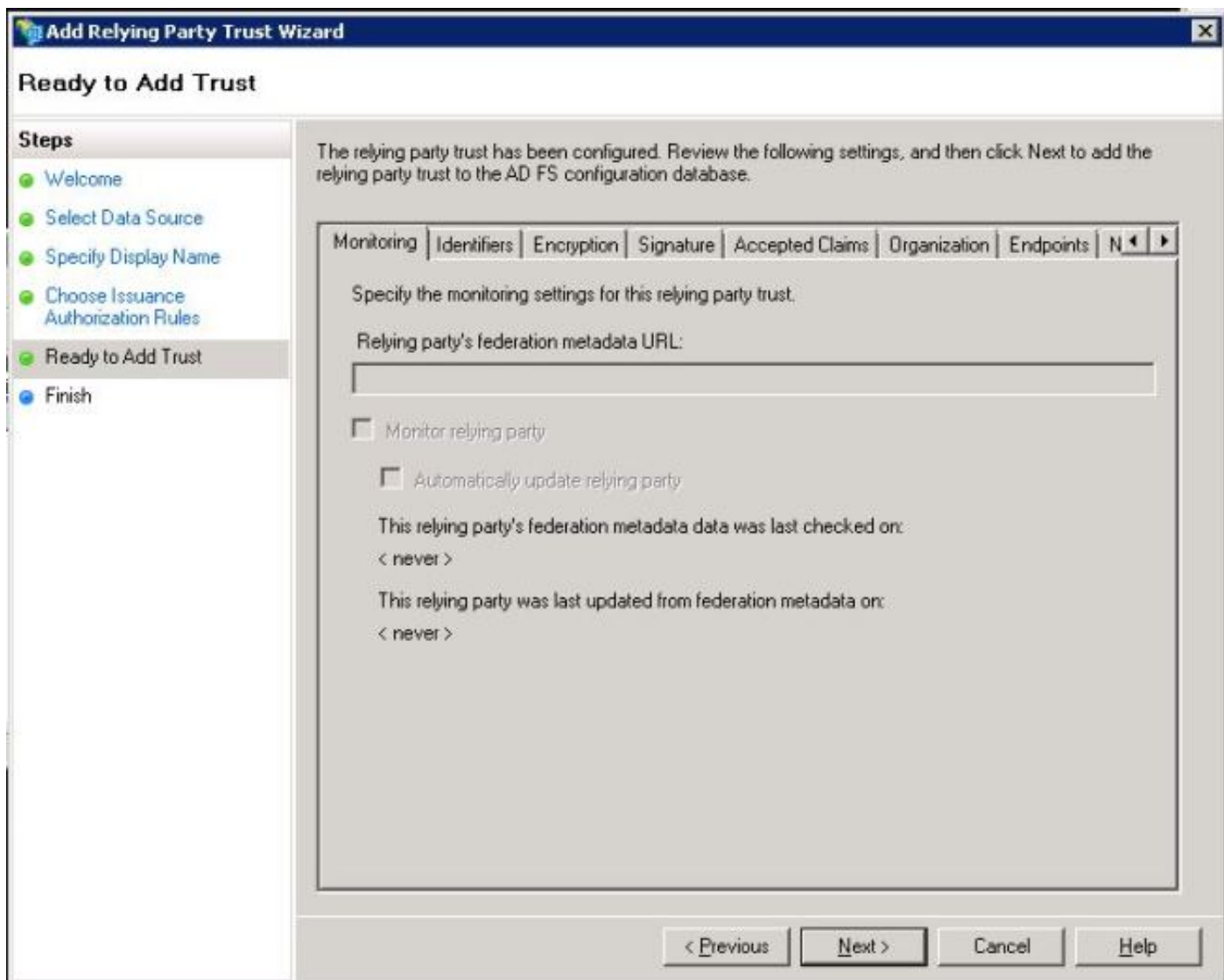
Digitare il nome visualizzato ed eventuali note facoltative per il componente. Fare clic su **Next**. (Avanti), come mostrato nell'immagine:



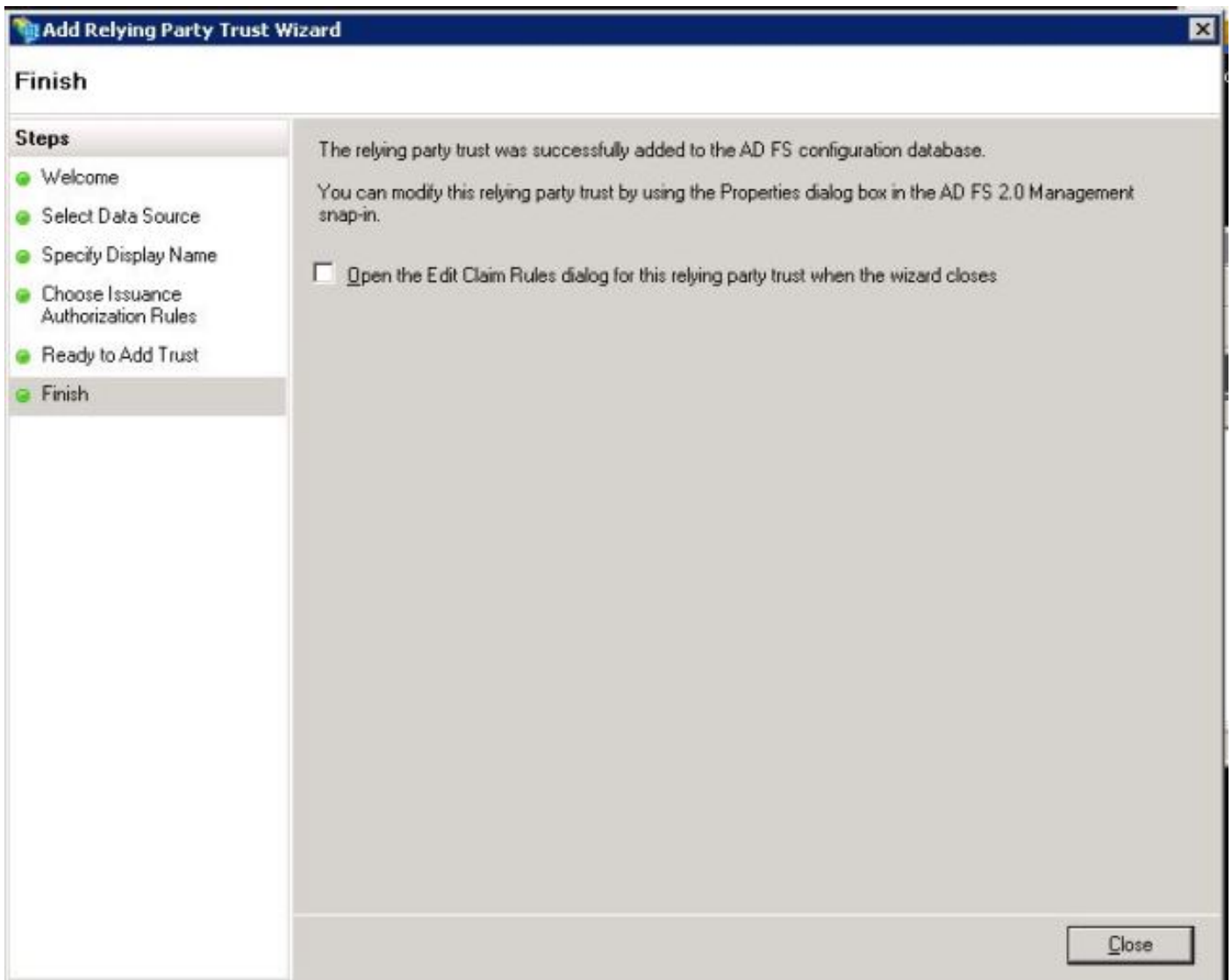
Selezionare **Consenti a tutti gli utenti di accedere a questo componente** per consentire a tutti gli utenti di accedere a questo componente, quindi fare clic su **Avanti**, come mostrato nell'immagine:



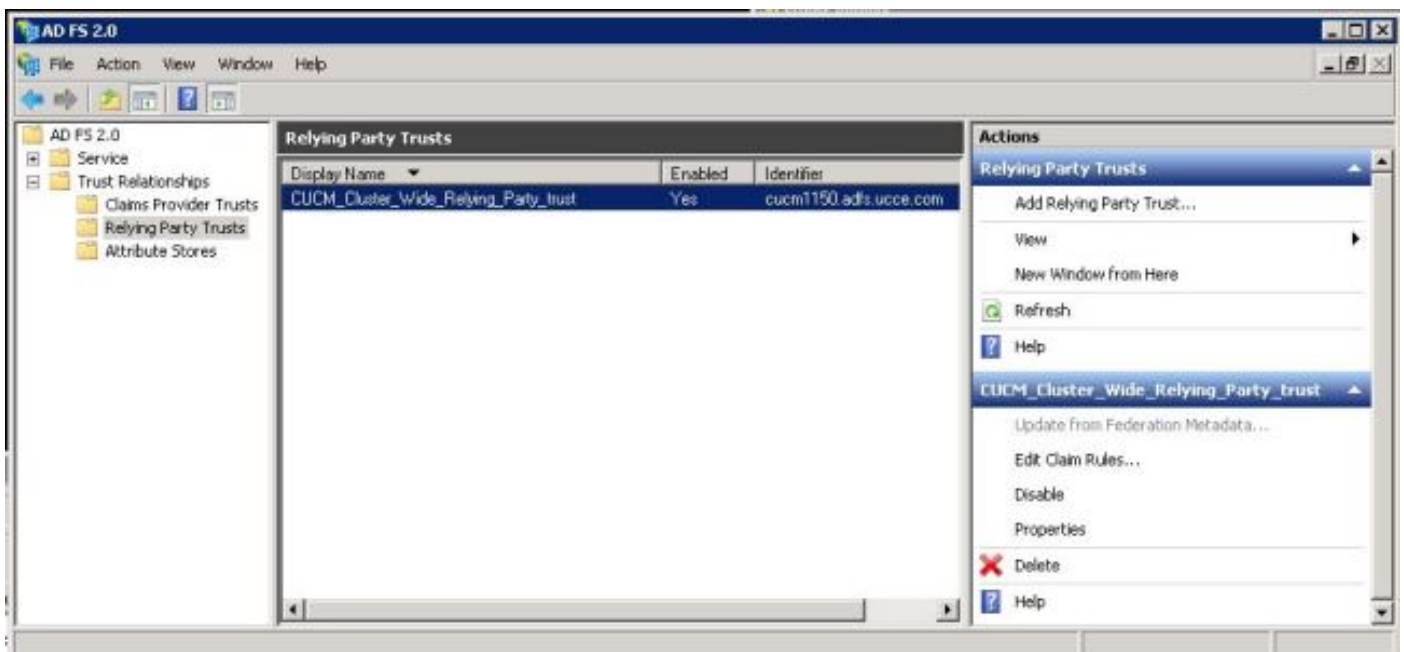
Nella pagina **Pronto per l'aggiunta del trust** è possibile rivedere le impostazioni per il trust della relying party configurato. Fare clic su **Next** (Avanti), come mostrato nell'immagine:



