

# AD FS バージョン 2.0 でクラスタごとに単一の SAML IdP 接続/アグリーメントを設定する

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ1:CUCMからSPメタデータをエクスポートする](#)

[ステップ2:AD FSからIDPメタデータをダウンロードする](#)

[ステップ3:IdPのプロビジョニング](#)

[ステップ4:SAML SSOの有効化](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Active Directory フェデレーション サービス (AD FS) を使用して、クラスタごとにシングルセキュリティアサシオンマークアップ言語 (SAML) アイデンティティプロバイダー (IdP) 接続/アグリーメントを設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager (CUCM) 11.5 以降
- Cisco Unified Communications Manager IM and Presence バージョン 11.5 以降
- Active Directory フェデレーション サービス バージョン 2.0

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Active Directory フェデレーション サービス バージョン 2.0 (IdP)
- Cisco Unified Communications Manager バージョン 11.5
- Cisco Unified Presence サーバ バージョン 11.5

## 背景説明

SAML SSOでは、サービスプロバイダー(SP)とIdPの間の信頼の輪である必要があります。この信頼は、信頼(メタデータ)が交換されるときに、SSOイネーブルメントの一部として作成されます。CUCMからメタデータをダウンロードしてIdPにアップロードします。同様に、IdPからメタデータをダウンロードしてCUCMにアップロードします。

以前のCUCM 11.5では、発信元ノードがメタデータファイルを生成し、クラスタ内の他のノードからメタデータファイルを収集します。すべてのメタデータファイルを1つのzipファイルに追加し、管理者に提示します。管理者はこのファイルを解凍し、IdP上の各ファイルをプロビジョニングする必要があります。たとえば、8ノードクラスタの8個のメタデータファイルです。

クラスタ機能ごとの単一SAML IdP接続/アグリーメントは、11.5から導入されました。この機能の一部として、CUCMは、クラスタ内のすべてのCUCMおよびIMPノードに対して単一のサービスプロバイダーメタデータファイルを生成します。メタデータファイルの新しい名前形式は `<hostname>-single-agreement.xml` です

基本的に、1つのノードがメタデータを作成し、クラスタ内の他のSPノードにプッシュします。これにより、プロビジョニング、メンテナンス、管理が容易になります。たとえば、8ノードクラスタに対して1つのメタデータファイルがあります。

クラスタ全体のメタデータファイルは、クラスタ内のすべてのノードでキーペアが確実に使用されるマルチサーバtomcat証明書を使用します。メタデータファイルには、クラスタ内の各ノードのアサーションコンシューマサービス(ACS)URLのリストもあります。

CUCMおよびCisco IM and Presenceバージョン11.5クラスタ全体(クラスタごとに1つのメタデータファイル)とノードごと(既存のモデル)の両方をサポートします。

このドキュメントでは、AD FS 2.0を使用してSAML SSOのクラスタ全体モードを設定する方法について説明します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

### ステップ1:CUCMからSPメタデータをエクスポートする

Webブラウザを開き、管理者としてCUCMにログインし、[System] > [SAML Single Sign On]に移動します。

デフォルトでは、[クラスタワイド]オプションボタンが選択されています。[すべてのメタデータをエクスポート]をクリックします。管理者に`<hostname>-single-agreement.xml`という名前で提示されるメタデータファイル

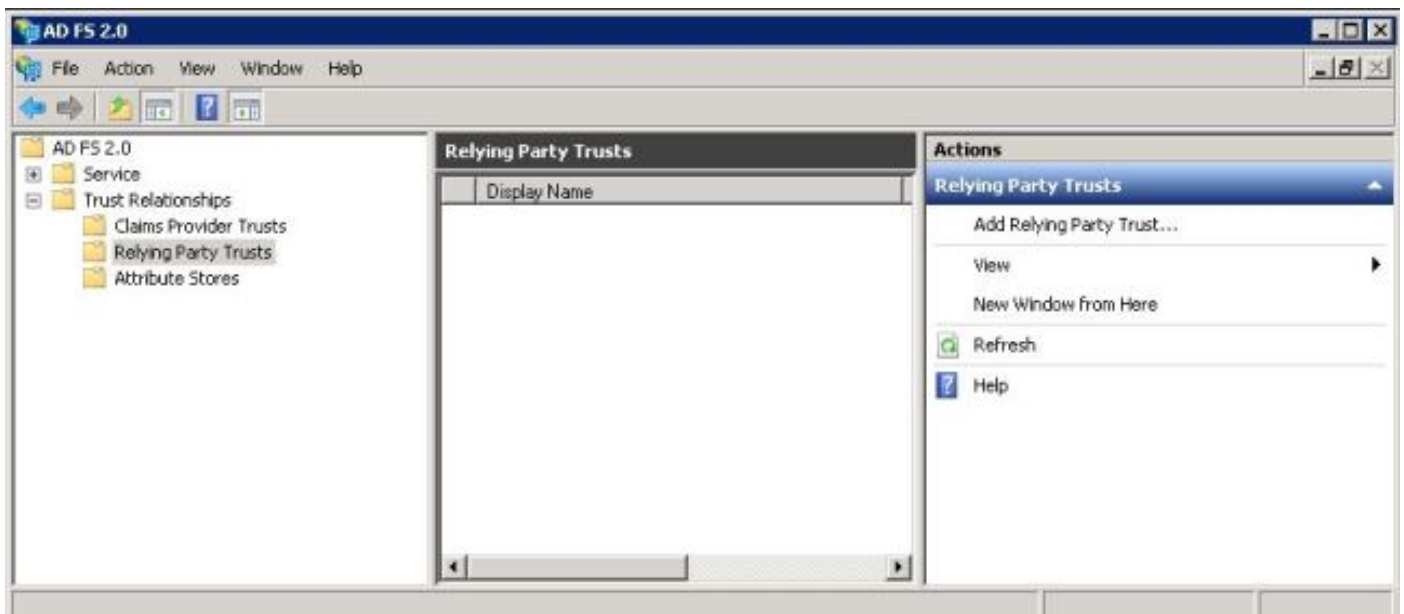


## ステップ2:AD FSからIDPメタデータをダウンロードする

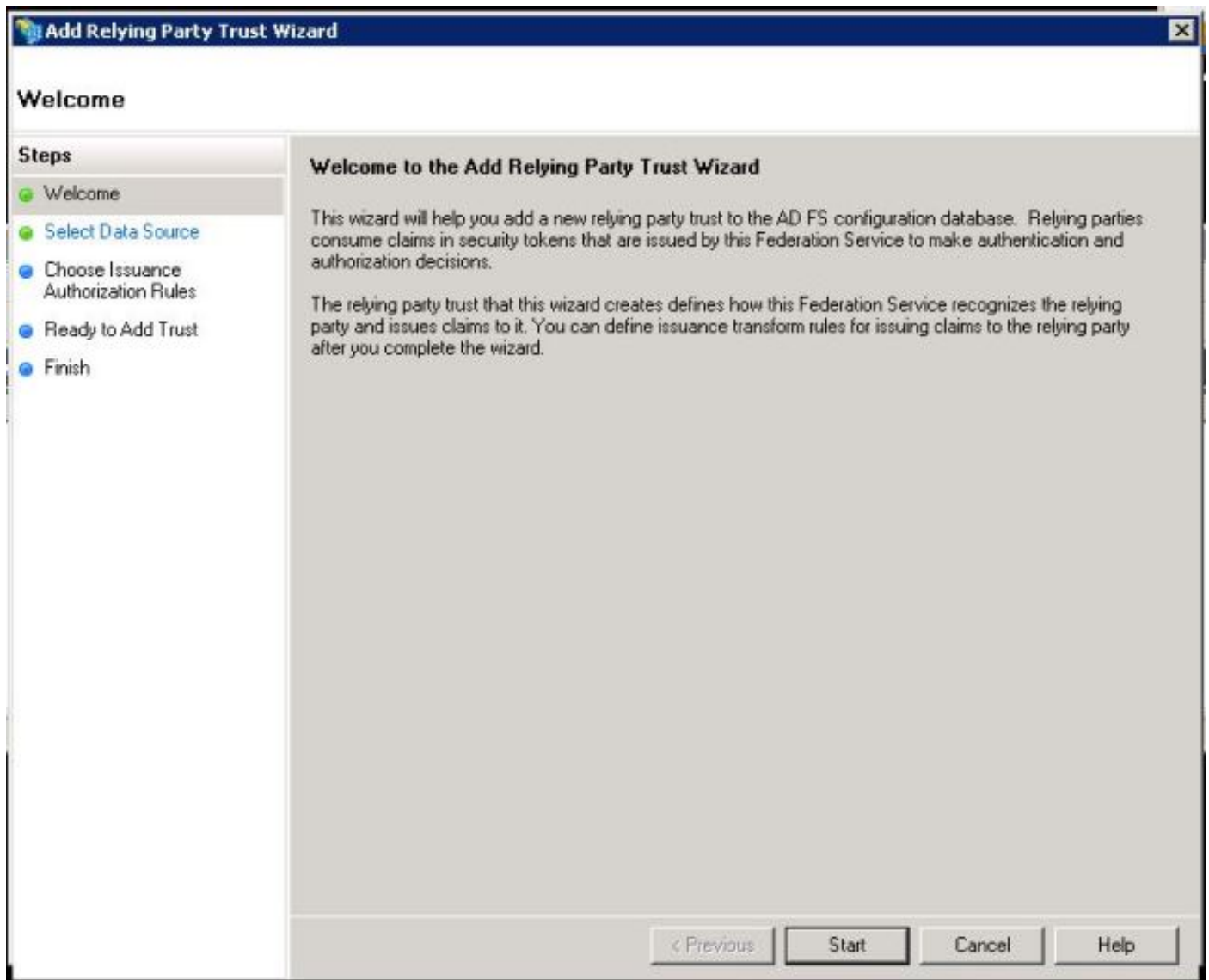
IdPメタデータをダウンロードするには、リンク[https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml](https://<FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml)

