BMS and ADFS - SAML 2.0 Single Sign-On (SSO) Just-in-Time (JIT) Provisioning

Release 4.0.27 | Version 1.0

Copyright Agreement

Contents

ADFS Setup

This article explains how to configure the SSO integration of a self-hosted Active Directory Federation Services (ADFS) server and BMS.

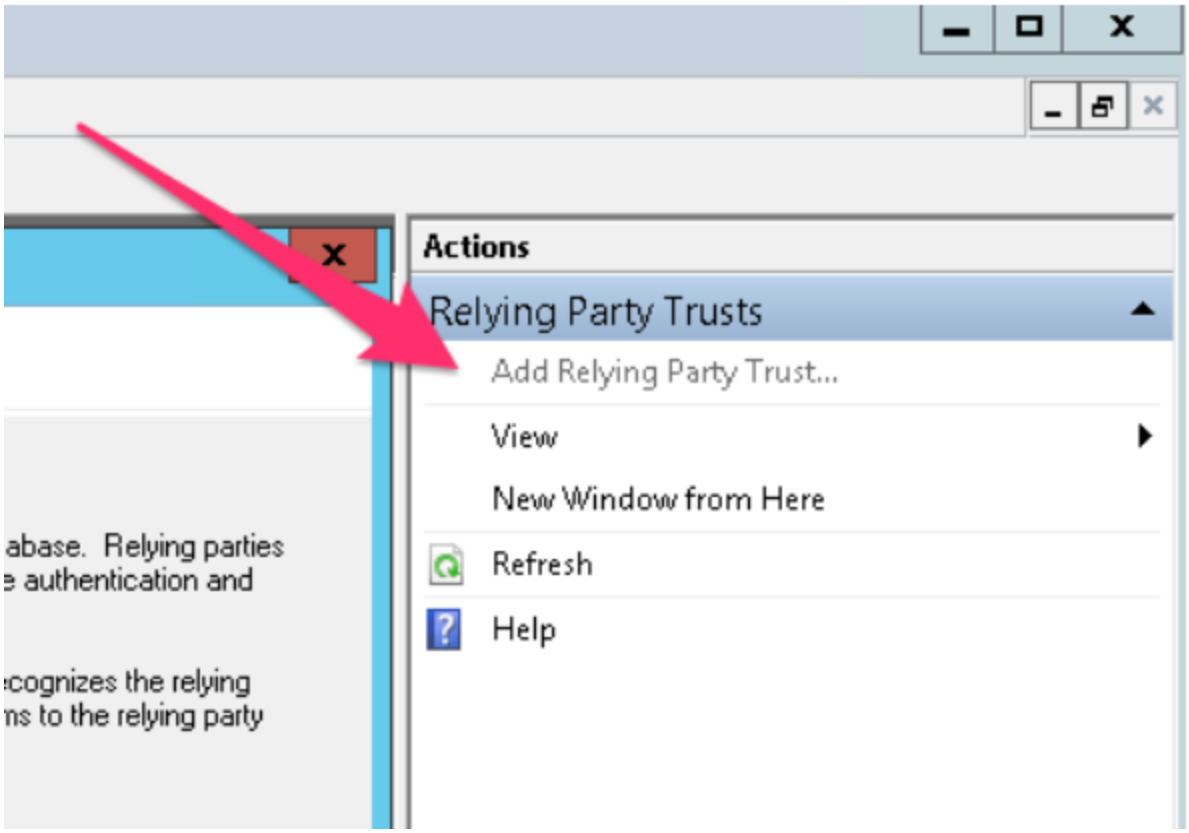
Adding a new relying party trust

The connection between ADFS and BMS is defined using a relying party trust.