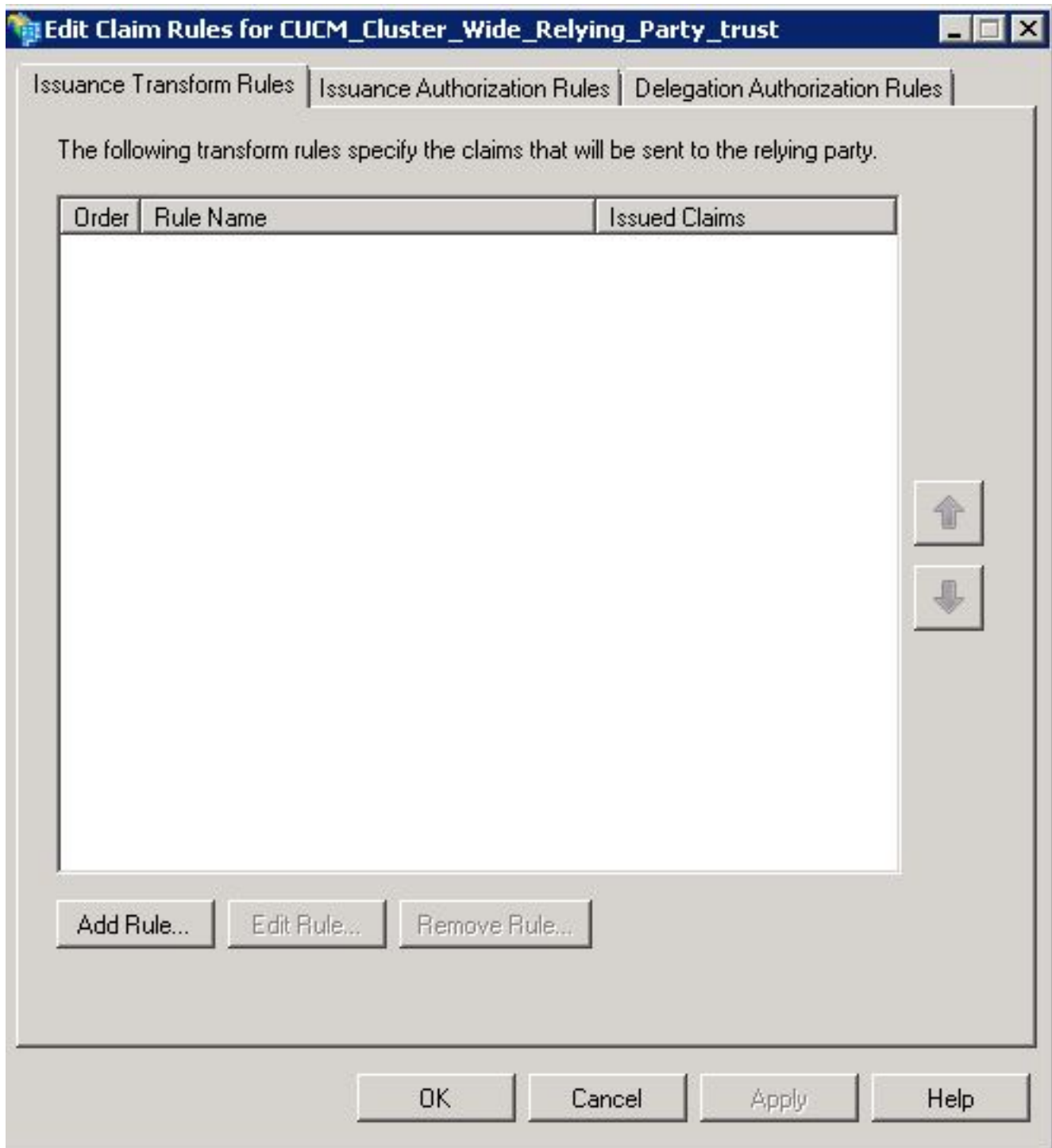
Pagina Fine conferma che l'attendibilità del componente è stata aggiunta correttamente al database di configurazione di AD FS. Deselezionare la casella e fare clic su **Chiudi**, come mostrato nell'immagine:



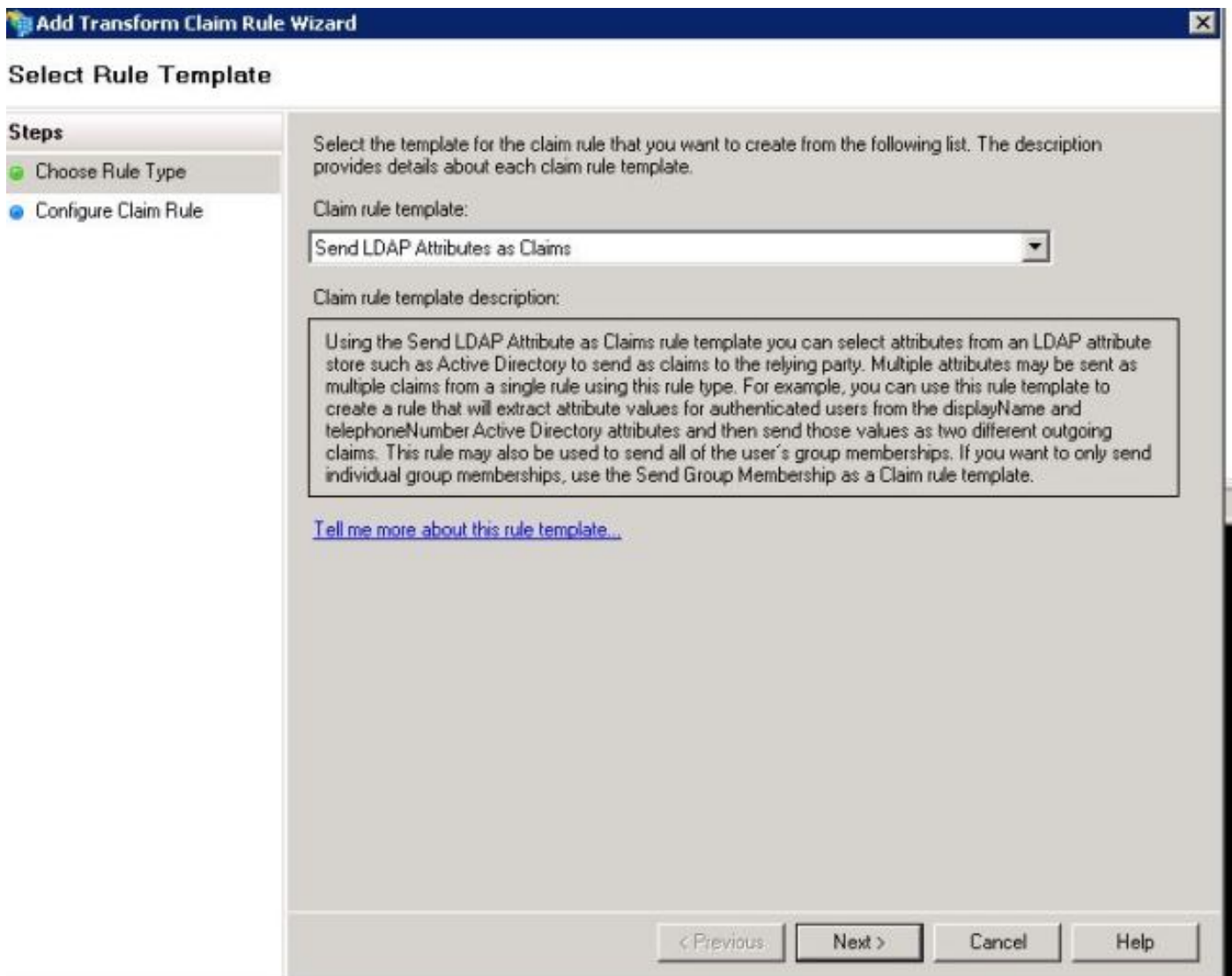
Fare clic con il pulsante destro del mouse su **Attendibilità componente** e scegliere **Modifica regole attestazione**, come illustrato nell'immagine:



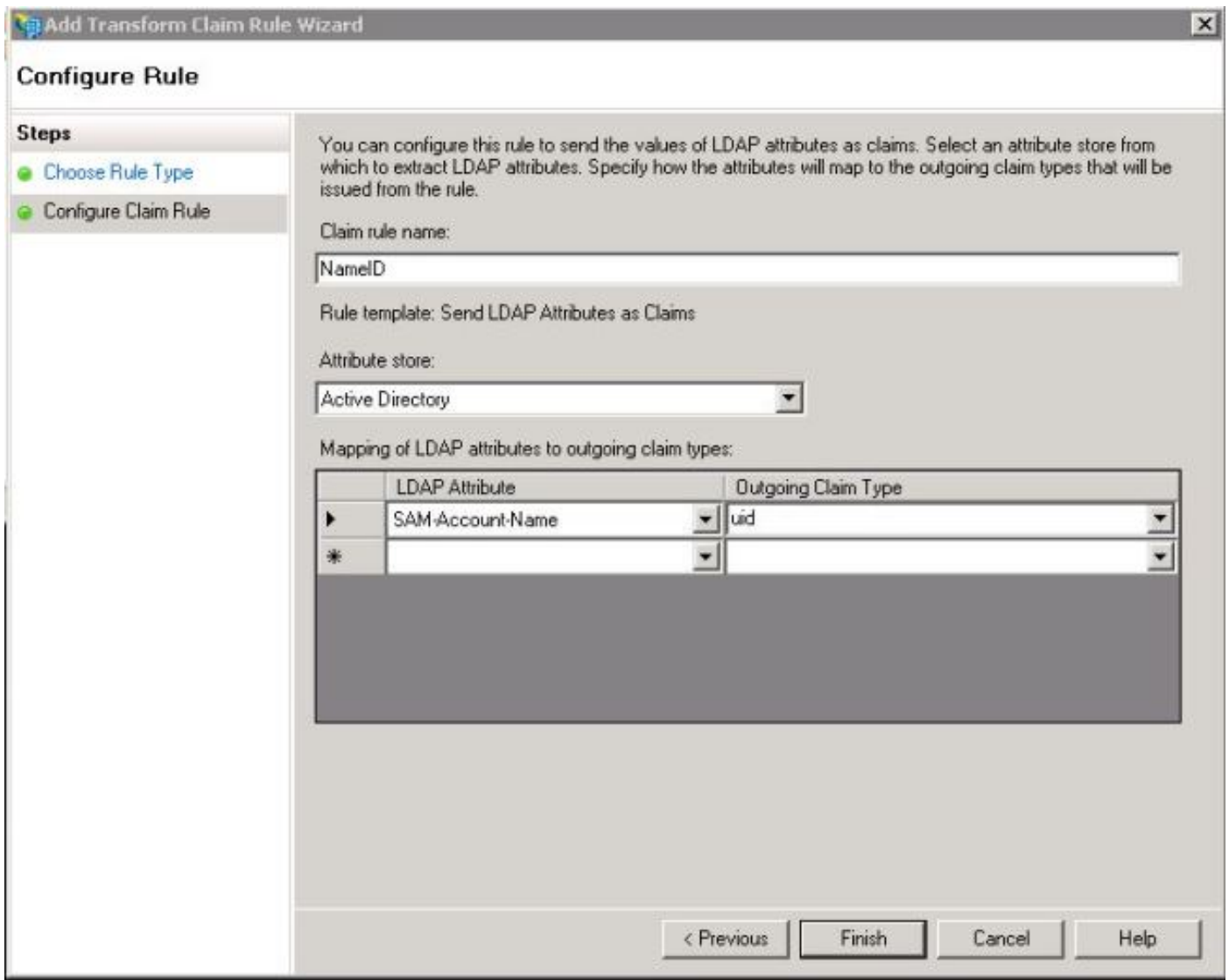
Fare clic su **Add Rule.**, come mostrato nell'immagine:



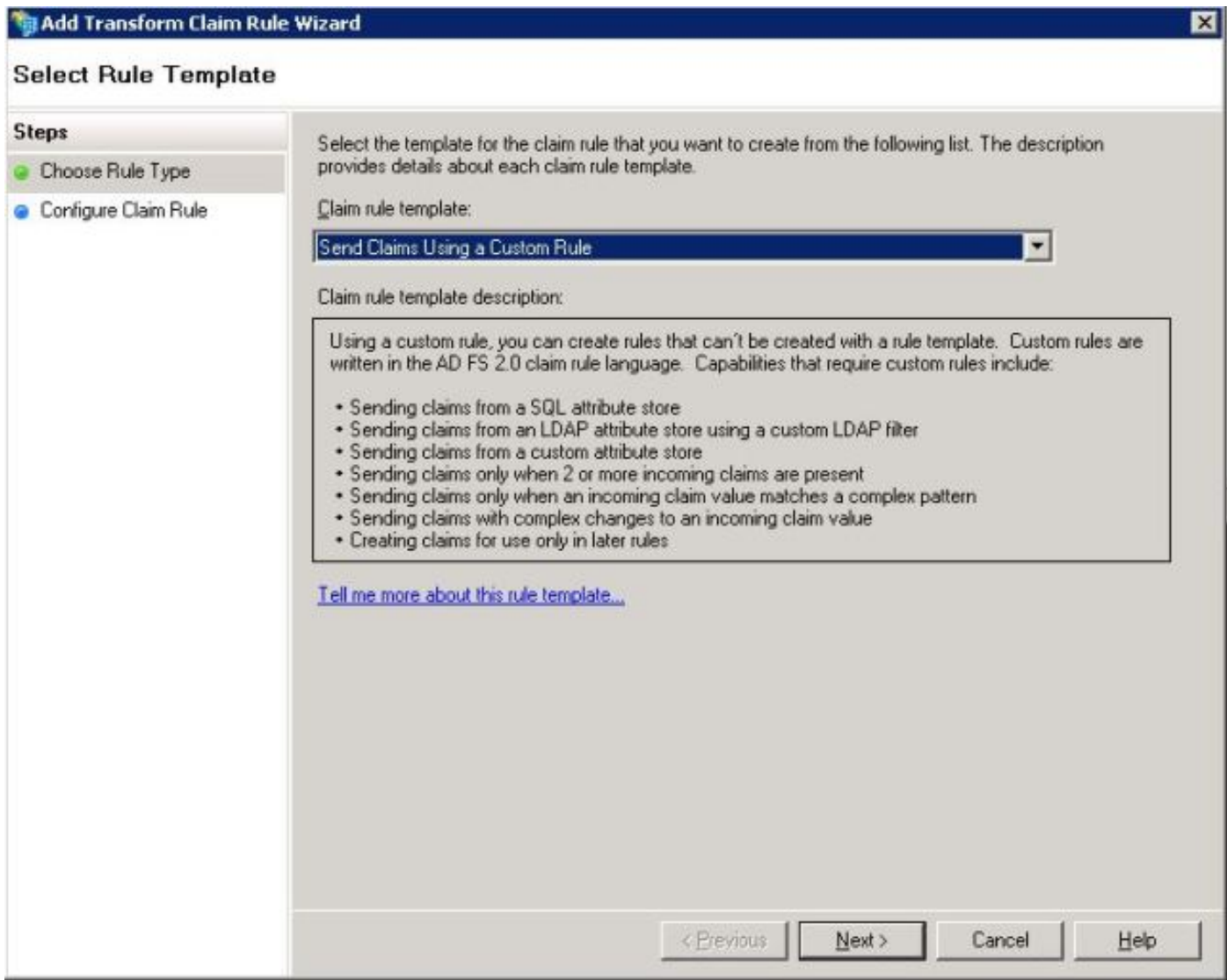
Quando si apre **Aggiungi regola attestazione di trasformazione**, fare clic su **Avanti** con il modello di regola attestazione predefinito **Invia attributi LDAP come attestazioni**, come mostrato nell'immagine:



Fare clic su **Configura regola attestazione** come mostrato in questa immagine. L'attributo LDAP deve corrispondere all'attributo LDAP nella configurazione della directory LDAP in CUCM. Gestire il tipo di attestazione in uscita come **uid**. Fare clic su **Finish** (Fine), come mostrato nell'immagine:



Aggiungere la regola personalizzata per il componente. Fare clic su **Aggiungi regola**. Selezionare **Invia attestazioni utilizzando una regola personalizzata** e quindi fare clic su **Avanti**, come illustrato nell'immagine:

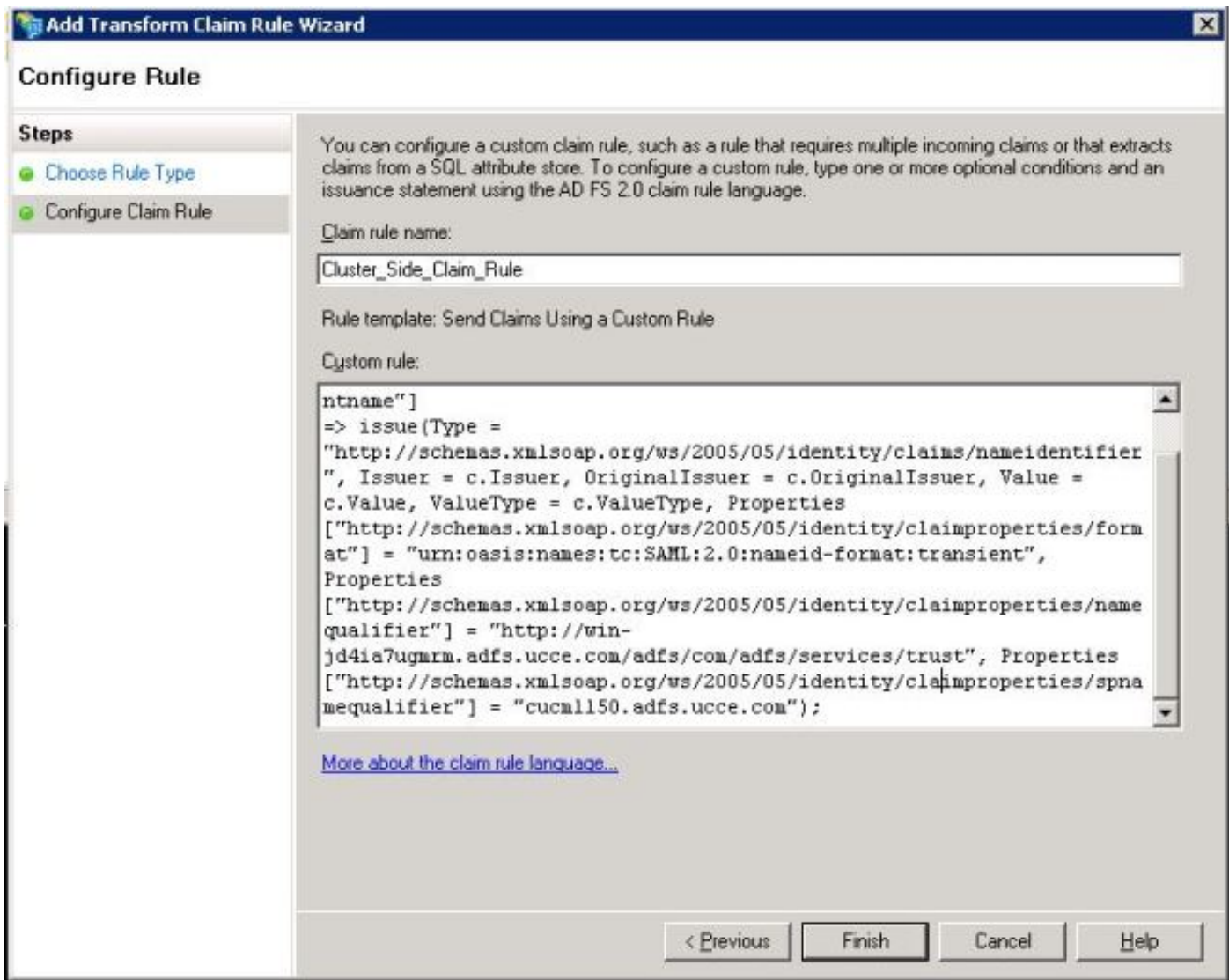


In Configura regola attestazione digitare un Nome regola attestazione, quindi Copiare la regola attestazione specificata e passata nel campo Regola personalizzata della procedura guidata per modificare il qualificatore namequalifier e spname nella regola attestazione. Fare clic su **Finish.**, come mostrato nell'immagine:

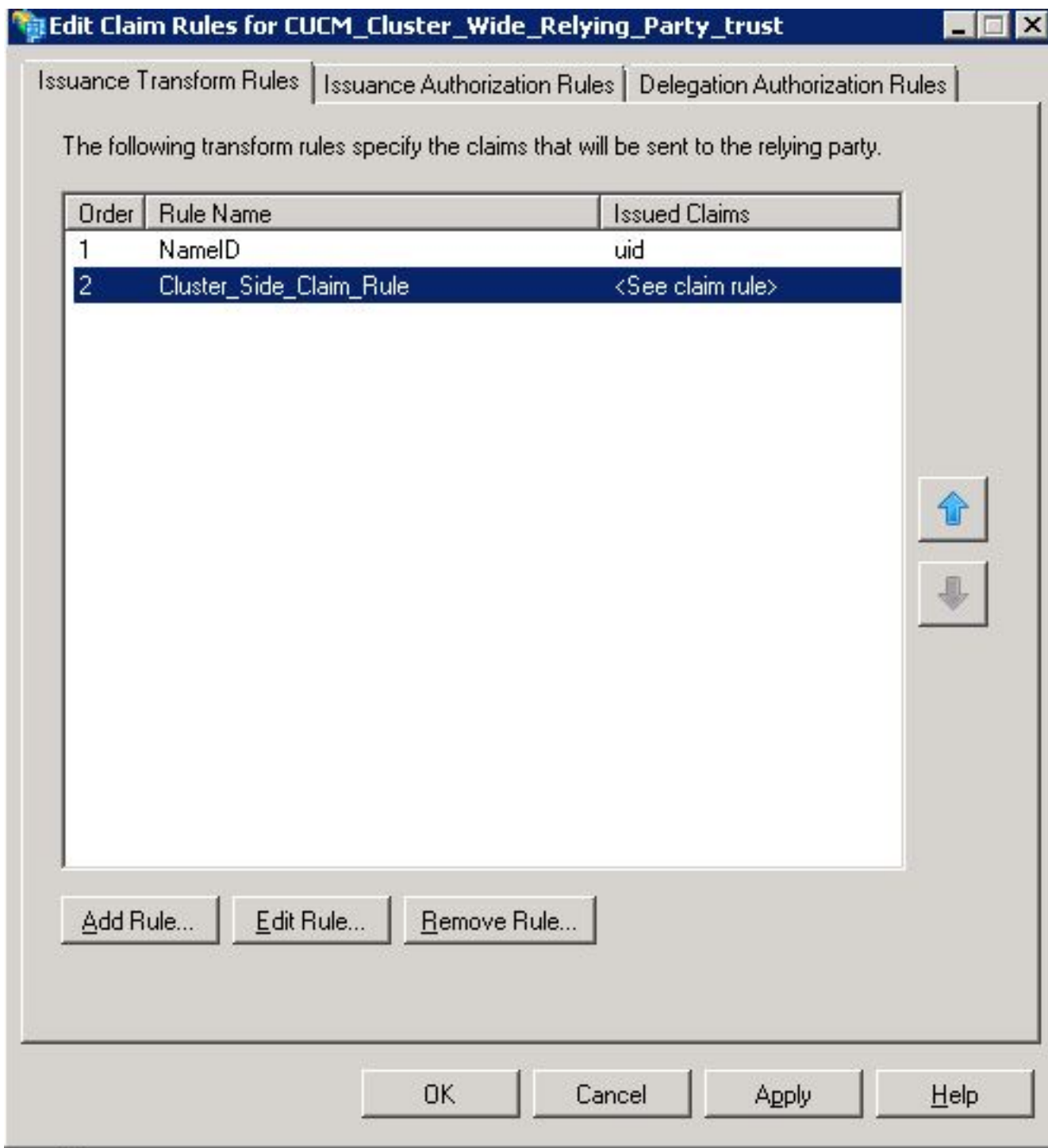
