Part 2: Configuring Self-Hosted Active Directory SAML with Omnilert

Pre-Installed Environment Used

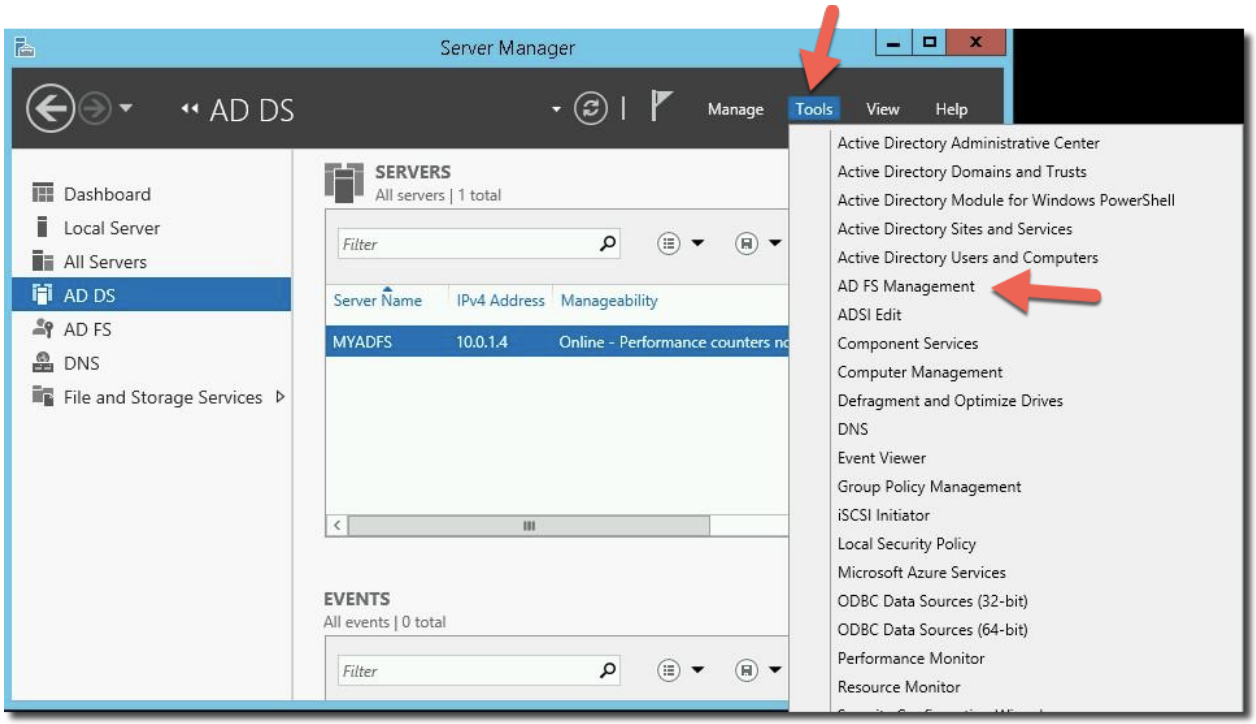
- Windows Server 2012 R2
- Active Directory Domain Services
- Active Directory Federation Service (Covered in Previous Document)

This guide walks through the process of configuring a self-hosted Microsoft Active Directory Federated Services (ADFS) instance as an Identity Provider (IdP) for use with Omnilert's Shibboleth/SAML Service Provider.

(If your server is not already running ADFS, please see "Part 1: Installing and Configuring ADFS")

