AD FS Version 2.0 - Setup für SAML SSO-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Active Directory Federation Service (AD FS) Version 2.0 konfiguriert wird, um die Single Sign-On (SAML) für Cisco Collaboration-Produkte wie Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN), CUCM IM and Presence und Cisco Prime Collaboration zu aktivieren.

Voraussetzungen

Anforderungen

AD FS Version 2.0 muss installiert und getestet werden.

> **Vorsicht**: Dieser Installationsleitfaden basiert auf einer Laboreinrichtung, und es wird davon ausgegangen, dass AD FS Version 2.0 nur für SAML SSO mit Cisco Collaboration-Produkten verwendet wird. Falls sie von anderen geschäftskritischen Anwendungen verwendet wird, muss die erforderliche Anpassung gemäß der offiziellen Microsoft-Dokumentation erfolgen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

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

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

AD FS Version 2.0 Identity Provider (IdP)-Metadaten herunterladen

Führen Sie zum Herunterladen von IdP-Metadaten diesen Link in Ihrem Browser aus: https://<FQDN of ADFS>/FederationMetadata/2007-06/FederationMetadata.xml.

Collaboration Server (SP)-Metadaten herunterladen

CUCM IM- und Presence-Service

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

Unity-Verbindung

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

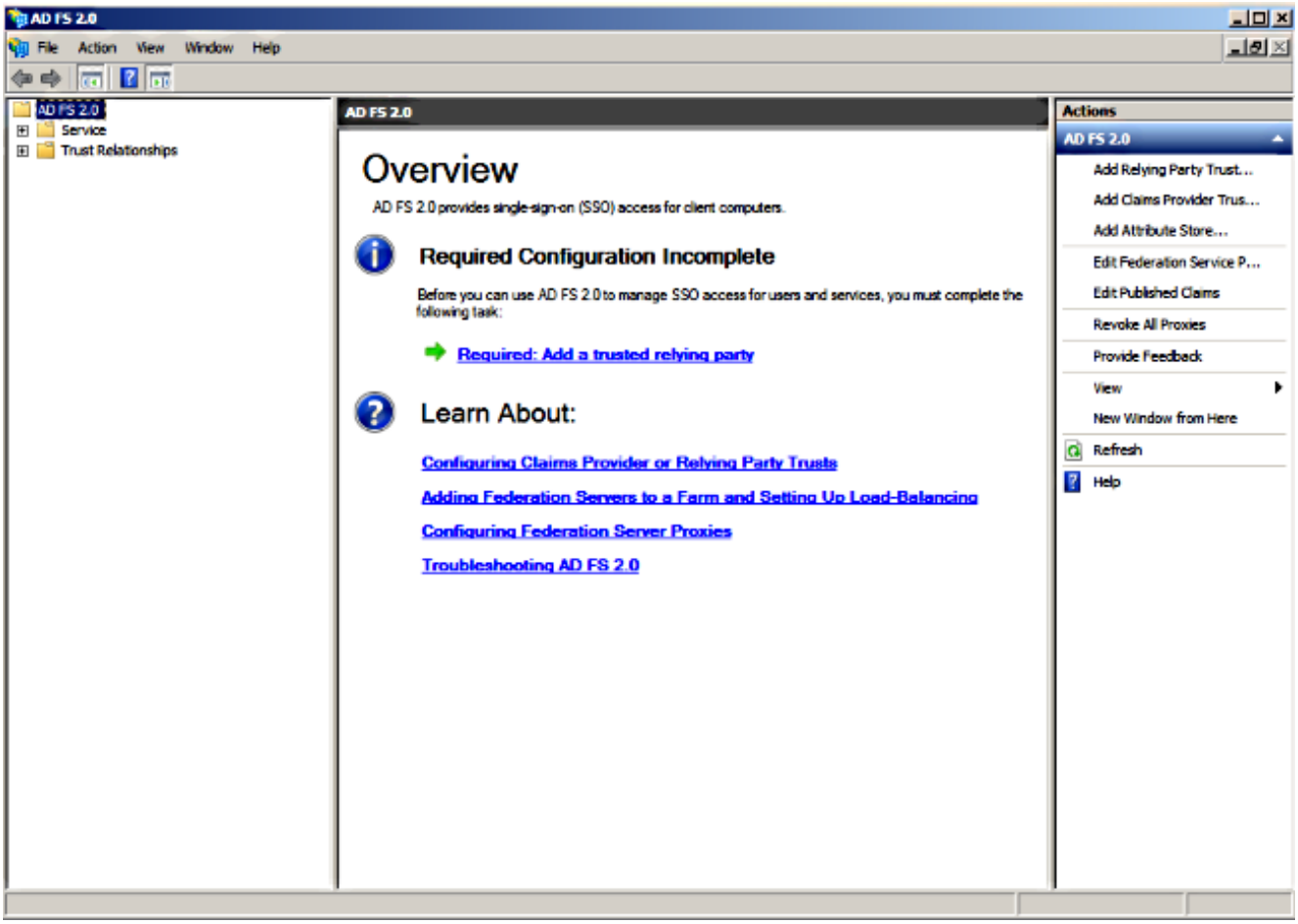
Cisco Prime Collaboration-Bereitstellung

Öffnen Sie einen Webbrowser, melden Sie sich als globales Admin bei Prime Collaboration Assurance an, und navigieren Sie zu **Administration > System Setup > Single Sign On**.

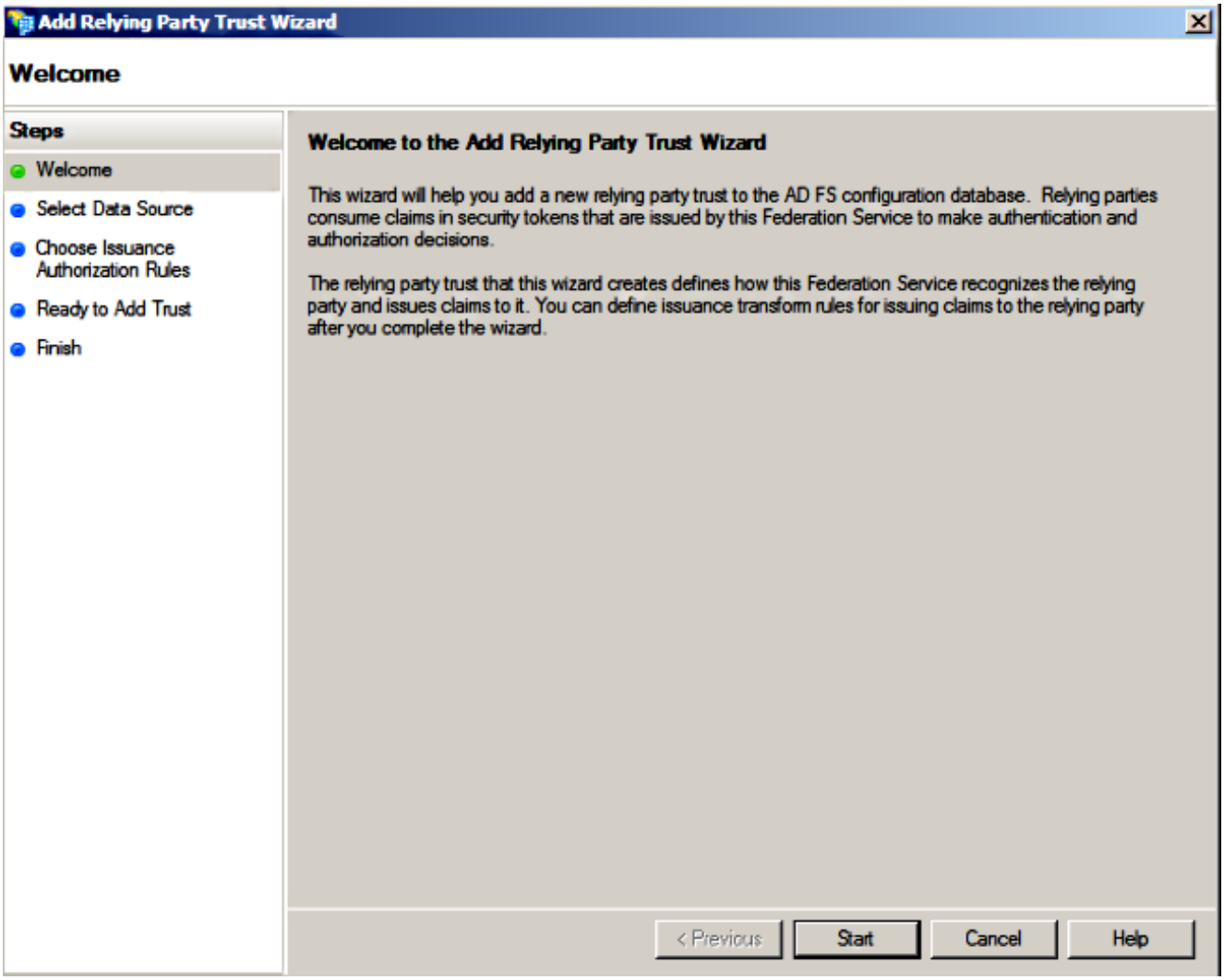
Hinzufügen von CUCM als Vertrauen der Partei