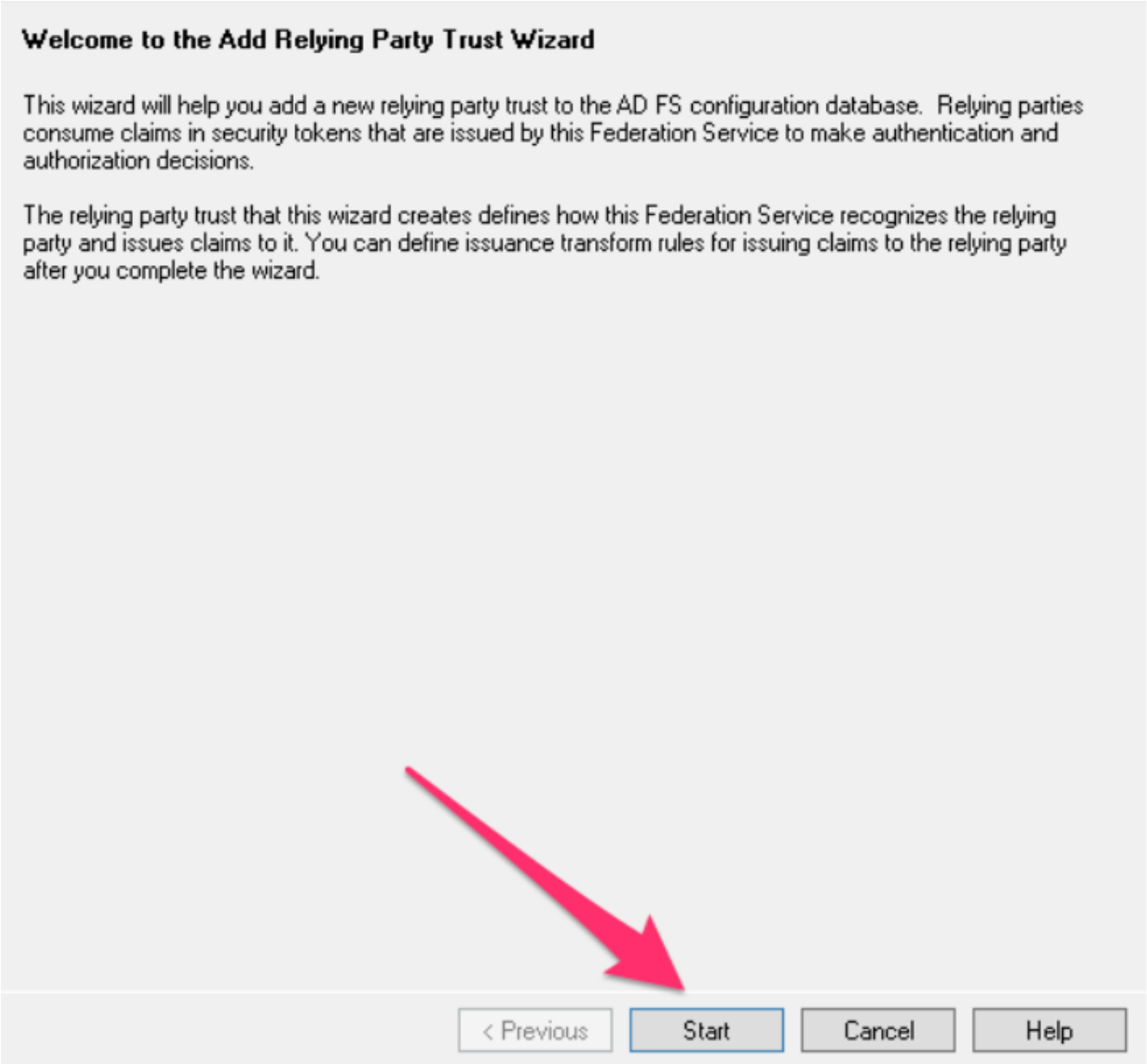
1 Log into the server where ADFS is installed.

2 Launch the **AD FS Management** application (click Start, Administrative Tools, AD FS Management) and select the *Trust Relationships* > *Relying Party Trusts node*.

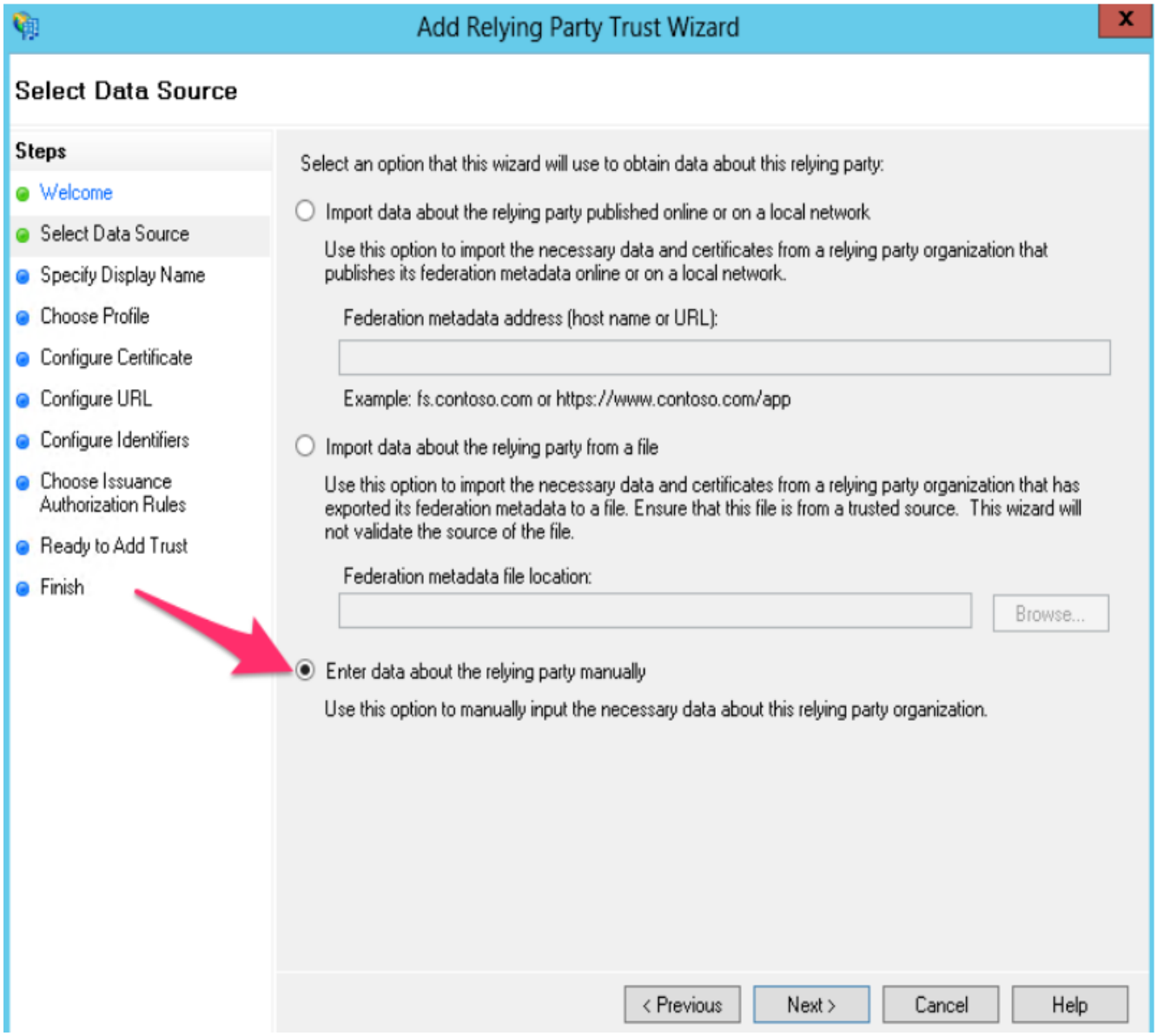
3 Click **Add Relying Party Trust** from the Actions sidebar.



