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

Sommario

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.

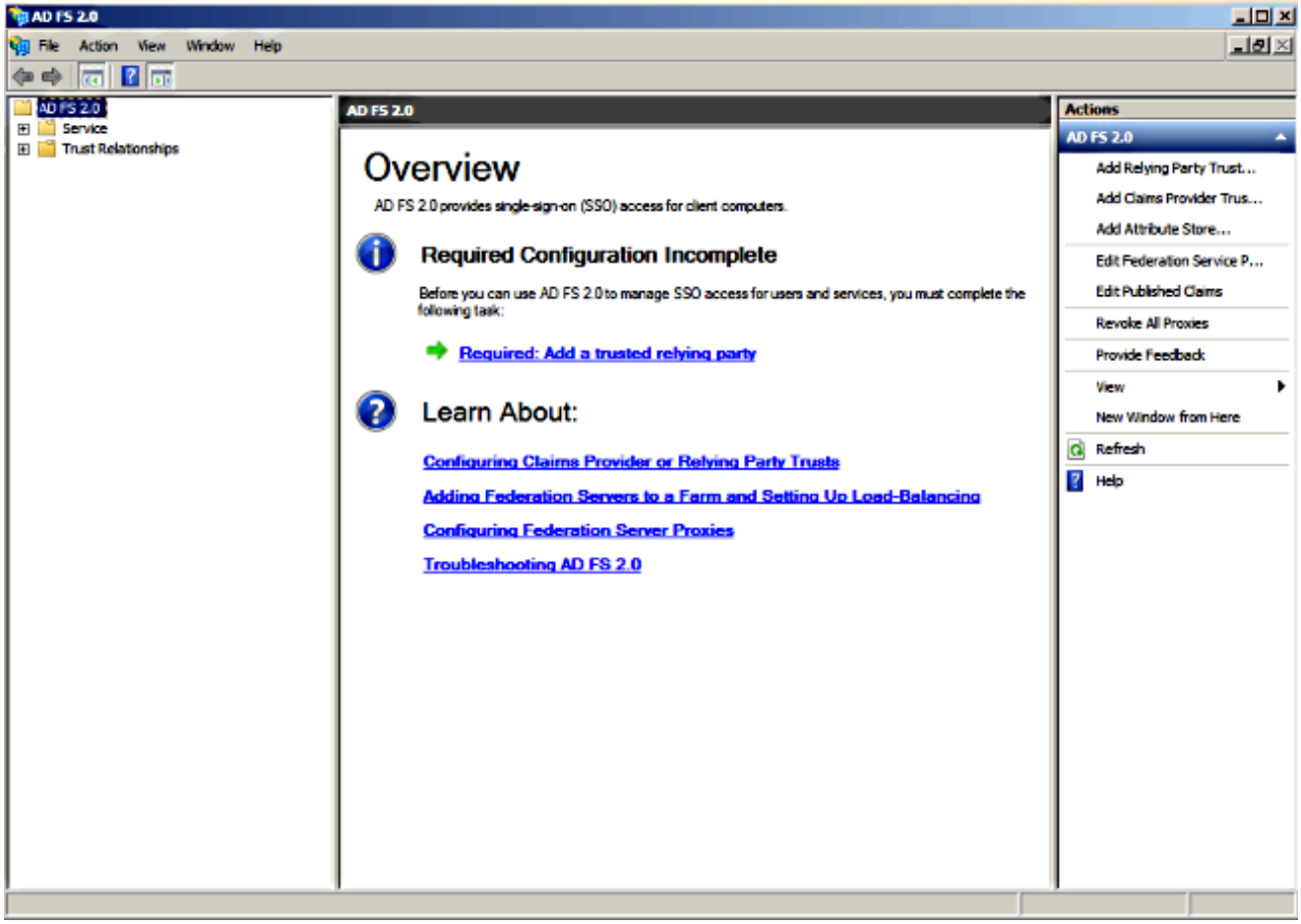
Cisco Prime Collaboration Provisioning

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

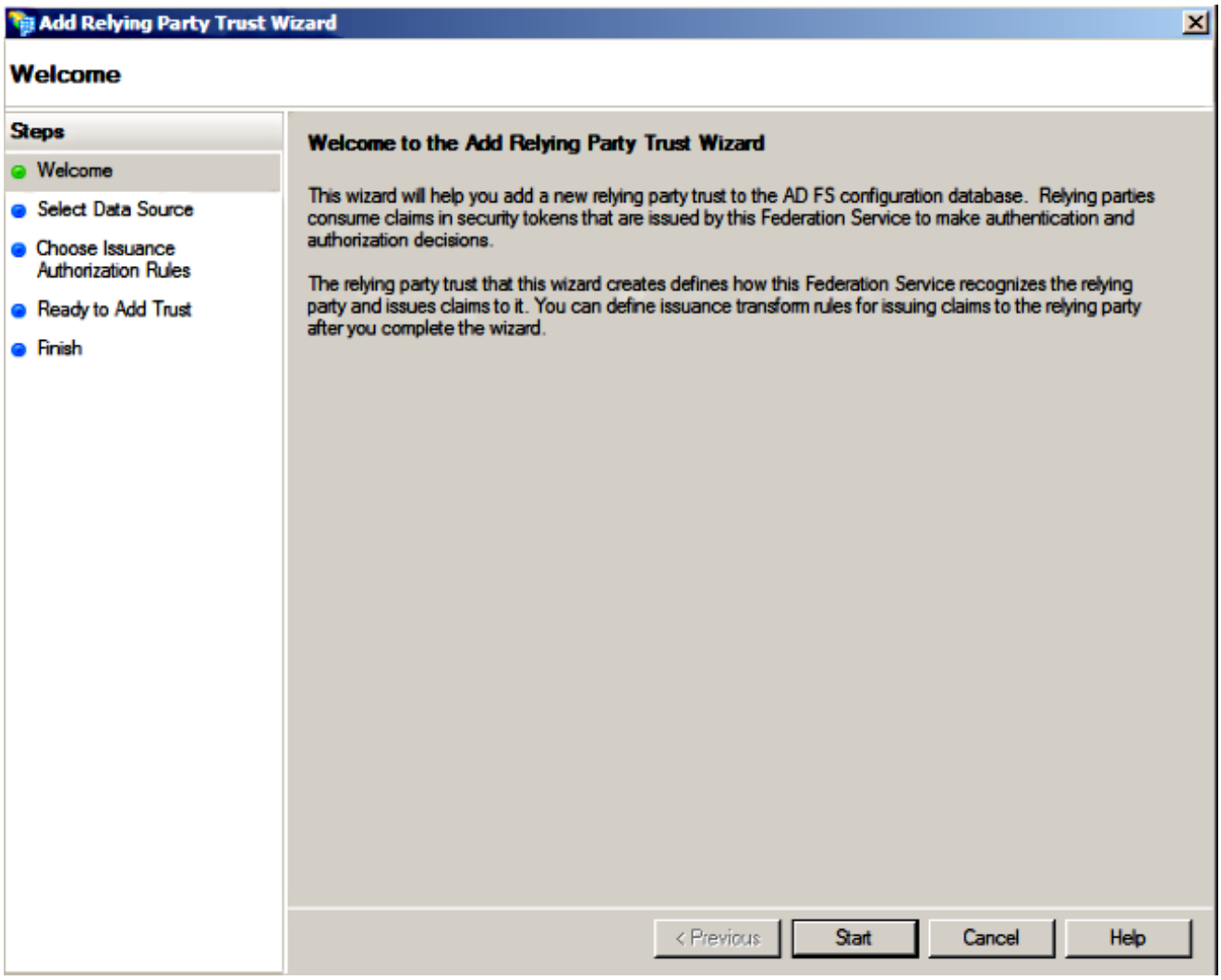
Aggiungi CUCM come attendibilità componente