1. Melden Sie sich beim AD FS-Server an, und starten Sie AD FS Version 2.0 im Microsoft Windows **Programs** Menü.

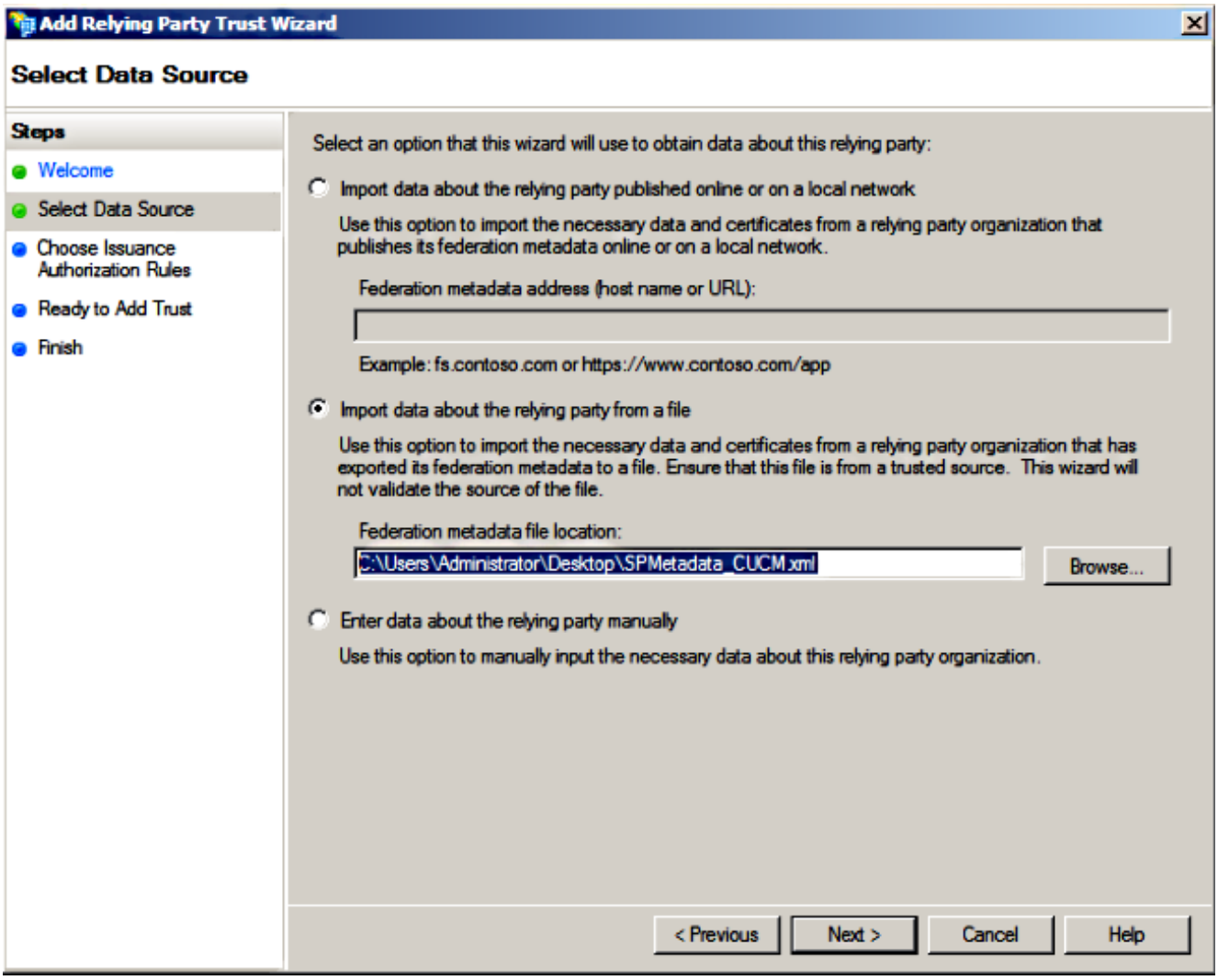
2. Wählen Sie **Vertrauenswürdige Partei hinzufügen aus**.



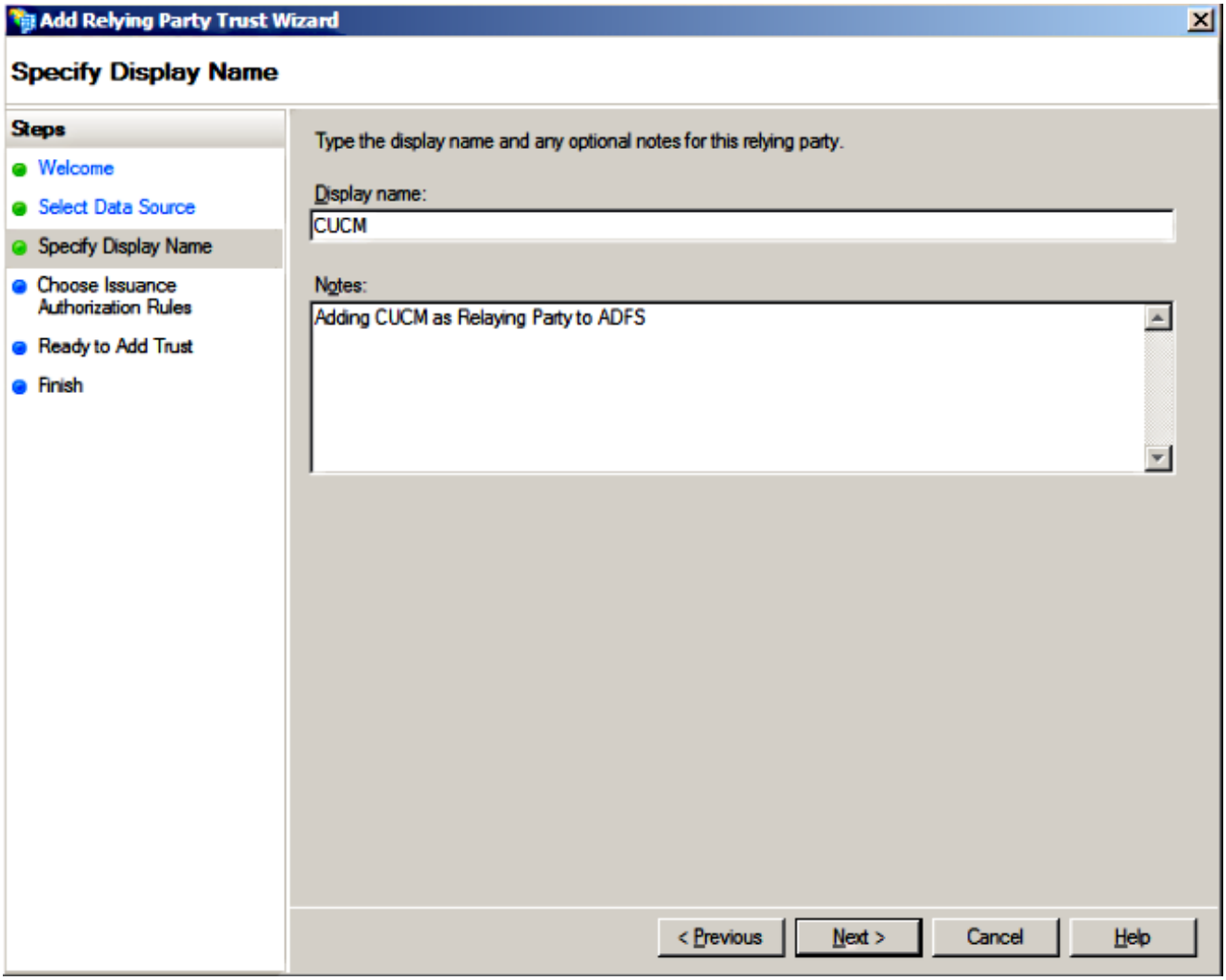
3. Klicken Sie auf **Start**.



