SAML Authentication

SAML authentication is documented in the application help center but is a little unclear on the full steps that need to be taken.

This document is to help an admin step through the process provide additional information where appropriate.

URL for online documentation:
https://docs.microfocus.com/ITSMA/2018.02/NG/SM_X/Content/9900_Suite_Admin/saEditAccount.htm#Authentication

For these instructions we assume that you have:

- Installed SMA-X
- Created an Account and an associated Tenant.
- have a working SAML 2.0 compliant Identity Provider (IdP).
- Identified someone in your customers organization who is familiar with configuring and managing your organization's IdP.
- Your IdP's system clock is synchronized with a reliable time source. If it is not, tokens generated will be unusable and SSO will fail.

Note: Currently Back Office administration only allows 1 SAML authentication per account.

Set-up SAML Authentication on SMAX Account

Download metadata from AD server

- Download metadata from AD(replace the ad_host with real host name):
- https://ad_host/FederationMetadata/2007-06/FederationMetadata.xml
- Rename file to metadata.xml
- Copy metadata.xml file to SMAX master node {nfs-global-volume}/certificate/samlmeta
    - Default location of nfs-global-volume:
        - /var/vols/itom/itsma/itsma-itsma-global/certificate/samlmeta
    - make sure the file name is unique in this folder
- Go to CDF management console, open IDM deployment configuration
    - Resources -> Workloads->Deployments -> right click on idm -> view/edit yaml
    - Change replicas to 0, click update
    - Change replicas back to 1, then click update
    - Wait several minutes for IdM to start up

Prerequisites

1. (Optional) If you are establishing the mutual trust between external IdP and IdM via https, upload an external IdP certificate to the following directory:

{nfs_global_volume}/certificate/idm

Note in most instances where it is a shared environment for multiple customers the above step is not required

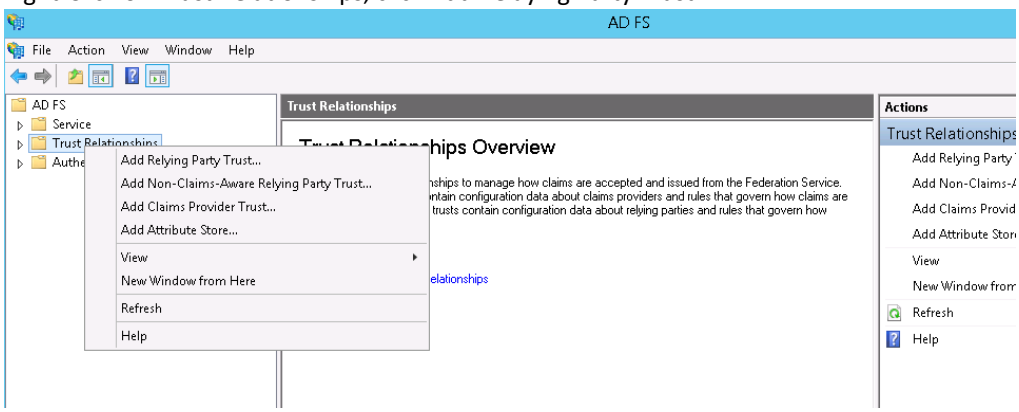
Download metadata from SMAX instance

- Use the following URL to download spring_saml_metadata.xml file from SMAX IDM
- Exchange hostname with your SMAX hostname
    - http://hostname/idm-service/saml/metadata
- Copy this xml to Active Directory Server