## ステップ3:IdPのプロビジョニング

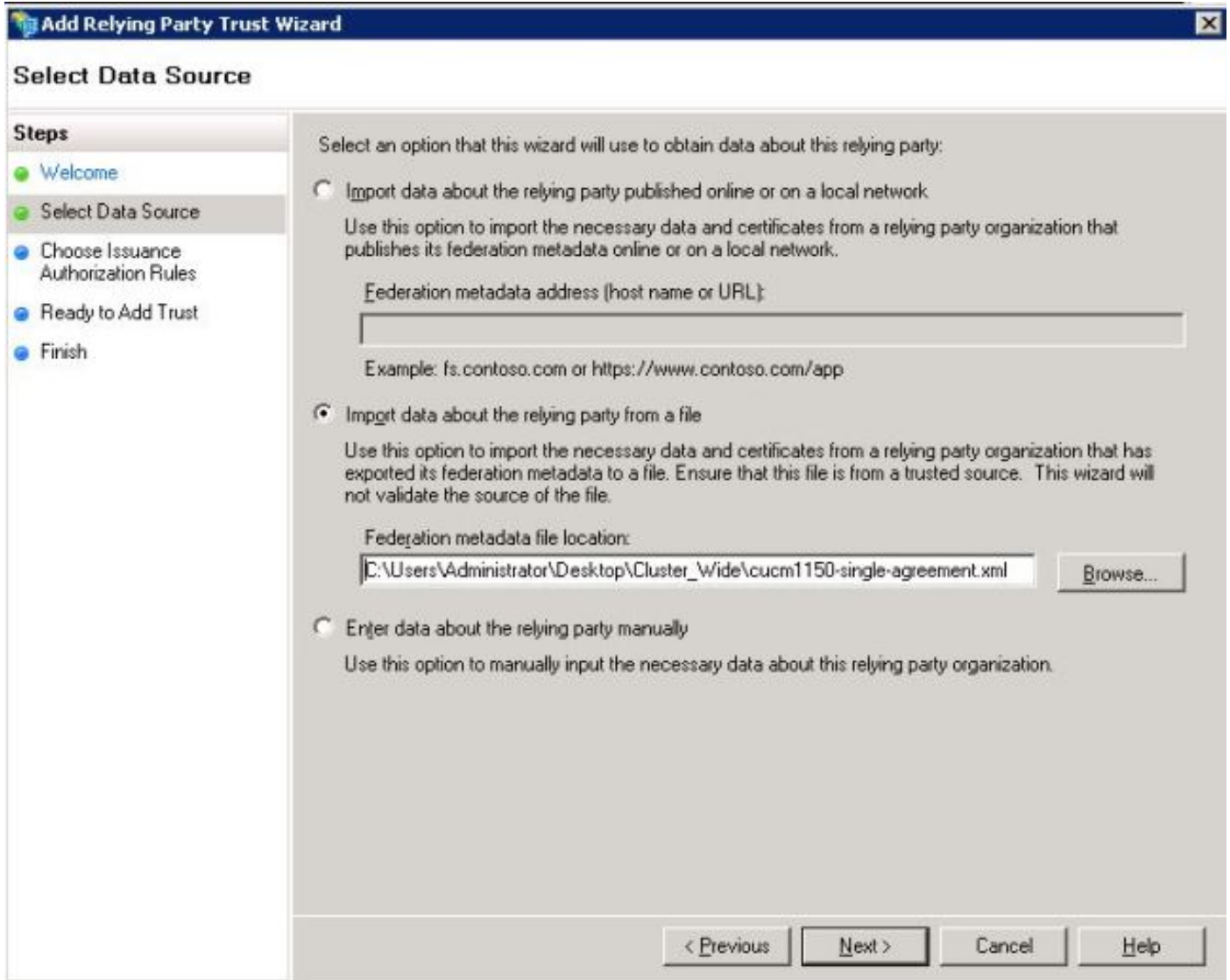
図に示すように、[AD FS 2.0 Management/Trust Relation Ships/Relying Party trust]に移動します。  
[Add Relying Party Trust]をクリックします。



図に示すように、[Add Relying Party Trust Wizard]が開き、[Start]をクリックします。



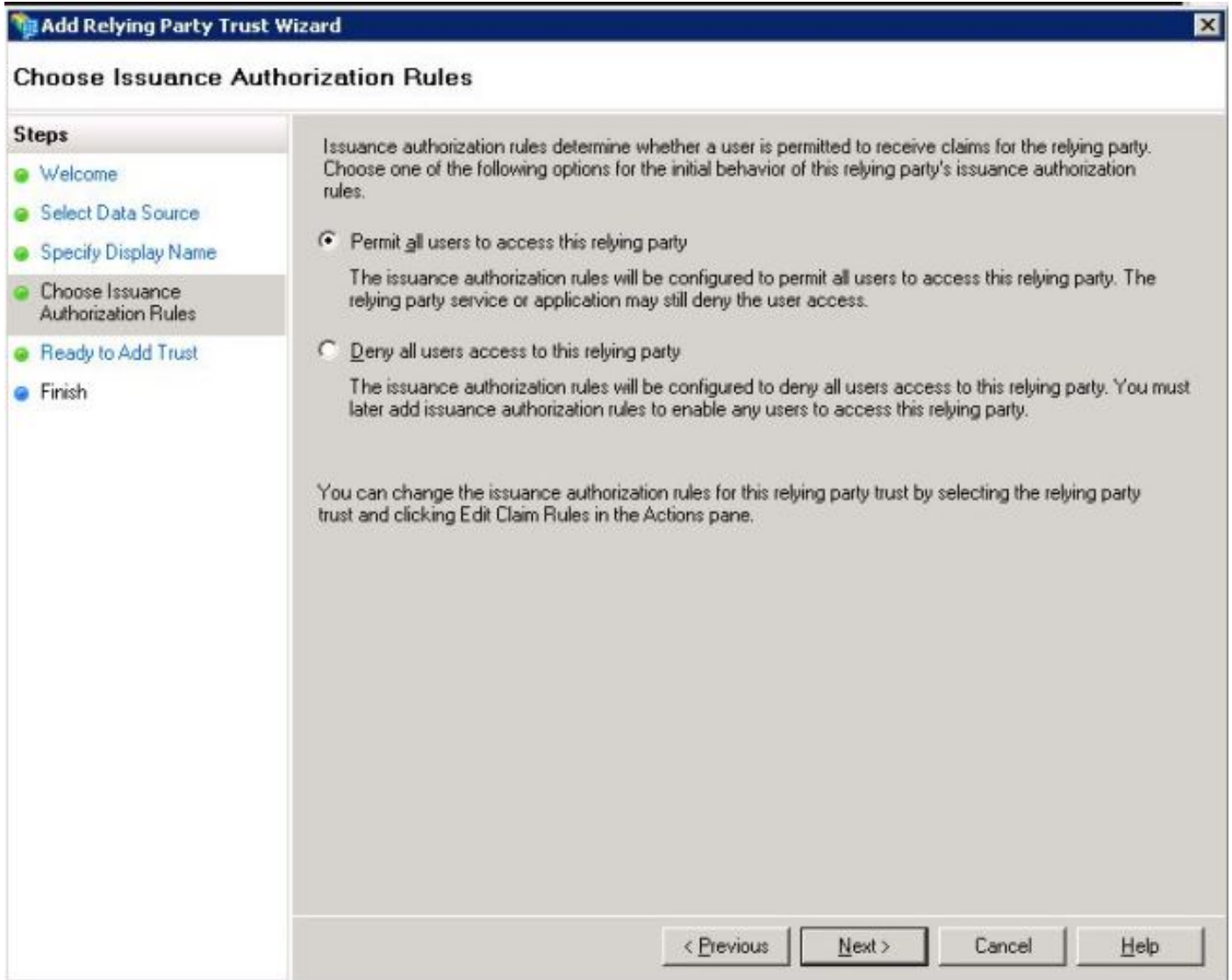
証明書利用者に関するインポートデータをファイルからクリックします。CUCM SAML SSO設定ページからダウンロードしたSPメタデータを参照します。次に、図に示すように[Next]をクリックします。



