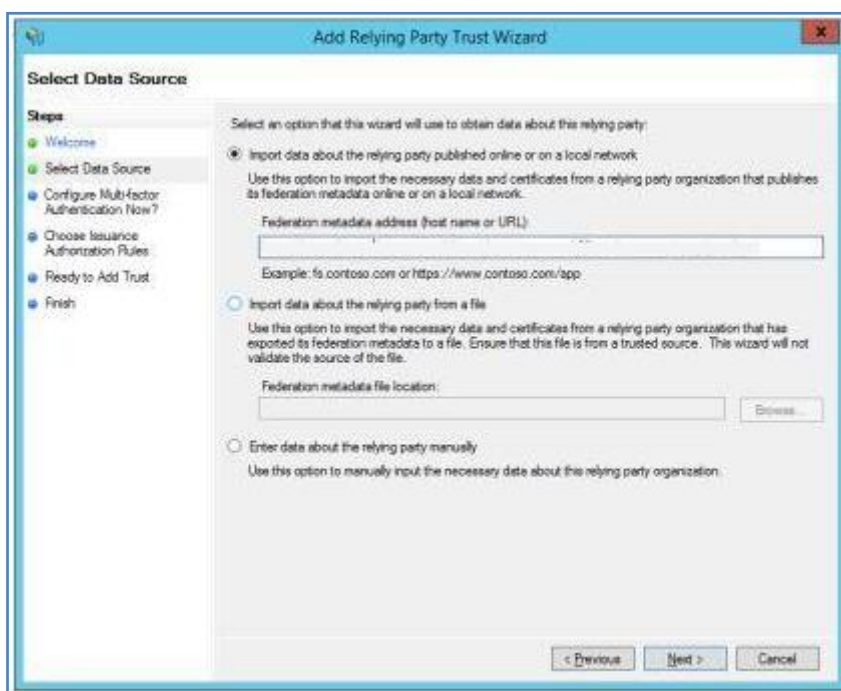


## SETUP GUIDE FOR ADFS AS IdP

**STEP 1:** In ADFS, click on **Add Relying party Trust**. Then click on **Start**.

**STEP 2:** In Select Data Source: Select **Import data about the relying party published online or on a local network** and enter the metadata URL provided in the Configure IDP tab of the plugin. Click **Next**.



**STEP 3:** In Specify Display name: Enter **Display name**. Click Next.

**STEP 4:** In Configure Multi-factor Authentication Now, select **I do not want to configure multi factor authentication settings for this relying party trust**. Click **Next**.

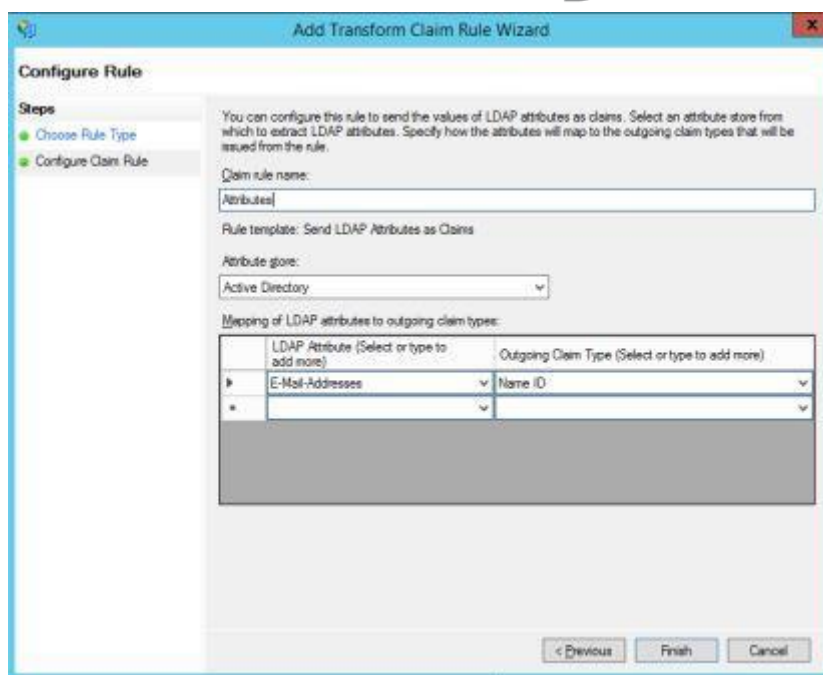
**STEP 5:** In Choose Issuance Authorization Rules, select **Permit all users to access this relying party**. Click **Next**.

**STEP 6:** In Ready to Add Trusts, select click **Next**.

**STEP 7:** Check **Open the Edit Claim Rules dialog** and click close. Click **Add rule** and then select **Send LDAP Attributes as Claims**. Enter the following:

- Claim rule name: **Attributes**
- Attribute Store: **Active Directory**
- LDAP Attribute: **E-Mail-Addresses**
- Outgoing Claim Type: **Name ID**

Click **Finish**.



## **STEP 8:**

In miniOrange SAML plugin, go to **Configure SP** Tab. Enter the following values:

- **IDP Entity ID:** http://<your\_ADFS\_domain>/adfs/services/trust
- **Single Sign On URL:** https://<your\_ADFS\_domain>/adfs/ls
- **Single Logout URL:** https://<your\_ADFS\_domain>/adfs/ls
- **X.509 Certificate:** Paste the certificate value you copied from the ADFS Metadata file.

## **STEP 9:**

In miniOrange SAML plugin, go to **Attribute Mapping** tab. Enter the following values:

- **Username:** Name of the username attribute from IDP (Keep NameID by default)
- **Email:** Name of the email attribute from IDP (Keep NameID by default)
- **FirstName:** Name of the firstname attribute from IDP
- **LastName:** Name of the lastname attribute from IDP

## Attribute Mapping

Username: \*

Enter the Attribute Name that contains Confluence Username. Use *NameID* if Username is in Subject element.

Email: \*

Enter the Attribute Name that contains Email. Use *NameID* if Email is in Subject element.

Full Name Attribute:

Enter the Attribute Name that contains Full Name.

Separate Name  
Attributes:☐ (Select this if your IDP is sending First name and Last name as separate attributes.)

First Name:

Enter the Attribute Name that contains First Name.

Last Name:

Enter the Attribute Name that contains Last Name.

**STEP 10:**

Go to **Role Mapping** tab. Enter the following values:

- **Role Mapping:** Name of the Role attribute from IDP

You can check the **Test Configuration Results** to get a better idea as to which values to map here.

Under the Role Mapping Section configure which GROUP value coming in the SAML response needs to be mapped to which role. The Group value coming in the SAML response will be mapped to the Role assigned here and the user will be assigned that role.

## Role Mapping

Role Attribute:

Enter the Attribute Name that contains Roles of the User.

Create Users: ☐ If checked, Users will be created only if roles are mapped.

Default Group:

Select Default Group to assign to new Users.

confluence-administrators:

confluence-users:

**Note:** Enter semi-colon separated list of role values in the textbox.

Save

### STEP 11:

Go to **Sign In Settings** tab. Enable auto-redirect to IDP using **Disable Confluence login** option.

## Sign In Settings

Login Button Text:

Disable Confluence login: ☒

Enable backdoor: ☒ Use `http://localhost:8091/login.action?saml_sso=false`  
For administrative tasks use `http://localhost:8091/authenticate.action?saml_sso=false`

Save