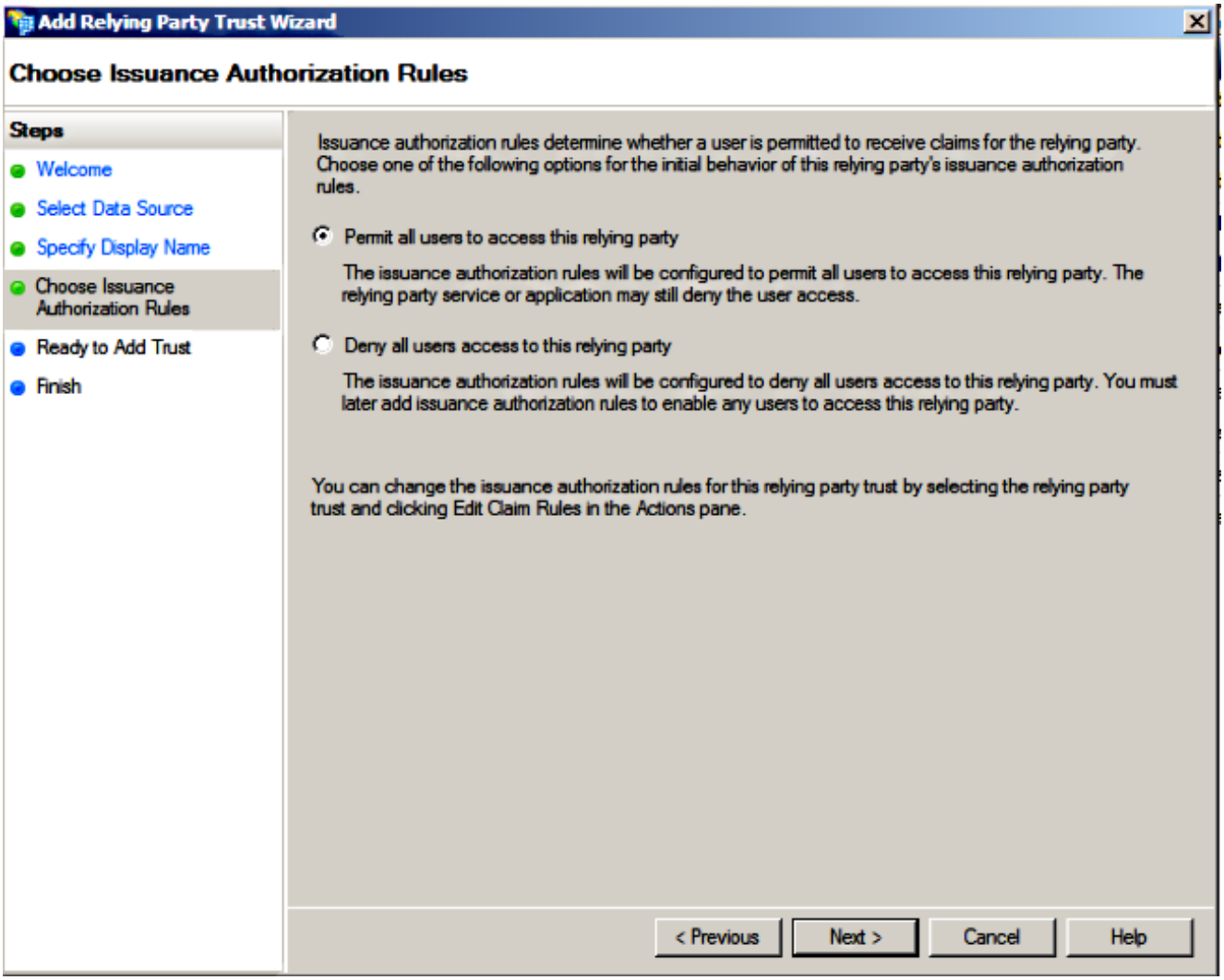
4. Wählen Sie die Option **Import data about the Relying Party from a file** aus, wählen Sie die **SPMetadata_CUCM.xml-**Metadatendatei aus, die Sie zuvor von CUCM heruntergeladen haben, und klicken Sie auf **Next.**



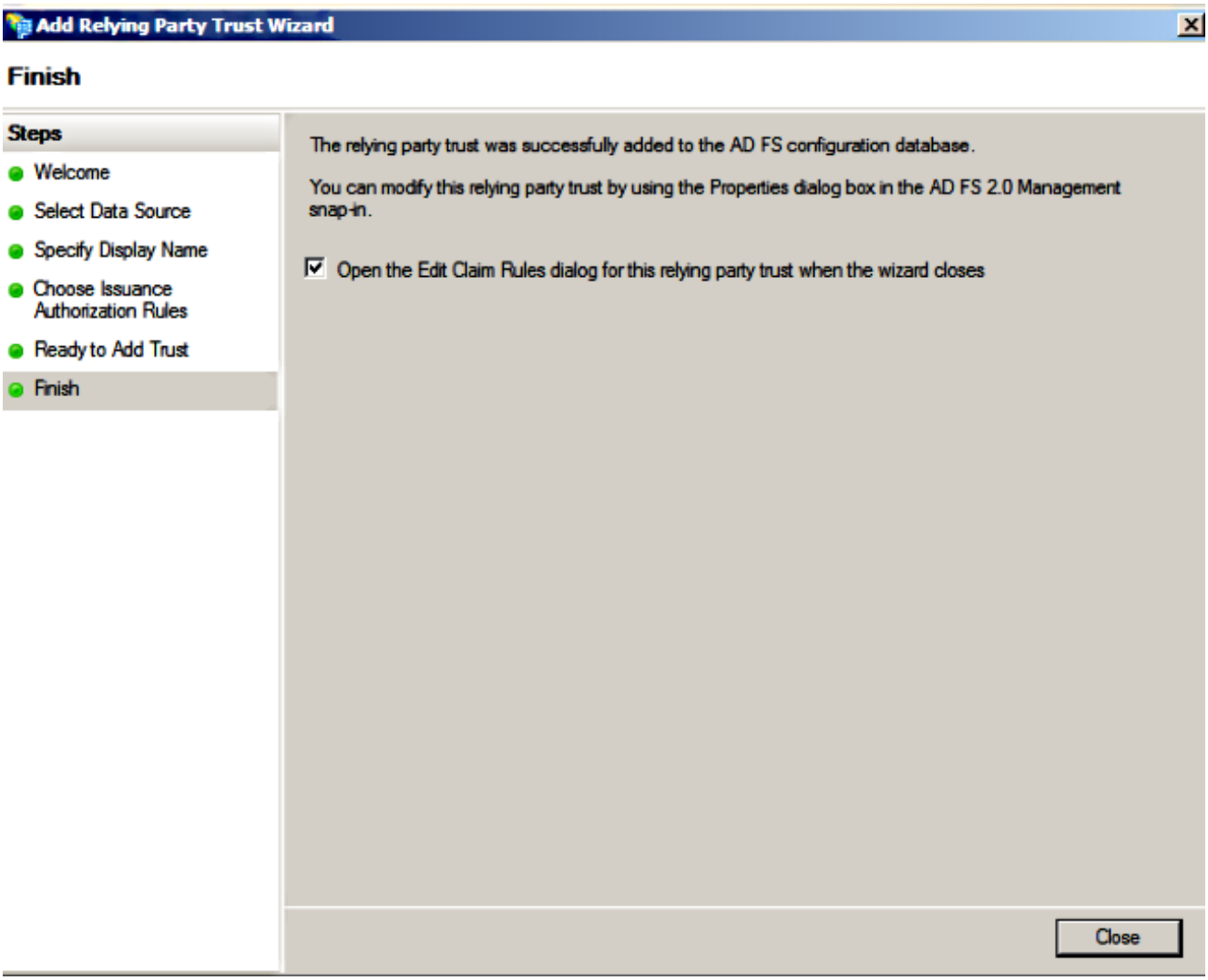
5. Geben Sie den **Anzeigenamen ein**, und klicken Sie auf **Weiter**.