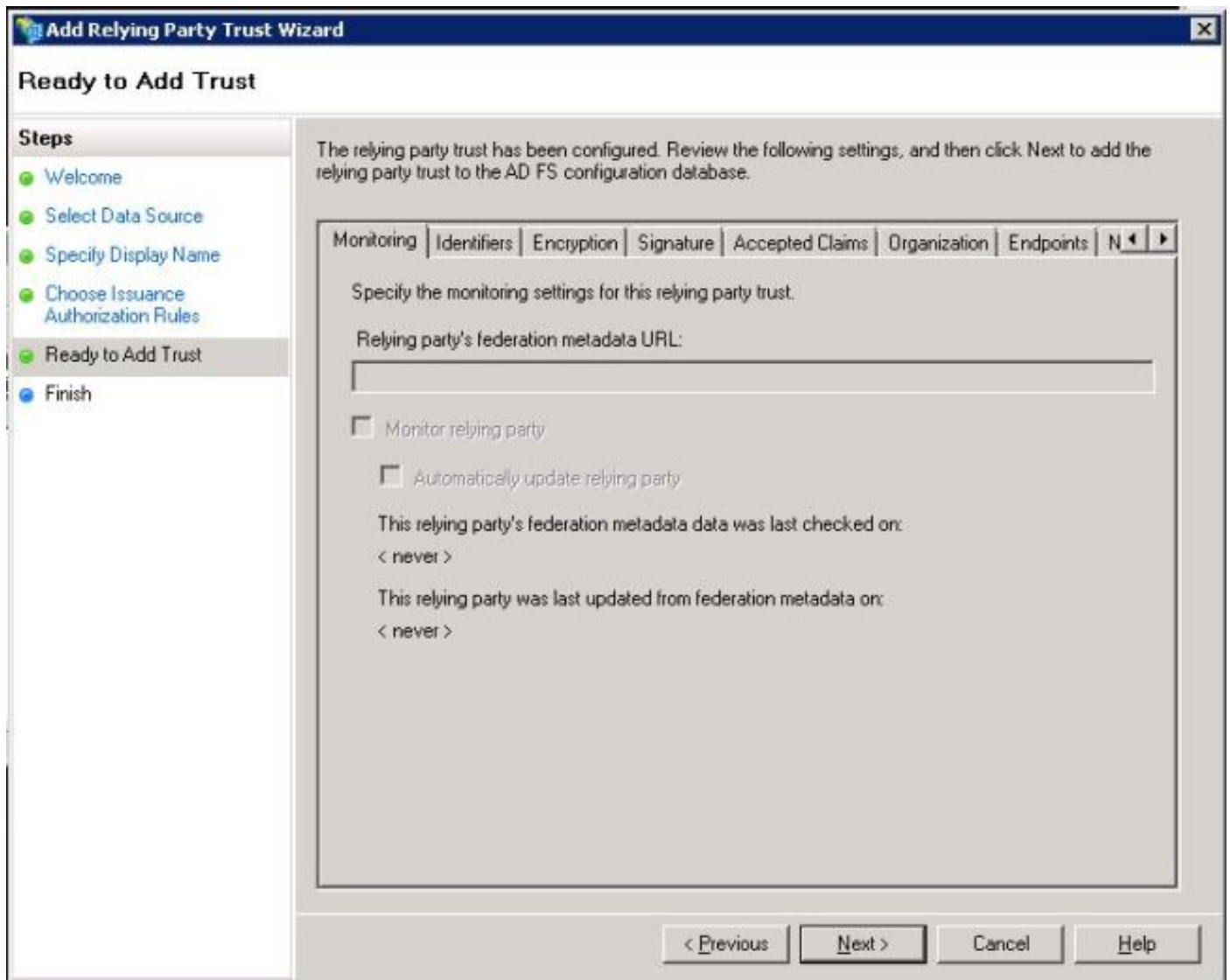
証明書利用者の[Display Name]とオプションのメモを入力します。図に示すように、[Next]をクリックします。

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". The main title bar includes a close button (X). The dialog is divided into two main sections. On the left is a "Steps" pane with a list of steps: "Welcome", "Select Data Source", "Specify Display Name" (which is highlighted in grey), "Choose Issuance Authorization Rules", "Ready to Add Trust", and "Finish". The main area on the right contains the text "Type the display name and any optional notes for this relying party." Below this text is a "Display name:" label followed by a text input field containing the text "CUCM\_Cluster\_Wide\_Relying\_Party\_trust". Below the input field is a "Notes:" label followed by a large, empty text area with a vertical scrollbar. At the bottom right of the dialog, there are four buttons: "< Previous", "Next >", "Cancel", and "Help".

[Permit all users to access this relying party]を選択して、すべてのユーザがこの証明書利用者にアクセスできるようにして、図に示すように[Next]をクリックします。

