

Konfiguration einer einzelnen SAML-IDP-Verbindung/Vereinbarung pro Cluster mit AD FS Version 2.0

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: SP-Metadaten aus CUCM exportieren](#)

[Schritt 2: IDP-Metadaten von AD FS herunterladen](#)

[Schritt 3: Bereitstellungs-IDP](#)

[Schritt 4: SAML SSO aktivieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird beschrieben, wie die SAML (Single Security Assertion Markup Language) Identity Provider-Verbindung bzw. -Vereinbarung pro Cluster mit AD FS (Active Directory Federation Service) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager (CUCM) 11.5 oder höher
- Cisco Unified Communications Manager IM und Presence, Version 11.5 oder höher
- Active Directory Federation Service Version 2.0

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Active Directory Federation Service Version 2.0 als IDP
- Cisco Unified Communications Manager Version 11.5
- Cisco IM und Presence Server Version 11.5

Hintergrundinformationen

Bei SAML SSO muss es sich um einen Vertrauenskreis zwischen dem Service Provider (SP) und dem IdP handeln. Diese Vertrauenswürdigkeit wird im Rahmen von SSO Enablement erstellt, wenn Vertrauenswürdigkeit (Metadaten) ausgetauscht wird. Laden Sie die Metadaten vom CUCM herunter und laden Sie sie auf IdP hoch, laden Sie die Metadaten ähnlich von IdP herunter und laden Sie sie in CUCM hoch.

Vor CUCM 11.5 generiert der Ausgangsknoten die Metadatendatei. Außerdem werden die Metadatendateien von anderen Knoten im Cluster gesammelt. Es fügt alle Metadatendateien einer einzelnen ZIP-Datei hinzu und präsentiert sie dann dem Administrator. Der Administrator muss diese Datei entpacken und alle Dateien auf der IDP bereitstellen. Beispielsweise 8 Metadatendateien für einen Cluster mit 8 Knoten.

Eine SAML-ID-Verbindung/Vereinbarung pro Cluster-Funktion wird ab 11.5 eingeführt. Im Rahmen dieser Funktion generiert CUCM eine einzige Metadatendatei für Service Provider für alle CUCM- und IMP-Knoten im Cluster. Das neue Namensformat für die Metadatendatei ist **<hostname>-single-agreement.xml**

Grundsätzlich erstellt ein Knoten die Metadaten und leitet sie an andere SP-Knoten im Cluster weiter. Dadurch wird die Bereitstellung, Wartung und Verwaltung vereinfacht. Beispiel: 1 Metadatendatei für einen Cluster mit 8 Knoten.

Die Metadatendatei für den Cluster verwendet ein Multiserver-Tomcat-Zertifikat, das sicherstellt, dass das Schlüsselpaar für alle Knoten im Cluster identisch ist. Die Metadatendatei verfügt außerdem über eine Liste von ACS-URLs (Assertion Consumer Service) für die einzelnen Knoten im Cluster.

CUCM und Cisco IM and Presence Version 11.5 unterstützen sowohl die SSO-Modi, **clusterweit** (eine Metadatendatei pro Cluster) und pro Knoten (vorhandenes Modell).

In diesem Dokument wird beschrieben, wie der clusterweite Modus der SAML SSO mit AD FS 2.0 konfiguriert wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: SP-Metadaten aus CUCM exportieren

Öffnen Sie einen Webbrowser, melden Sie sich als Administrator bei CUCM an, und navigieren Sie zu **System > SAML Single Sign On**.

Standardmäßig ist das Optionsfeld **Clusterweit** aktiviert. Klicken Sie auf **Alle Metadaten exportieren**. Die Metadatendatei wird dem Administrator im Namen **<hostname>-single-agreement.xml** präsentiert.

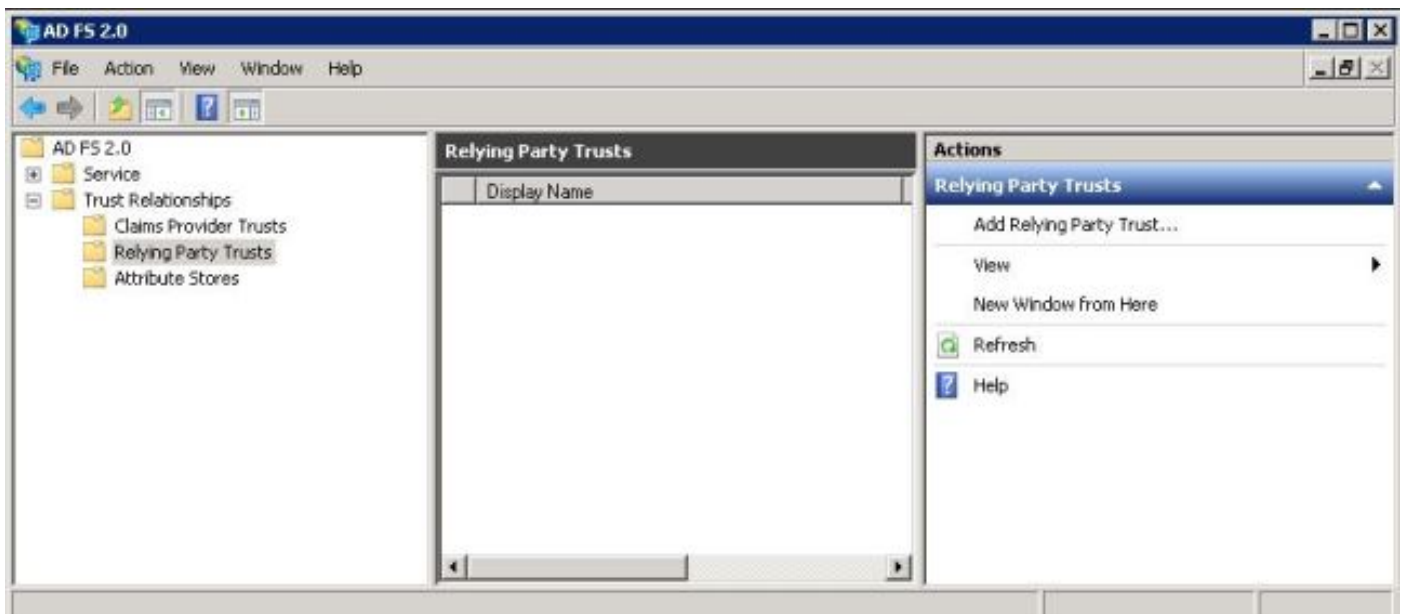


Schritt 2: IDP-Metadaten von AD FS herunterladen

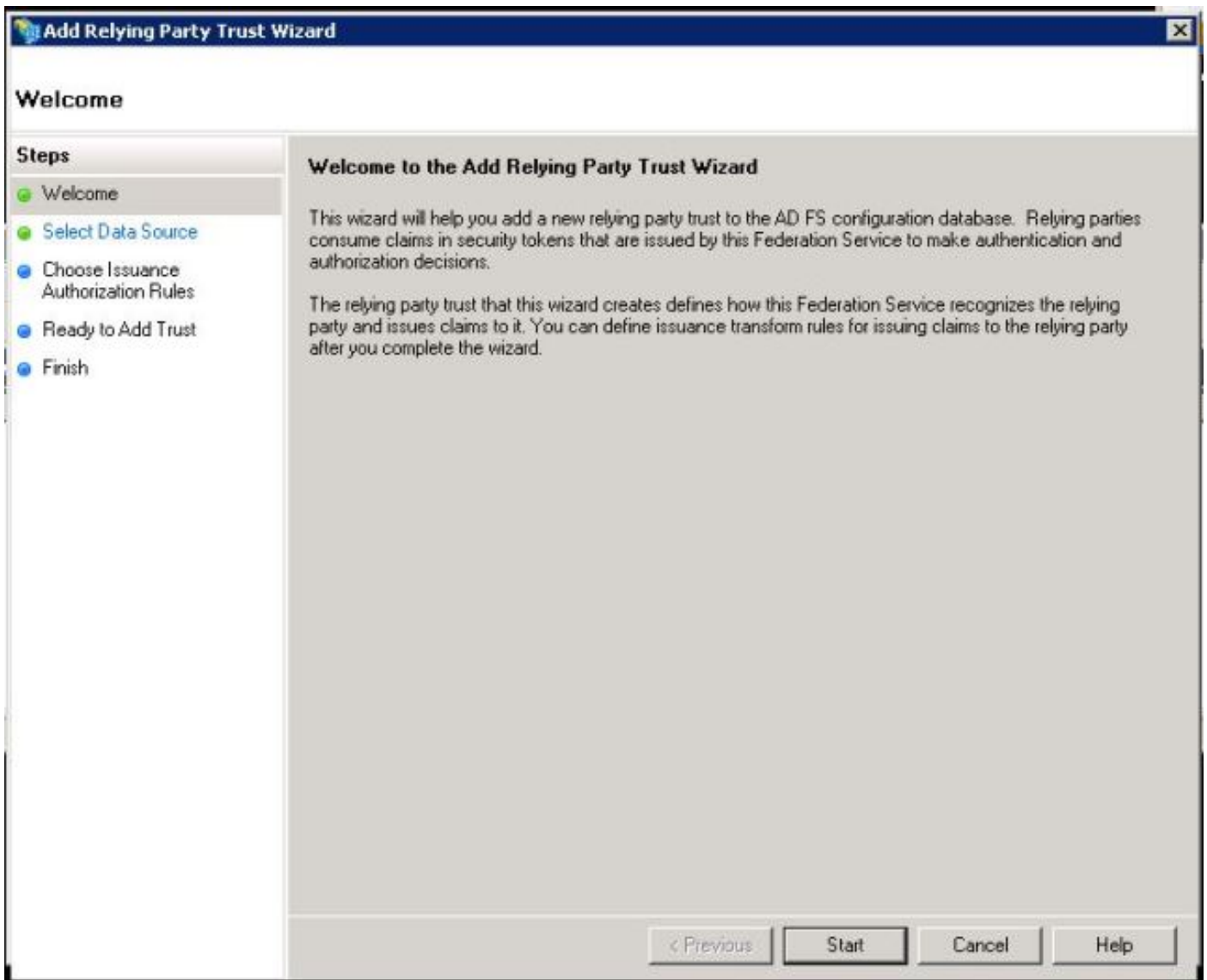
Informationen zum Herunterladen von IdP-Metadaten finden Sie unter [https:// <FQDN des ADFS>/federationmetadata/2007-06/federationmetadata.xml](https://<FQDN des ADFS>/federationmetadata/2007-06/federationmetadata.xml)