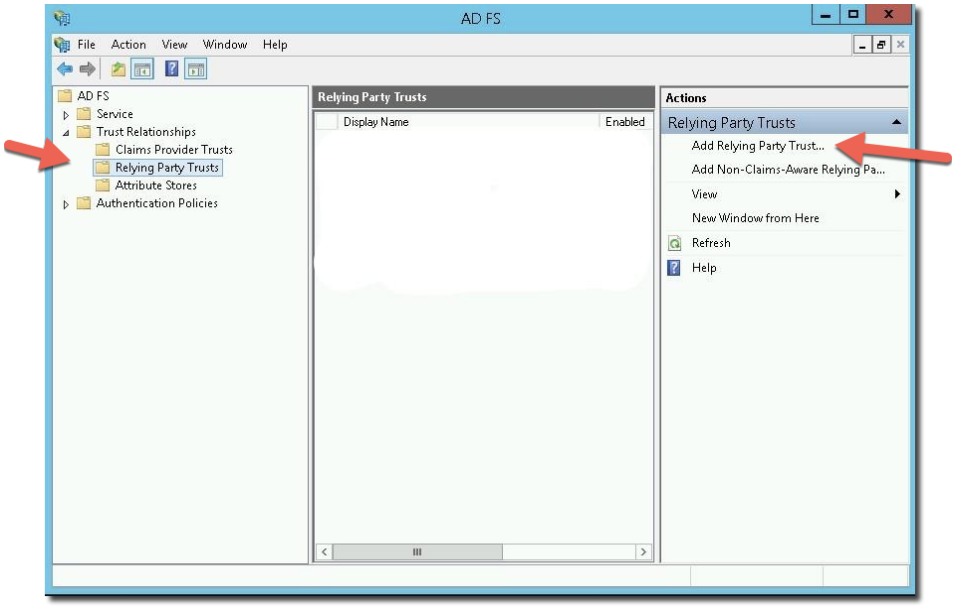
Configuring ADFS Relying Party Trust

1. Open **Server Manager** > **Tools** > **AD FS Management.**

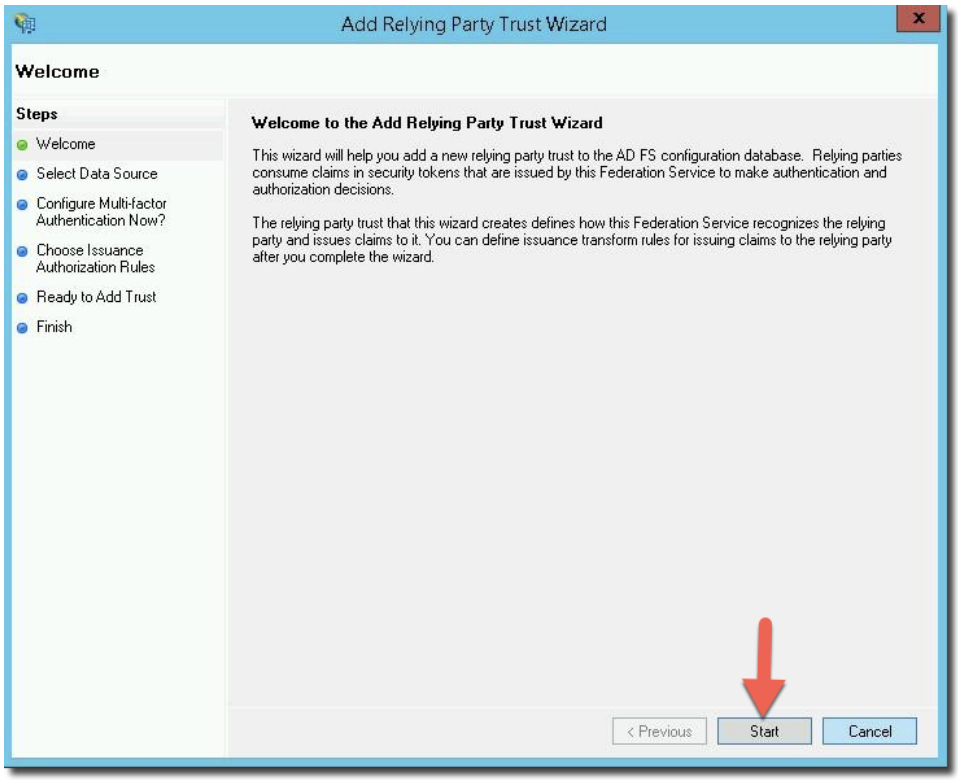


This will open MMC Console of ADFS.