Regola attestazione:

```
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.



Come mostrato nell'immagine, fare clic su **Apply (Applica)**, quindi su **OK**.



Passaggio 4. Abilitazione di SAML SSO

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

Per impostazione predefinita, è selezionato il pulsante di opzione **Cluster Wide**. Fare clic su **Enable Saml SSO** (Abilita SSO SAML), come mostrato nell'immagine:

SAML Single Sign-On

SSO Mode

- Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)
- Per node (One metadata file per node)



Enable SAML SSO



Export All Metadata



Update IdP Metadata File



Fix All Disabled Servers

Come mostrato nell'immagine, il popup notifica l'avviso per il riavvio del server Web e le informazioni per scegliere l'SSO SAML a livello di cluster o l'SSO SAML per nodo in base all'idp. Fare clic su **Continue** (Continua).



Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.



Click "Export All Metadata" button

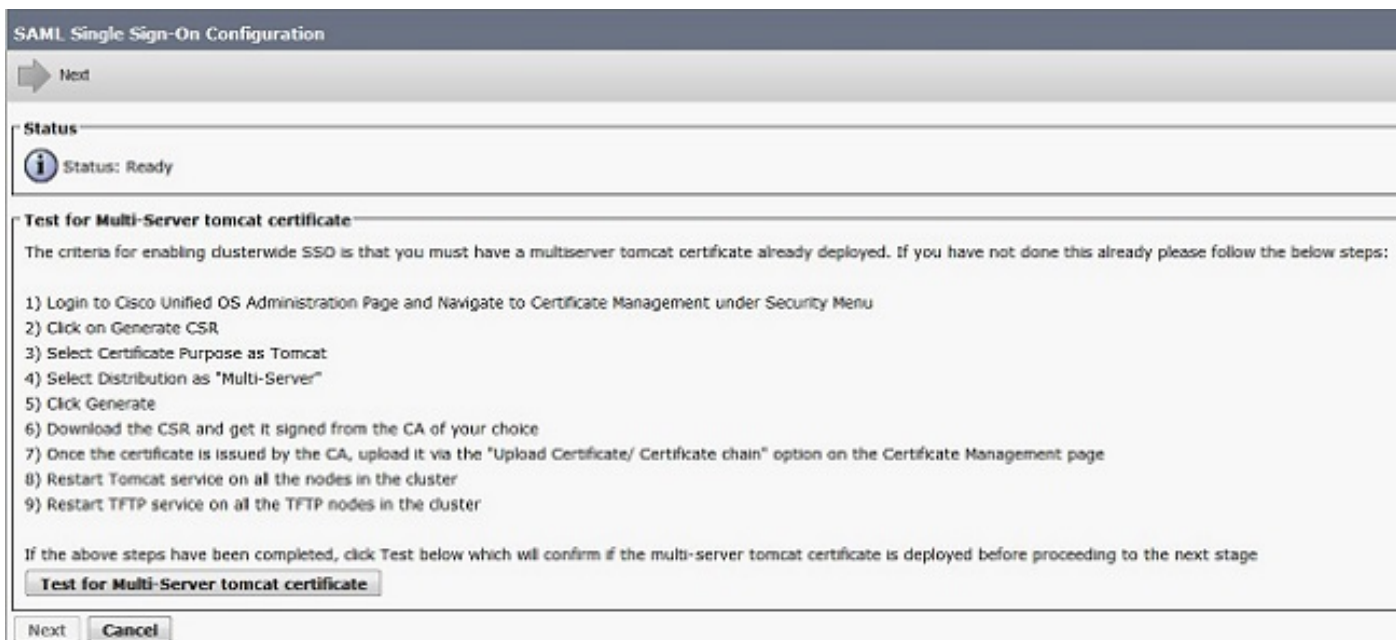
If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.

If IDP is provisioned with cluster-wide SP metadata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.

