1. **FNMS: Register ADFS**
2. (Optionally) Download ADFS Meta Data URL

This step is required if your ADFS system is not internet facing. In that case you will need to manually download the file for later upload to FNMS. The ADFS SAML 2.0 Metadata file is normally located at the following URL on your ADFS server:

<https://myadfsserver/FederationMetadata/2007-06/FederationMetadata.xml>

1. Log on to your FNMS cloud instance. E.g. <https://myorg.flexnetmanager.com/Suite>
2. Go to the **System Settings** page



1. Click on the **Security** tab
2. In the **SAML identity provider metadata** section either:

Enter the ADFS metadata URL (Only if your ADFS web server is internet facing)

e.g. <https://myadfsserver/FederationMetadata/2007-06/FederationMetadata.xml>

OR

Upload the ADFS federationmetadata.xml file that you uploaded in the step above.



1. In the **Active identity provider(s)** section choose an option that includes the SAML provider. See the Flexera online documentation for more details about the differences between these options.



1. Click on the **Save** button save your changes.
2. **FNMS: Gather authentication information**
3. Log on to your FNMS cloud instance. E.g. <https://myorg.flexnetmanager.com/Suite>
4. Go to the **System Settings** page



1. Click on the Security tab and take a note of the following properties. They will be used in later steps. These will be specific to your organization.
* Entity ID (e.g. <https://myorg.flexnetmanager.com/Suite>)
* Single sign-on URL (e.g. <https://myorg.flexnetmanager.com/Suite>/AuthServices/ACS)



1. **Register a user account**

This process must be followed for each user that needs access to FNMS using SAML authentication.

1. Log on to your FNMS cloud instance. E.g. <https://myorg.flexnetmanager.com/Suite>
2. Go to the **Accounts** page



1. On the **Accounts** page select **Create an account > Interactive SAML account** and enter the at least the following information:
	1. Account: The email address of the user as recorded in their Active Directory user account. e.g. johnbrown@myorg.com
	2. Name: A display name for the user in FNMS. e.g. John Brown
	3. Status: Enabled
	4. Role: Add to at least one role



1. Click **Save** to save the new account.
2. **ADFS: Create Relying Party Trusts**
3. Open **ADFS**
4. Right click on the **Trust Relationships > Relying Party Trusts** page and select **Add Relying Party Trust …**
5. Click **Start** on the **Welcome** page.



1. On the **Select Data Source** page select **Enter data about the relying party manually**



1. On the **Specify Display Name** page enter a **display name** of your choosing for the FNMS cloud system. (e.g. “MyOrg FNMS Cloud Instance”) Click **Next**.



1. On the **Choose Profile** page select **AD FS profile**. Click **Next**.



1. Do not make any changes on the **Configure Certificate** page. Click **Next**.

Note: The certificate should not be configured as FNMS does not support SAML assertion encryption.



1. On the **Configure URL** page check the **Enable support for the SAML 2.0 SSO service URL** checkbox. Enter FNMS Single sign-on URL in the **Relying party SAML 2.0 SSO service URL** field.

Use the **Single sign-on URL** that you gathered from your FNMS system earlier in this article.

e.g. <https://myorg.flexnetmanager.com/Suite/AuthServices/ACS>



1. On the **Configure Identifiers** page **Add** a Relying party trust identifier.

Use the **Entity ID** that you gathered from your FNMS system earlier in this article.

e.g. <https://myorg.flexnetmanager.com/Suite>



1. On the **Choose Issuance Authorization Rules** page select **Permit all users to access this relying party**. Click **Next**.



1. On the **Ready to Add Trust** page click **Next** and then **Close**.



1. **Configure Relying Party Trusts**
2. In the right hand pane select your FNMS system relying party trust and select **Edit Claim Rules …**



1. On the **Issuance Transform Rules** page click on the **Add Rule** button:



1. In the Add Transform Claim Rule Wizard, create a rule that is configured as follows:
* **Claim rule template:** Send LDAP Attributes as Claims



* **Claim Rule Name**:    My Email Claim rule
* **Attribute store**:        Active Directory
* Add one mapping configured as follows:
	+ **LDAP Attribute**: E-Mail-Addresses
	+ **Outgoing Claim Type**: Name ID



1. Click **Finish** then **OK** to save the changes
2. **Test the result**

To test that the authentication is working:

1. Browse to your ADFS single sign-on page

E.g. <https://myadfsserver/adfs/ls/IdpInitiatedSignOn.aspx>

1. Sign in to the site using your Active Directory user credentials



1. Select the FNMS Relying Party Trust and click on Go



1. You should be redirected to FNMS and be successfully logged on!