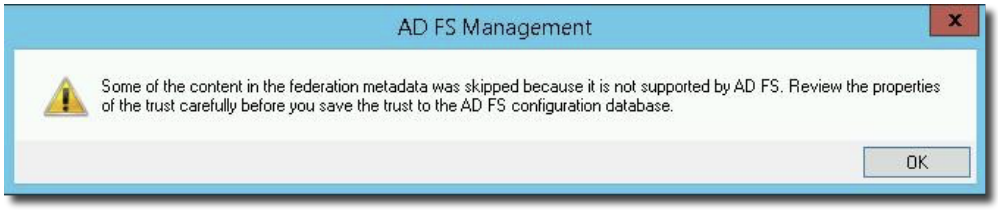
2. In **Actions Pane** click **Add Relying Party Trust** to open the *Add Relying Party Trust Wizard*



3. From the *Add Relying Party Trust Wizard* screen click **Start**

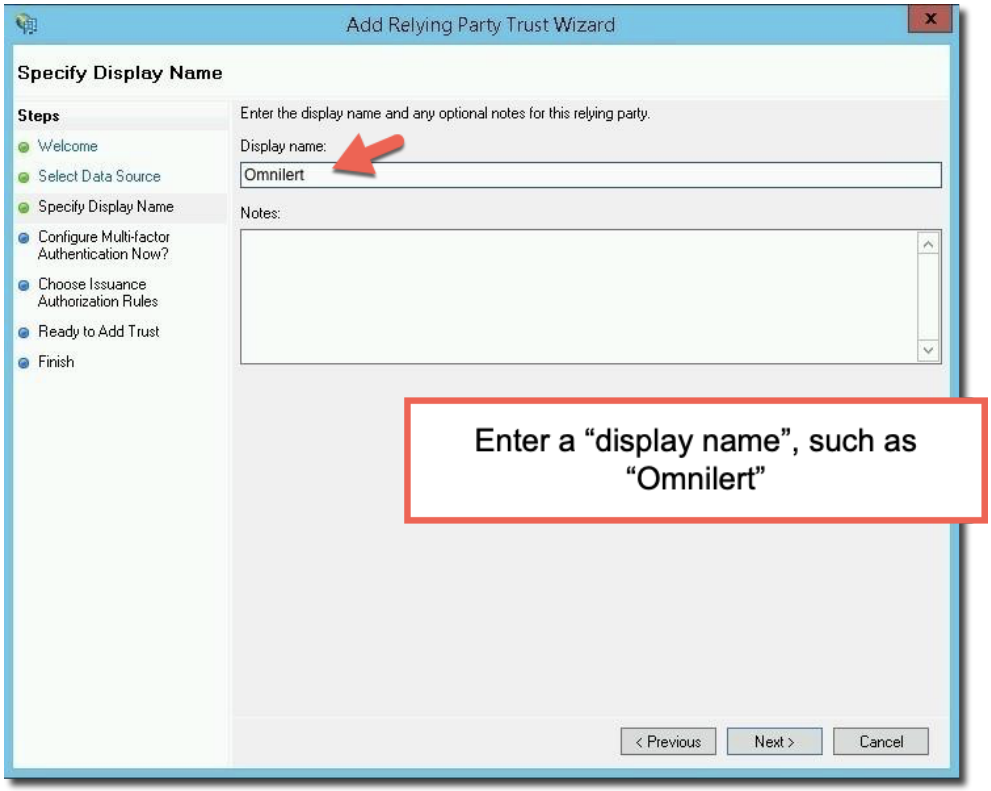


4. Select **Import data about relying party from a file** then Select the Metadata provided by **Omnilert** and click **Next.**