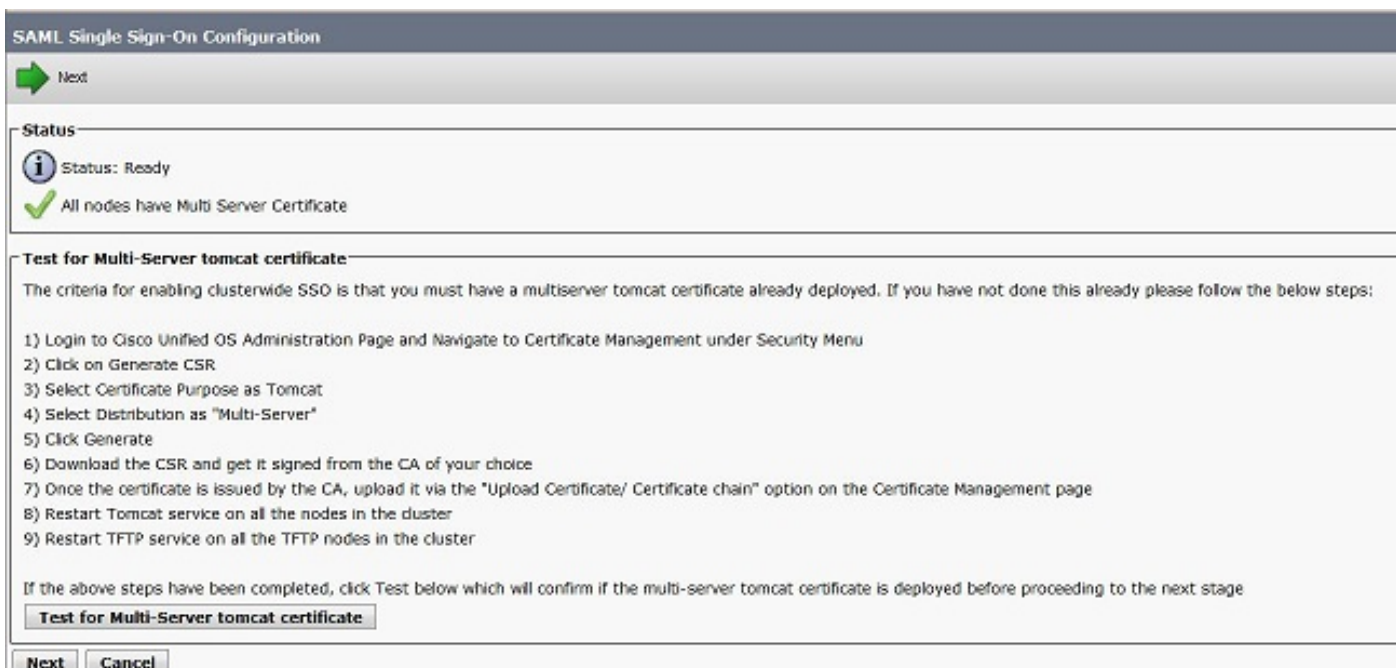
Continue

Cancel

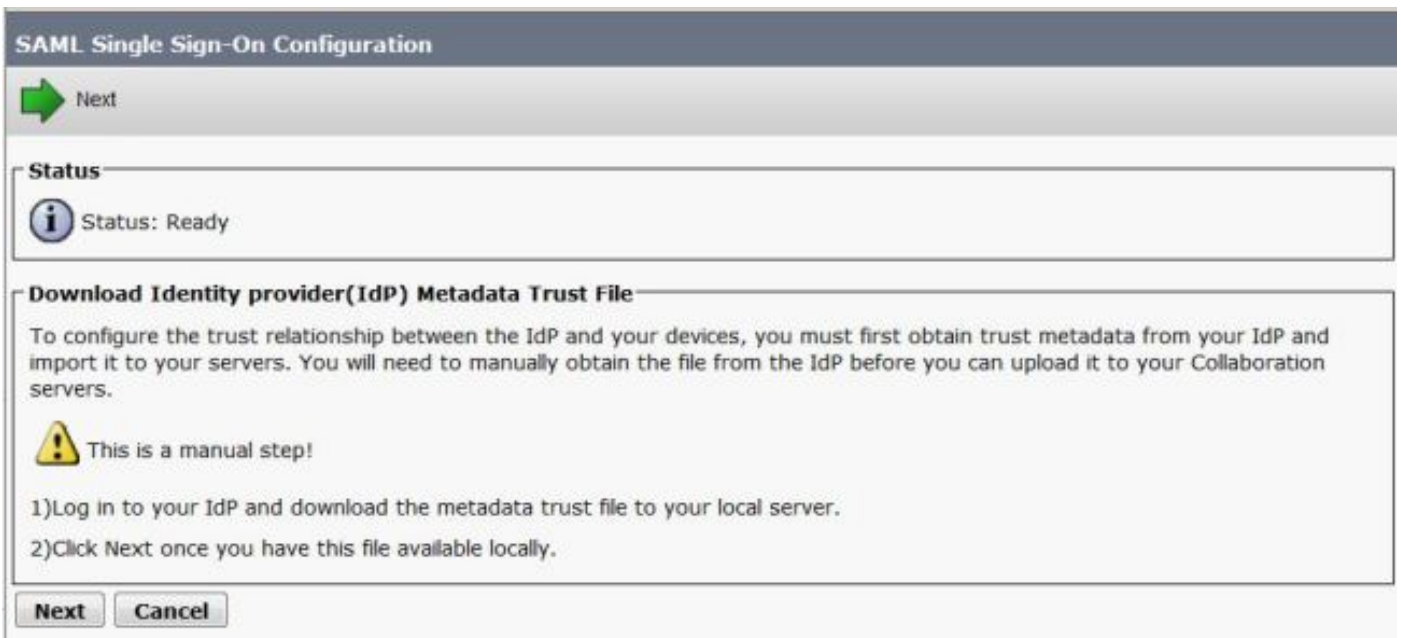
Per abilitare l'SSO a livello di cluster, è necessario disporre di un certificato tomcat multiserver già distribuito. Fare clic su **Test for Multi-Server tomcat Certificate**, come mostrato nell'immagine:



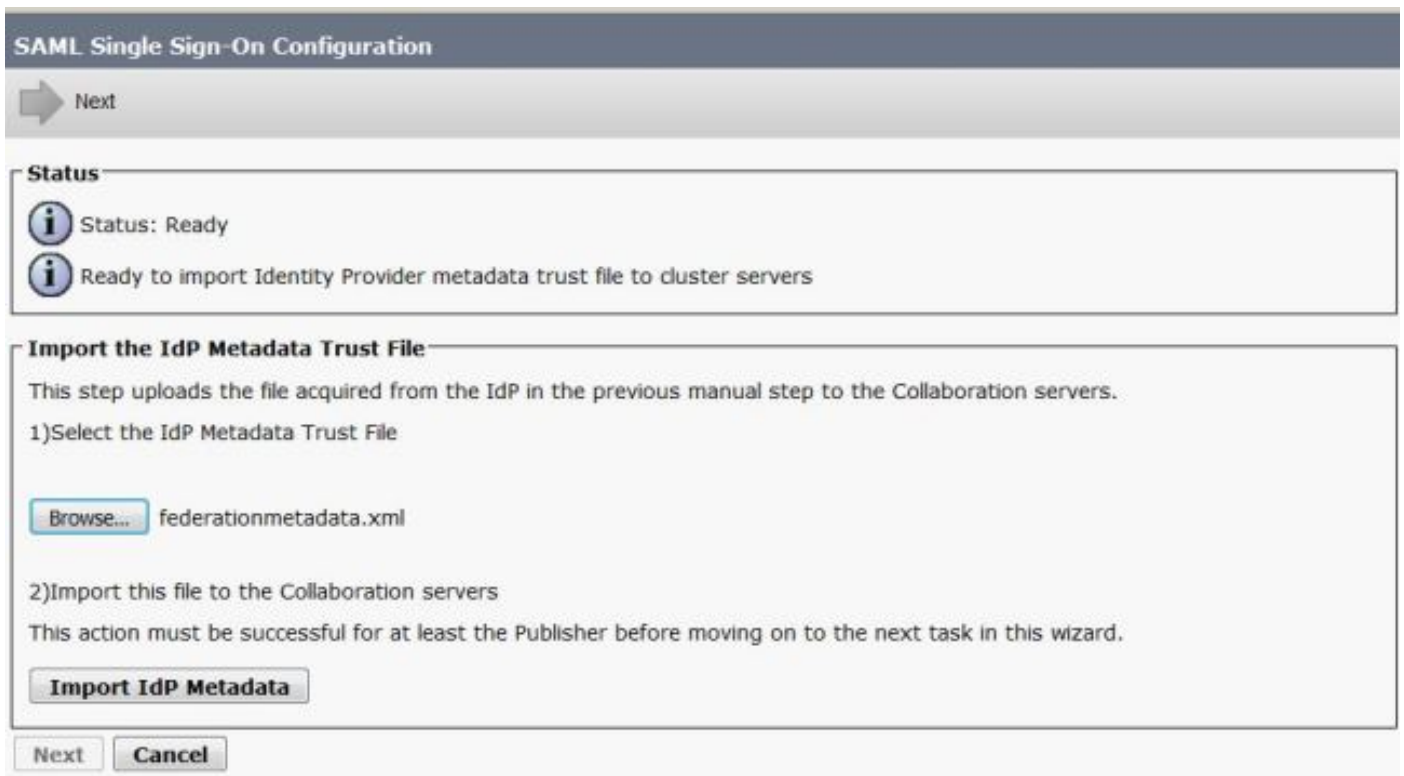
Dopo la conferma, in tutti i nodi viene visualizzato il messaggio Certificato multiserver in cui è indicato che **Tutti i nodi dispongono di un certificato multiserver** e quindi fare clic su **Avanti**, come illustrato nell'immagine:



Come mostrato nell'immagine, fare clic su **Avanti**.




Individuare e selezionare i metadati IdP scaricati. Fare clic su **Importa metadati IdP**, come mostrato nell'immagine:





La pagina conferma che l'importazione è stata completata per tutti i server e quindi fa clic su **Avanti**, come mostrato nell'immagine:

SAML Single Sign-On Configuration

 Next

Status

-  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

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 succeeded for all servers

Come mostrato nell'immagine, fare clic su **Avanti**, poiché i metadati SP sono già stati esportati dalla pagina di configurazione iniziale di SAML SSO.

SAML Single Sign-On Configuration

 Back  Next


Status

-  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


 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.

CUCM deve essere sincronizzato con l'elenco LDAP. La procedura guidata mostra gli utenti amministratori validi configurati nella directory LDAP. Selezionare l'utente e fare clic su **Esegui test SSO**, come mostrato nell'immagine:

SAML Single Sign-On Configuration

 Back

Status


 The server metadata file must be installed on the IdP before this test is run.

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

1) Pick a valid username to use for this test

You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.


Valid administrator Usernames

samluser

2) Launch SSO test page

Come mostrato nell'immagine, immettere l'ID utente e la password quando richiesto.

Authentication Required

 Enter username and password for <https://win-jd4ia7ugmrm.adfs.ucce.com>

User Name:

Password:

Il popup, come mostrato nell'immagine, conferma che il test è riuscito.

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

Close

Come mostrato nell'immagine, fare clic su **Finish** (Fine) per completare la configurazione per l'abilitazione dell'SSO.

The screenshot shows the 'SAML Single Sign-On Configuration' page in a web interface. At the top, there is a navigation menu with items: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, and Bulk Administration. Below the menu, the page title is 'SAML Single Sign-On Configuration'. There are two navigation buttons: 'Back' (left arrow) and 'Finish' (right arrow). The main content area has a 'Status' section with a green checkmark and the text 'SSO Metadata Test Successful'. Below this is a 'Ready to Enable SSO' section with the following text: 'Clicking "Finish" will complete enabling SSO on all the servers in this cluster. There will be a short delay while the applications are being updated. To verify the SSO status of each server, check the main SSO Configuration page. Additional testing and manual uploads may be performed from the main page if necessary.' At the bottom of the page, there are three buttons: 'Back', 'Finish', and 'Cancel'.