1. Accedere al server AD FS e avviare AD FS versione 2.0 dal menu Programmi di Microsoft Windows.

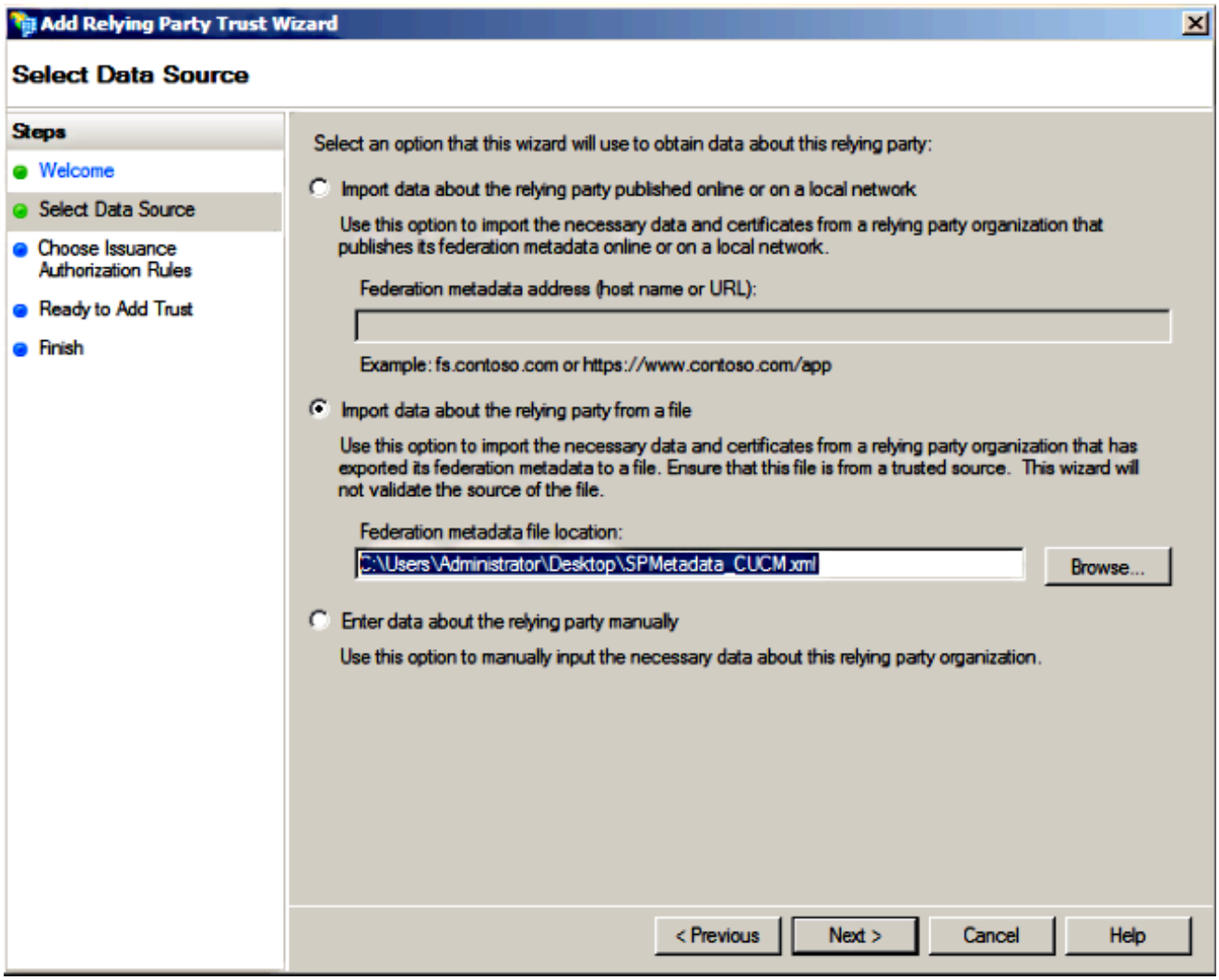
2. Selezionare Aggiungi attendibilità componente.



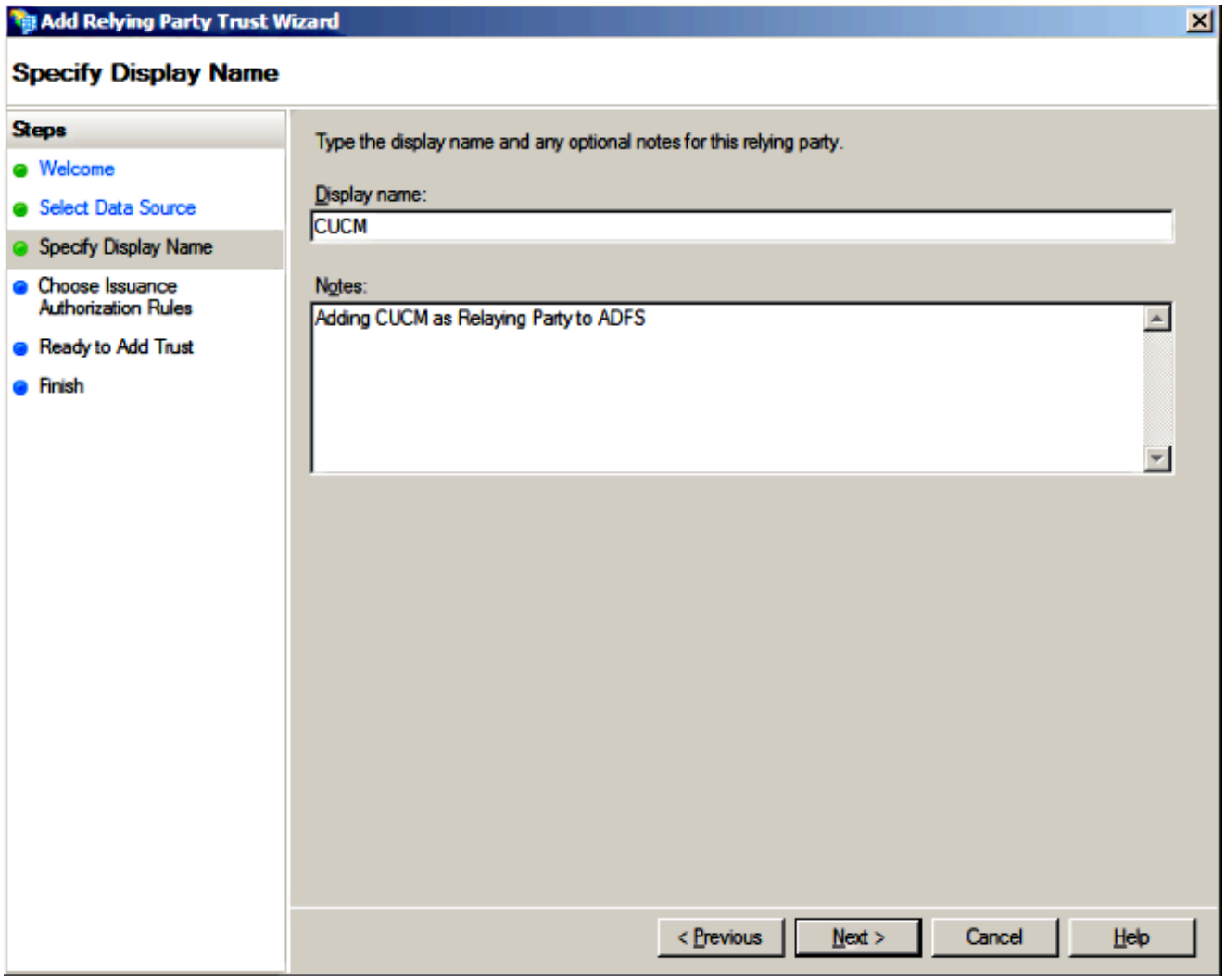
3. Fare clic su Start.