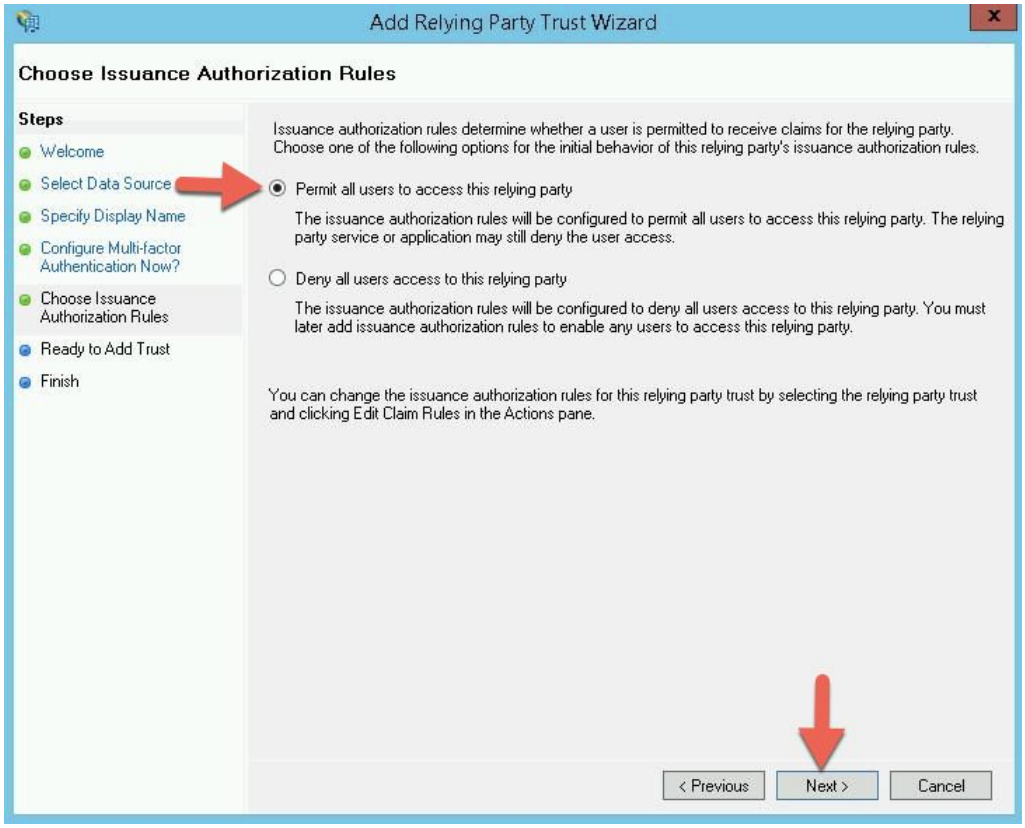


(This will prompt you that some content was skipped as it is not supported by ADFS)

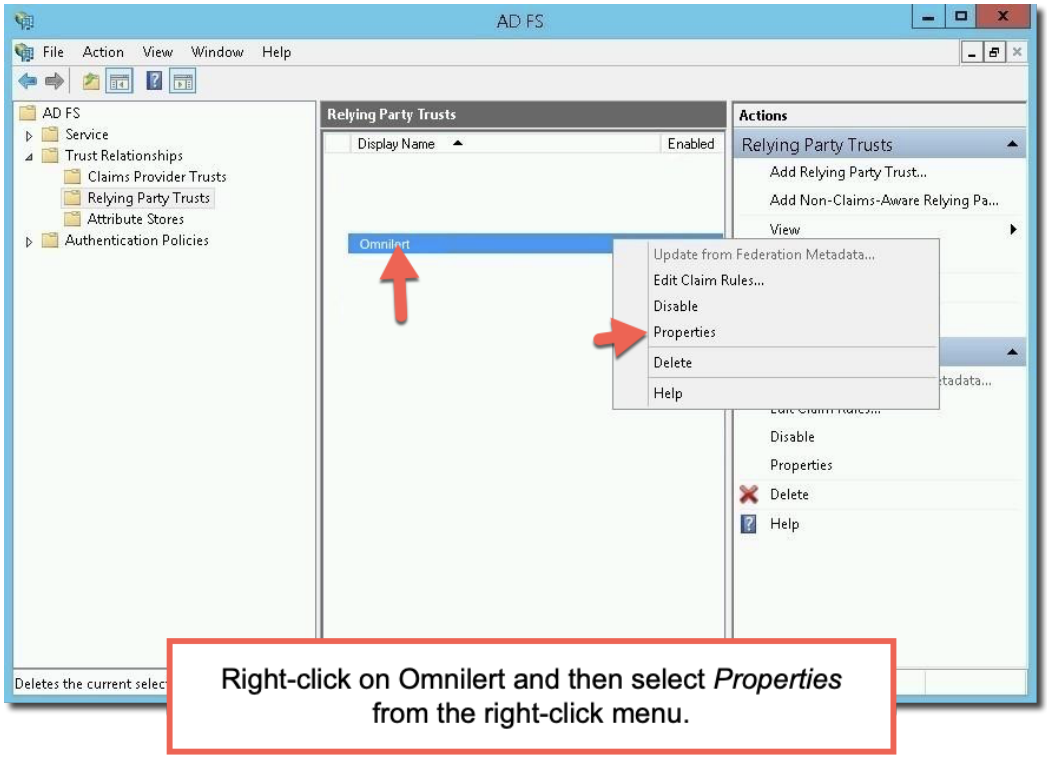
5. On **Specify Display Name** give Display Name (e.g. **"Omnilert"**) and click **Next**