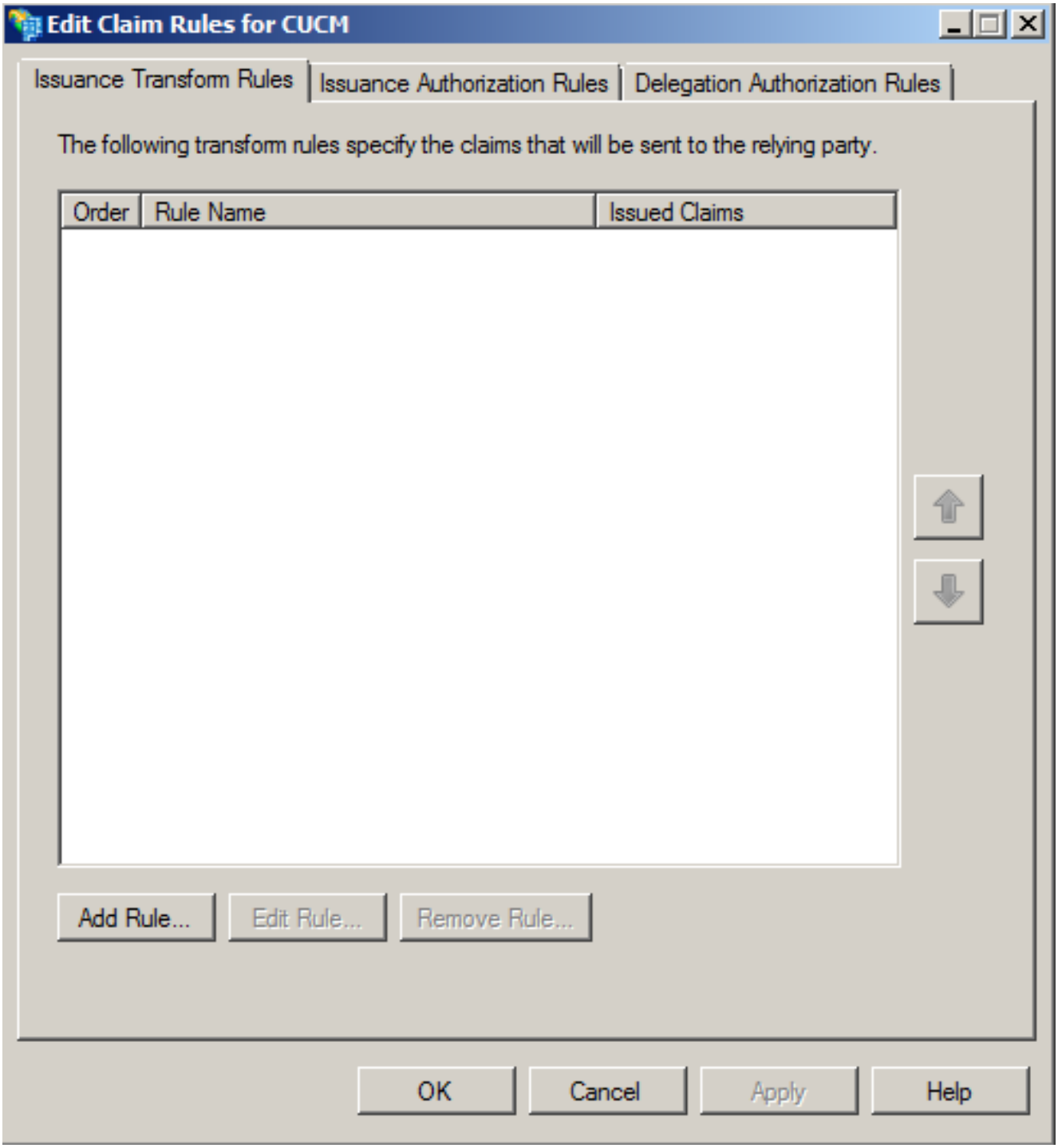
6. Wählen Sie **Zulassen aller Benutzer für den Zugriff auf diese vertrauliche Partei aus,** und klicken Sie auf **Weiter.**



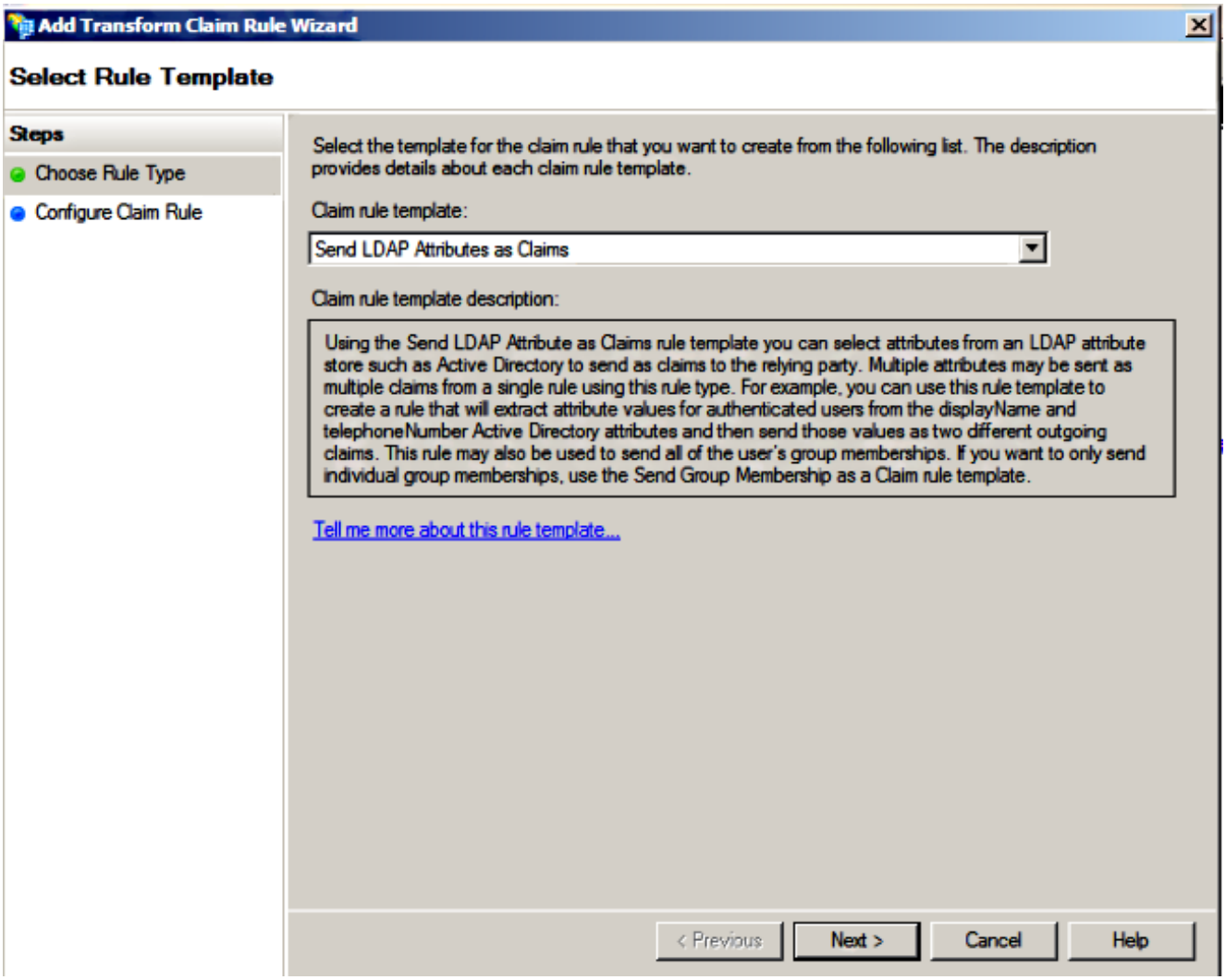
7. Wählen Sie **beim Schließen des Assistenten die Option Anspruchsregeln bearbeiten für die Vertrauenswürdigkeit der vertrauenden Partei öffnen aus,** und klicken Sie auf **Schließen.**