4 Click **Start** on the Add Relying Party Trust wizard.



5 On the **Select Data Source** screen, click **Enter data about the relying party manually** and click Next.



Provide information for each screen in the Add Relying Party Trust wizard.

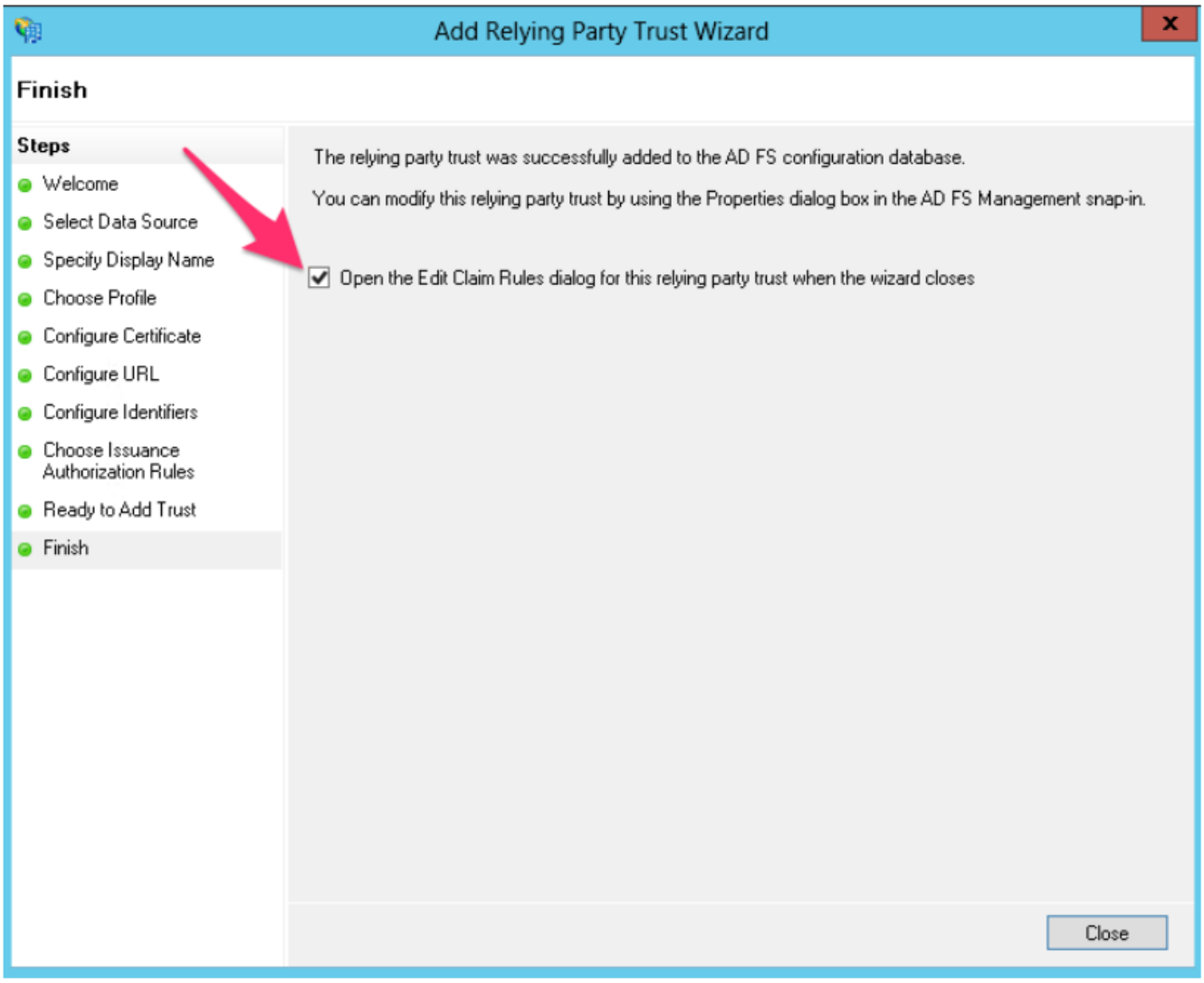
1. On the **Specify Display Name** screen, enter a **Display name** of your choosing and any notes (e.g. BMS SSO), select AD FS profile, and then click **Next**.
2. Skip the **Configure Certificate screen** by clicking Next.
3. On the **Configure URL**, select the box labeled **Enable Support for the SAML 2.0 WebSSO protocol**. The URL will be https://{host-name}/saml/connect.aspx, replacing hostname with your BMS Domain. Note that there's no trailing slash at the end of the URL.
4. On the **Configure Identifiers** screen, enter the Relying party trust identifier. This is the URL of your BMS Domain. The URL will be https://{host-name}, click **Next**.