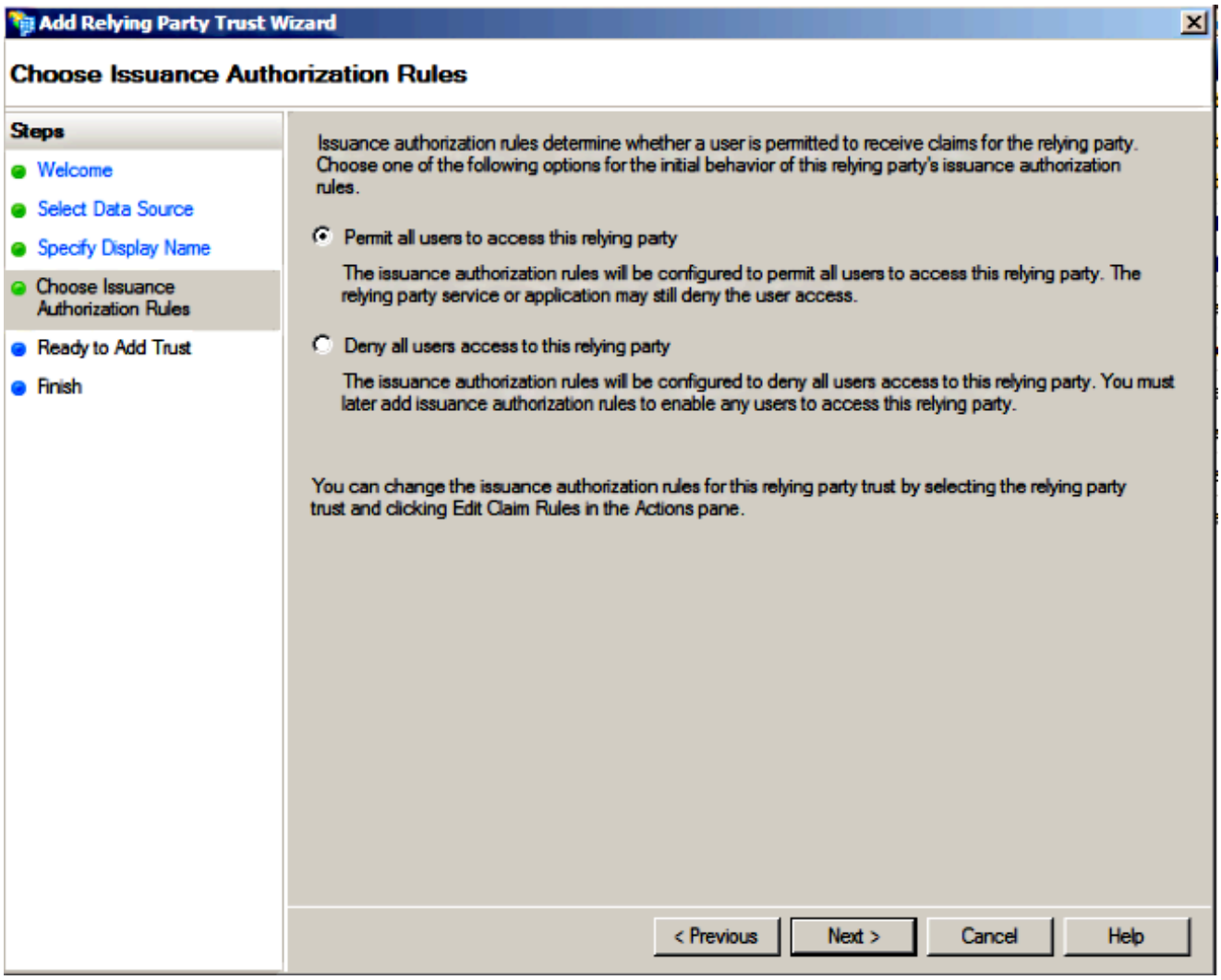
4. Selezionare l'opzione Importa dati sul componente da un file, scegliere il file di metadati SPMetadata_CUCM.xml scaricato in precedenza da CUCM e fare clic su Avanti.



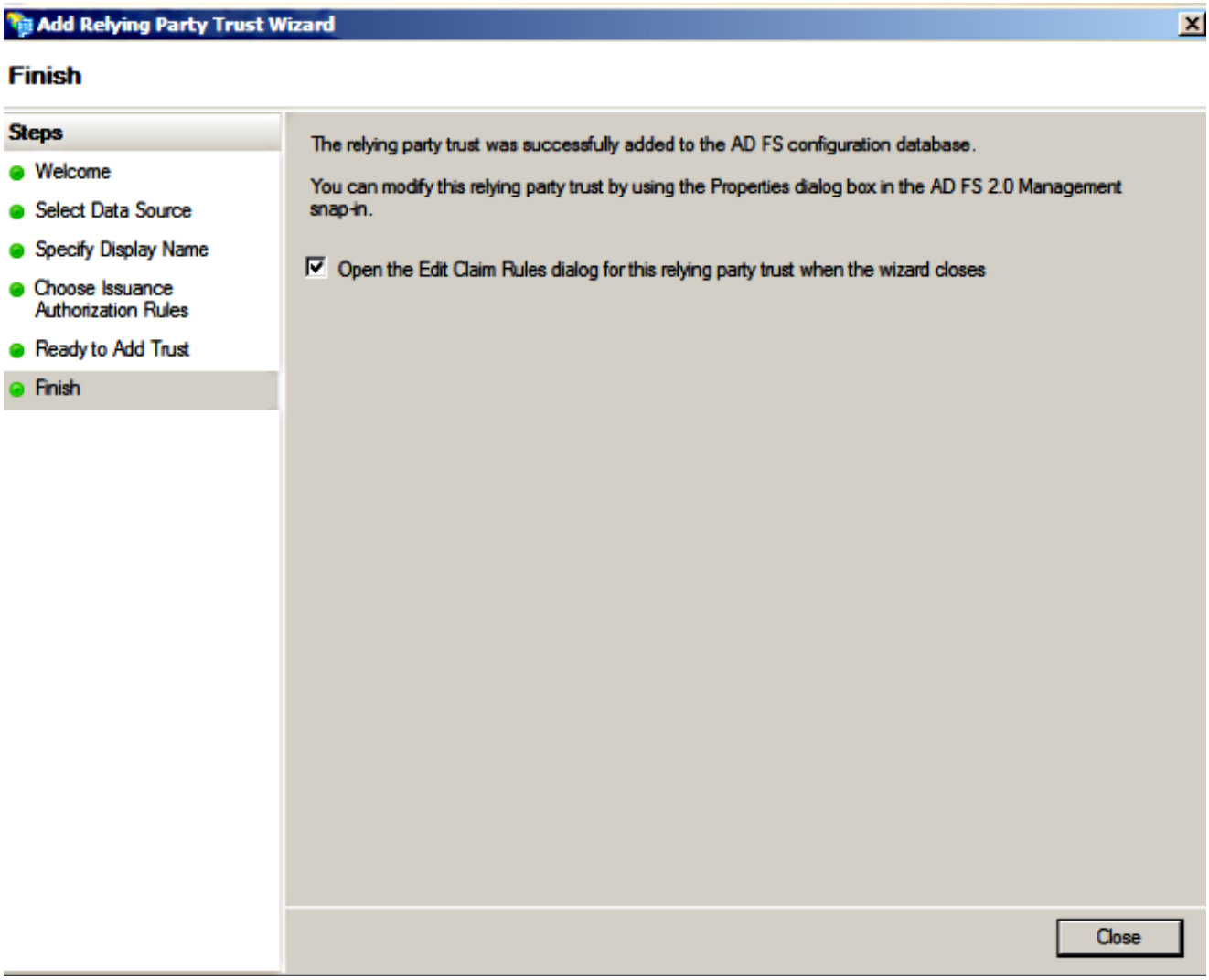
5. Immettere il nome visualizzato e fare clic su Avanti.