8. Klicken Sie auf **Regel hinzufügen**.

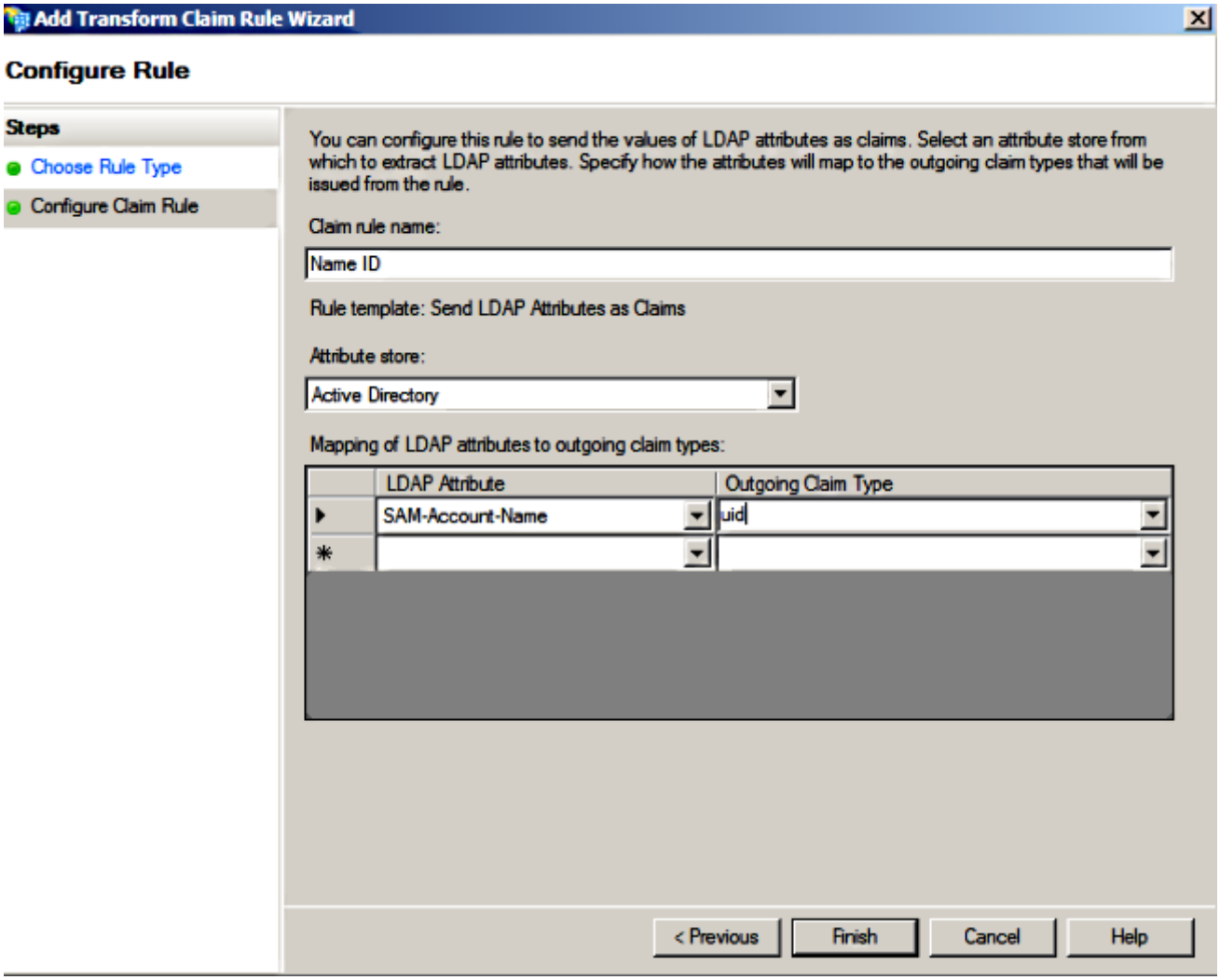


9. Klicken Sie auf **Weiter**, wobei die Standardvorlage für Anspruchsregeln auf **LDAP-Attribute als Ansprüche senden** festgelegt ist.