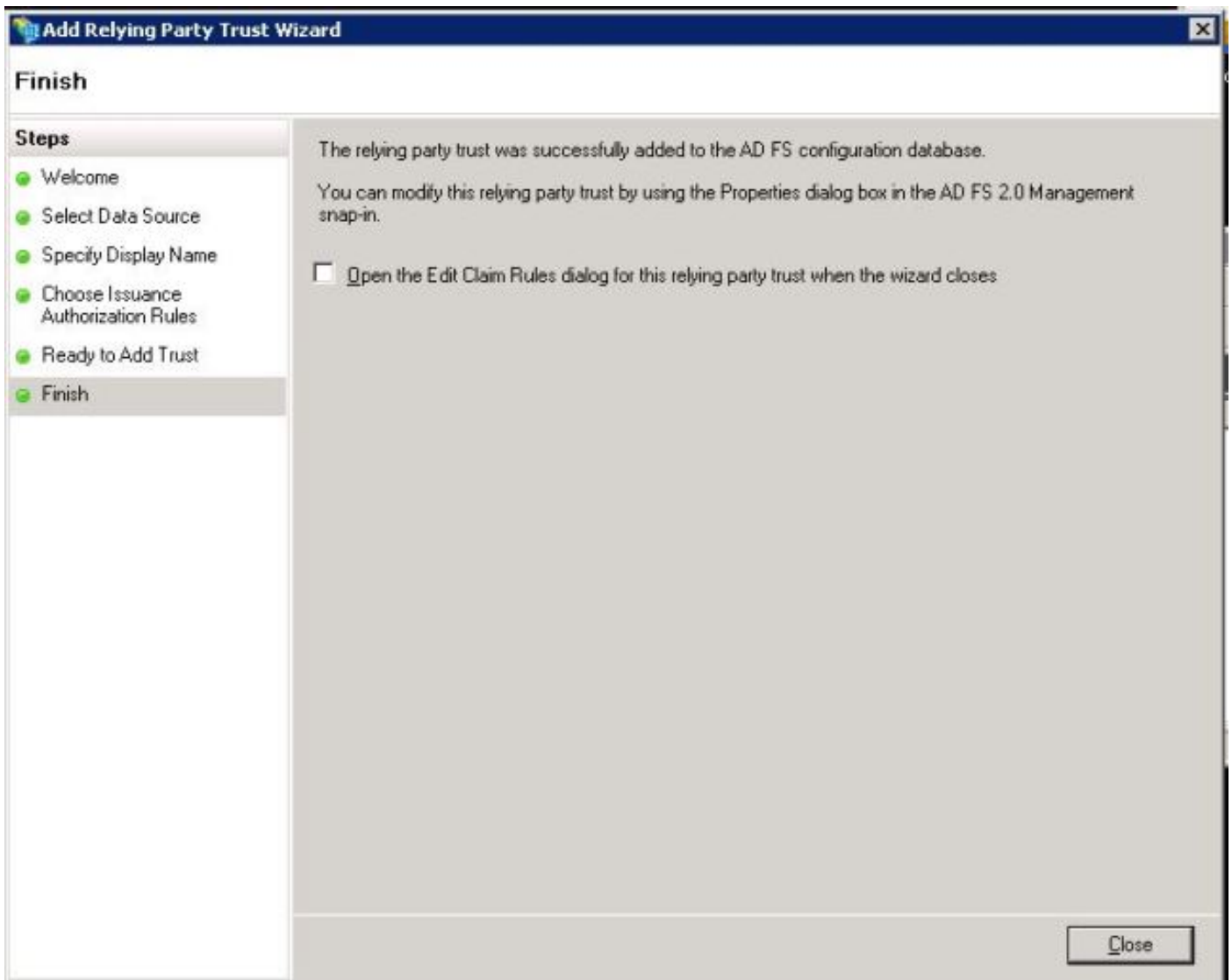


[Ready to Add Trust] ページで、設定されている証明書利用者信頼の設定を確認できます。次に、図に示すように[Next]をクリックします。

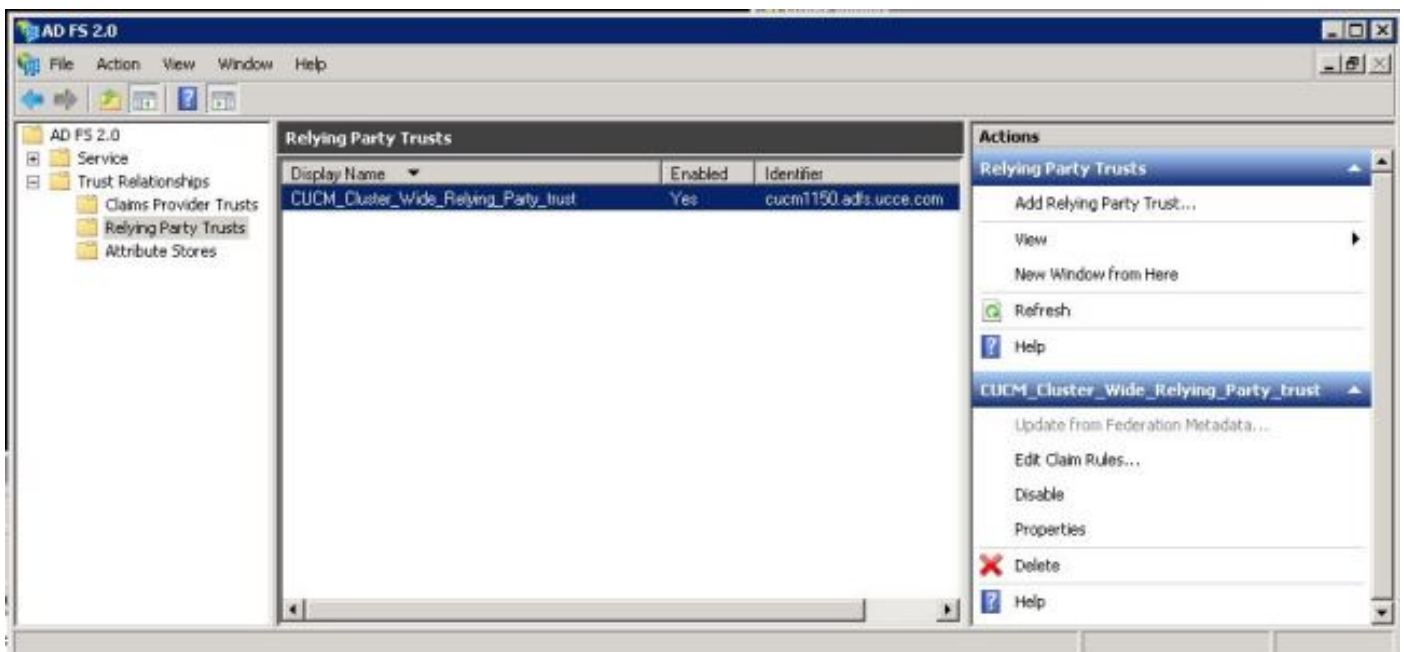


[完了]ページで、証明書利用者信頼がAD FS構成データベースに正常に追加されたことを確認します。図に示すように、[Box]のチェックマークを外し、[Close]をクリックします。