Schritt 3: Bereitstellungs-IDP

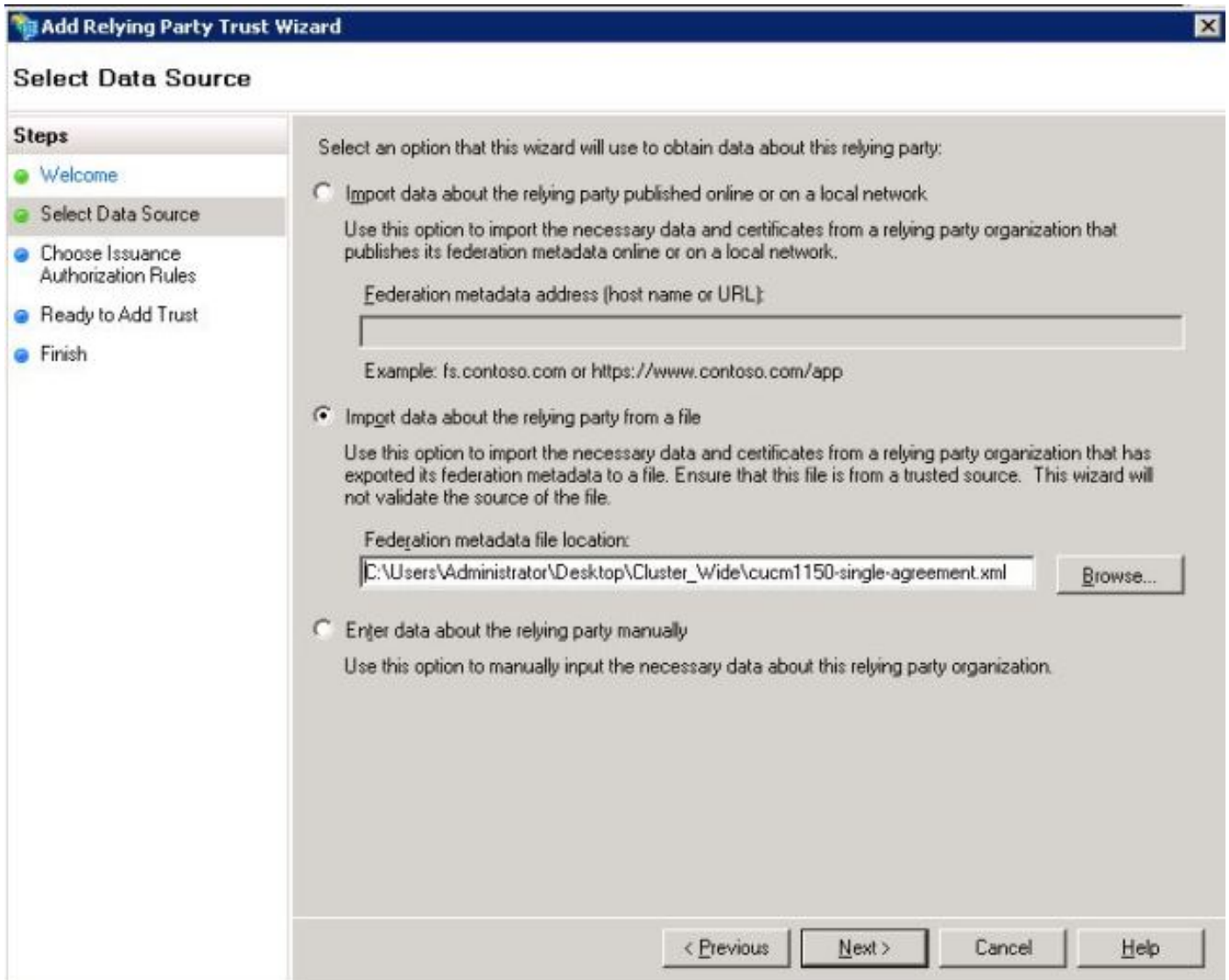
Navigieren Sie, wie im Bild gezeigt, zu **AD FS 2.0 Management/Trust Relation Ships/Relying Party Trust**. Klicken Sie auf **Vertrauenswürdige Partei hinzufügen**.



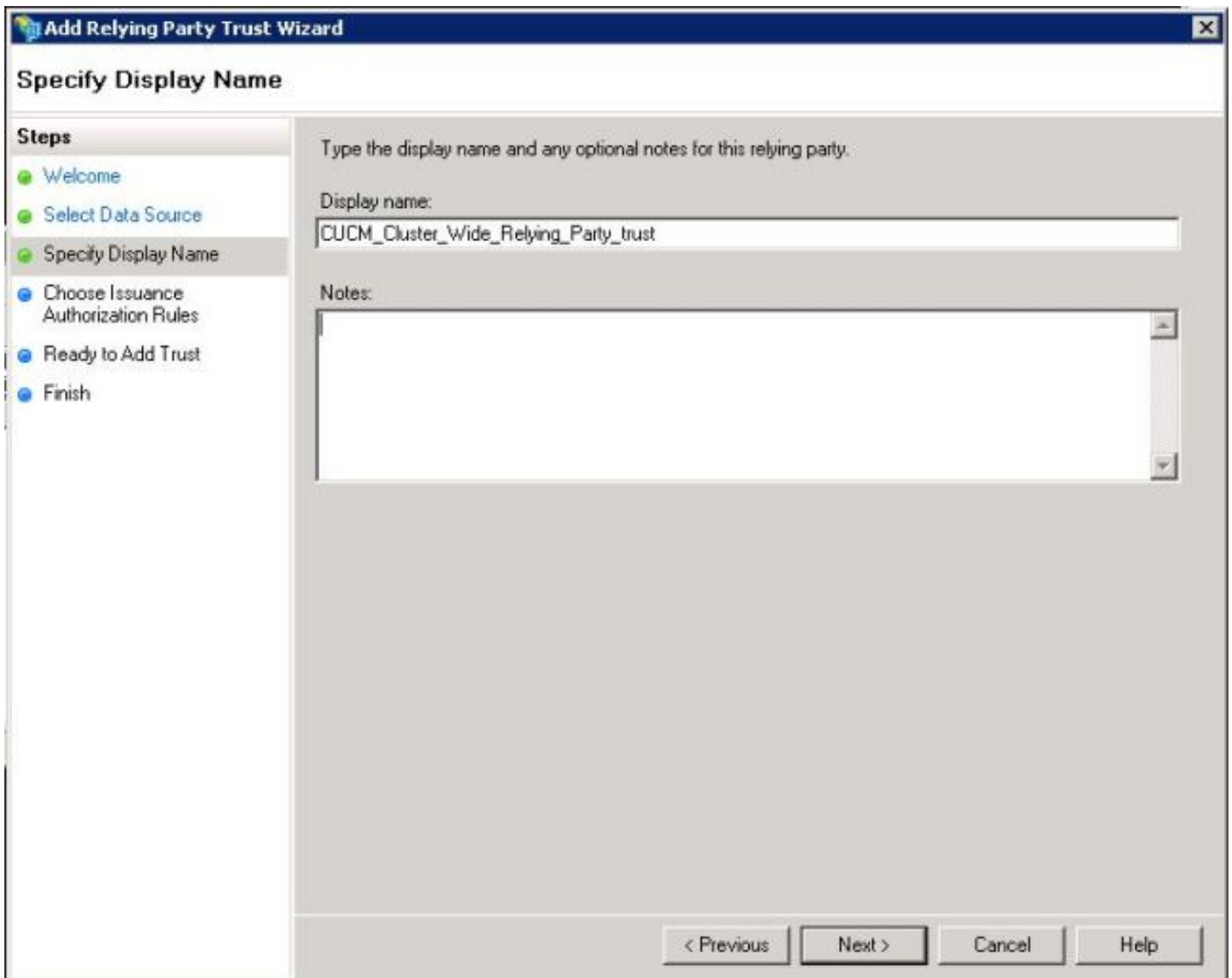
Der Assistent für das Hinzufügen von Gruppenvertrauen wird geöffnet, wie im Bild gezeigt. Klicken Sie jetzt auf **Start**.