La pagina visualizzata nell'immagine conferma che il processo di abilitazione di SAML SSO è stato avviato su tutti i server.

The screenshot shows the 'SAML Single Sign-On Configuration' page. The 'Status' section has a green checkmark and the text: '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.'

Disconnettersi e riconnettersi a CUCM utilizzando le credenziali SSO SAML. Passare a **System > SAML Single Sign-On**. Fare clic su **Esegui test SSO** per altri nodi del cluster, come mostrato nell'immagine:

SAML Single Sign-On

SSO Mode

Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)

Per node (One metadata file per node)

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

Status

RTMT is enabled for SSO. You can change SSO for RTMT [here](#).

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3)							Rows 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 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	
cucm1150sub.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never	
imp115.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never	

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verificare che il test SSO sia riuscito per i nodi abilitati per SAML SSO. Passare a **System > SAML Single Sign On**. I test SSO riusciti mostrano lo stato Superato.

SAML Single Sign-On

SSO Mode

Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)

Per node (One metadata file per node)

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

Status

RTMT is enabled for SSO. You can change SSO for RTMT [here](#).

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3)							Rows 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	
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	
imp115.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 10:12:40 PM IST	

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

Una volta attivato SAML SSO, le applicazioni installate e le applicazioni della piattaforma vengono elencate per la pagina di accesso a CUCM, come mostrato in questa immagine.

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

Una volta attivato SAML SSO, le applicazioni installate e le applicazioni della piattaforma vengono elencate per la pagina di accesso a IM e Presenza, come mostrato nella seguente immagine:

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per impostare i log SSO su debug, usare il comando **set samltrace level DEBUG**

Raccogliere i log SSO utilizzando RTMT o dalla posizione **active log /tomcat/logs/ssosp/log4j/*.log** utilizzando CLI.

Esempio di log SSO che mostra i metadati generati e inviati ad altri nodi

```
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 cucm1150sub.adfs.ucce.com
```