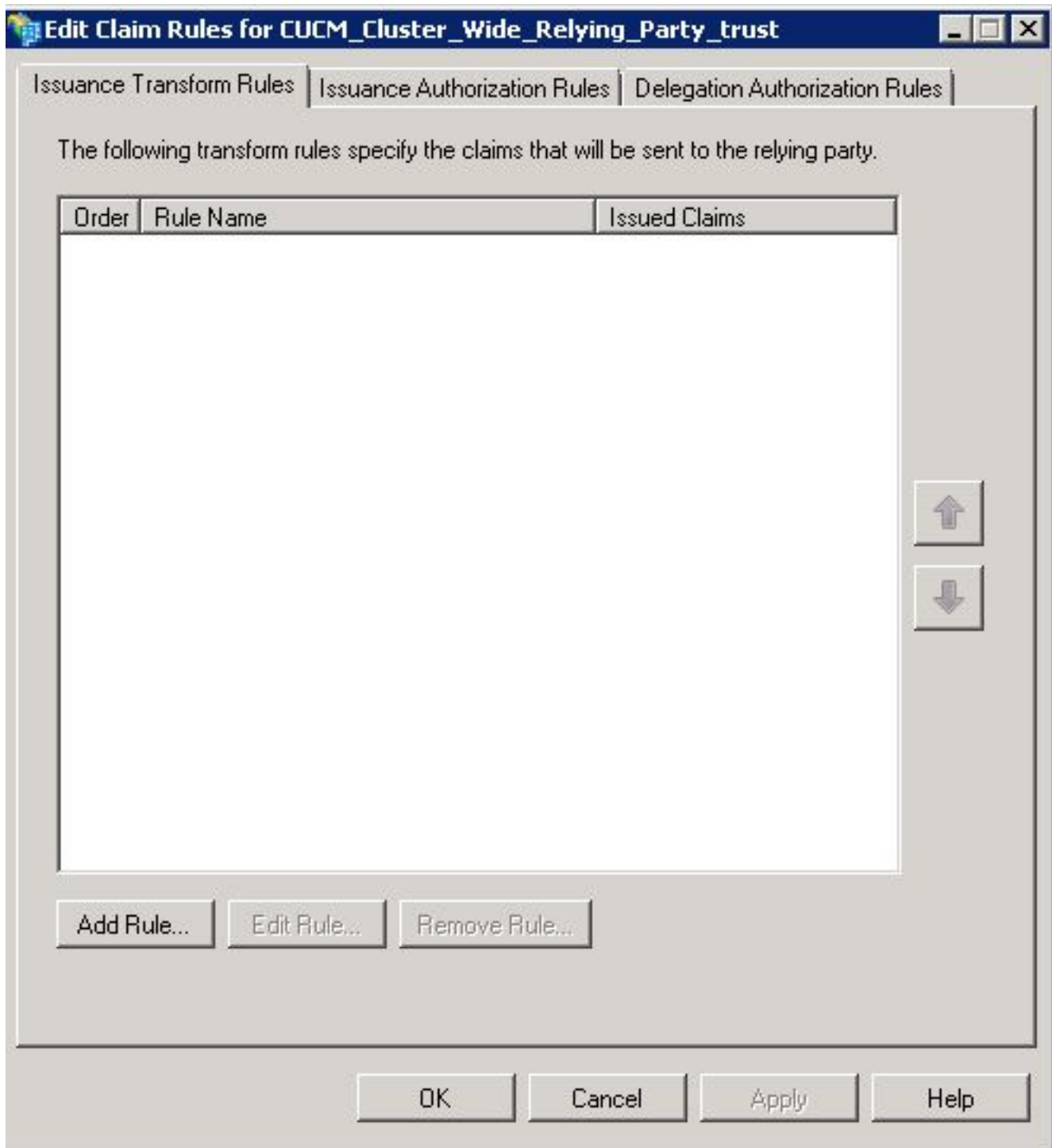




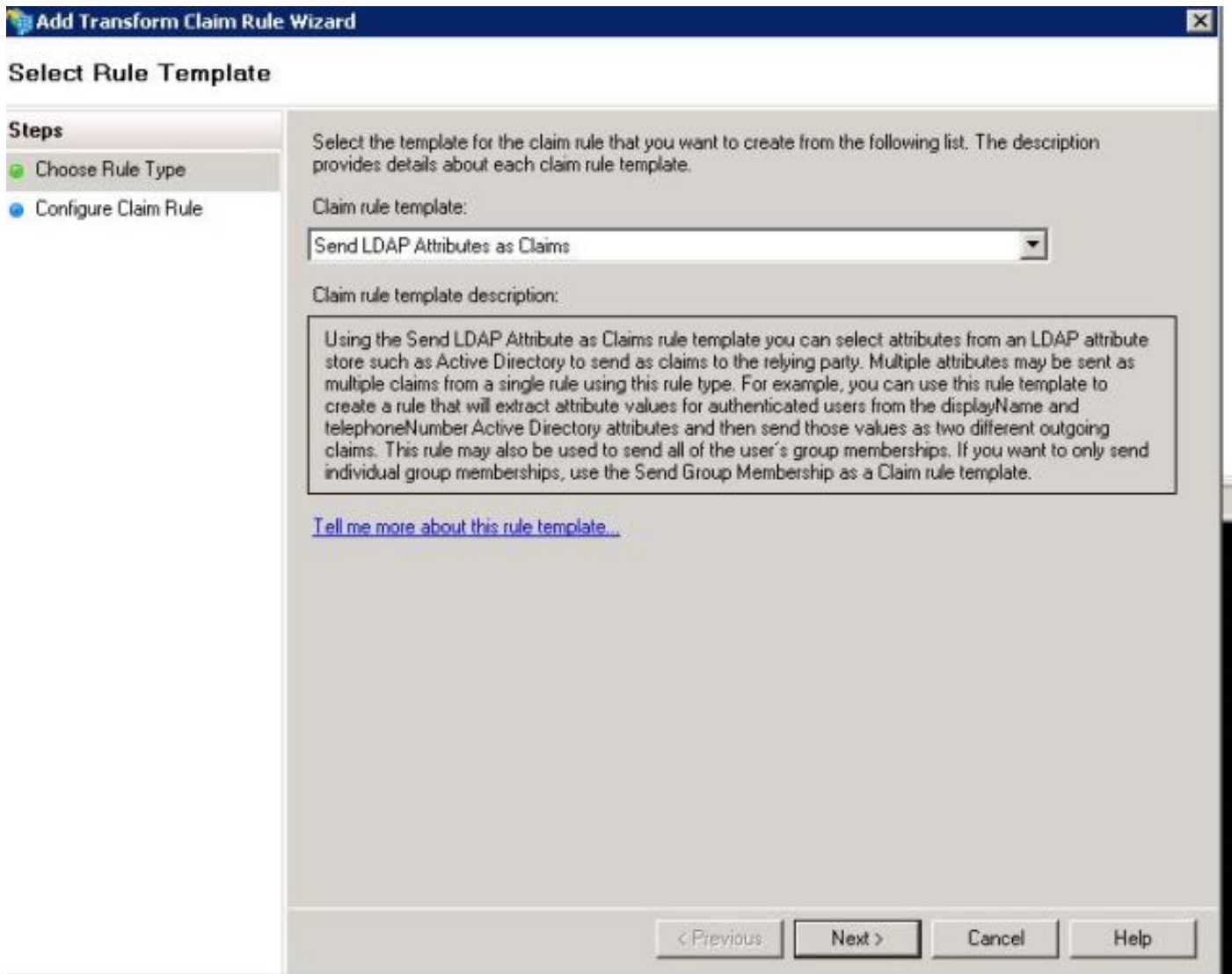
図に示すように、[Relying Party Trusts]を右クリックして[Edit Claim Rules]をクリックします。