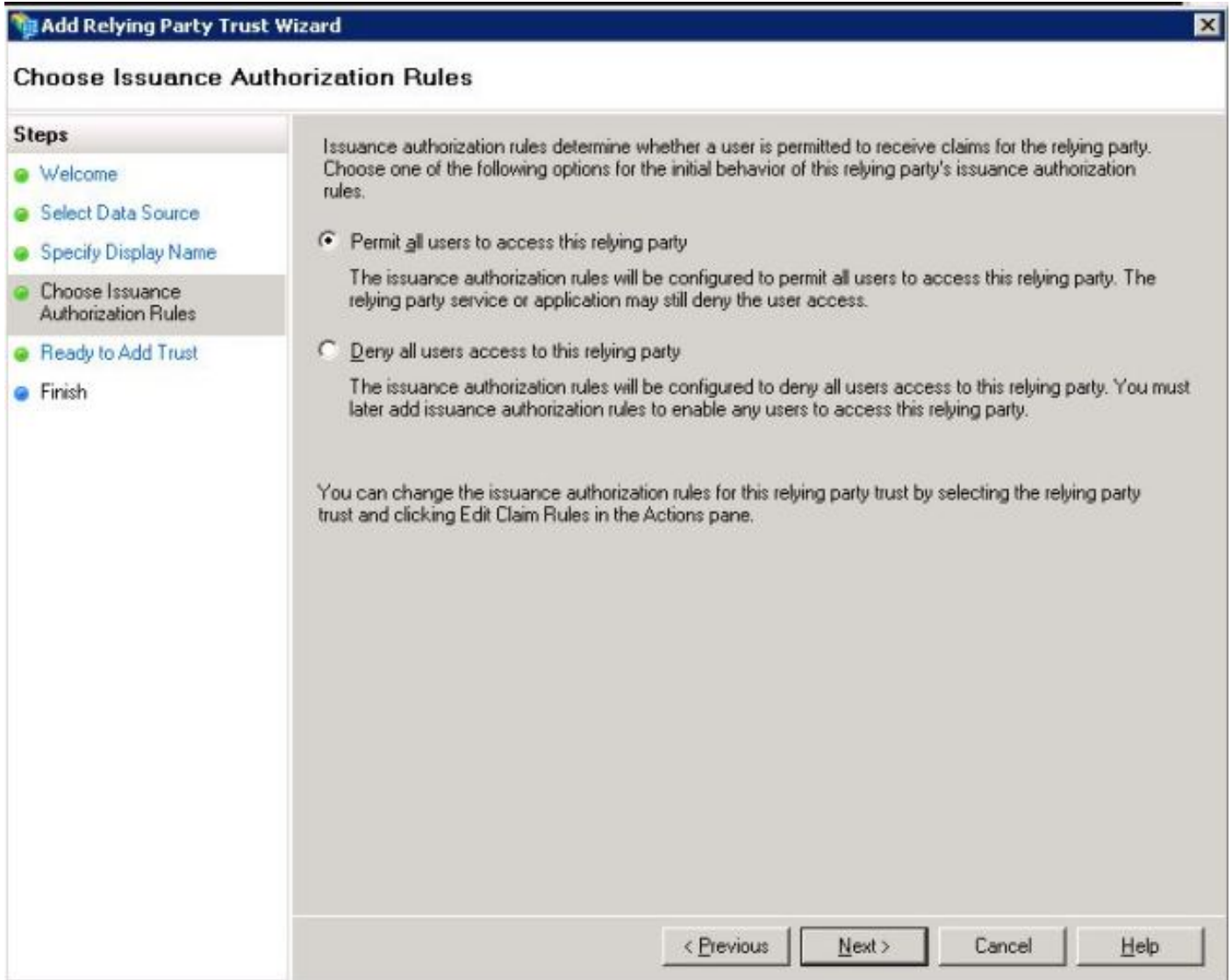
Klicken Sie auf Importdaten, die angeben, ob eine Partei aus einer Datei stammt. Durchsuchen Sie die von der CUCM SAML SSO-Konfigurationsseite heruntergeladenen SP-Metadaten. Klicken Sie anschließend auf **Weiter**, wie im Bild gezeigt:



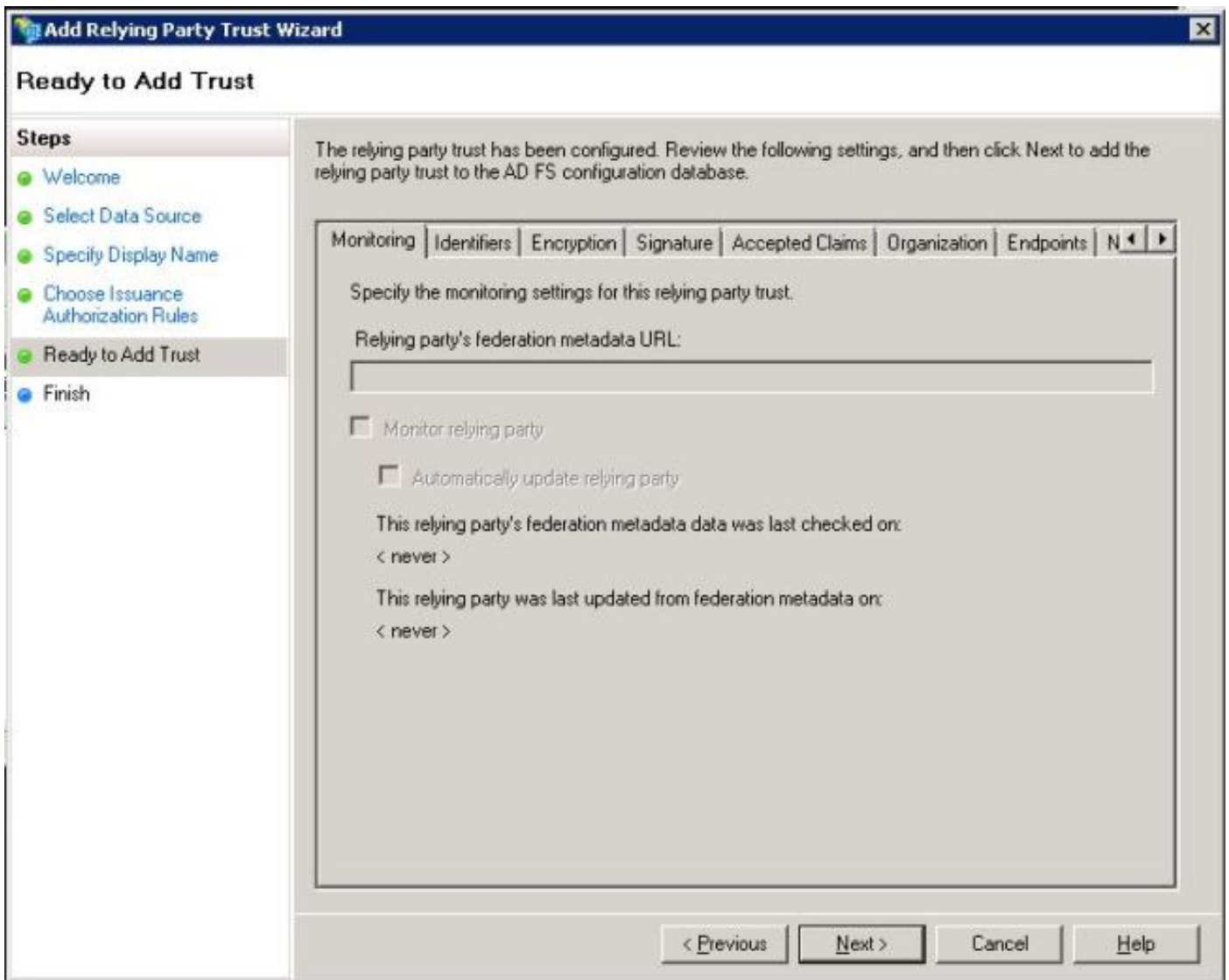
Geben Sie den Display Name (Anzeigenamen) und alle optionalen Notizen für die Relying Party (Partei) ein. Klicken Sie auf **Weiter**, wie im Bild gezeigt:



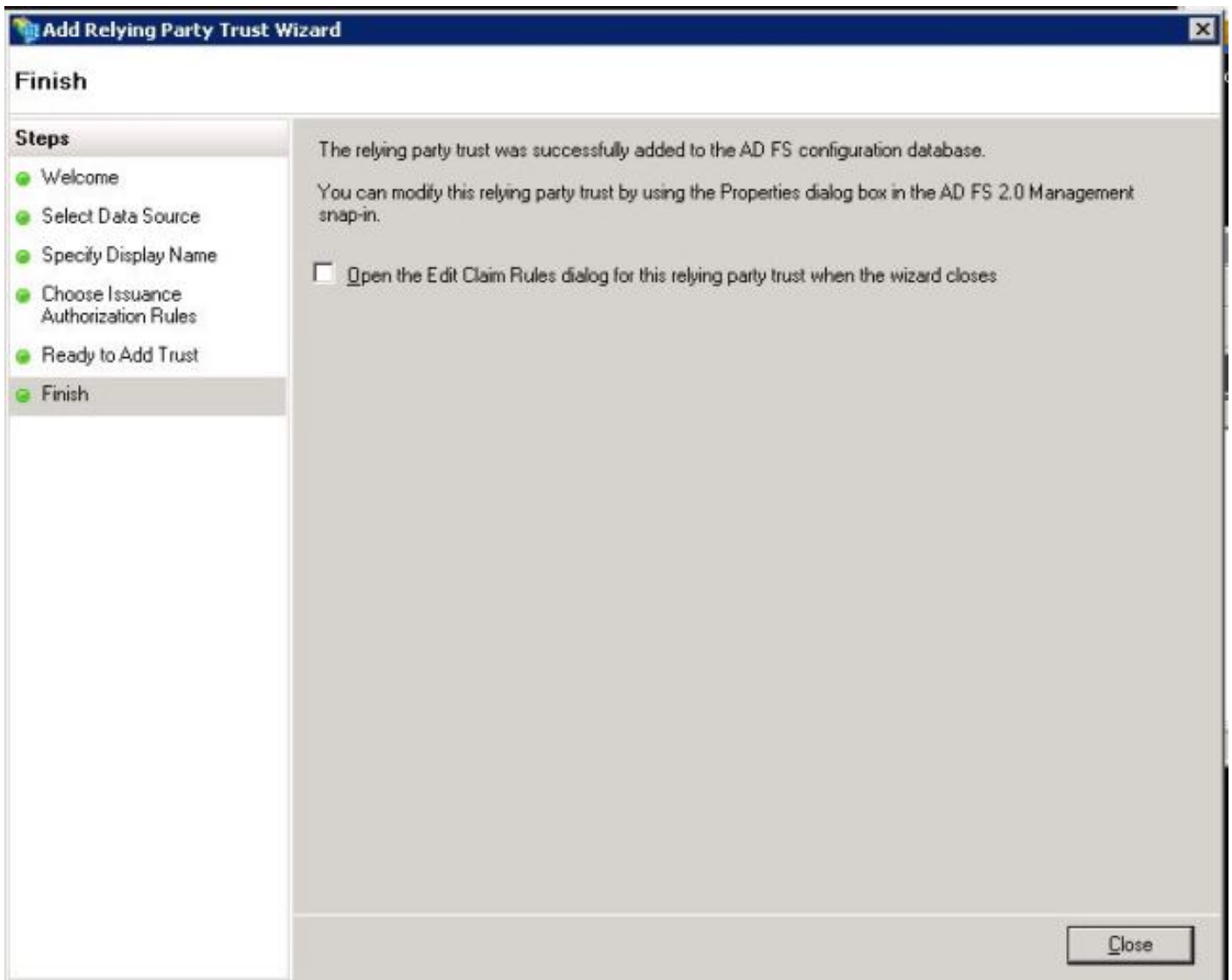
Wählen Sie **Zulassen aller Benutzer für den Zugriff auf diese vertrauliche Partei**, um allen Benutzern den Zugriff auf diese Partei zu gestatten, und klicken Sie dann auf **Weiter**, wie im Bild gezeigt:



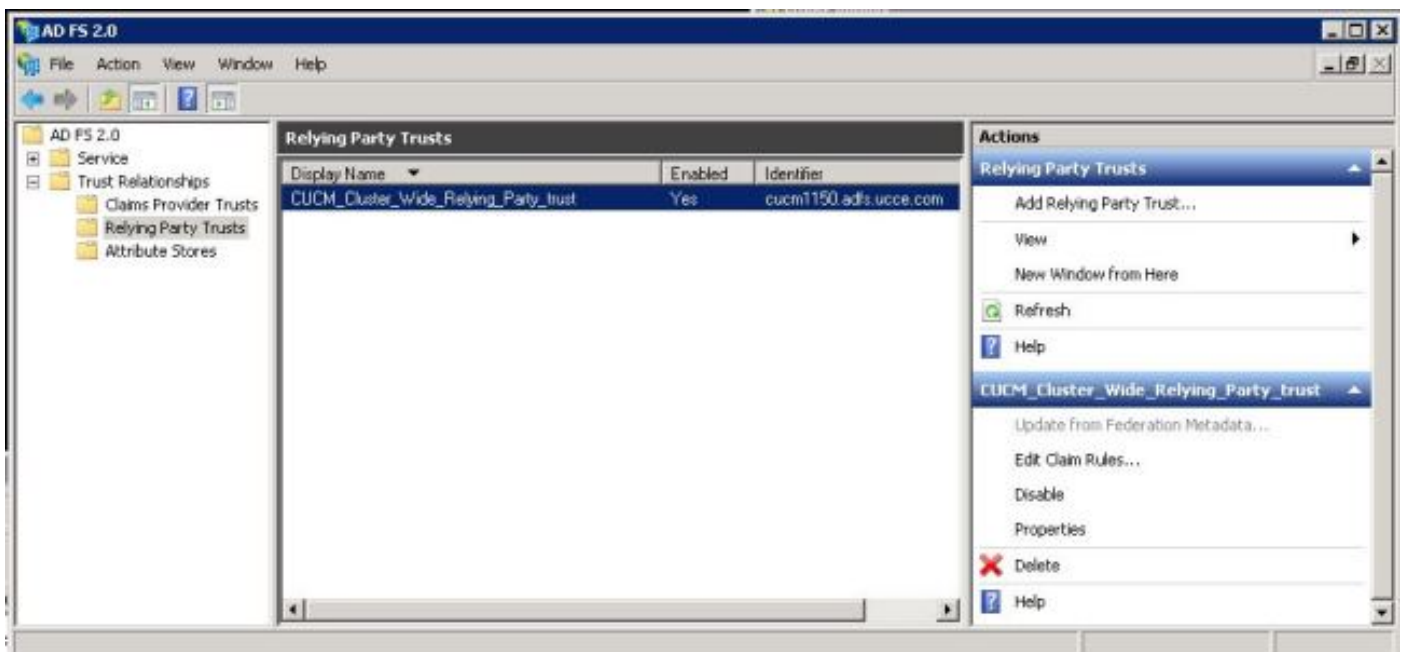
Auf der Seite **Ready to Add Trust (Bereit zum Hinzufügen von Vertrauenswürdigkeit)** können Sie die Einstellungen für die konfigurierte Relying Party Trust (Vertrauenswürdigkeit) überprüfen. Klicken Sie jetzt auf **Weiter**, wie im Bild gezeigt:



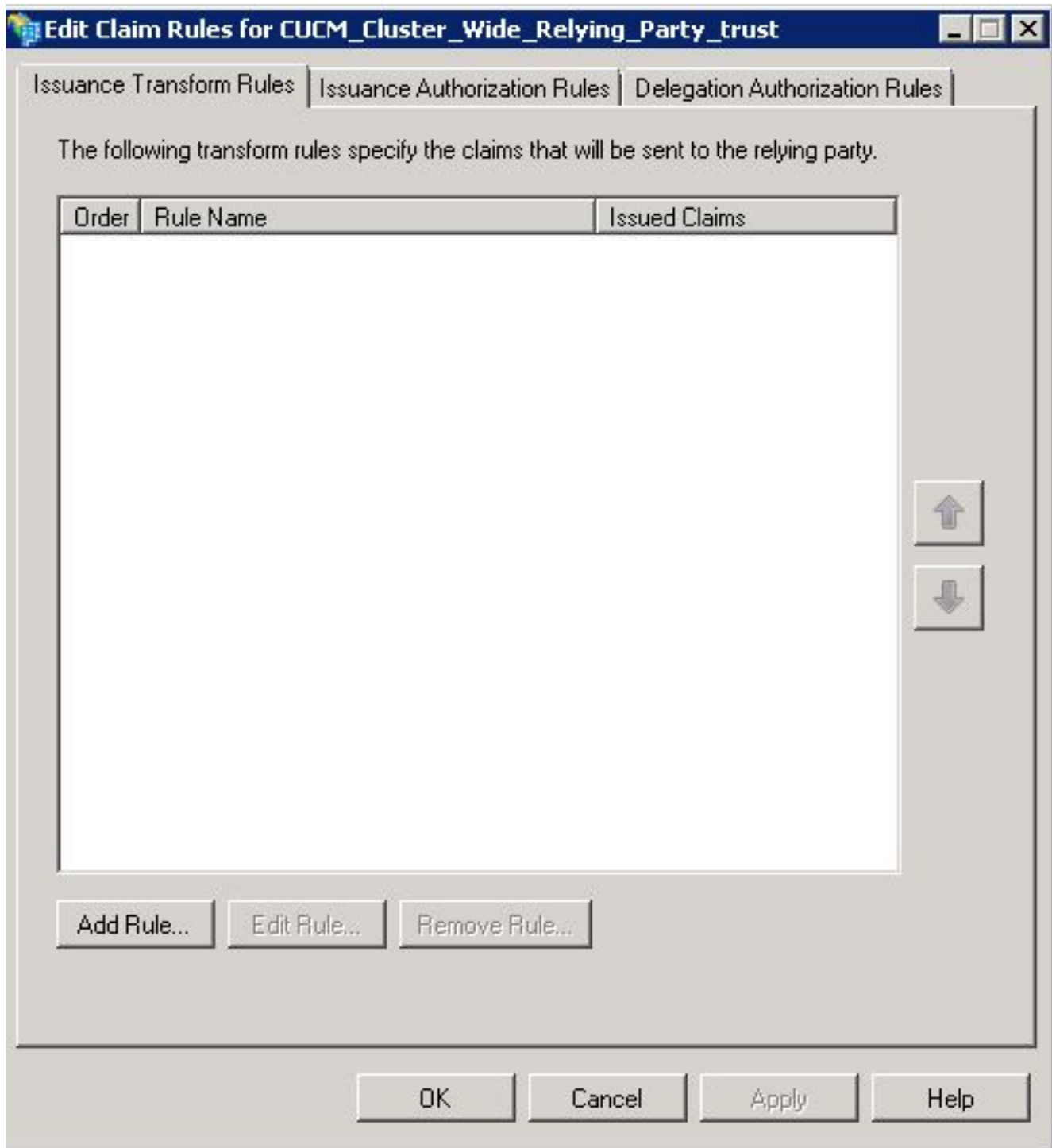
Finish Page (Abschließende Seite) bestätigt, dass die Vertrauenswürdigkeit der Partei erfolgreich der AD FS-Konfigurationsdatenbank hinzugefügt wurde. Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **Schließen**, wie im Bild gezeigt:



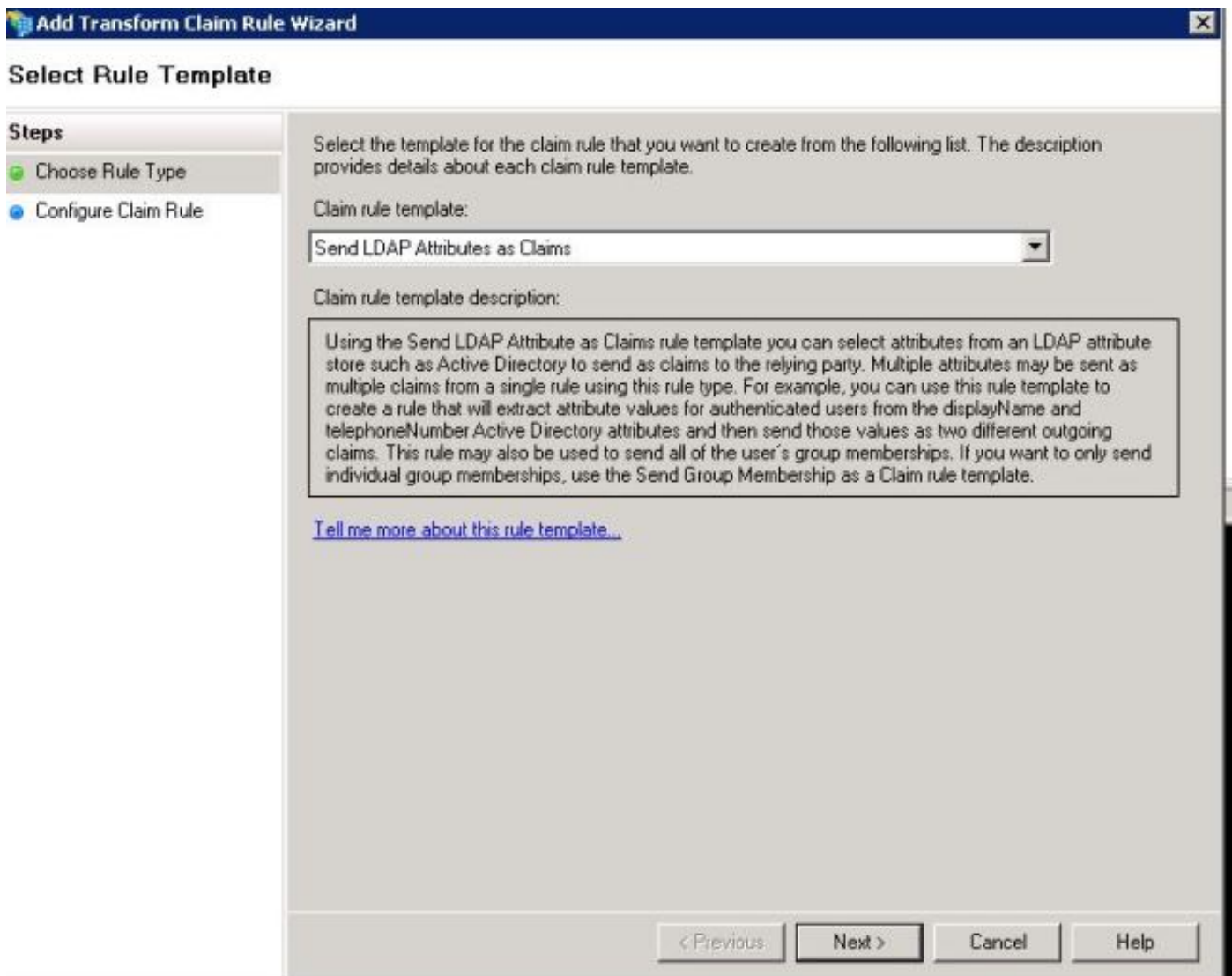
Klicken Sie mit der rechten Maustaste auf **Relying Party Trusts**, und klicken Sie auf **Edit Claim Rules** (Anspruchsregeln bearbeiten), wie im Bild gezeigt:



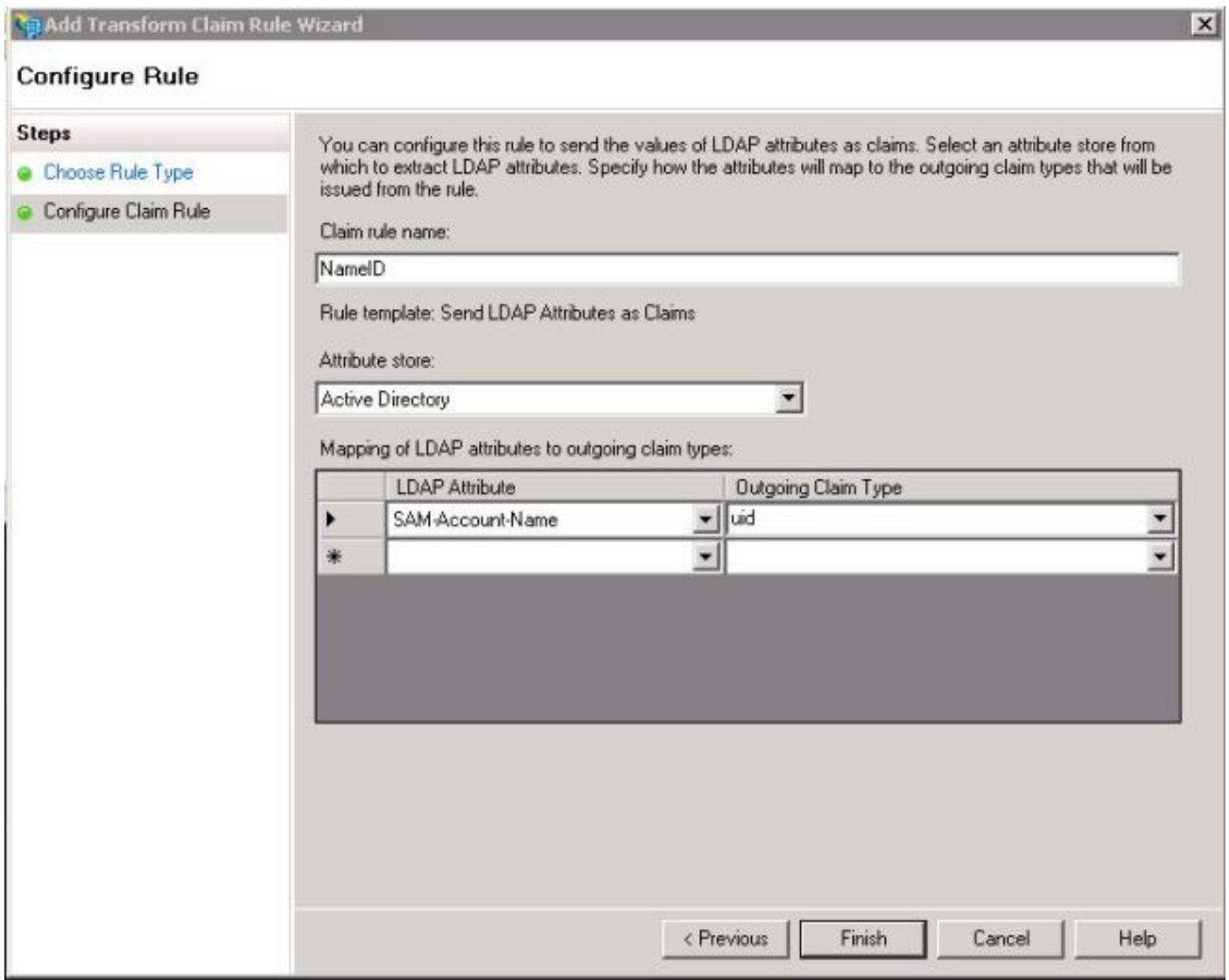
Klicken Sie jetzt auf **Regel hinzufügen**, wie im Bild gezeigt:



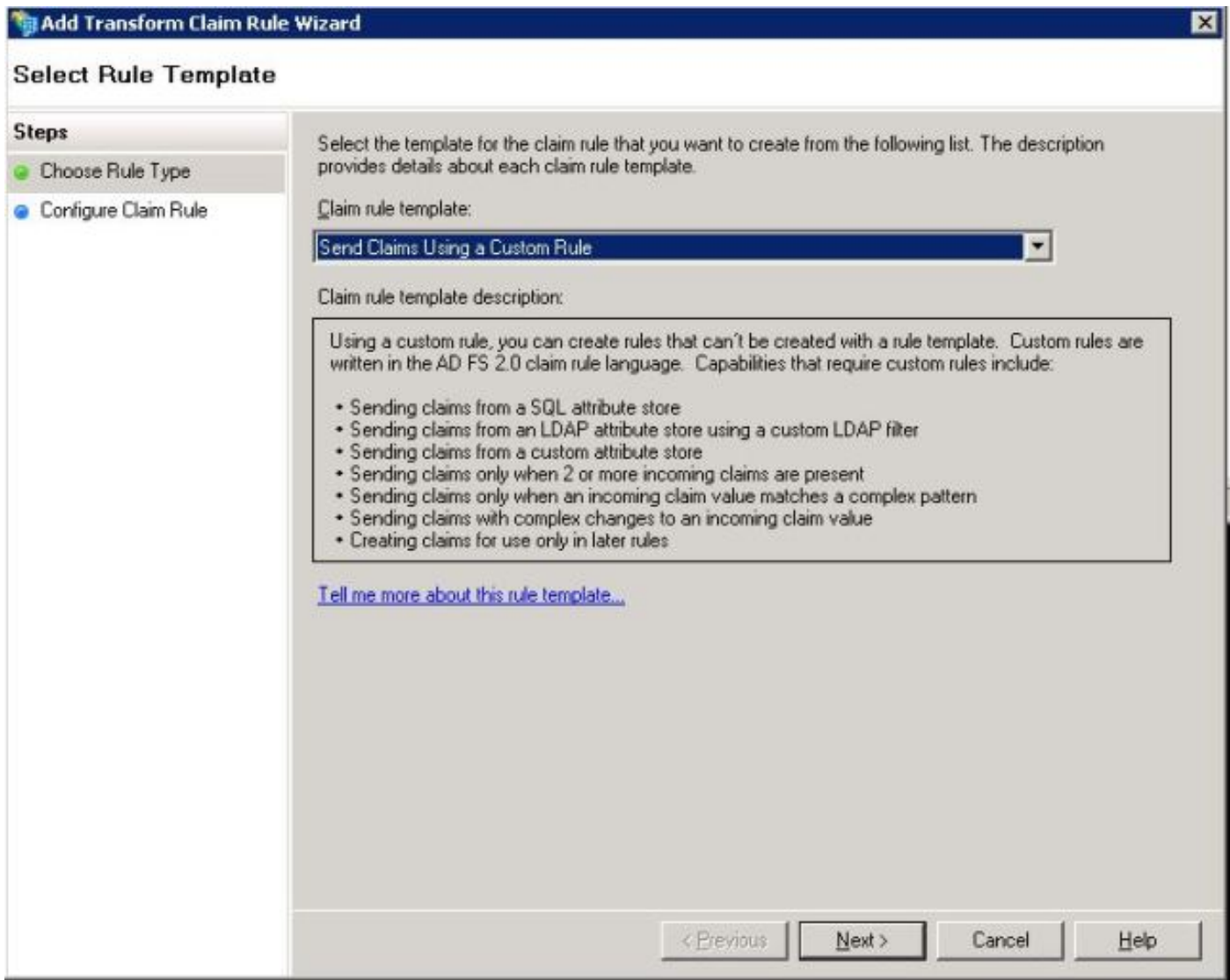
Wenn die **Regel für das Hinzufügen von Umwandlungsforderungen** geöffnet wird, klicken Sie auf **Weiter** mit der Standardlastenvorlage **LDAP-Attribute als Ansprüche senden**, wie im Bild gezeigt:



Klicken Sie auf **Anspruchsregel konfigurieren**, wie in diesem Bild gezeigt. Das LDAP-Attribut muss mit dem LDAP-Attribut in der LDAP-Verzeichniskonfiguration im CUCM übereinstimmen. Verwalten Sie den ausgehenden Anspruchstyp als **uid**. Klicken Sie auf **Fertig stellen**, wie im Bild gezeigt:



Fügen Sie die benutzerdefinierte Regel für die vertrauende Partei hinzu. Klicken Sie auf **Regel hinzufügen**. Wählen Sie **Anträge mit einer benutzerdefinierten Regel senden aus**, und klicken Sie dann auf **Weiter**, wie im Bild gezeigt:



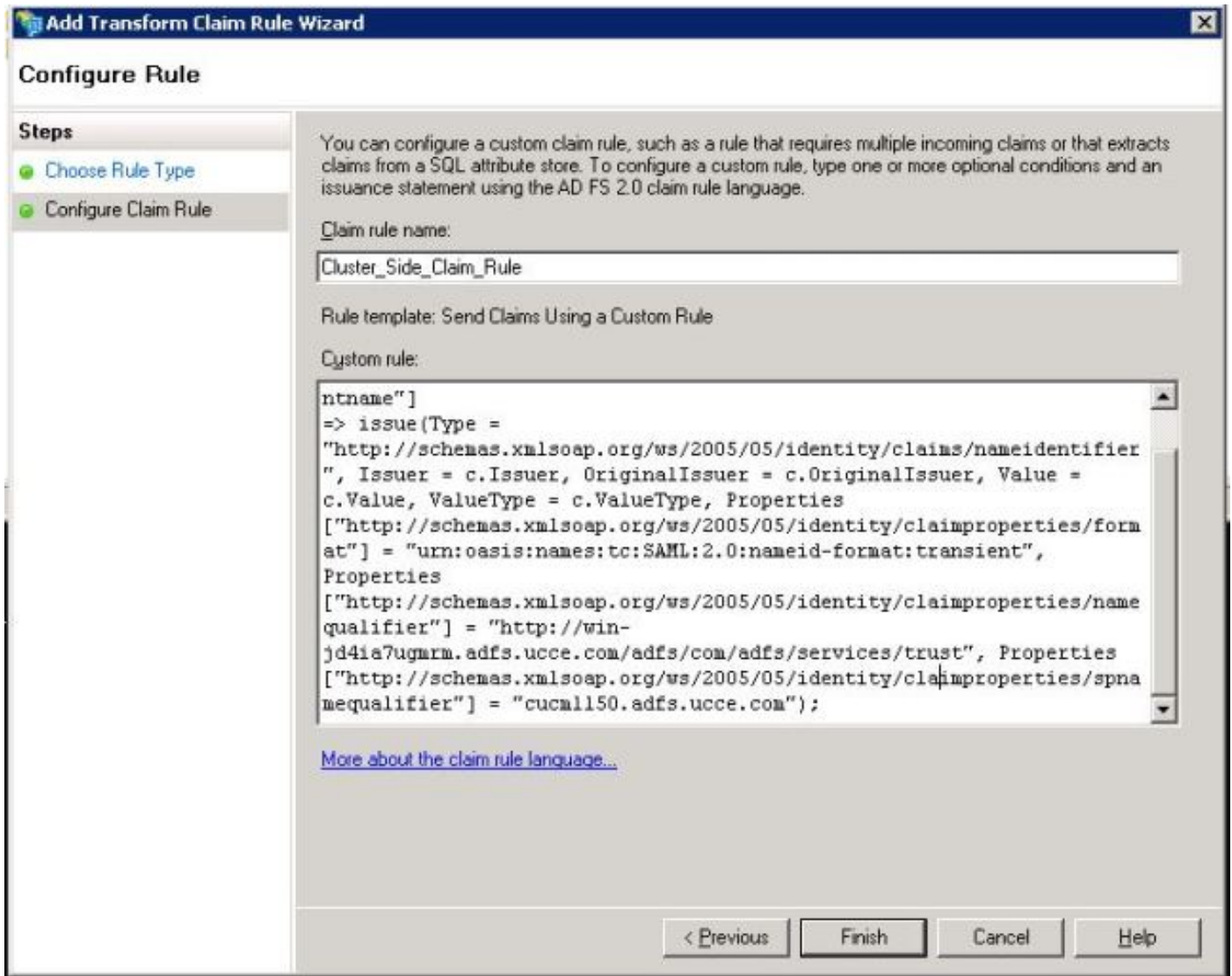
Geben Sie in der Regel zur Anspruchsregel einen Namen für eine Anspruchsregel ein, und kopieren Sie anschließend die angegebene und die Vergangenheit der Anspruchsregel im Feld Benutzerdefinierte Regel im Assistenten. Damit wird der Namensgleichrichter und der Spname-Qualifizierer in der Anspruchsregel geändert. Klicken Sie auf **Fertig stellen**, wie im Bild gezeigt:

Anspruchsregel:

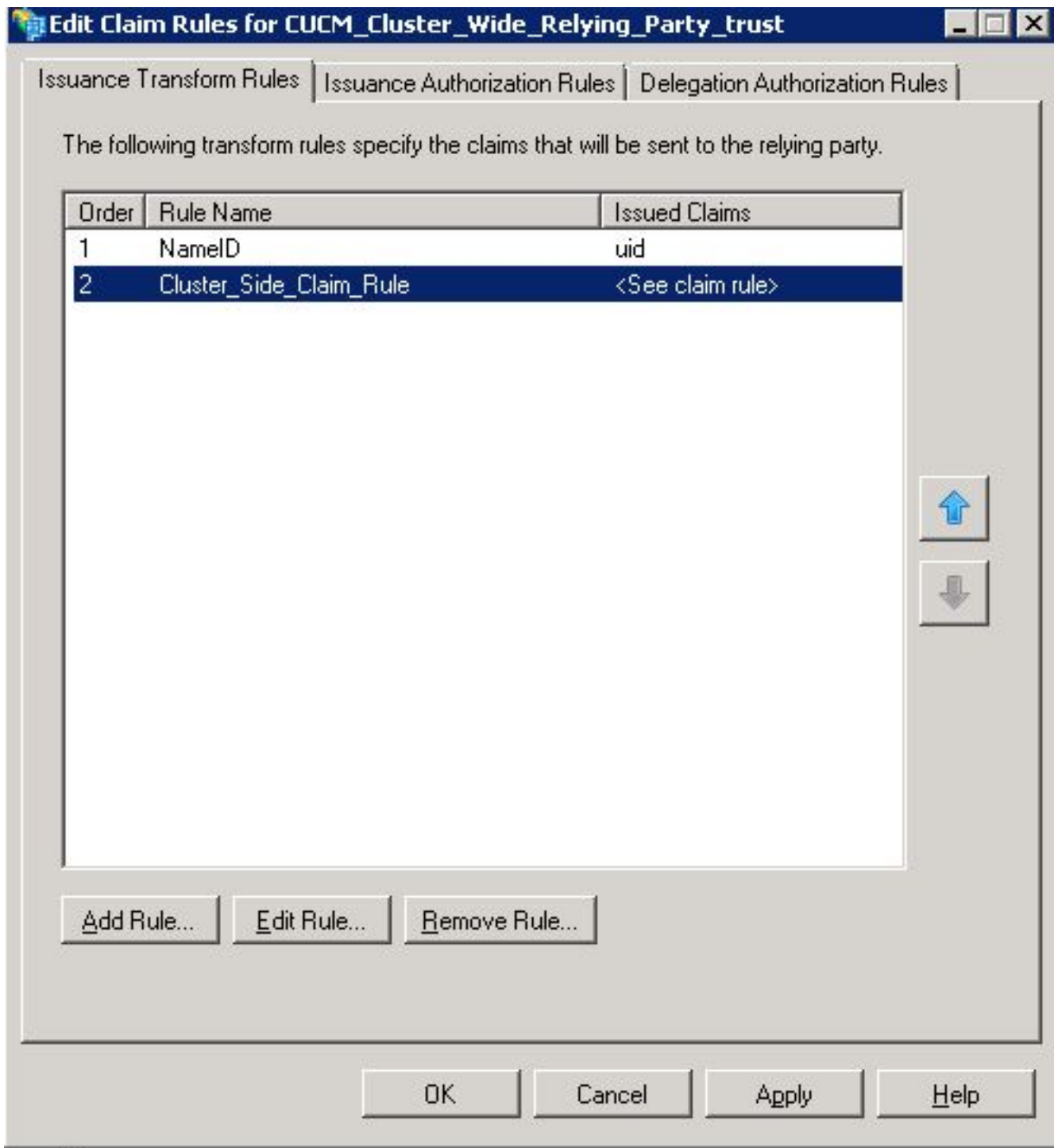
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> 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.



Klicken Sie, wie im Bild gezeigt, auf **Übernehmen** und dann auf **OK**.



Schritt 4: SAML SSO aktivieren

Öffnen Sie einen Webbrowser, melden Sie sich als Administrator bei CUCM an, und navigieren Sie zu **System > SAML Single Sign On**.

Standardmäßig ist das Optionsfeld **Clusterweit** aktiviert. Klicken Sie auf **Saml SSO aktivieren**, wie im Bild gezeigt:


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

Wie im Bild gezeigt, benachrichtigt das Popup-Fenster die Warnung für den Neustart des Webservers und informiert, dass die clusterweite SAML SSO oder Per-Node SAML SSO gemäß idp ausgewählt wird. Klicken Sie auf **Weiter**.

 **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.

Das Kriterium für die Aktivierung der clusterweiten SSO besteht darin, dass Sie bereits über ein Multiserver-Tomcat-Zertifikat verfügen müssen. Klicken Sie auf **Test for Multi-Server Tomcat Certificate**, wie im Bild gezeigt:

SAML Single Sign-On Configuration

Next

Status

 Status: Ready

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 cluster
- 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


Nach der Bestätigung wird für alle Knoten das Multi-Server-Zertifikat angezeigt. Alle **Knoten verfügen über das Multi-Server-Zertifikat**, und klicken Sie dann auf **Weiter**, wie im Bild gezeigt:

SAML Single Sign-On Configuration

 Next

Status

 Status: Ready

 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:

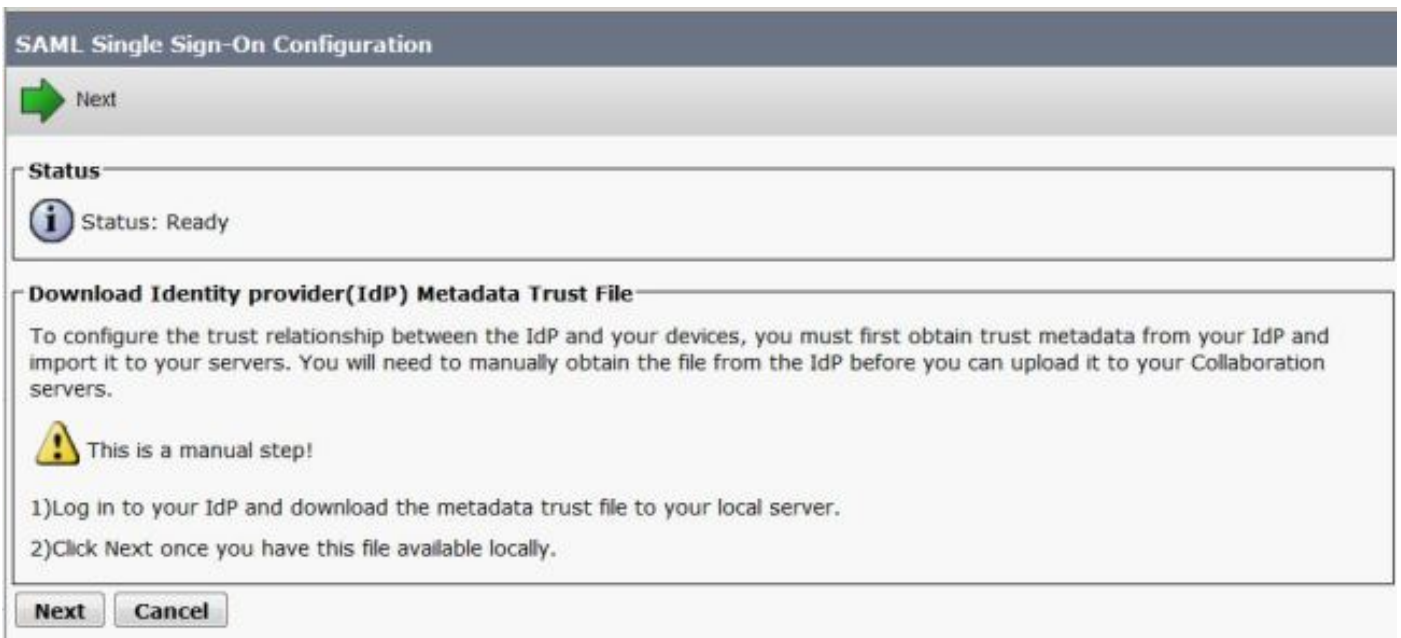
- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your 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 cluster
- 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