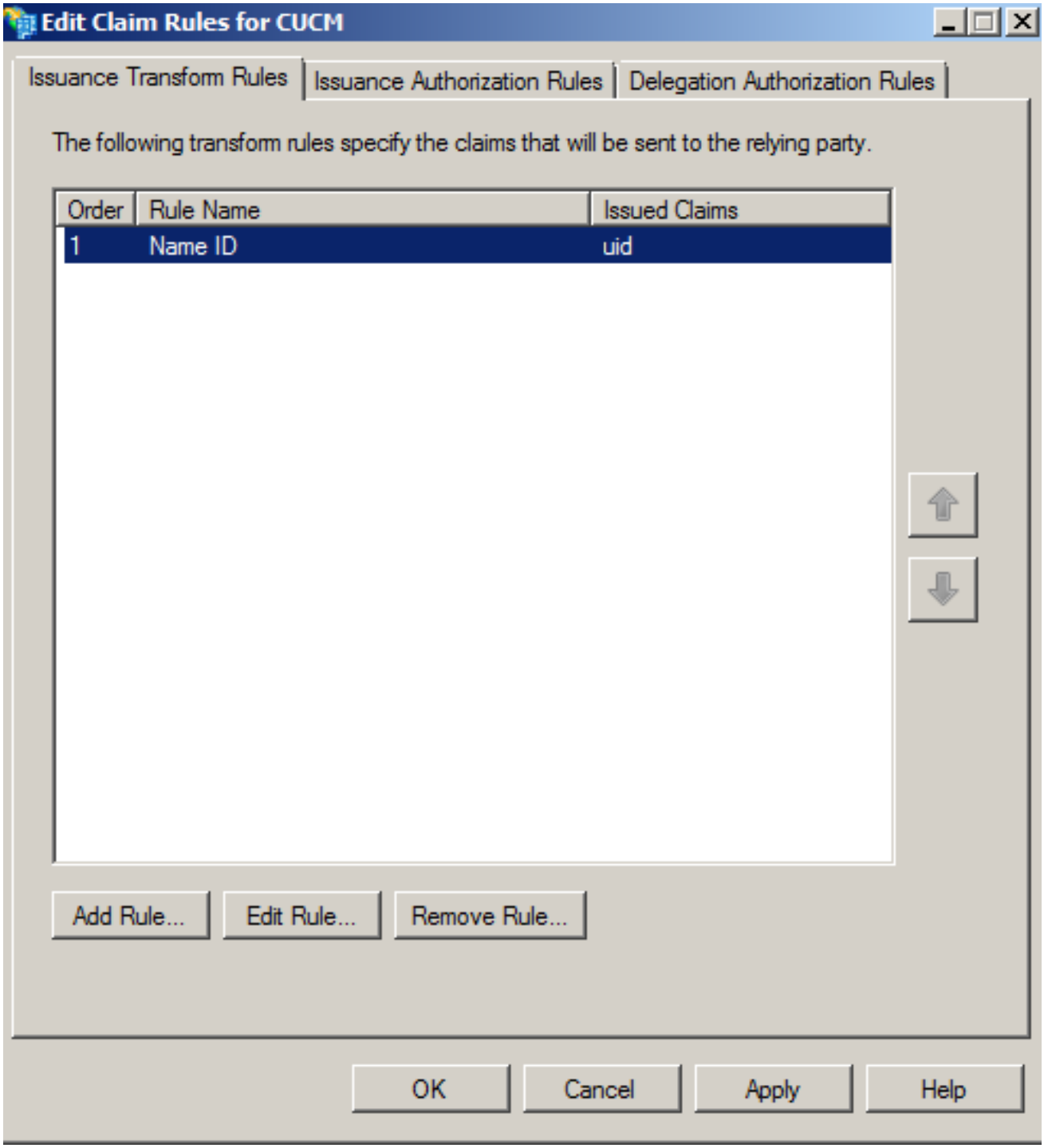


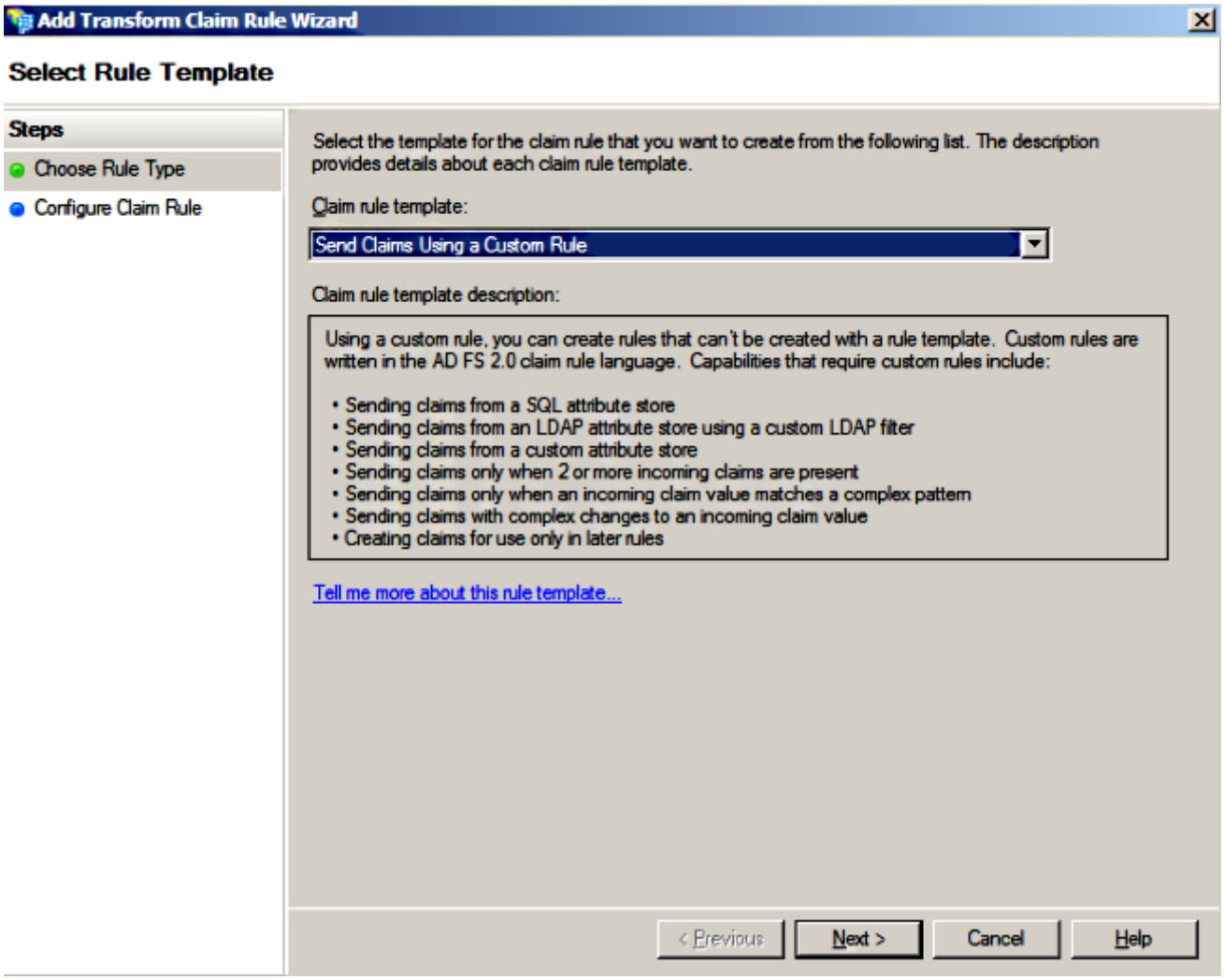
10. Geben Sie unter Configure Rule (Regel konfigurieren) den Namen der Anspruchsregel ein, wählen Sie **Active Directory** als Attributspeicher aus, konfigurieren Sie **LDAP-Attribut** und **Outgoing Claim Type (Ausgehender Anspruchstyp)** wie in diesem Bild gezeigt, und klicken Sie auf **Beenden**.

    Hinweis:
    - Das LDAP-Attribut (Lightweight Directory Access Protocol) sollte dem Directory Sync-Attribut auf CUCM entsprechen.
    - "uid" sollte in Kleinbuchstaben angegeben werden.



11. Klicken Sie auf **Regel hinzufügen**, wählen Sie **Anträge mithilfe einer benutzerdefinierten Regel** als Vorlage für Anspruchsregel **senden** aus, und klicken Sie auf **Weiter**.

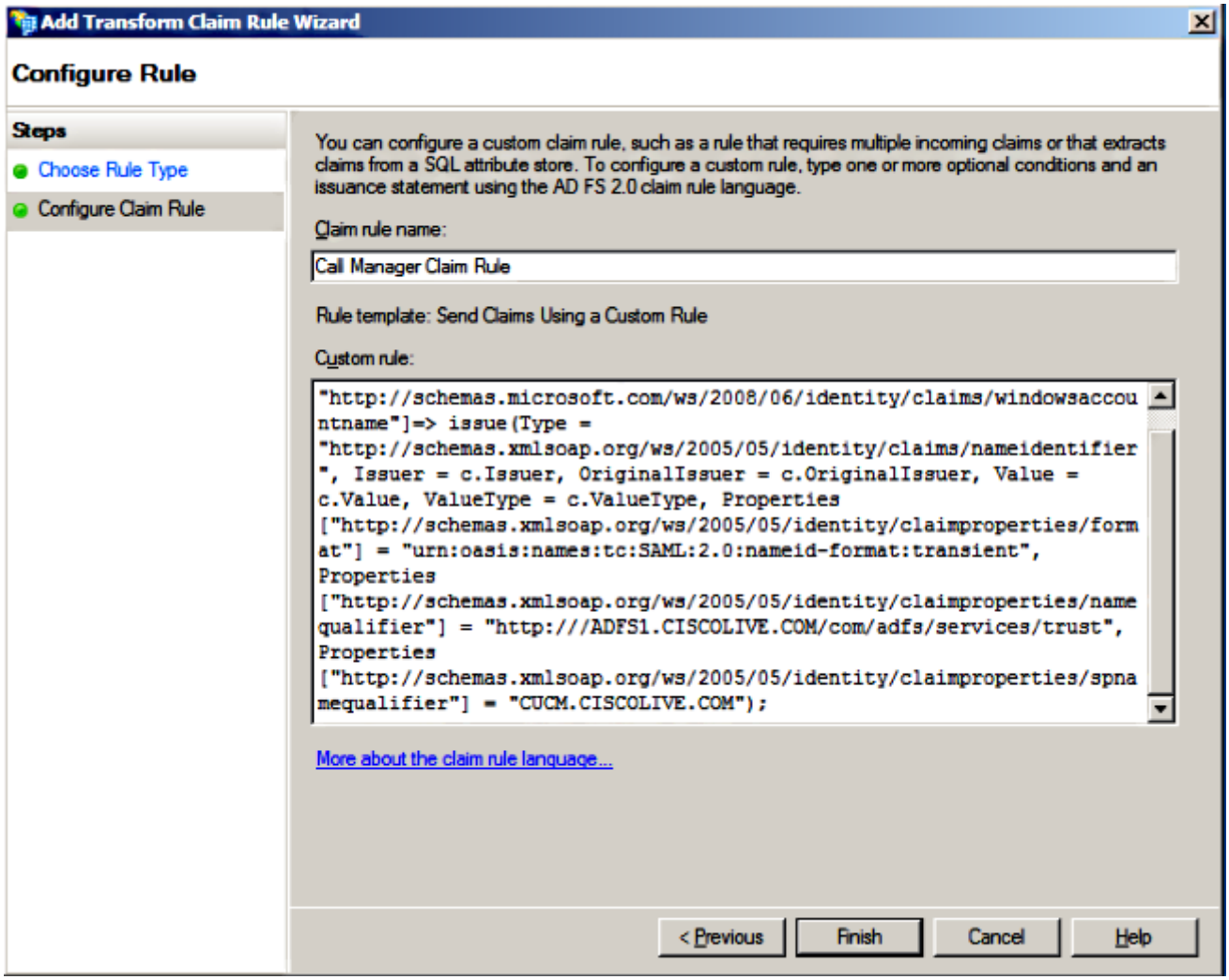

Edit Claim Rules for CUCM
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
Name ID
uid
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help