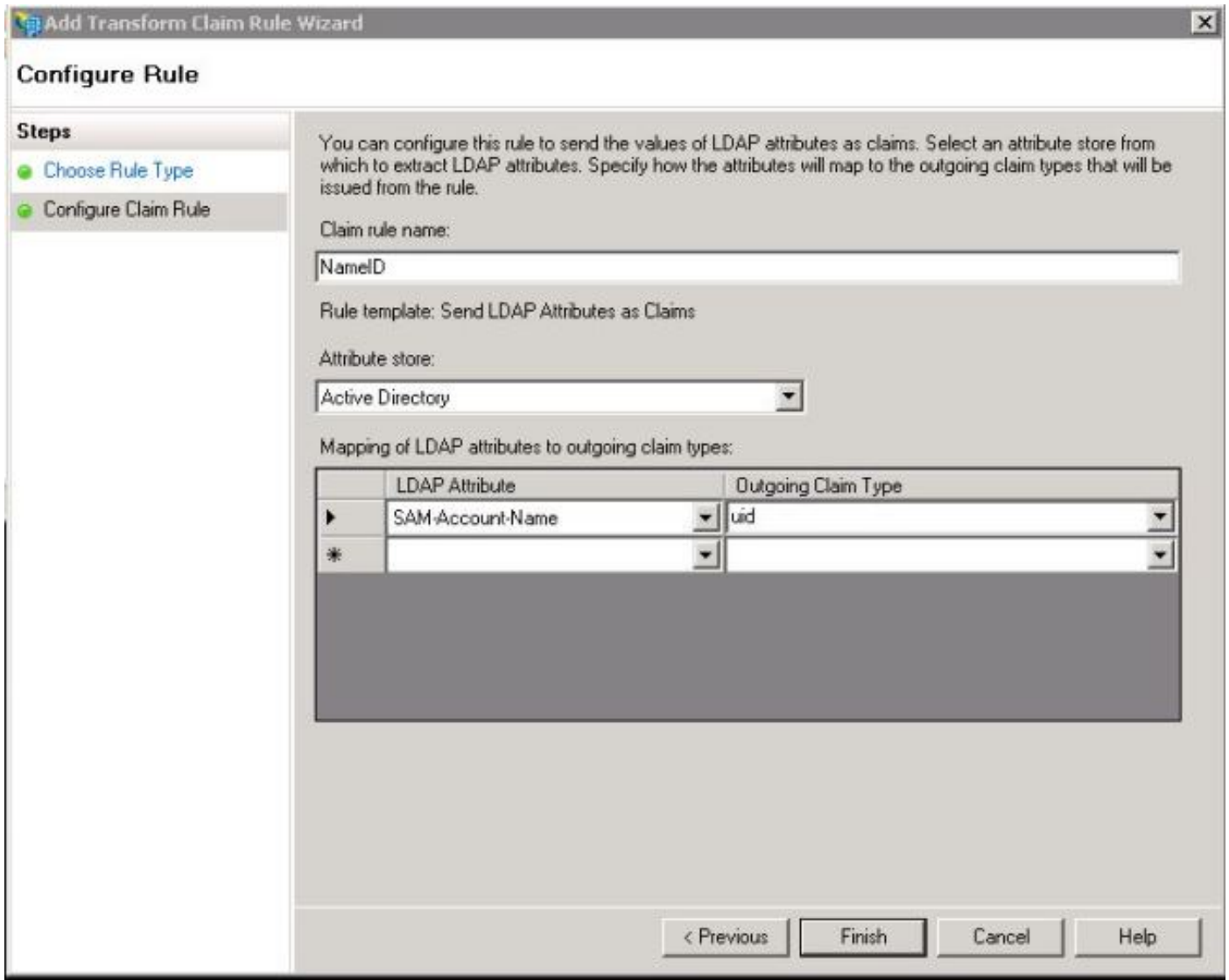
次に、図に示すように[Add Rule]をクリックします。



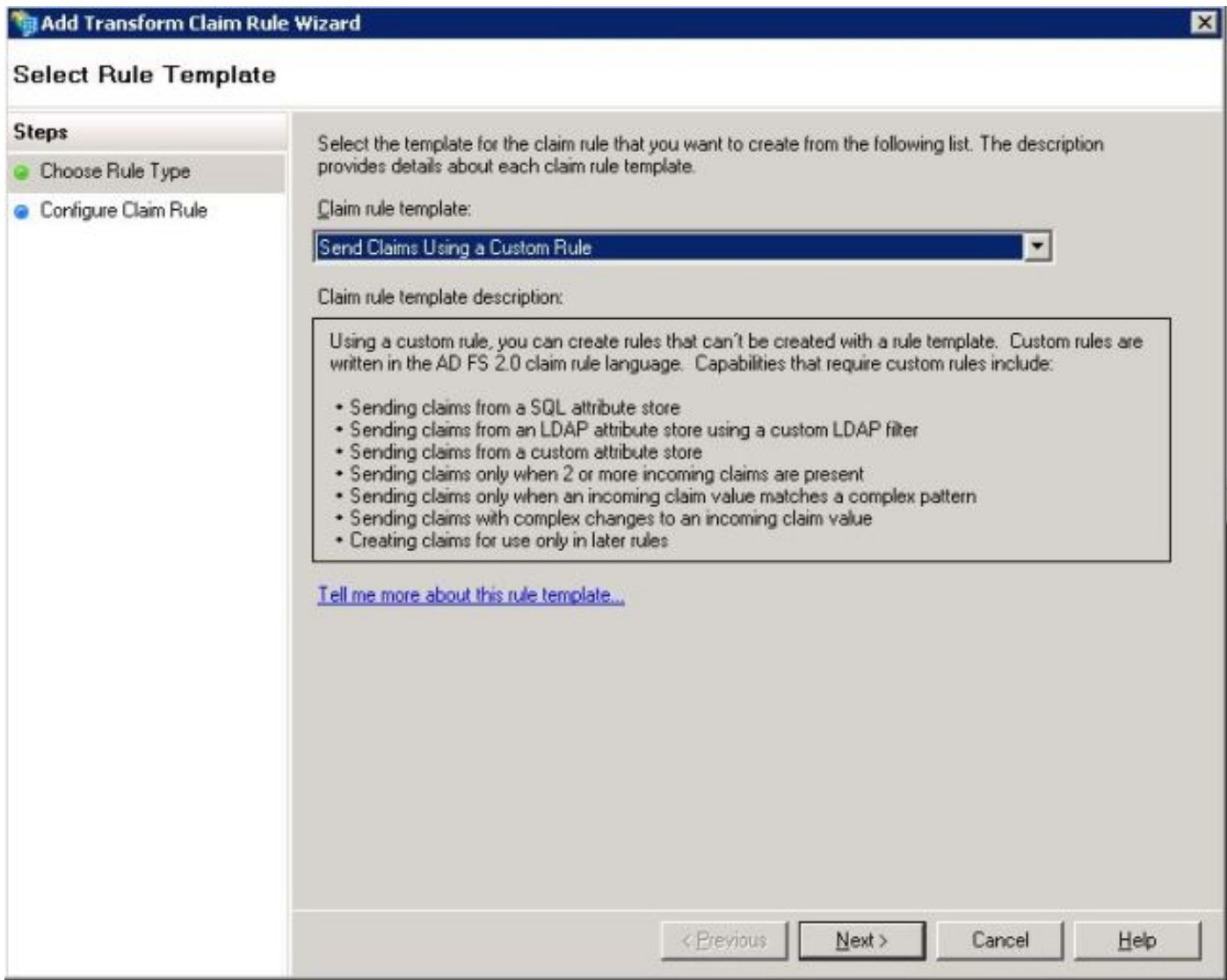
[Add Transform Claim Rule]が開いたら、図に示すように、デフォルトのクレームルールテンプレート[Send LDAP Attributes as Claims]をクリックします。



次の図に示すように、[Configure Claim Rule]をクリックします。LDAP属性は、CUCMのLDAPディレクトリ設定のLDAP属性と一致している必要があります。送信要求の種類をuidとして管理します。図に示すように[Finish]をクリックします。



証明書利用者のカスタムルールを追加します。[Add Rule] をクリックします。図に示すように、[カスタム規則を使用して要求を送信]を選択し、[次へ]をクリックします。