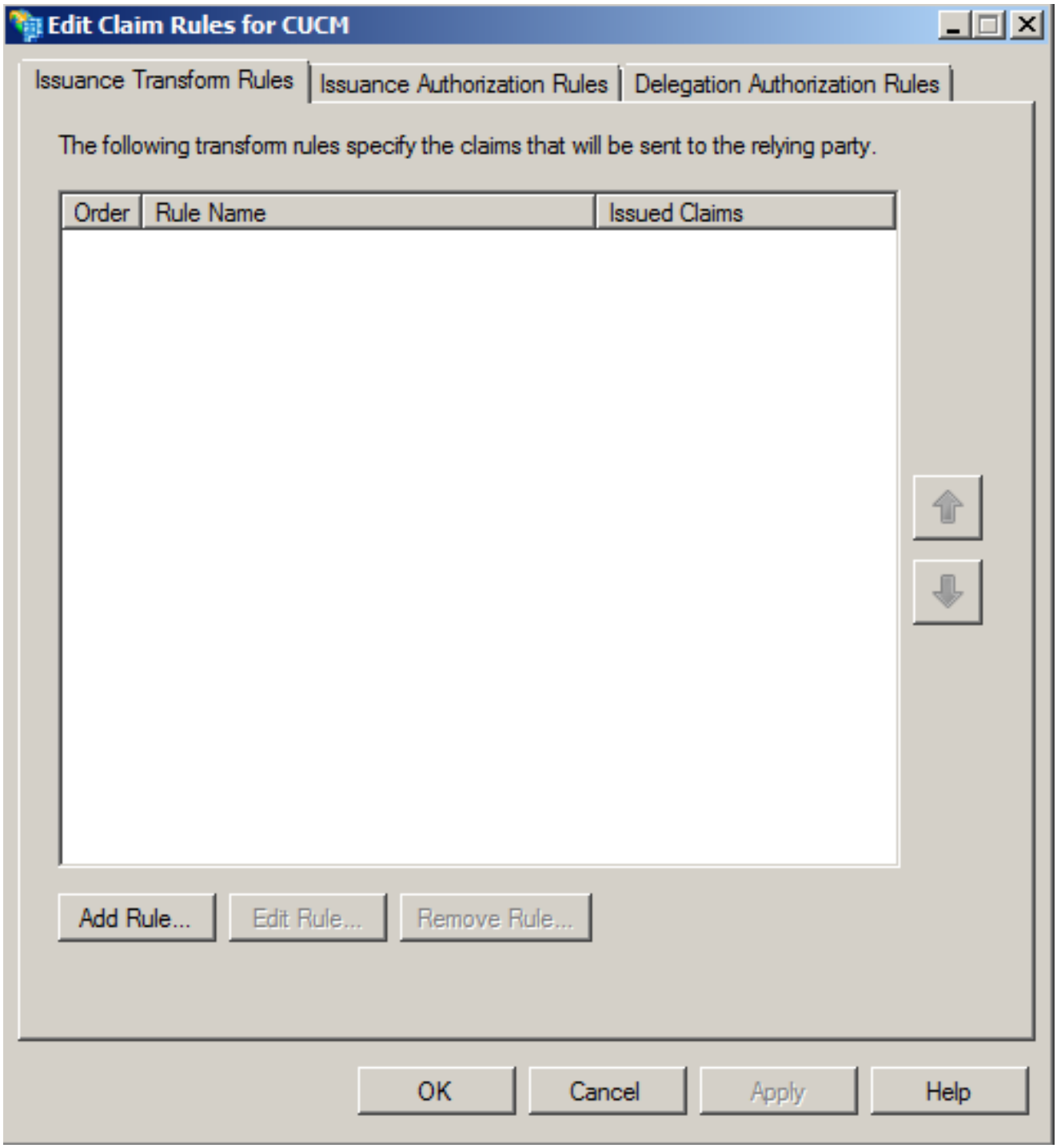
6. Scegliere Consenti a tutti gli utenti di accedere a questo componente e fare clic su Avanti.



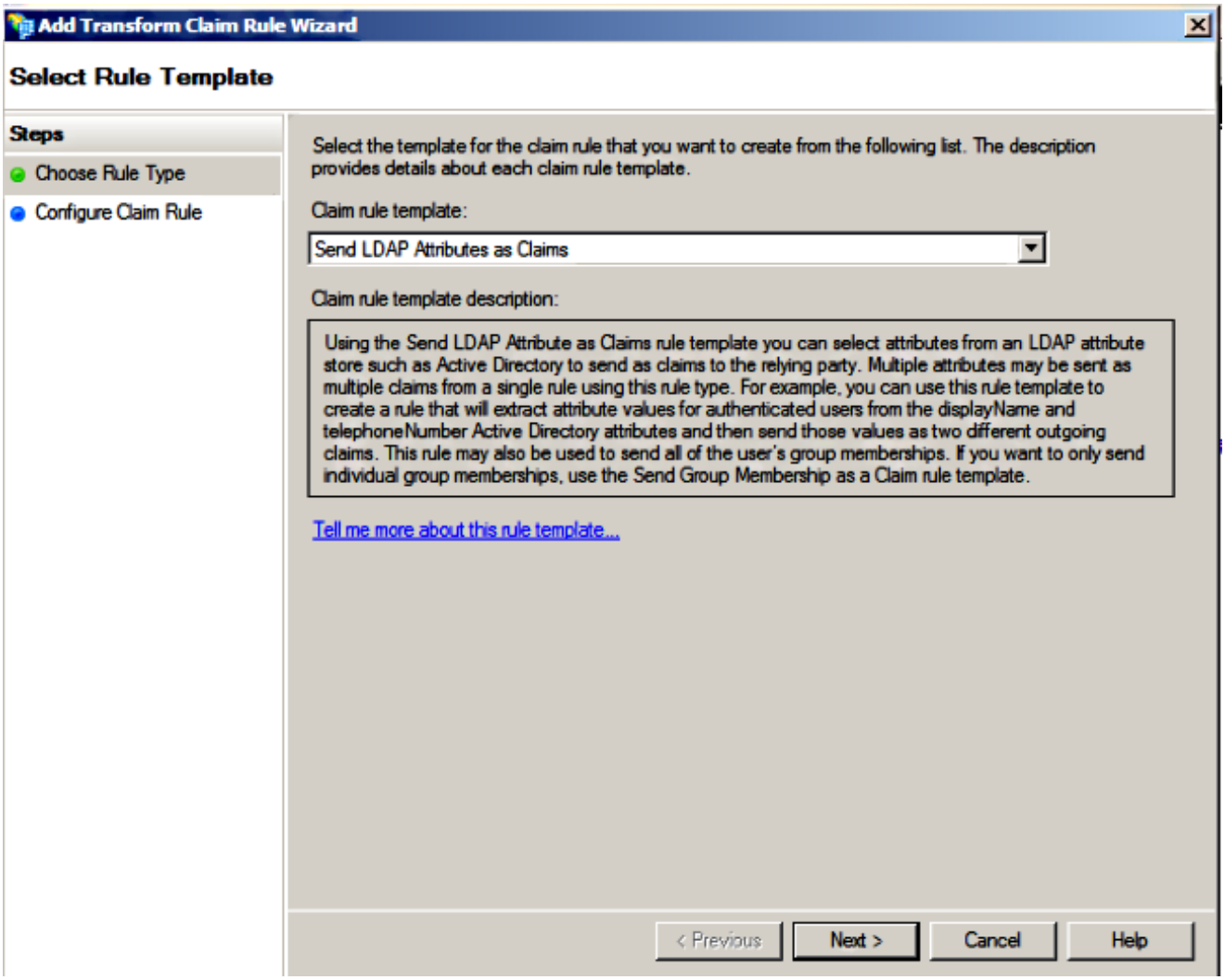
7. Selezionare Apri la finestra di dialogo Modifica regole attestazione per l'attendibilità del componente alla chiusura della procedura guidata e fare clic su Chiudi.