5 Skip the **Configure Multi-factor Authentication** screen (unless you want to configure this) by clicking Next.

6 Skip the **Choose Issuance Authorization Rules** screen by clicking Next.

7 On the **Ready to Add Trust** screen, review your settings and then click **Next**.

8 On the final screen, make sure the **Open the Edit Claim Rules** dialog for this relying party trust when the wizard closes checkbox is selected and click **Finish**. This opens the claim rule editor.



Creating claim rules

After you create the relying party trust, you can create the claim rules and make minor changes that aren't set by the wizard.

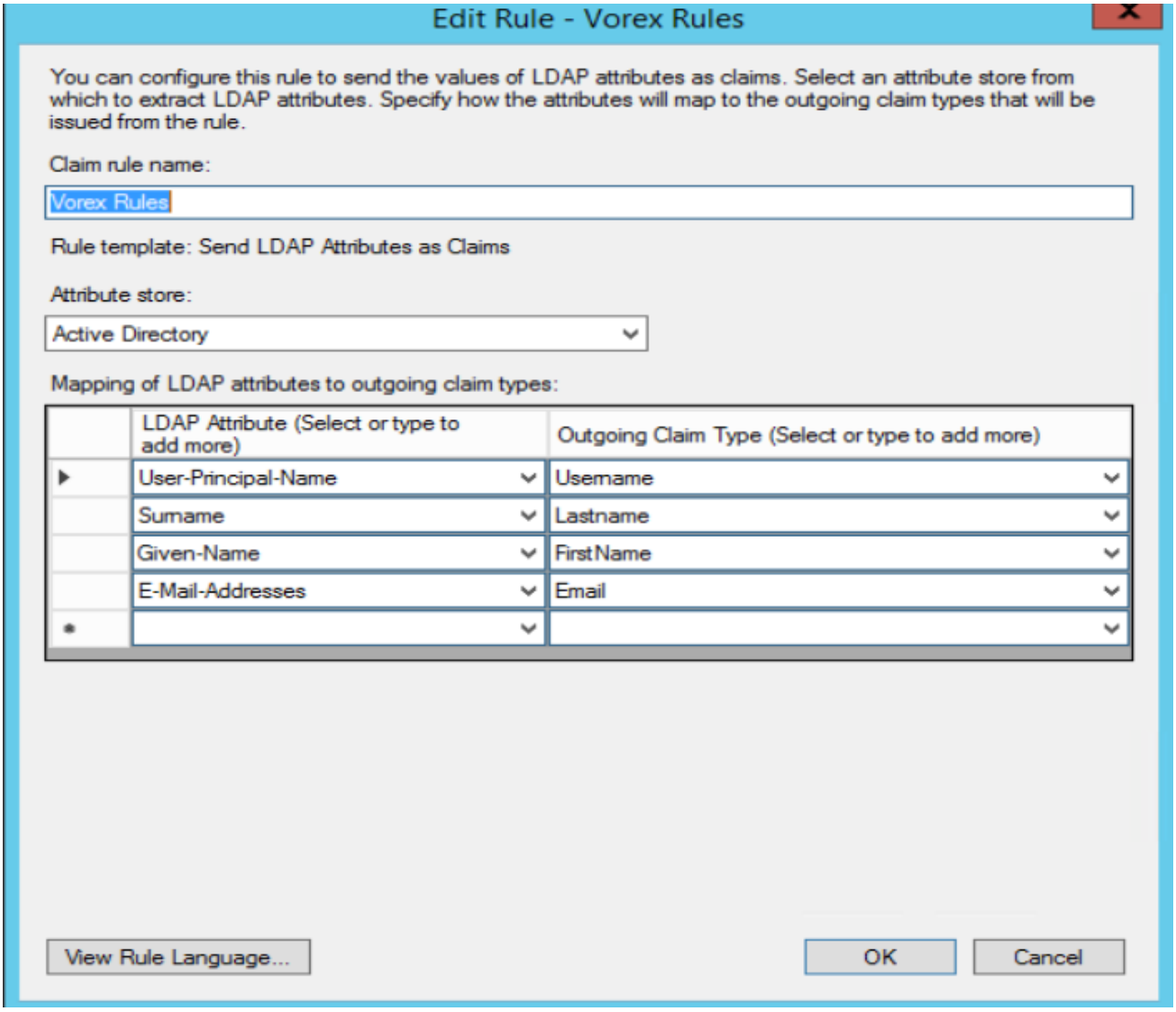
- If the claim rules editor appears, click **Add Rule**. Otherwise, in the Relying Party Trusts list, right-click the relying party object that you created, click **Edit Claims Rules**, and then click **Add Rule**.

You Should add multiple rules as follow:

Note: All outgoing claims should be the same as in the screenshots (companyName, SecurityGroup, username, lastname, firstname and email).