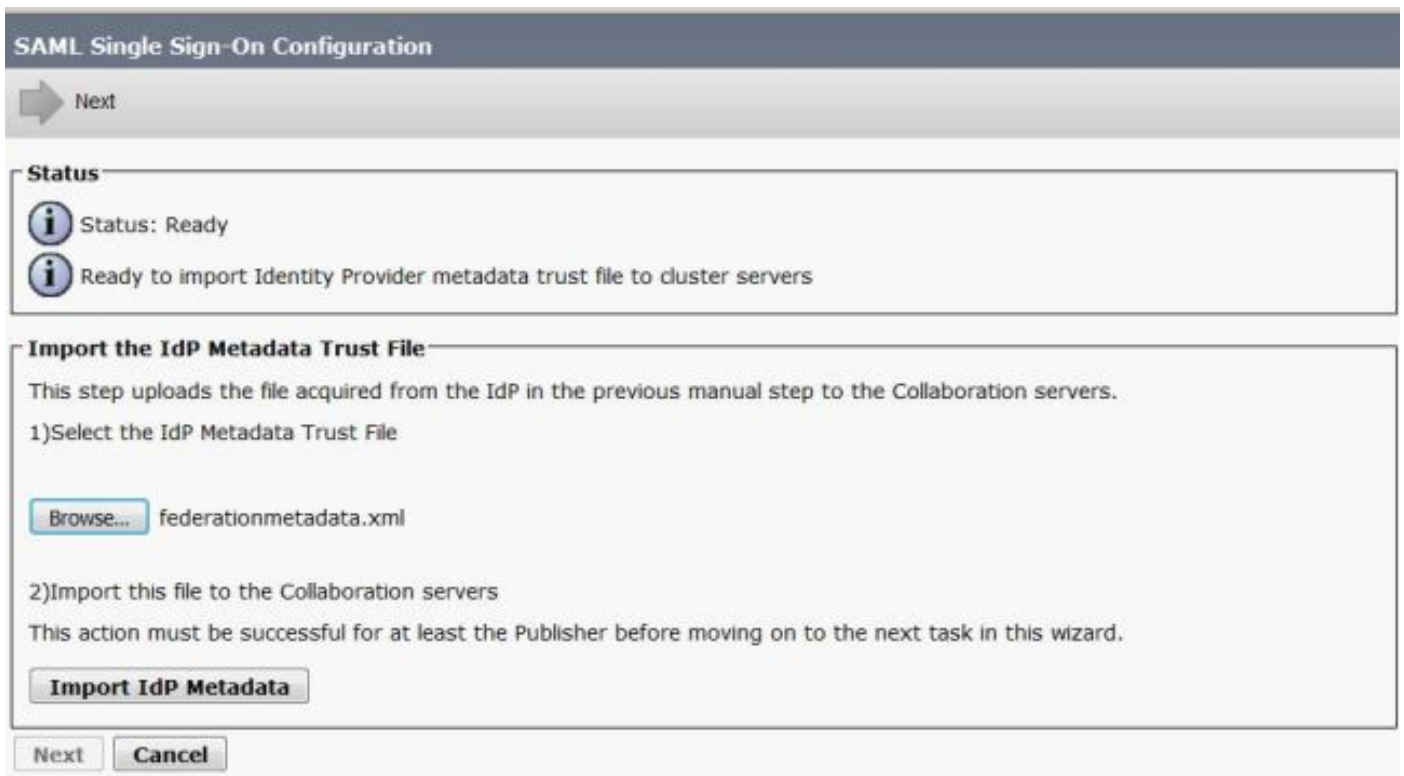
Test for Multi-Server tomcat certificate

Next Cancel

Klicken Sie, wie im Bild gezeigt, auf **Weiter**.



Durchsuchen und wählen Sie die heruntergeladenen IdP-Metadaten aus. Klicken Sie auf **Import IdP Metadata**, wie im Bild gezeigt:



Die Seite bestätigt den für alle Server erfolgreich importierten Import, und klicken Sie dann auf **Weiter**, wie im Bild gezeigt:

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

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

Import succeeded for all servers

Next Cancel

Klicken Sie, wie im Bild gezeigt, auf **Weiter**, da die SP-Metadaten bereits von der ersten SAML SSO-Konfigurationsseite exportiert wurden.

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

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

CUCM muss mit dem LDAP-Verzeichnis synchronisiert sein. Der Assistent zeigt die gültigen, im LDAP-Verzeichnis konfigurierten Administratorbenutzer an. Wählen Sie den Benutzer aus, und klicken Sie auf **SSO-Test ausführen**, wie im Bild gezeigt:

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

Geben Sie, wie im Bild gezeigt, die Benutzer-ID und das entsprechende Kennwort ein, sobald Sie dazu aufgefordert werden.

Authentication Required

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

User Name:

Password:

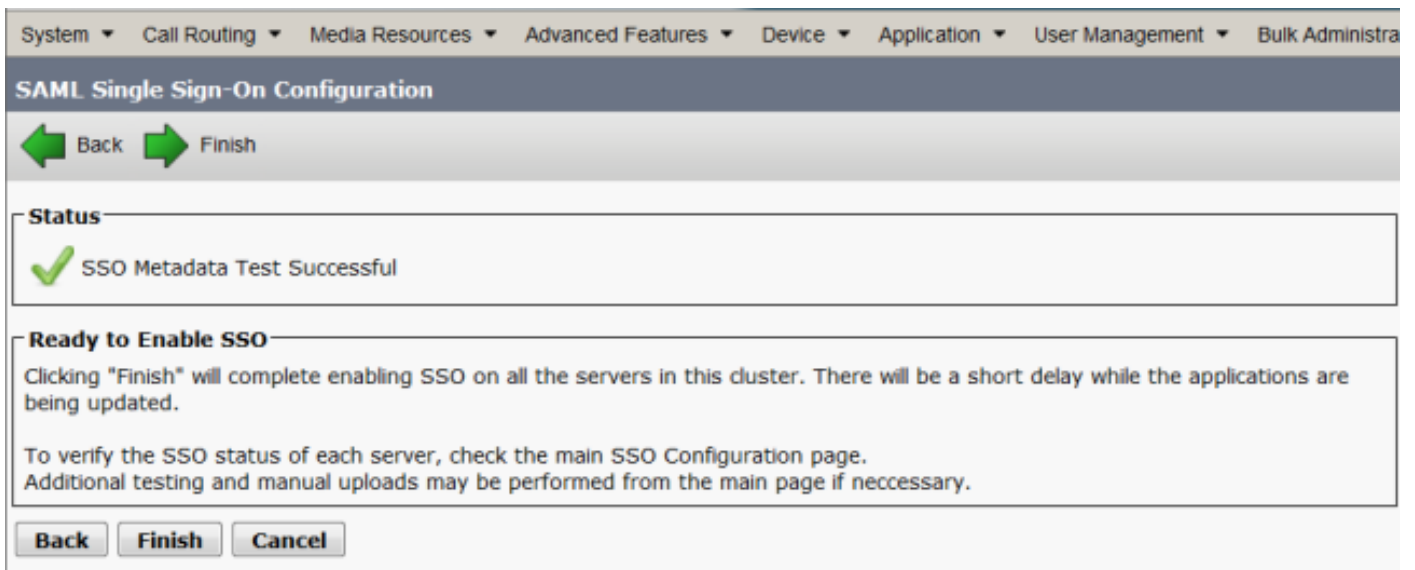
Wie im Bild gezeigt, bestätigt das Popup-Fenster, dass der Test erfolgreich war.

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

Klicken Sie, wie im Bild gezeigt, auf **Fertig stellen**, um die Konfiguration für die Aktivierung der SSO abzuschließen.



System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administra

SAML Single Sign-On Configuration

← Back → Finish

Status

✓ SSO Metadata Test Successful

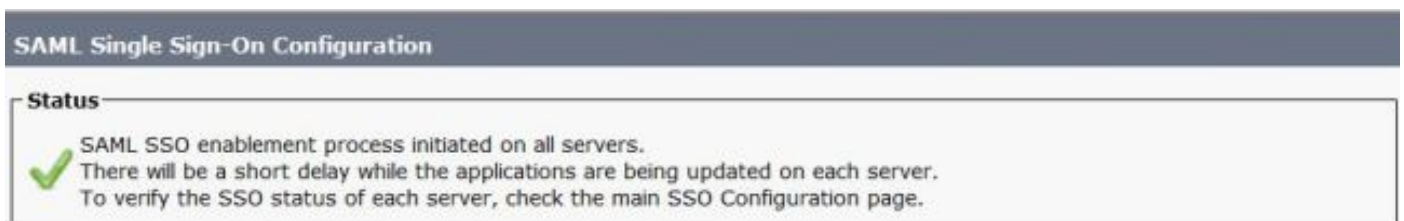
Ready to Enable SSO

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.

Back Finish Cancel

Die im Bild angezeigte Seite bestätigt, dass der SAML SSO-Aktivierungsprozess auf allen Servern initiiert wird.



SAML Single Sign-On Configuration

Status

✓ 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.

Melden Sie sich mit SAML SSO-Anmeldeinformationen ab, und melden Sie sich wieder beim CUCM an. Navigieren Sie zu **System >SAML Single Sign On**. Klicken Sie auf **SSO-Test** für andere Knoten im Cluster **ausführen**, wie im Bild gezeigt:

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestätigen Sie, dass der SSO-Test für die Knoten erfolgreich ist, für die SAML SSO aktiviert ist. Navigieren Sie zu **System >SAML Single Sign On**. Erfolgreiche SSO-Tests zeigen den Status Bestanden an.

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

Nach Aktivierung der SAML SSO werden installierte Anwendungen und Plattformanwendungen für die CUCM-Anmeldeseite aufgelistet, wie in diesem Bild gezeigt.

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

Nach Aktivierung der SAML SSO werden installierte Anwendungen und Plattformanwendungen für die Anmeldeseite IM und Presence aufgelistet, wie in diesem Bild gezeigt:

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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Um die SSO-Protokolle auf Debuggen festzulegen, verwenden Sie den Befehl **SampleTrace Level DEBUG**.

Erfassen Sie die SSO-Protokolle mithilfe von RTMT oder vom Speicherort **activelog /tomcat/logs/ssosp/log4j/*.log** mithilfe der CLI.

Beispiel für SSO-Protokolle zeigt die generierten und an andere Knoten gesendeten Metadaten

```
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
```