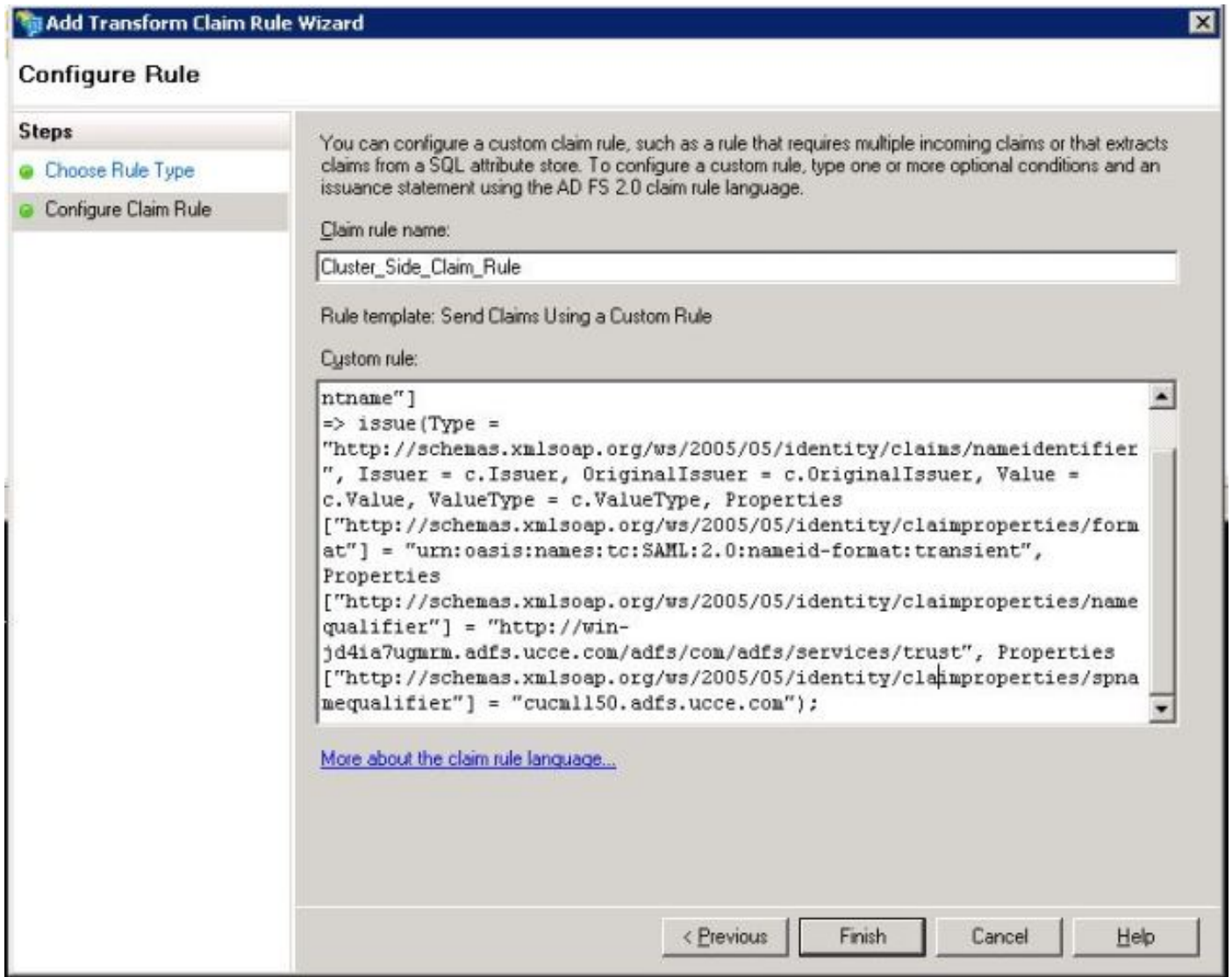


[要求ルールの構成]で、[要求ルール名]を入力し、ウィザードの[カスタムルール]フィールドに指定された過去の要求ルールをコピーします。その後、要求ルールの名前修飾子とspname修飾子を変更します。図に示すように[Finish]をクリックします。

