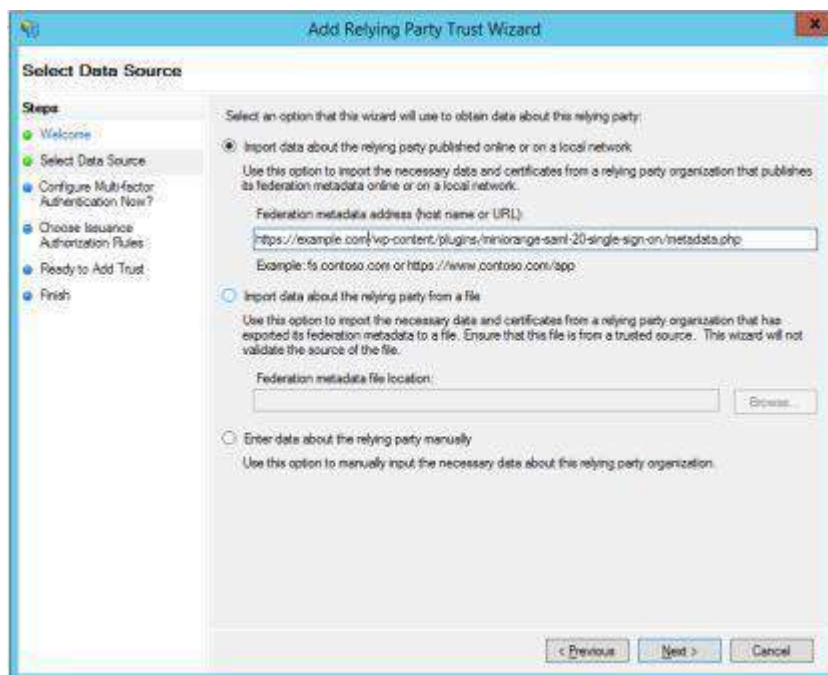


## SETUP GUIDE FOR ADFS AS IdP

**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 replying party published online or on a local network** and enter the metadata URL provided in the Identity Provider 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 relaying 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**.

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
E-Mail-Addresses	Name ID

< Previous Finish Cancel

**STEP 8:** In miniOrange SAML plugin, go to **Service Provider** tab. Enter the following values:

- **Identity Provider Name:** ADFS
- **SAML Login URL:** https://<your\_ADFS\_domain>/adfs/ls
- **SAML Logout URL:** https://<your\_ADFS\_domain>/adfs/ls
- **IdP Entity ID:** http://<your\_ADFS\_domain>/adfs/services/trust
- **X.509 Certificate:** Paste the certificate value you copied from the ADFS Metadata file.
- **Response Signed:** Unchecked
- **Assertion Signed:** Checked