12. Geben Sie einen Namen für den Namen einer Anspruchsregel ein, und kopieren Sie diese Syntax in das Feld unter Benutzerdefinierte Regel:

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "<FQDN of CUCM>");
```

(**HINWEIS:** Wenn Sie den Text aus diesen Beispielen kopieren und einfügen, beachten Sie, dass einige Textverarbeitungssoftware die ASCII-Anführungszeichen (") durch die UNICODE-Versionen ("") ersetzen wird. Die UNICODE-Versionen führen zum Ausfall der Anspruchsregel.)



Hinweis:
- CUCM und ADFS Fully Qualified Domain Name (FQDN) werden in diesem Beispiel mit dem CUCM und AD FS im Labor vorausgefüllt und müssen entsprechend Ihrer Umgebung geändert werden.
- Bei FQDN von CUCM/ADFS wird zwischen Groß- und Kleinschreibung unterschieden und muss mit den Metadatendateien übereinstimmen.

13. Klicken Sie auf **Fertig stellen**.

14. Klicken Sie auf **Übernehmen** und dann auf **OK.**

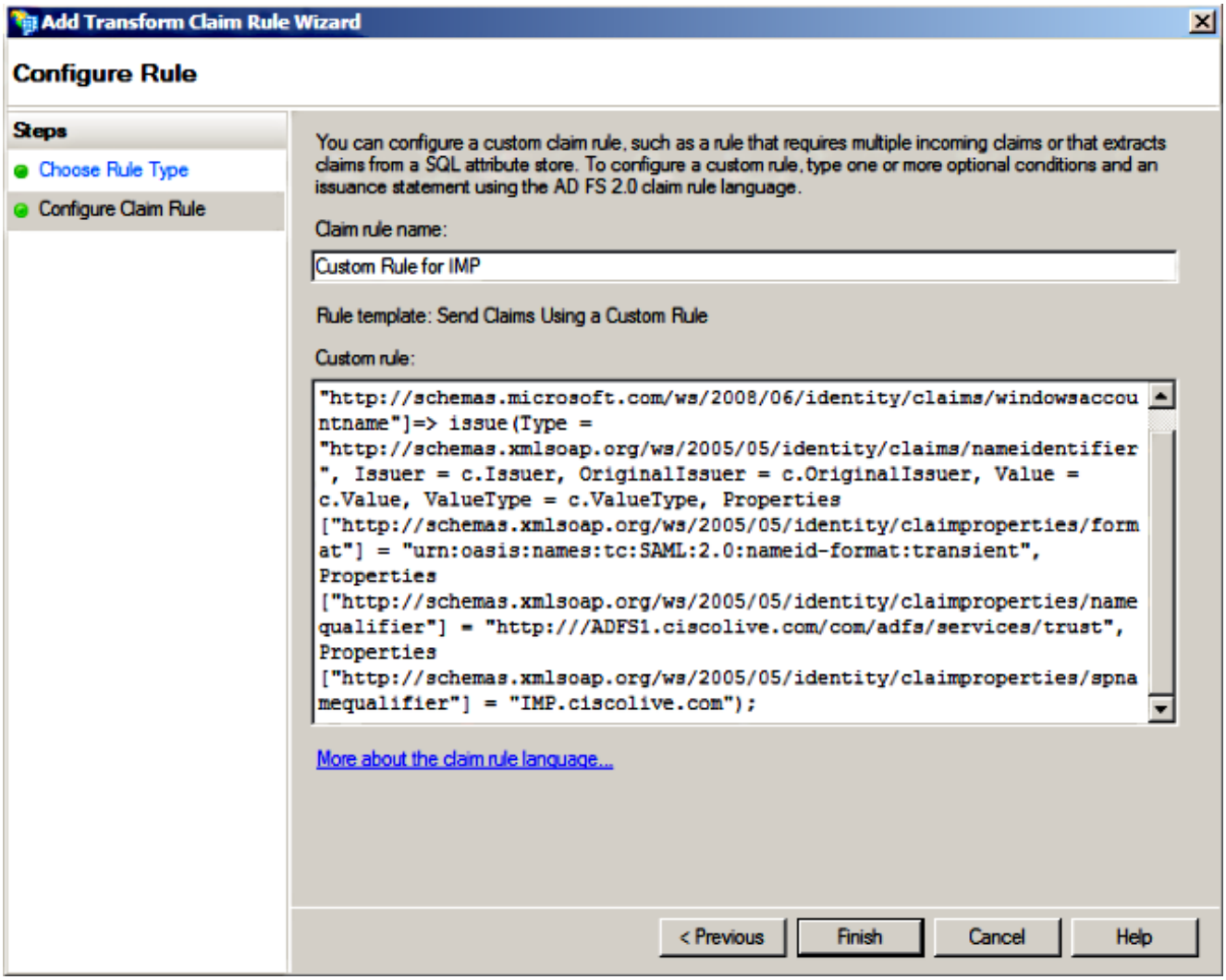
15. Starten Sie den Dienst AD FS Version 2.0 von **Services.msc** aus neu.

Hinzufügen von CUCM IM und Presence als Vertrauen der zuverlässigen Partei

1. Wiederholen Sie die Schritte 1 bis 11, wie für **Hinzufügen von CUCM als "Relying Party Trust"** beschrieben, und fahren Sie mit Schritt 2 fort.

2. Geben Sie einen Namen für den Namen einer Anspruchsregel ein, und kopieren Sie diese Syntax in das Feld unter Benutzerdefinierte Regel:

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of IMP>");
```



Beachten Sie, dass IM und Presence sowie AD FS FQDN in diesem Beispiel mit den Lab-IM und -Presence und AD FS vorbelegt sind und entsprechend Ihrer Umgebung geändert werden müssen.