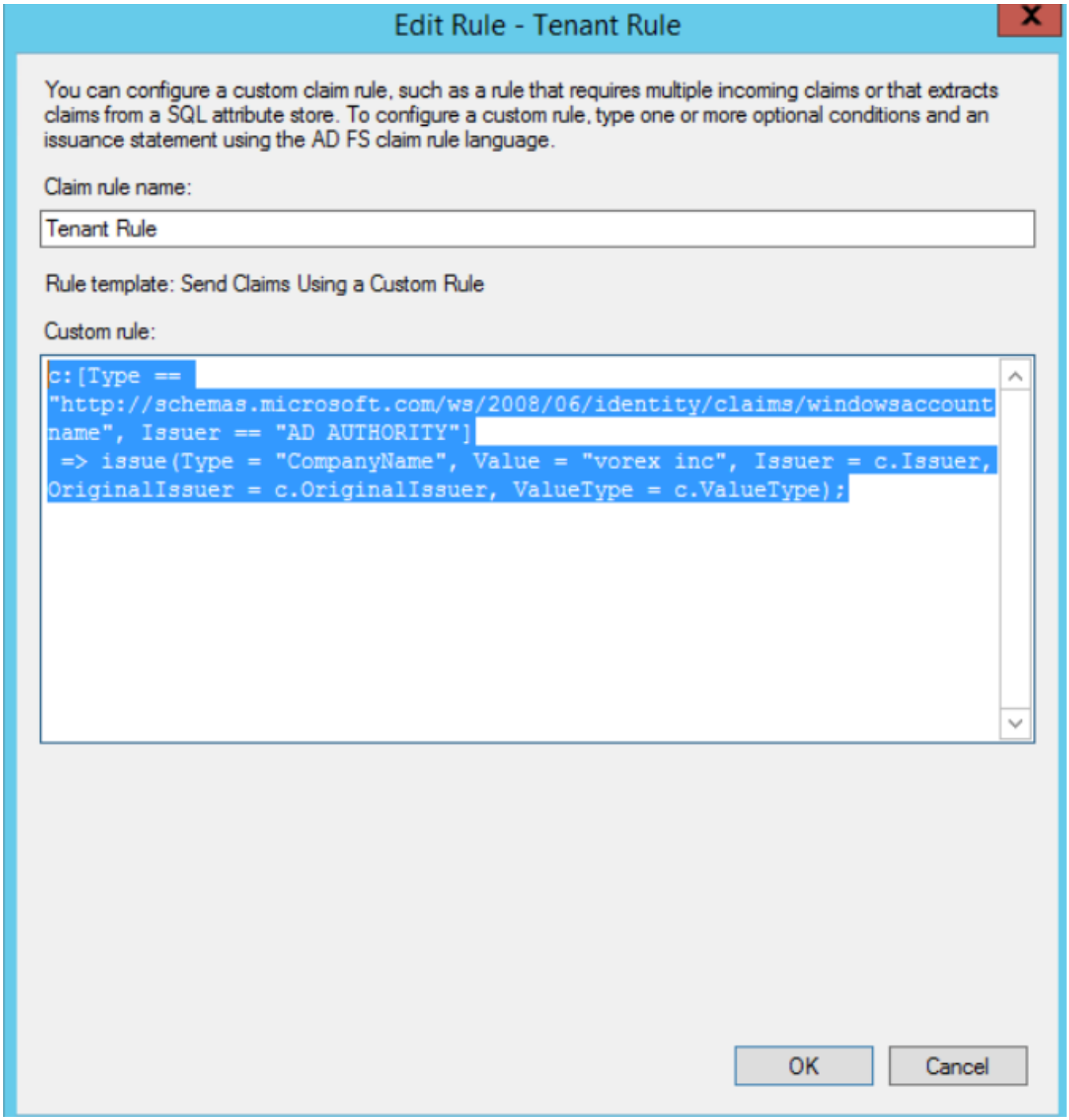
LDAP Attributes Rule to map all the required fields (firstname, lastname, username and email).

- On the **Select Rule Template** page, under Claim rule template, select **Send LDAP Attributes as Claim** from the list, and then click **Next**.



Custom Rule to add the companyName.

- On the **Select Rule Template** page, under Claim rule template, select **Custom Rule as Claim** from the list, and then click **Next**.