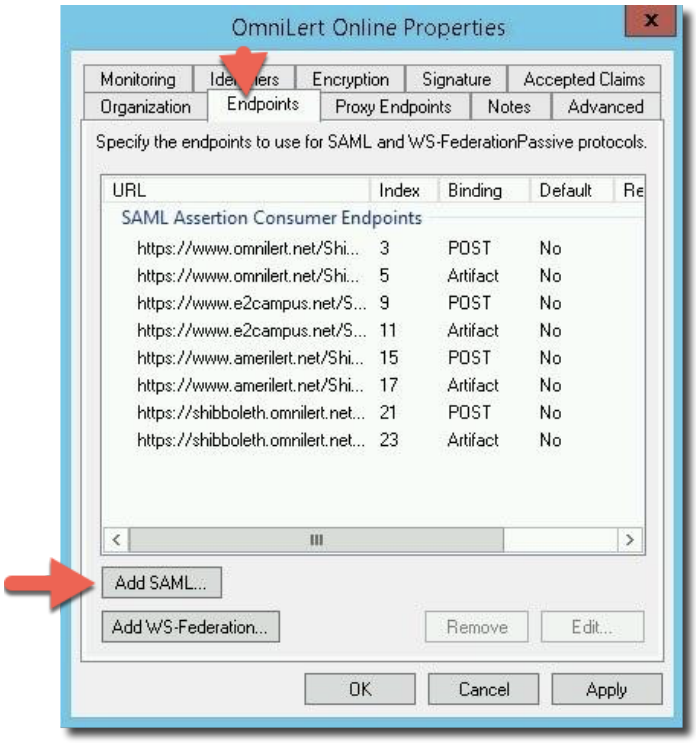
6. Select **I do not want to configure multi-factor authentication setting** and click **Next**Select **Permit all users to select this relying party** click **Next** then **Finish**