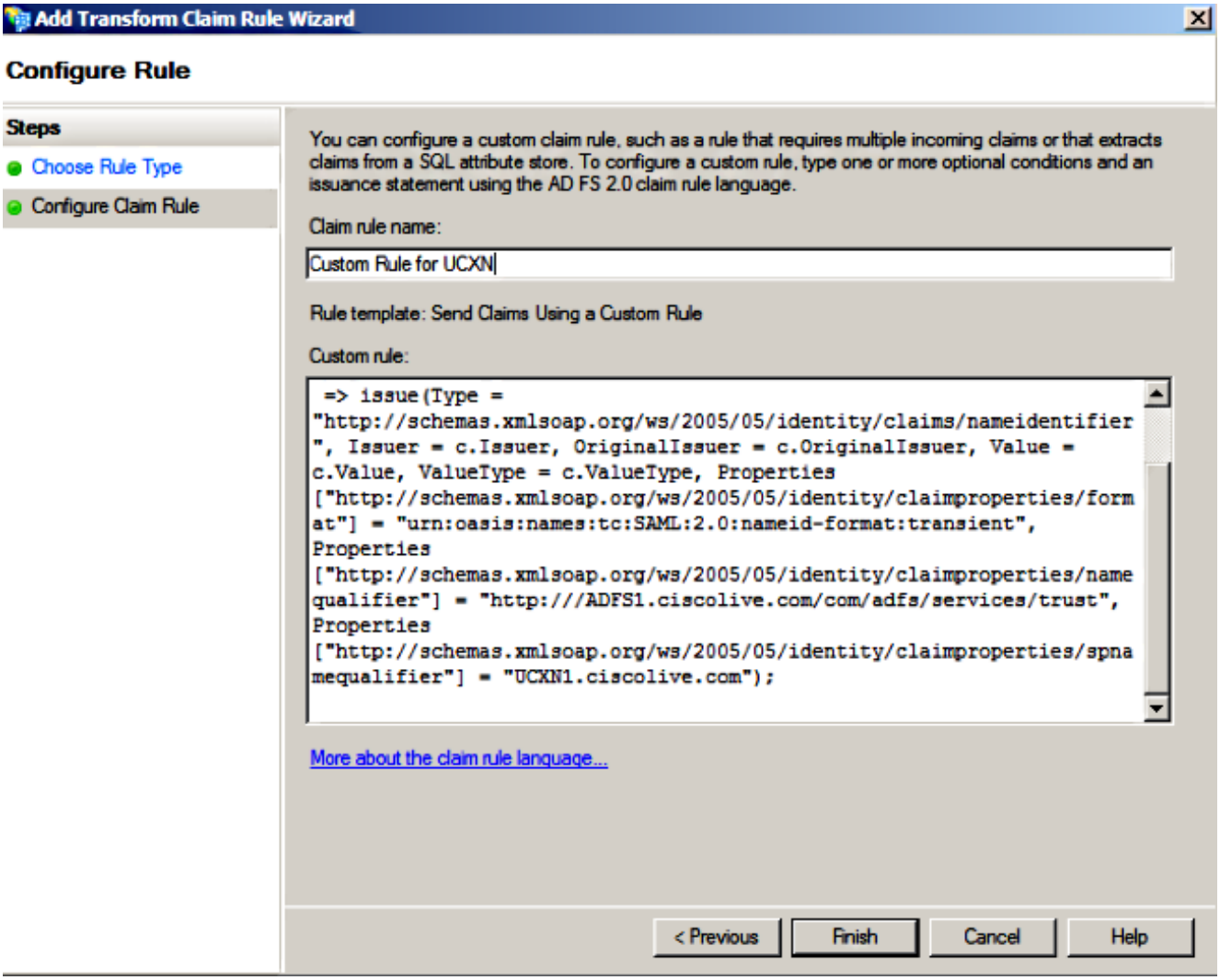
3. Klicken Sie auf **Fertig stellen**.
4. Klicken Sie auf **Übernehmen** und dann auf **OK.**
5. Starten Sie den Dienst AD FS Version 2.0 von **Services.msc** aus neu.

Hinzufügen von UCXN als Vertrauen der zuverlässigen Partei

1. Wiederholen Sie die Schritte 1 bis 12, wie für **Hinzufügen von CUCM als "Relying Party Trust"** beschrieben, und fahren Sie mit Schritt 2 fort.

2. Geben Sie einen Namen für den Namen der Anspruchsregel ein, und kopieren Sie diese Syntax in das Feld unter Benutzerdefinierte Regel:

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of UCXN>");
```



Beachten Sie, dass UCXN und AD FS FQDN in diesem Beispiel vorab mit UCXN und ADFS im Labor ausgefüllt wird und entsprechend Ihrer Umgebung geändert werden muss.

3. Klicken Sie auf **Fertig stellen**.

4. Klicken Sie auf **Übernehmen** und dann auf **OK**.

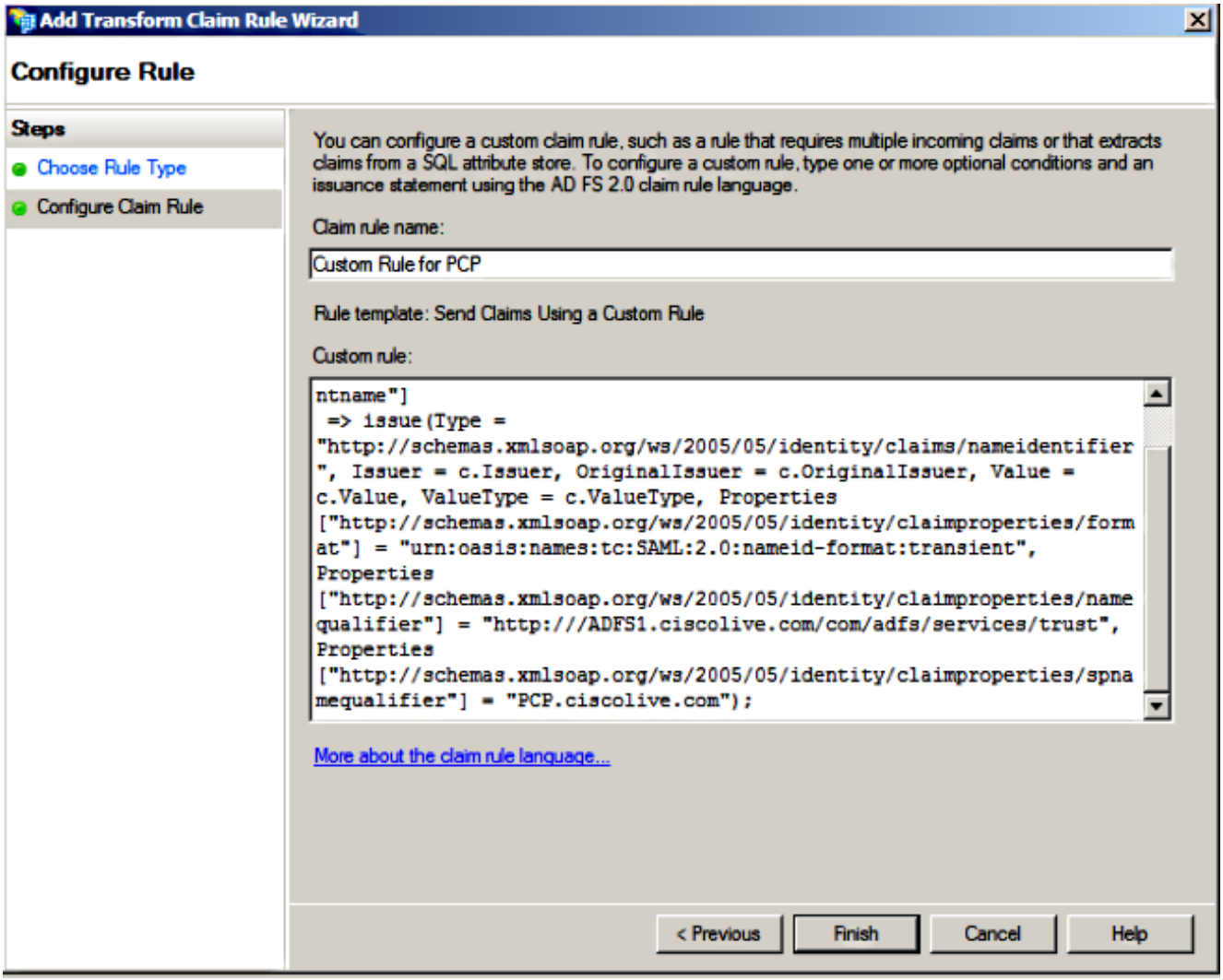
5. Starten Sie den Dienst AD FS Version 2.0 von **Services.msc** aus neu.

Hinzufügen von Cisco Prime Collaboration Provisioning als Relying Party Trust

1. Wiederholen Sie die Schritte 1 bis 12, wie für **Hinzufügen von CUCM als "Relying Party Trust"** beschrieben, und fahren Sie mit Schritt 2 fort.

2. Geben Sie einen Namen für den Namen einer Anspruchsregel ein, und kopieren Sie diese Syntax in das Feld unter Benutzerdefinierte Regel:

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of PCP>");
```



Beachten Sie, dass Prime Provisioning und AD FS FQDN in diesem Beispiel vorab mit Prime

Collaboration Provisioning (PCP) und AD FS ausgefüllt werden und entsprechend Ihrer Umgebung geändert werden müssen.

3. Klicken Sie auf **Fertig stellen**.

4. Klicken Sie auf **Übernehmen** und dann auf **OK**.

5. Starten Sie den Dienst AD FS Version 2.0 von **Services.msc** aus neu.

Sobald Sie AD FS Version 2.0 eingerichtet haben, fahren Sie mit der Aktivierung von SAML SSO für Cisco Collaboration-Produkte fort.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

AD FS protokolliert Diagnosedaten im Systemereignisprotokoll. Öffnen Sie im Server Manager des AD FS-Servers **Diagnostics -> Event Viewer -> Applications and Services -> AD FS 2.0 -> Admin.**

Fehlerprotokollierung für AD FS-Aktivität suchen