8. Fare clic su Aggiungi regola.

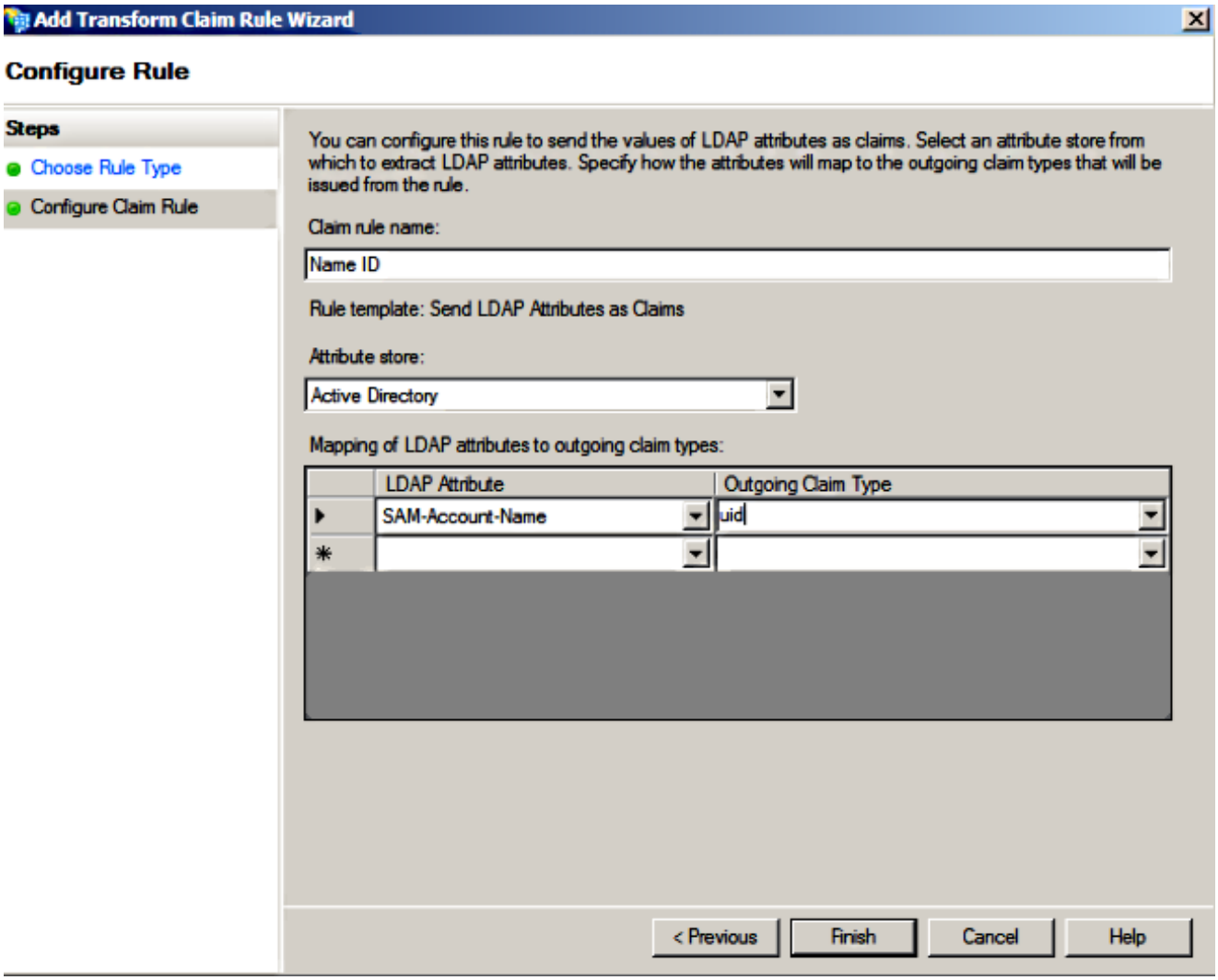


9. Fare clic su Avanti con il modello di regola Attestazione predefinito impostato su Invia attributi LDAP come attestazioni.