7. On **ADFS MMC Console** Right-Click **Omnilert** and click **Properties**

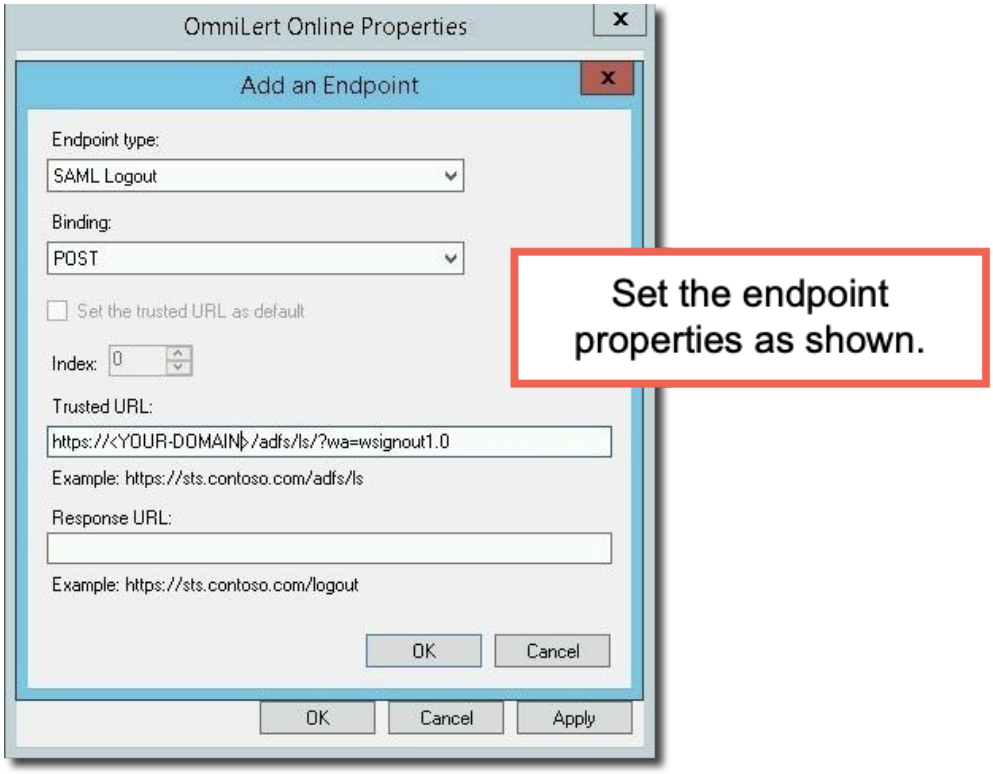


8. On **Properties Box** select **Endpoints** then click **Add SAML** to add an Endpoint

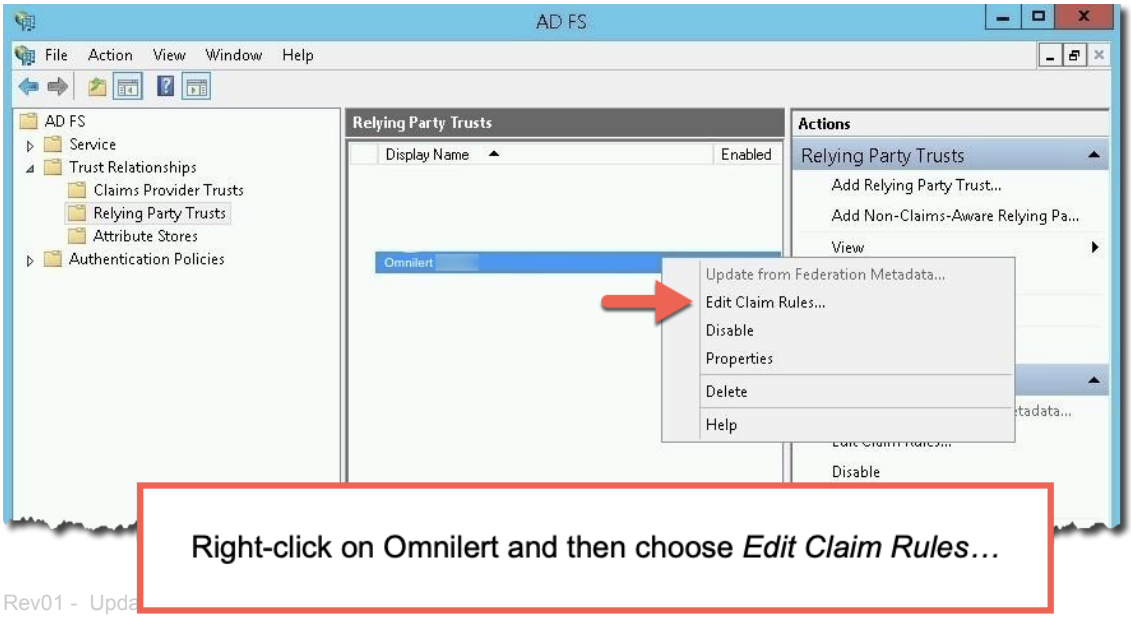


9. On **Endpoint Box** select the following parameters:

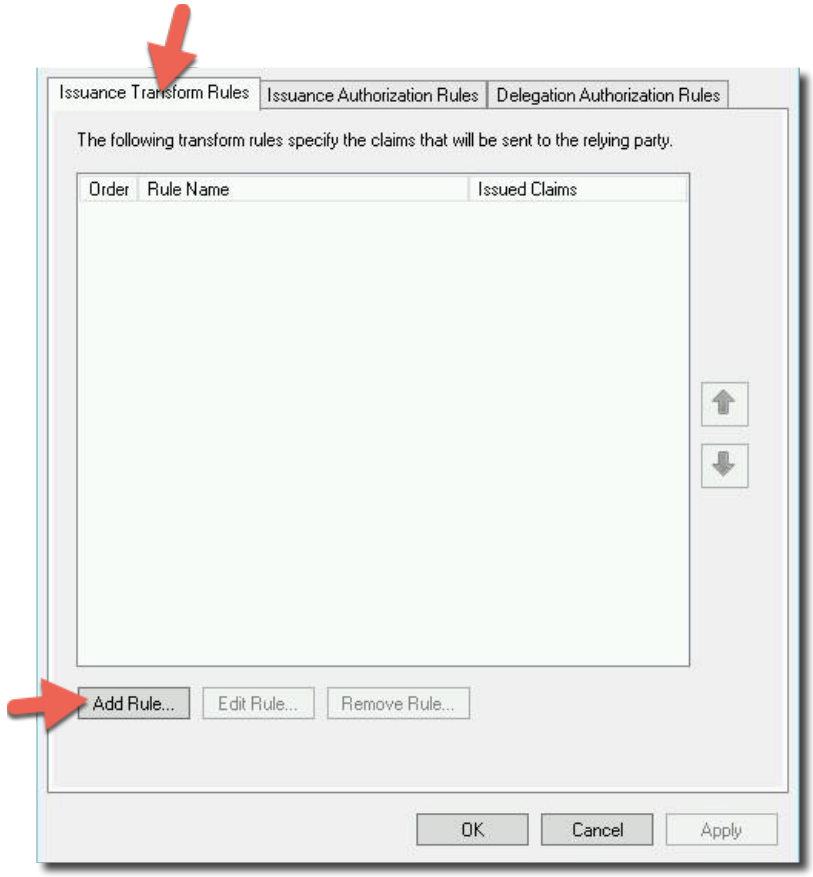
   - Endpoint Type: SAML Logout
   - Binding: POST
   - Trusted URL : `https://<YOUR-DOMAIN>/adfs/ls/?wa=signout1.0`
   - Then click **OK > Apply**



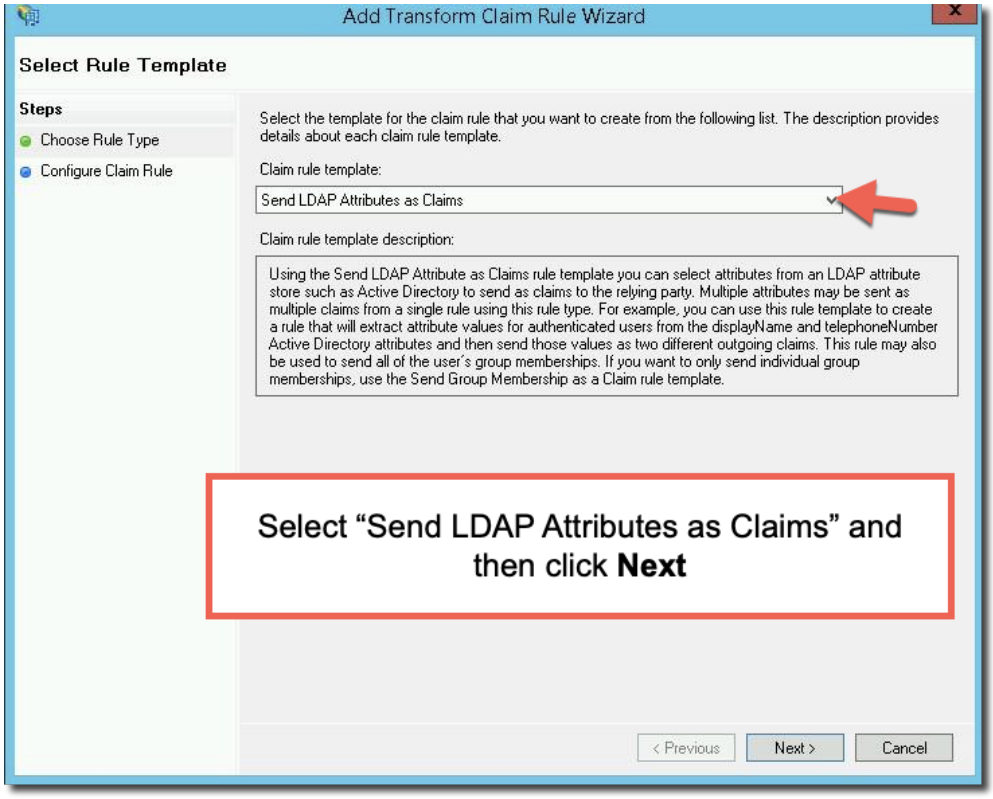
10. On **ADFS MMC Console** Right-Click **Omnilert** and click **Edit Claim Rules**