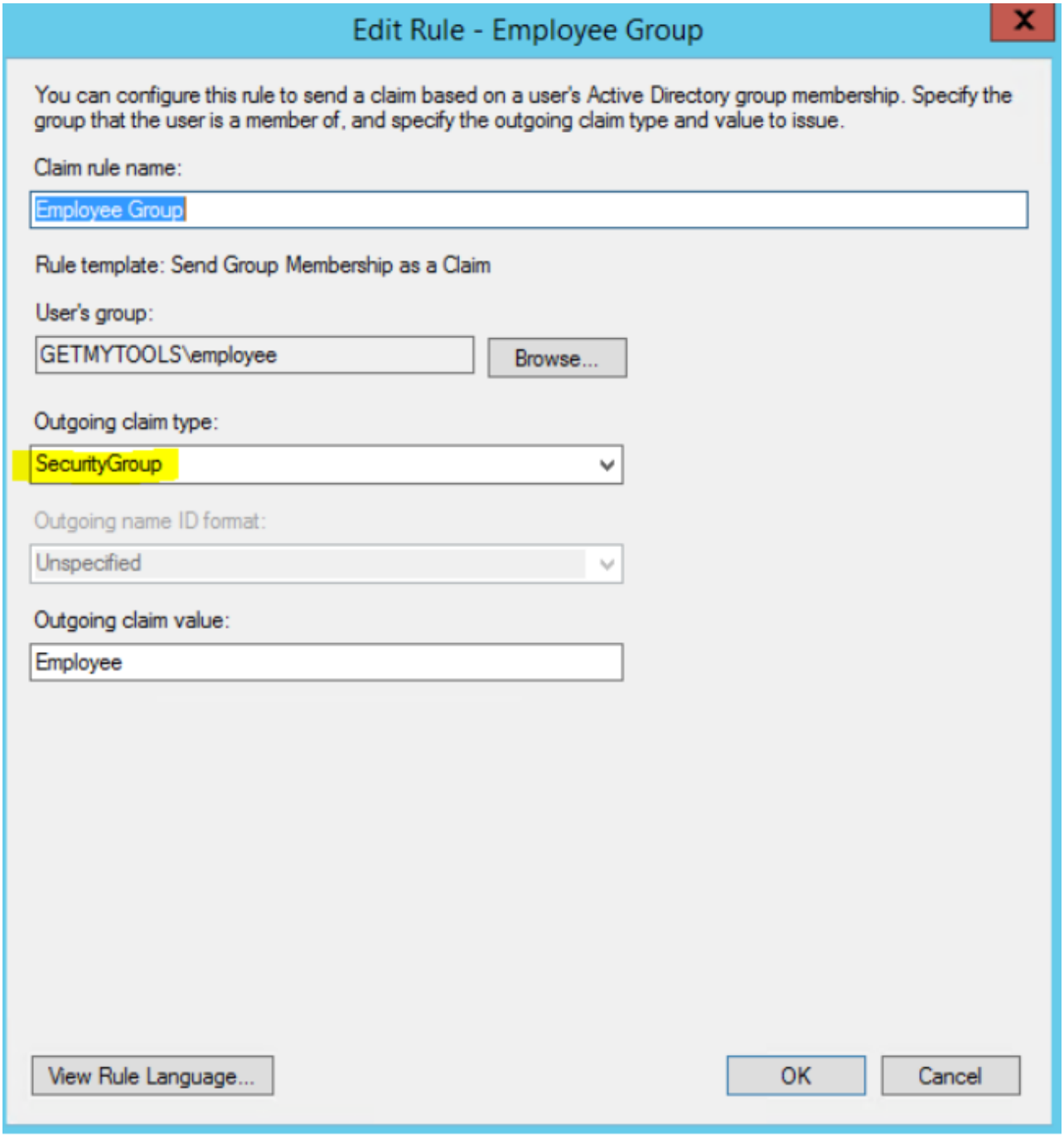


Custom Rule Template:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => issue(Type = "CompanyName", Value = "vorex inc", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, ValueType = c.ValueType);
```

Some rules for group claims.

- On the **Configure Rule** page under Claim rule name type the display name for this rule, in Employee's group click **Browse** and select a group, under Outgoing claim type select the **desired claim type** (should be SecurityGroup as mentioned above), and then under **Outgoing Claim Type** type a value.

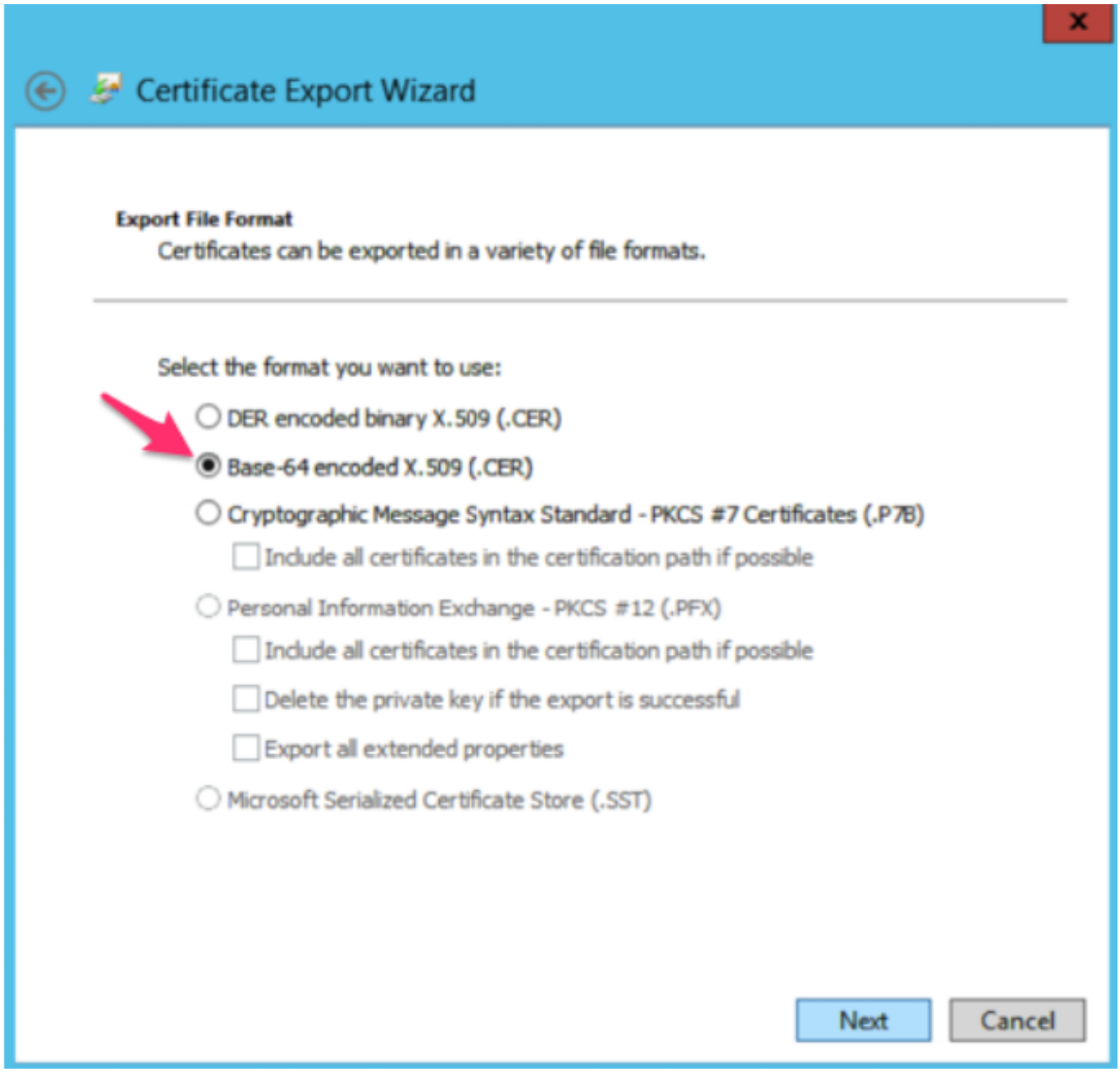


- In PowerShell enter the following command to make sure that both the message and assertion are signed:

```
Set-ADFSRelyingPartyTrust -SamlResponseSignature "MessageAndAssertion"
```

Download the Certificate

1. Export the token-signing certificate with the ADFS Microsoft Management Console.
2. When using the certificate exporting wizard, ensure you select **Base-64 encoded X.509 (.CER)** for the encoding format.
3. Open the exported file in a text editor to get the certificate value.

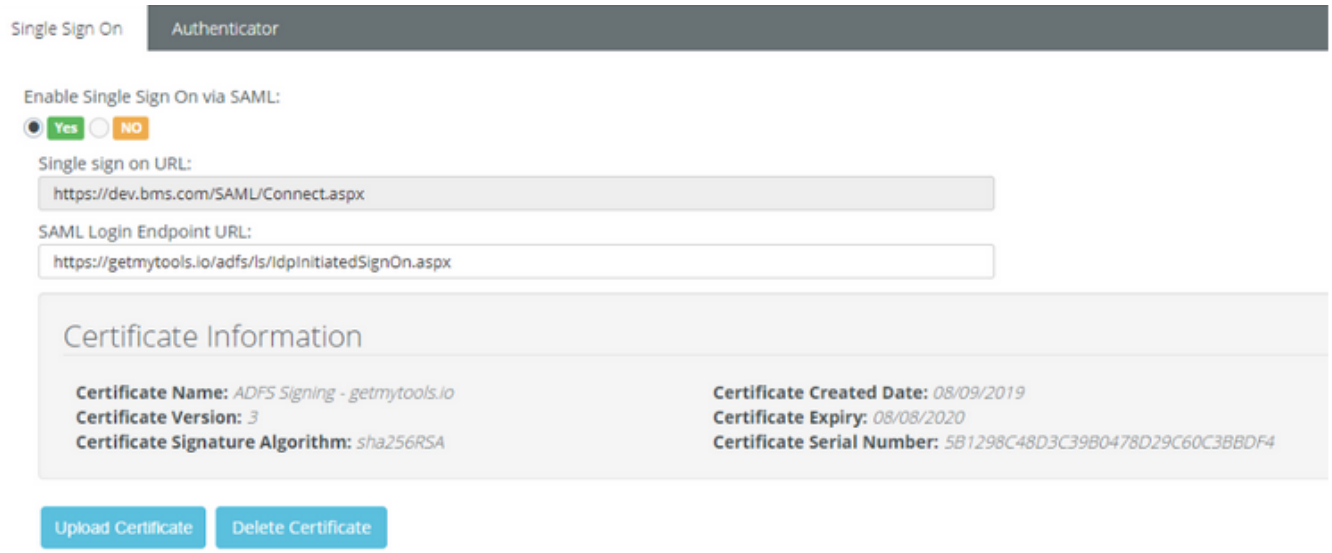


BMS setup

In BMS we need to setup the system to enable SAML authentication and that can be achieved under *Admin* > *My Company* > *Authentication*.

1 In the "Single Sign On" tab, upload the certificate downloaded previously, and set "Enable Single Sign On via SAML" to **Yes**, then click Save.

2 Enter the Login Endpoint, the URL will be https://{host-name}/adfs/ls/IdpInitiatedSignOn.aspx



This will enable BMS SAML authentication.

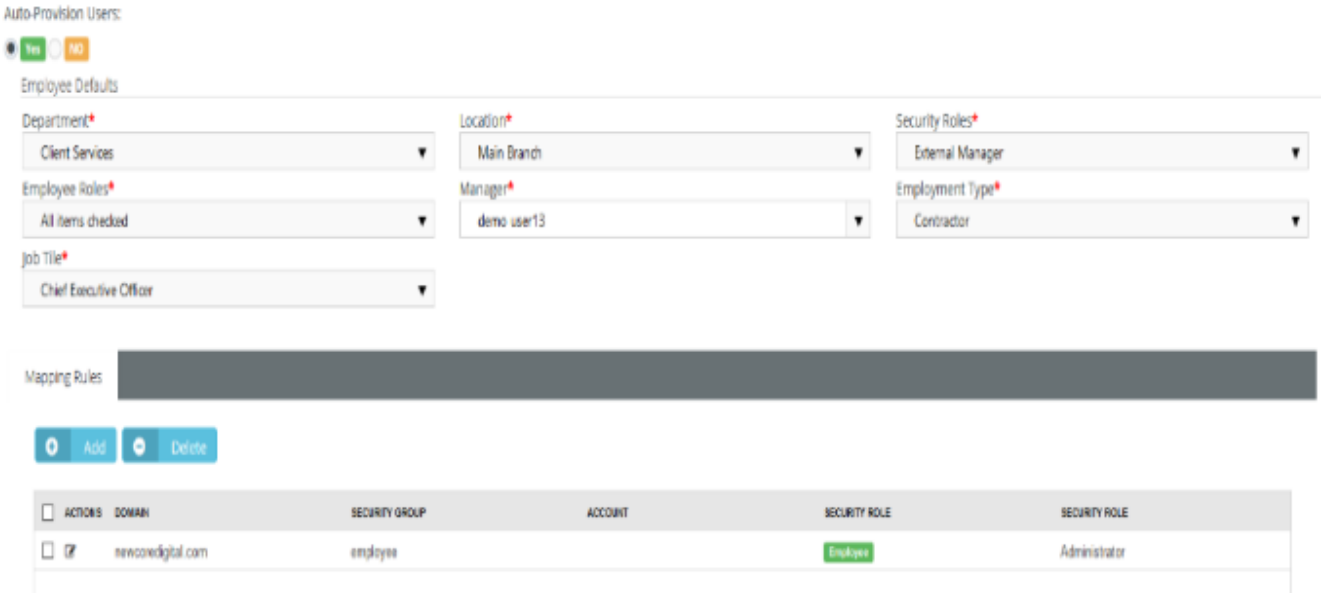
Create Mapping Rules and Enable Just in Time provisioning

In the authentication page we need to enable JIT provisioning with mapping rules matched to the one found in AD.

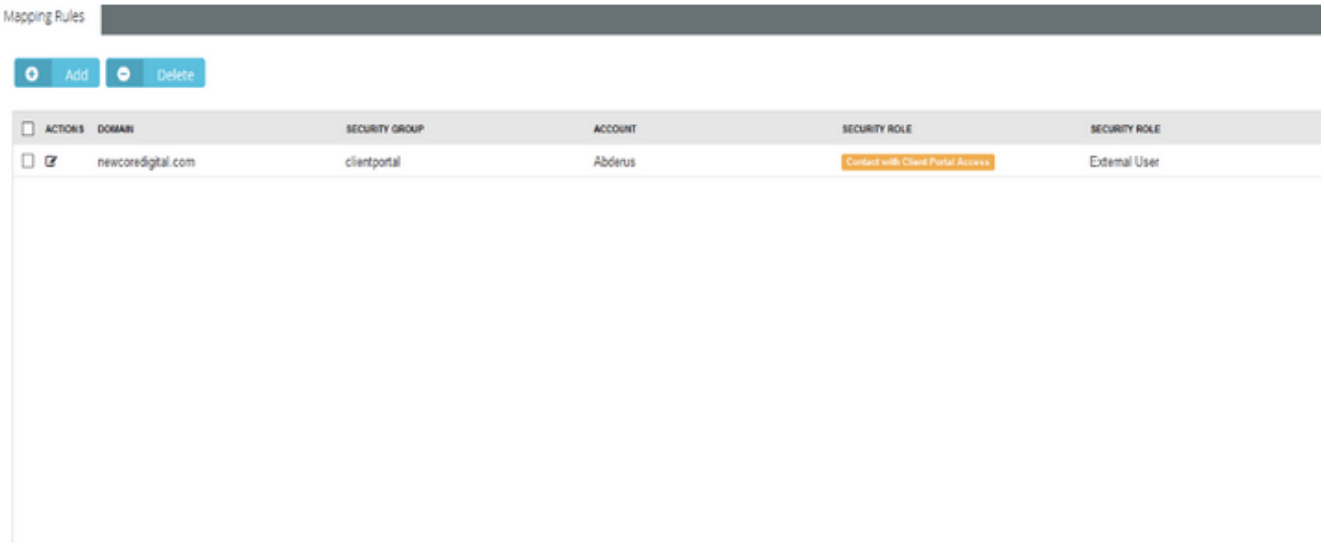
- Set "Auto-Provision Users" to yes.
- Create mapping rules matched with claim rules send from the IDP.

For Example:

1 If you add a user in AD member of employee's group then in BMS should have a matched rule with same domain and security group.



2 If you add a user in AD member of clientportal's group then in BMS should have a matched rule with same domain and security group.



3 If no rules matched with BMS the user will be created as external.

Note: If user is member of multiple AD groups then we choose the first matched rule based on order.

ADFS Application

Now Logout from BMS you will be redirect to the gateway page.

Enter **USERNAME** exist in the AD and hit next to directly open the ADFS authenticate page and then you will redirect back to BMS with the SAML response.

The action will be done based on the following:

- if the user not exist in BMS and auto provision enabled then a new user
- will be created and logged in with the mapped role.
- If the user not exist and auto provision disabled then it will be directly open the gateway page.
- If the user exist in BMS then directly should log in to the system.