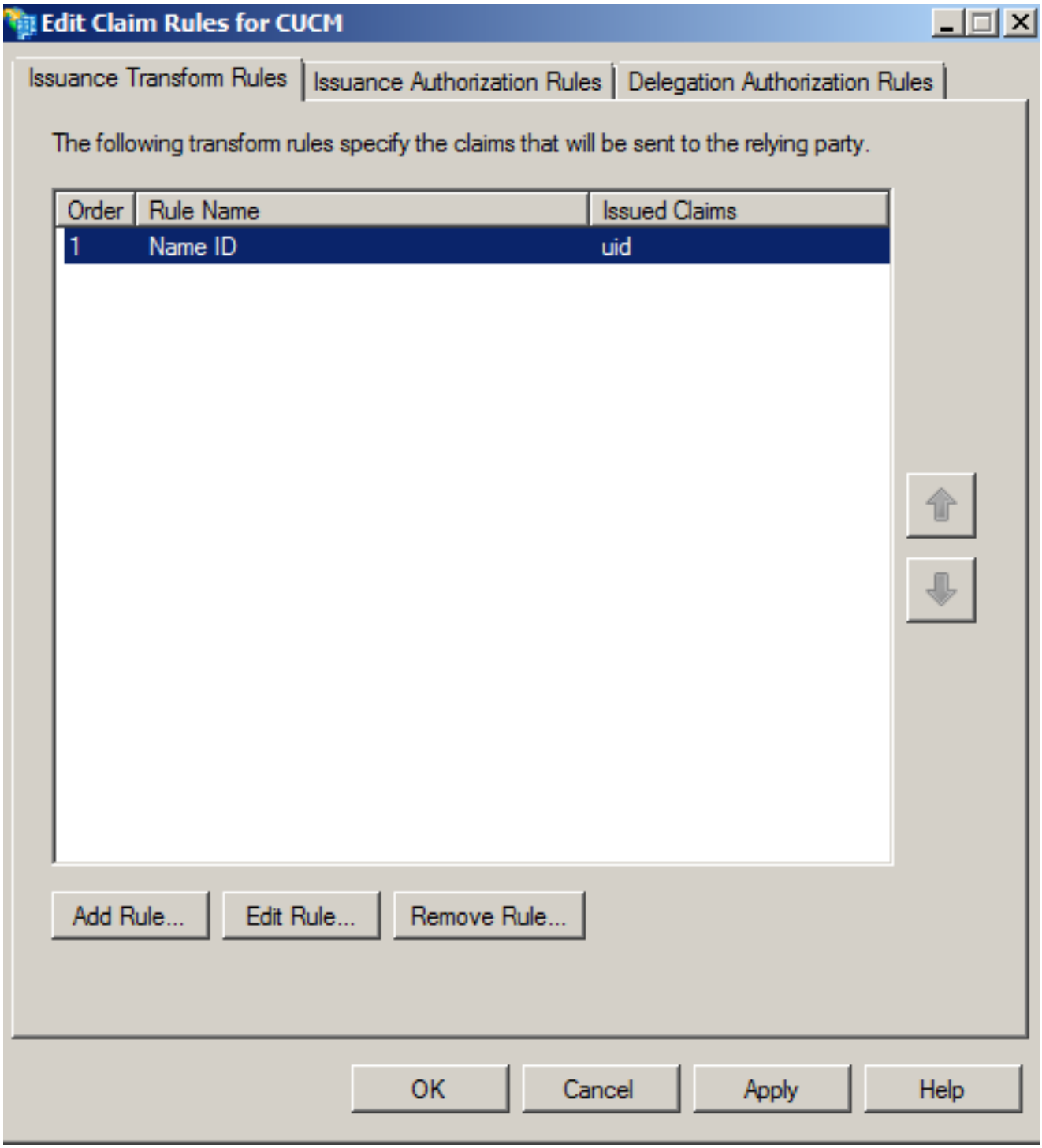


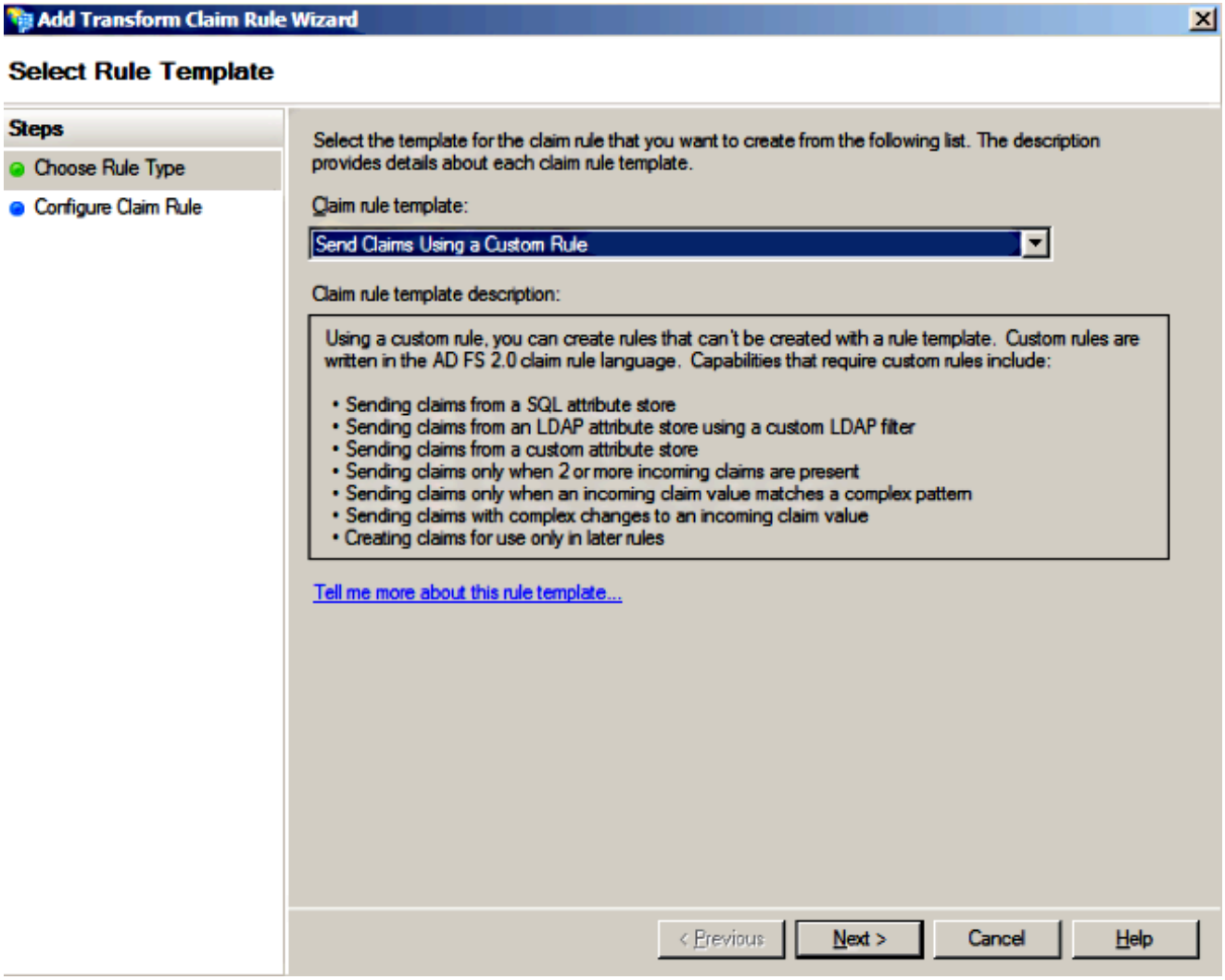
10. In Configura regola, immettere il nome della regola di attestazione, selezionare Active Directory come archivio attributi, configurare Attributo LDAP e Tipo di attestazione in uscita come mostrato in questa immagine e fare clic su Fine.

Nota:
- L'attributo LDAP (Lightweight Directory Access Protocol) deve corrispondere all'attributo Sincronizzazione directory in CUCM.
- "uid" deve essere in lettere minuscole.



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

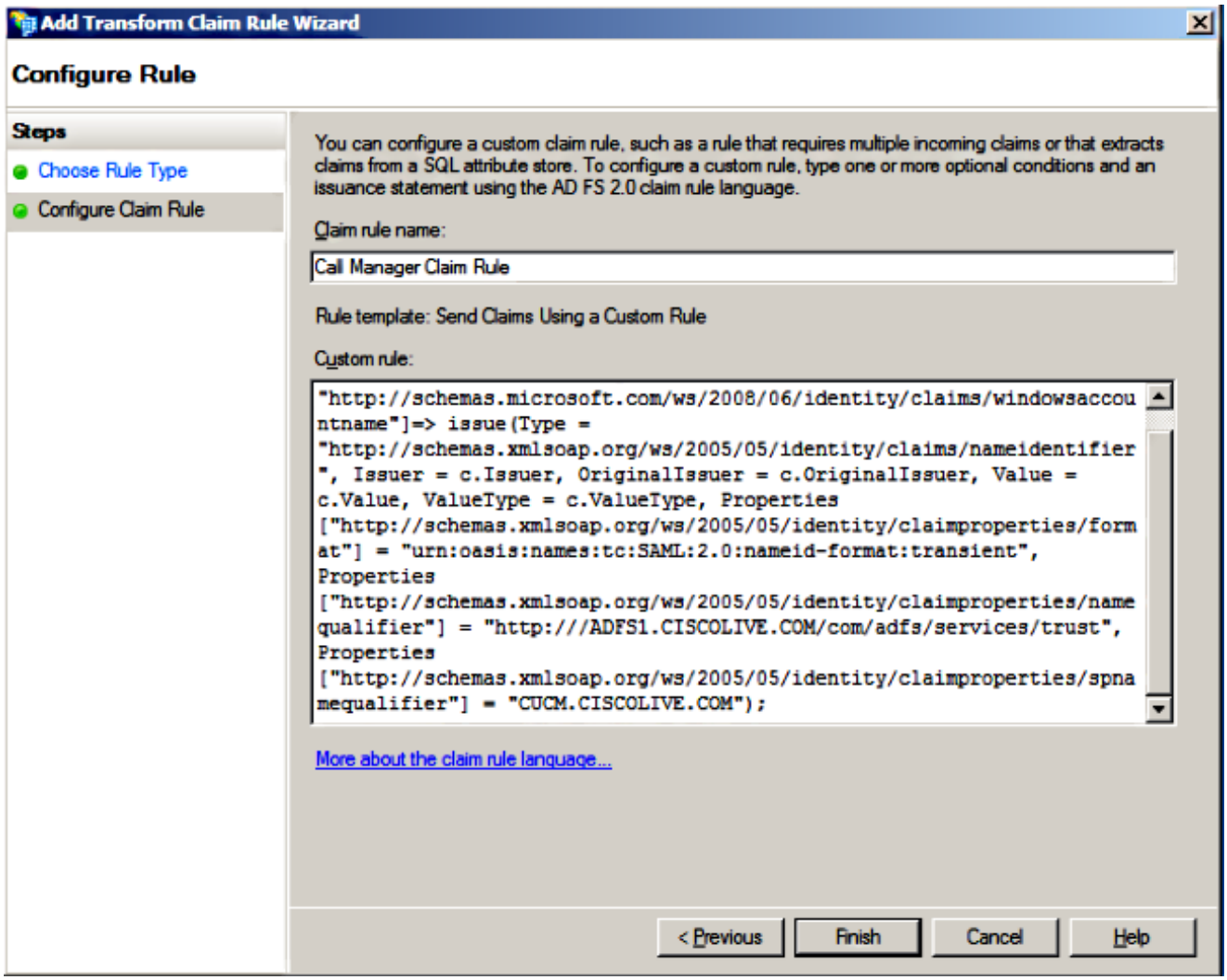

Edit Claim Rules for CUCM
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
Name ID
uid
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help