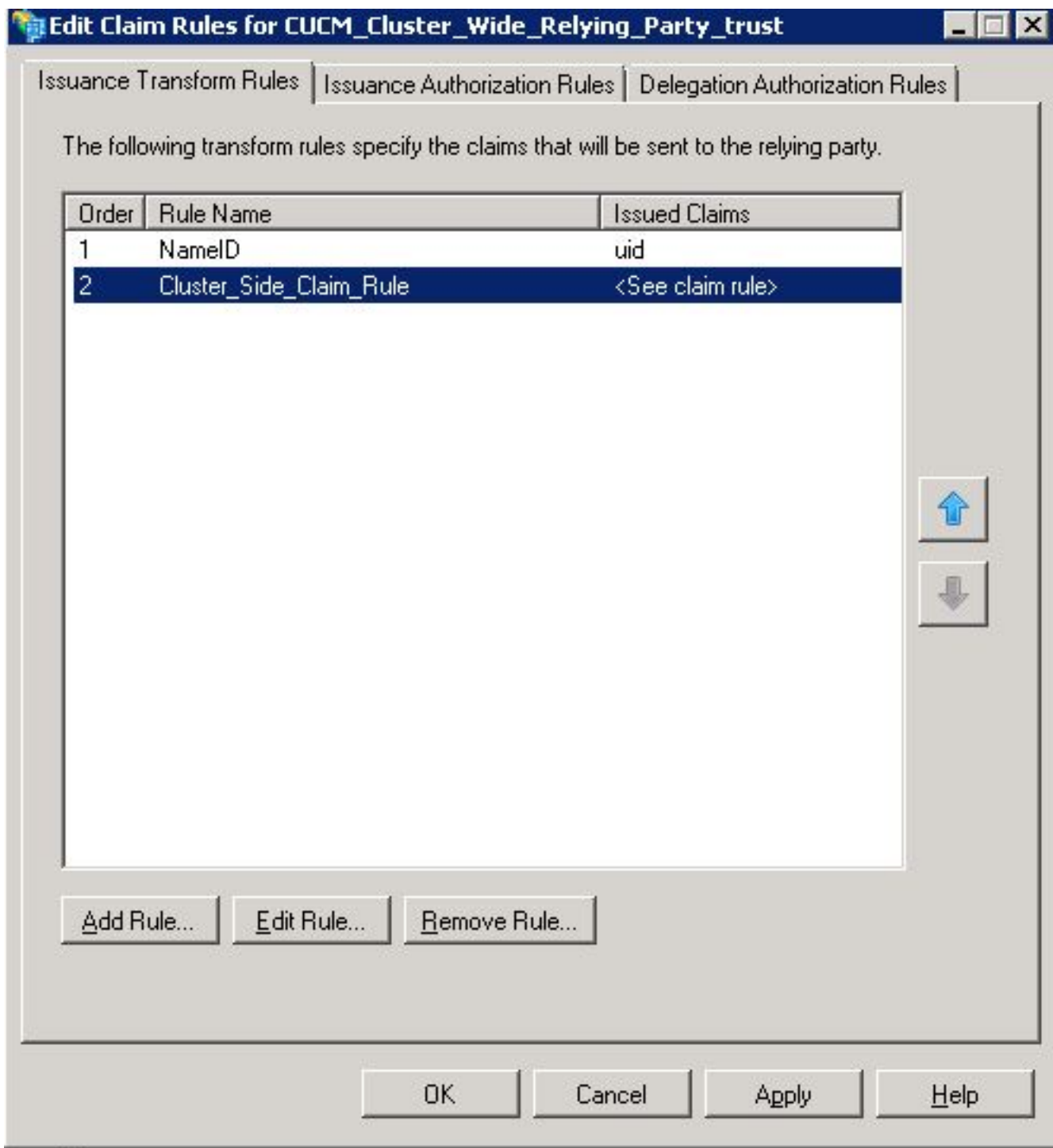
### クレームルール：

```
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.



図に示すように、[適用]をクリックして、[OK]をクリックします。



## ステップ4:SAML SSOの有効化

Webブラウザを開き、管理者としてCUCMにログインし、[System] > [SAML Single Sign On]に移動します。

デフォルトでは、[クラスタワイド]オプションボタンが選択されています。図に示すように[Enable Saml SSO]をクリックします。

## 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

図に示すように、ポップアップはWebサーバの再起動に関する警告と、idpに応じてクラスタ全体のSAML SSOまたはノードごとのSAML SSOを選択するための情報を通知します。[Continue] をクリックします。

 **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.


クラスタ全体のSSOを有効にする基準は、マルチサーバのtomcat証明書がすでに配備されている必要があることです。図に示すように、[Test for Multi-Server tomcat Certificate]をクリックします。



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


確認が完了したら、すべてのノードにマルチサーバ証明書が表示され、[すべてのノードにマルチサーバ証明書があります]と表示され、[次へ]をクリックします（図を参照）。

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:

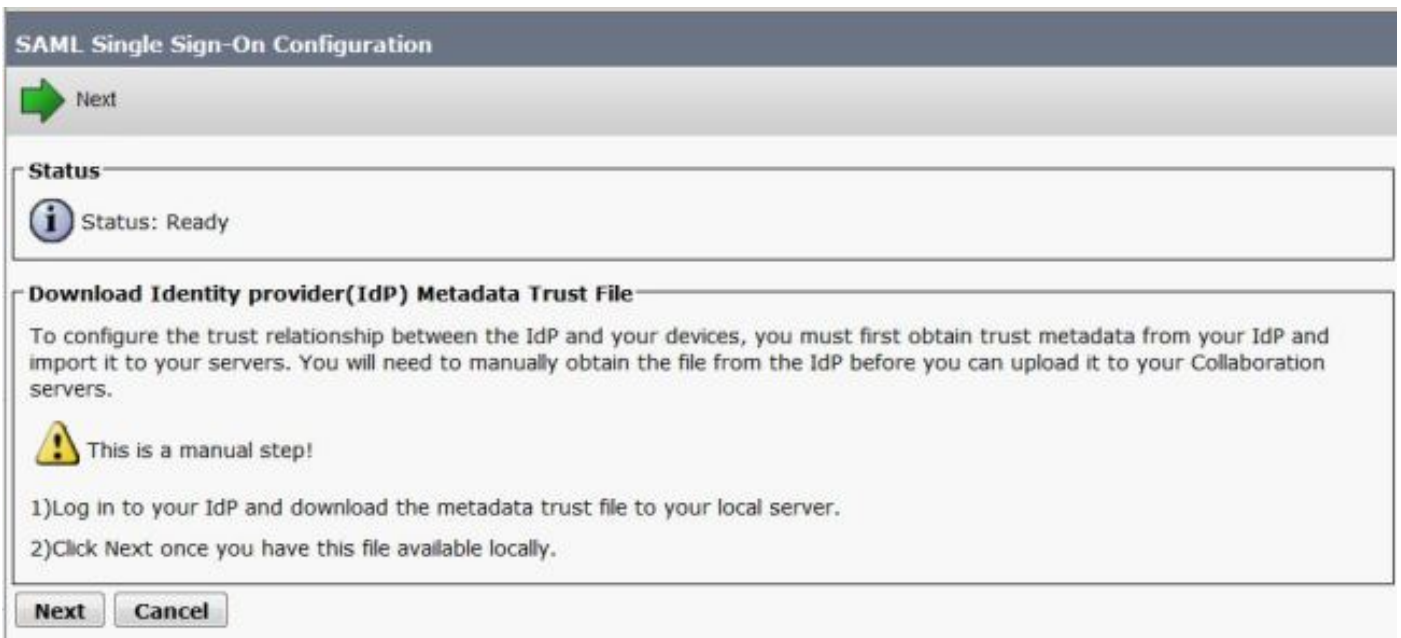
- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your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

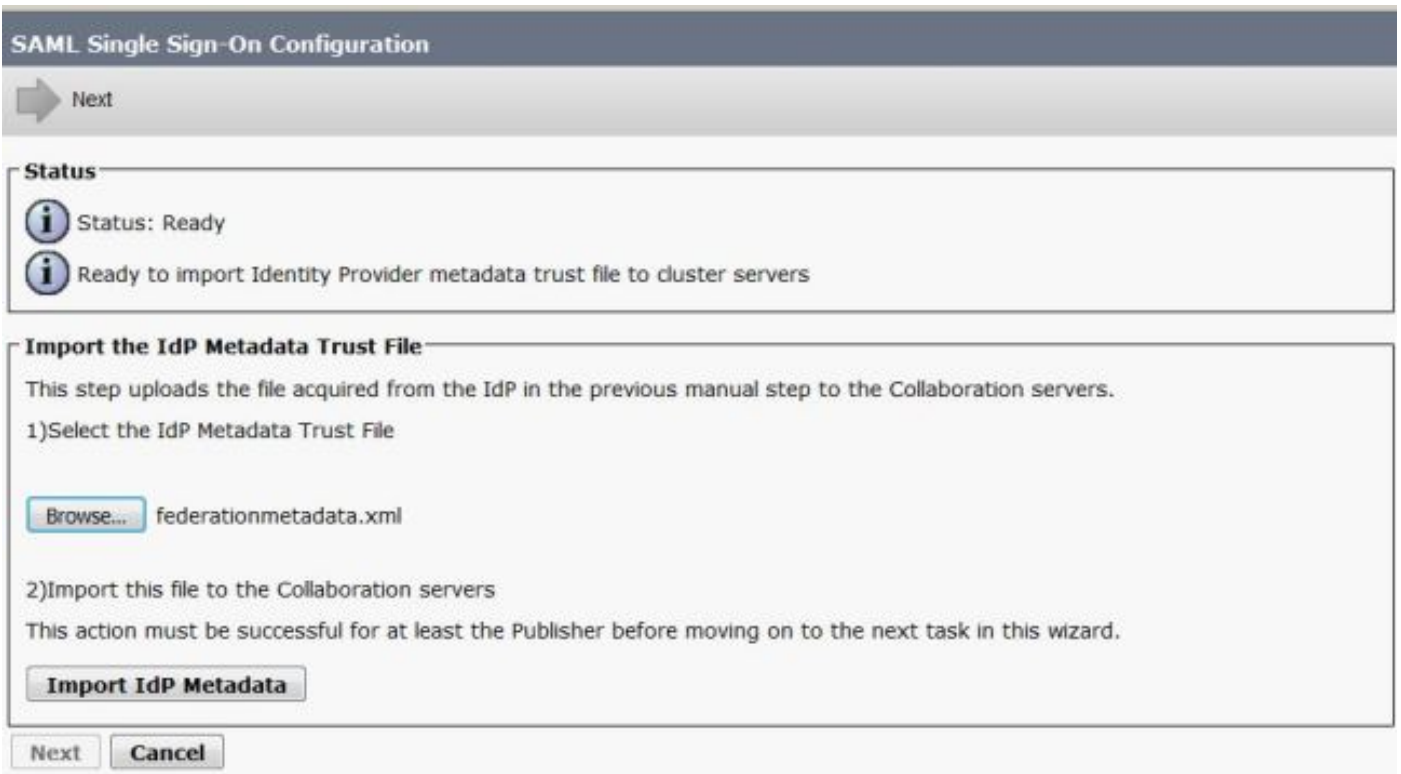
**Test for Multi-Server tomcat certificate**

Next Cancel

図に示すように、[次へ]をクリックします。




ダウンロードしたIdPメタデータを参照して選択します。図に示すように[Import IdP Metadata]をクリックします。





次の図に示すように、ページで[Import succeeded for all servers]が確認され、[Next]をクリックします。

**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

図に示すように、[Next] をクリックします。これは、初期SAML SSO設定ページからSPメタデータがすでにエクスポートされているためです。

**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はLDAPディレクトリと同期している必要があります。ウィザードには、LDAPディレクトリで設定されている有効な管理者ユーザが表示されます。図に示すように、ユーザを選択し、[Run SSO Test]をクリックします。

**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.

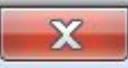
 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.


Valid administrator Usernames

samluser

2) Launch SSO test page

図に示すように、プロンプトが表示されたら、ユーザIDとそれぞれのパスワードを入力します。

**Authentication Required** 

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

User Name:

Password:


図に示すように、ポップアップはテストが成功したことを示します。

# 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

図に示すように、[Finish]をクリックして、SSOを有効にするための設定を完了します。



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

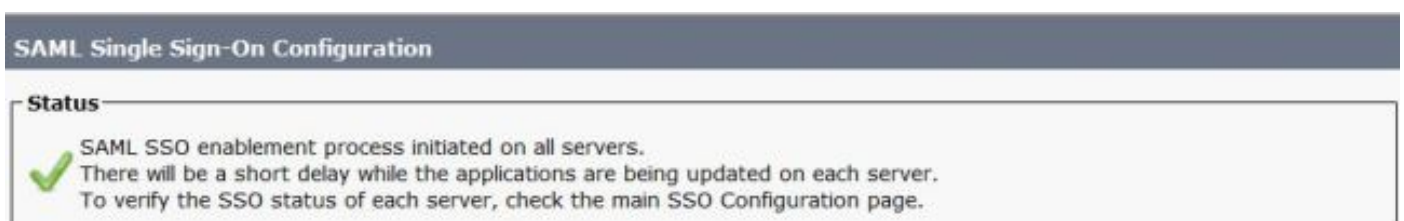
**Ready to Enable SSO**

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

図に示すページは、すべてのサーバでSAML SSOの有効化プロセスが開始されていることを示しています。



### 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.

ログアウトし、SAML SSOクレデンシャルを使用してCUCMに再度ログインします。[システム (System)] > [SAMLシングルサインオン(SAML Single Sign On)]に移動します。図に示すように、クラスタ内の他のノードに対して[SSOテストの実行(Run SSO Test)]をクリックします。

**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	

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

SAML SSOが有効になっているノードのSSOテストが成功したことを確認します。[System] > [SAML Single Sign On]に移動します。成功したSSOテストのステータスは[Passed]です。

**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	

SAML SSOがアクティブになると、次の図に示すように、CUCMログインページの[Installed Applications]および[Platform Applications]が表示されます。

## 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

SAML SSOがアクティブになると、次の図に示すように、IM and Presenceログインページの [Installed Applications and Platform Applications] がリストされます。

## 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

# トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

デバッグするSSOログを設定するには、コマンド**set samltrace level DEBUG**を使用します

RTMTを使用するか、CLIを使用して**activelog /tomcat/logs/ssosp/log4j/\*.log**の場所からSSOログを収集します。

SSOログの例は、生成されたメタデータと他のノードへの送信を示します

```
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 [cucml150, cucml150sub.adfs.uce.com]
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucml150
2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucml150sub.adfs.uce.com
```