11. On **Claims Box** > **Issuance Transform Rules** > **Add Rule**

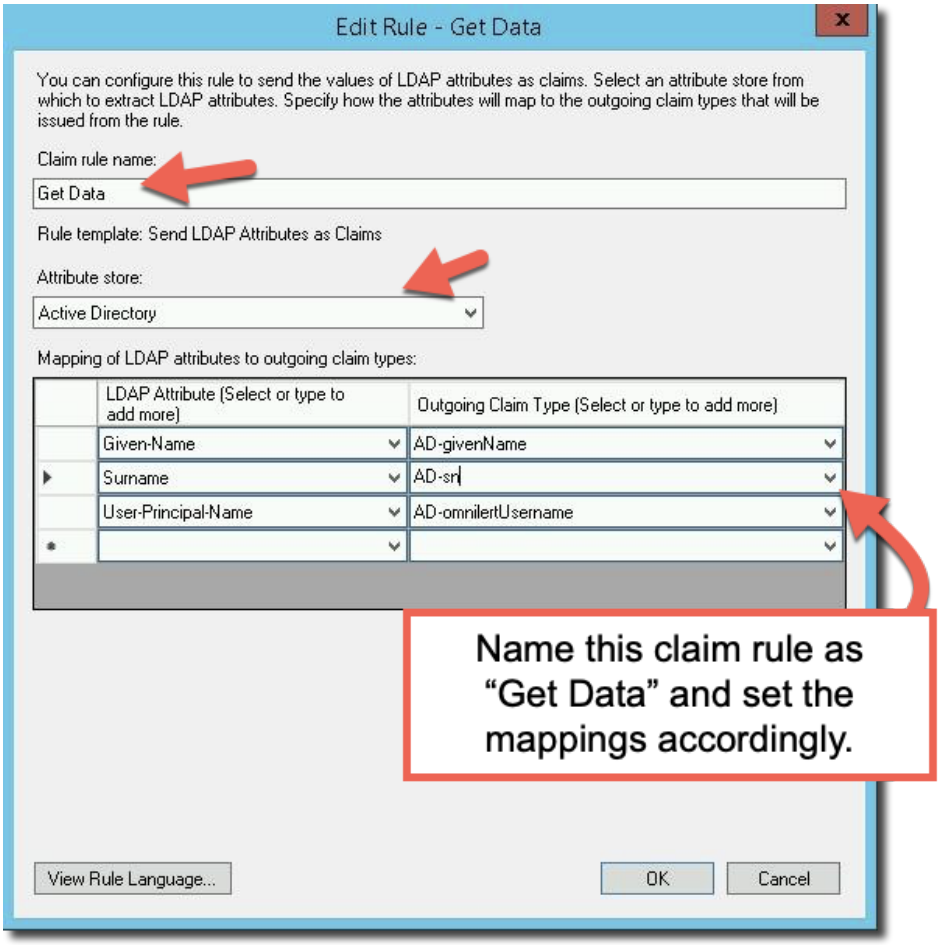


12. On **Add Transform Claim Rule Wizard** select ***Send LDAP Attributes as Claims*** and then click **Next**



13. Provide **Claim Rule Name "Get All Data"** > Select **Attribute Store "Active Directory"** and add Mapping as below > **OK** and **Apply**

- **Outgoing Claim Type :** AD-omnilertUsername, **LDAP Attribute :** User-Principle-Name
- **Outgoing Claim Type :** AD-givenName, **LDAP Attribute :** Given-Name
- **Outgoing Claim Type :** AD-sn, **LDAP Attribute :** Surname



14. Note that you have to configure your **Entity ID** and **Logout Url** on **Omnilert Admin Shibboleth/SAML Configuration page** which should be identical to:

- **Identity Provider Entity ID:** https://<YOUR-FQDN>/adfs/services/trust
- **Logout redirect URL:** https://<YOUR-FQDN>/adfs/ls/?wa=wsignout1.0

See https://support.omnilert.com/hc/en-us/articles/115008509908 for information on the Shibboleth / SAML settings within the Omnilert administrator portal.