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(T
```

(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.)



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.

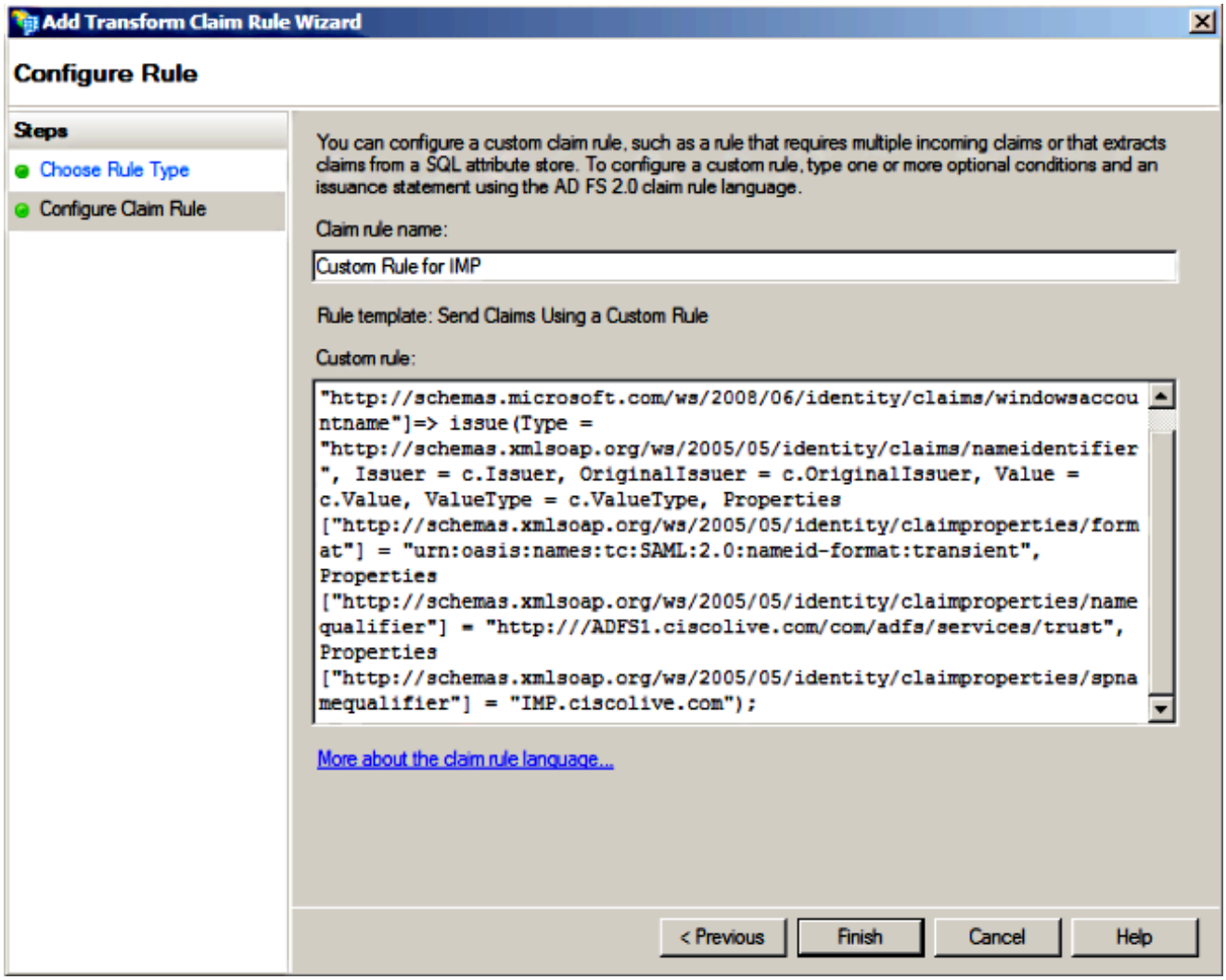
13. Fare clic su Finish (Fine).
14. Fare clic su Apply (Applica), quindi su OK.
15. Riavviare il servizio AD FS versione 2.0 da Services.msc.

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(T
```



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.

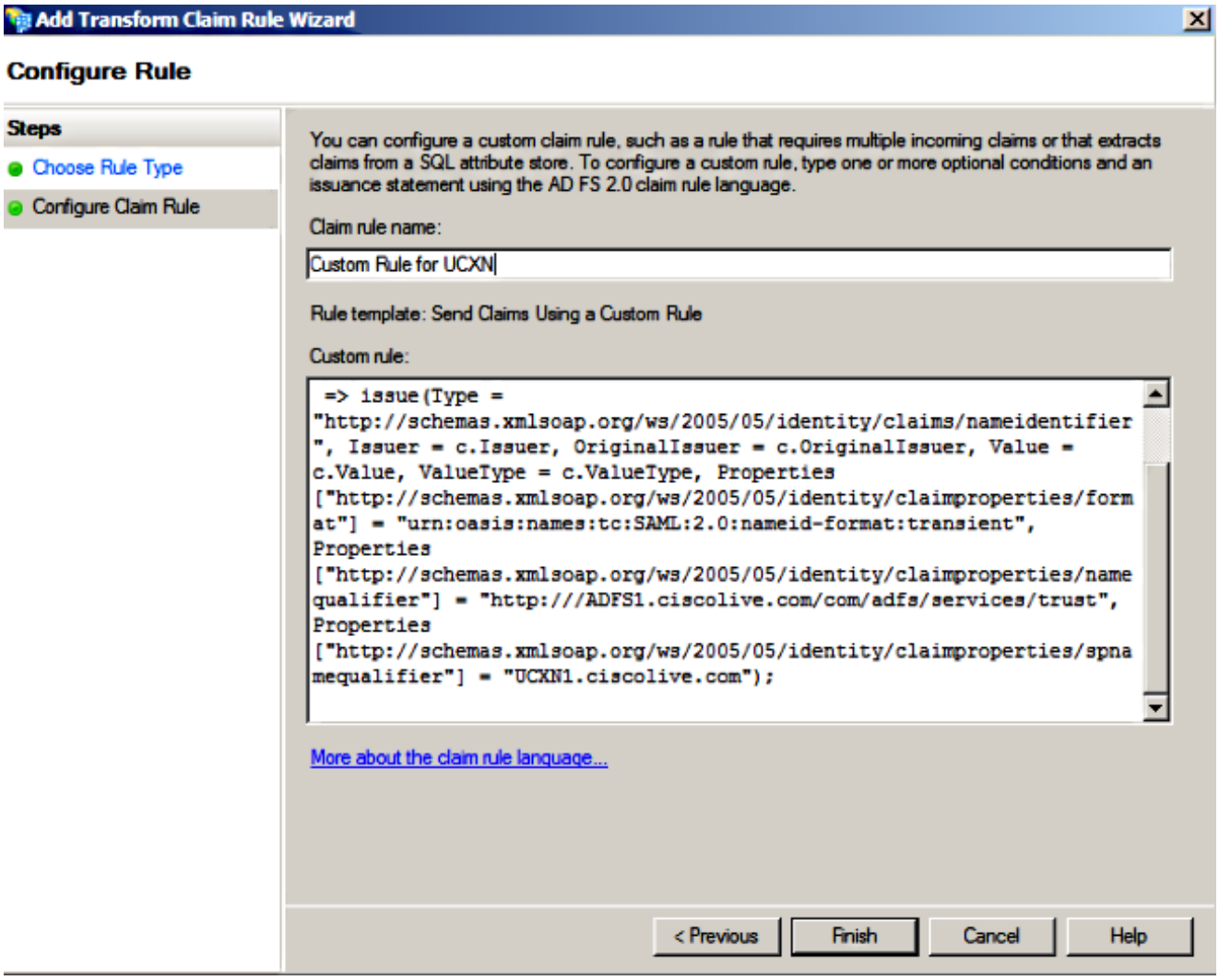
5. Riavviare il servizio AD FS versione 2.0 da Services.msc.

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(T
```



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.

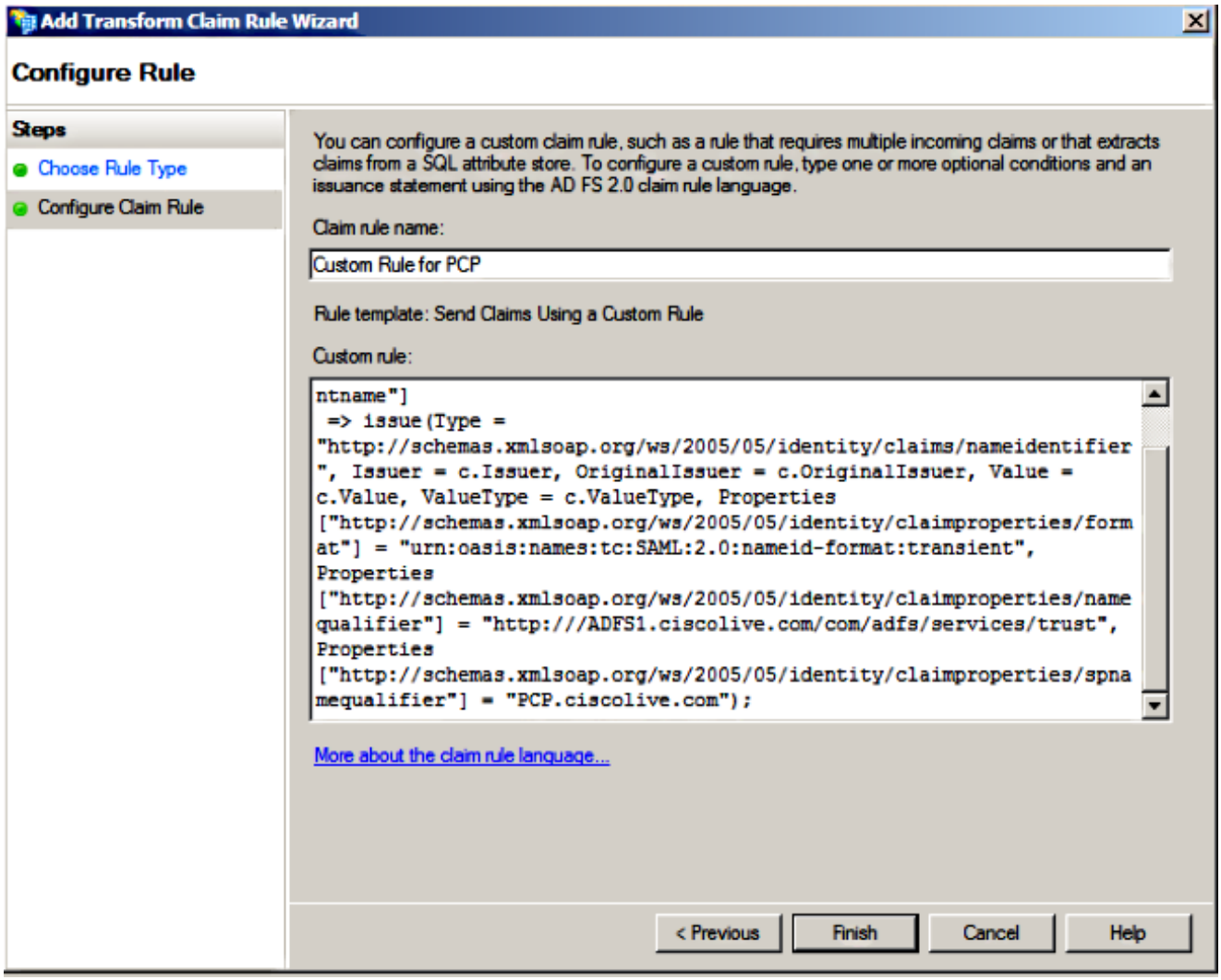
5. Riavviare il servizio AD FS versione 2.0 da Services.msc.

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
```



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.

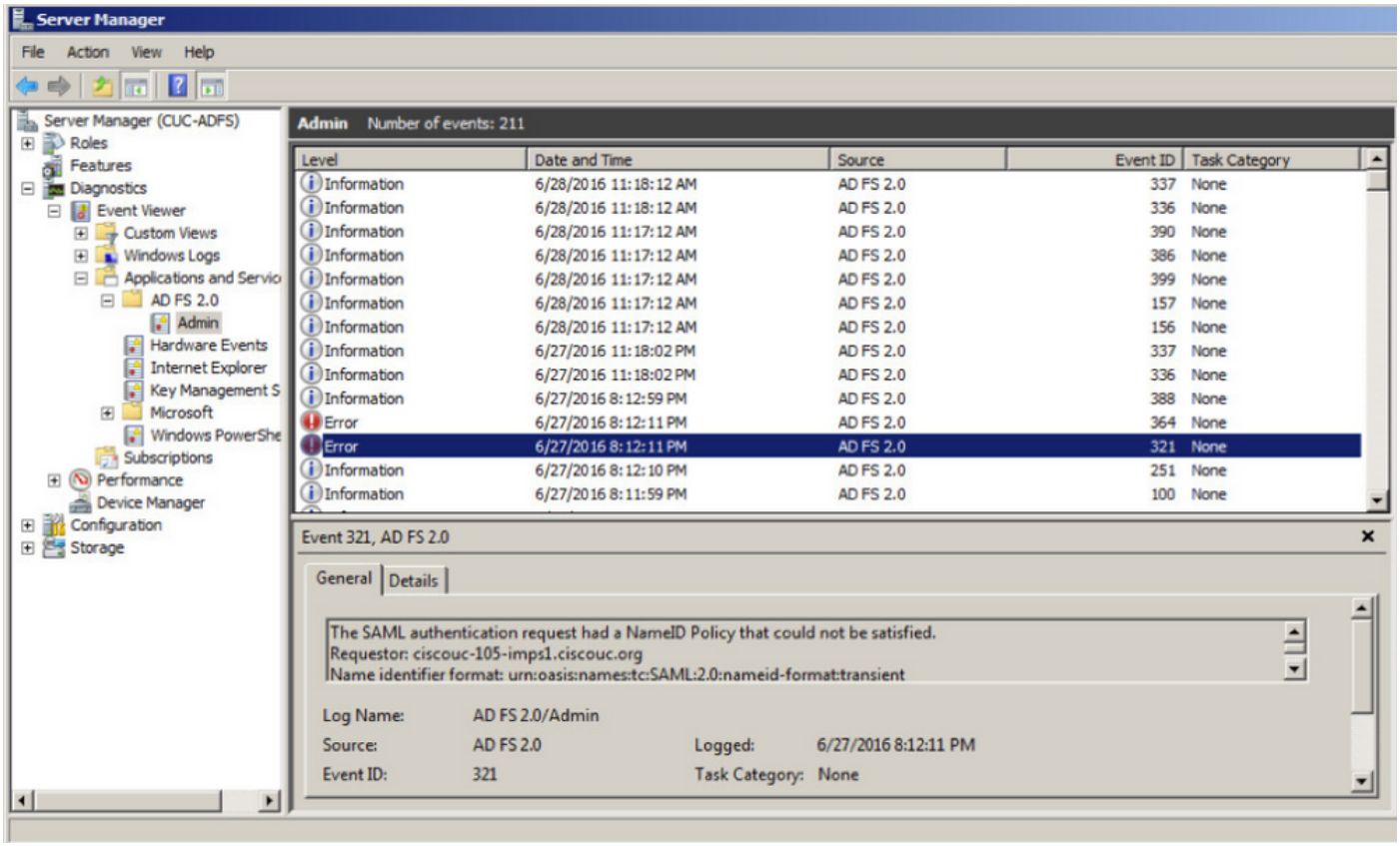
Verifica

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).