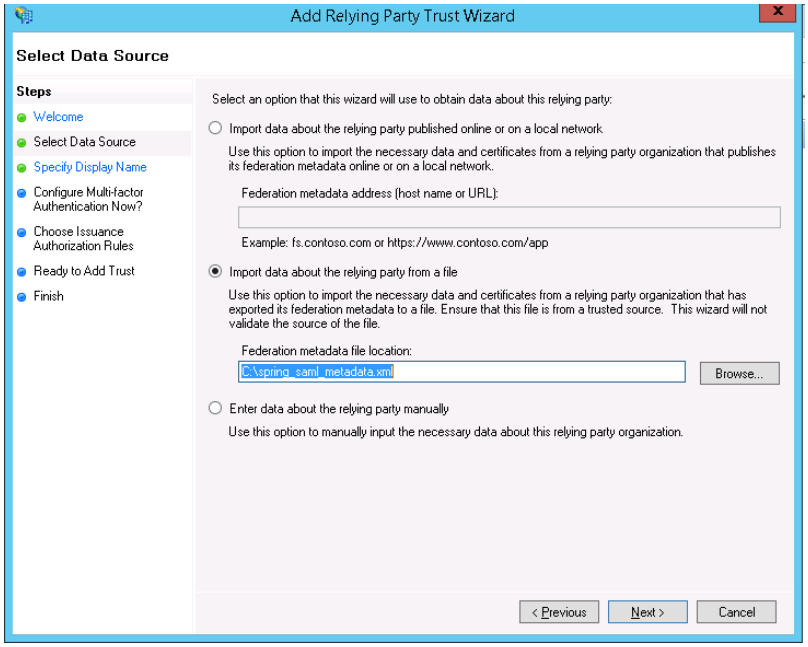
The generated metadata file will download as an XML file. Pass this to the appropriate resource to update the ADFS system so it can be added as a new relying party trust.

Add Relaying Party Trust in AD FS

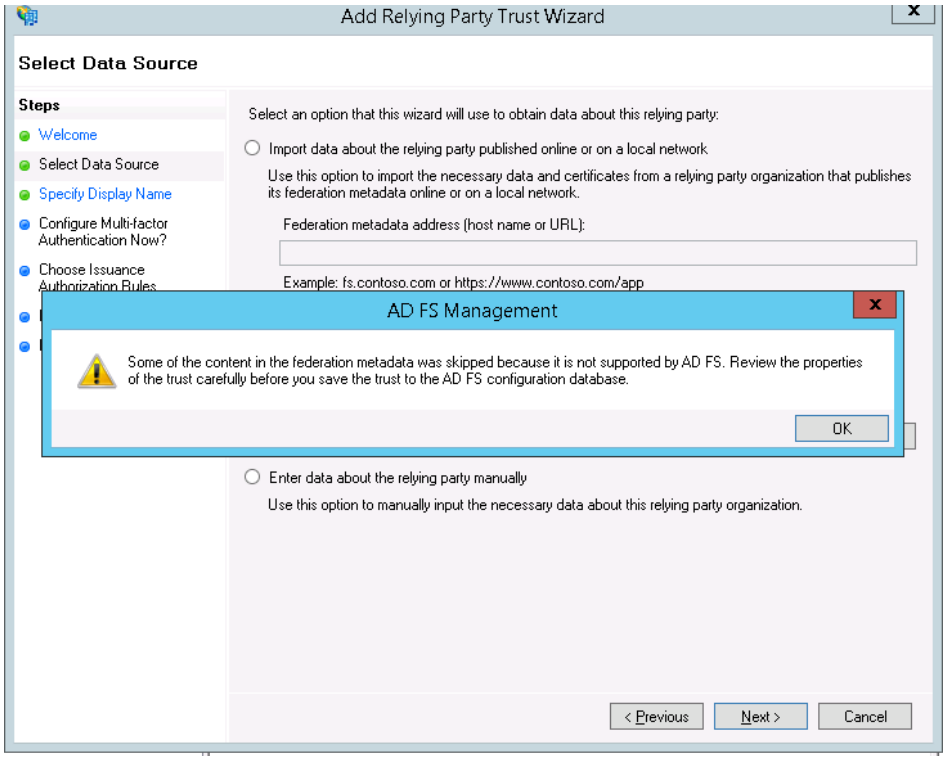
1. On AD Server, open Server Manager, tools, open AD FS Management
2. Right-Click on Trust Relationships, click Add Relaying Party Trust



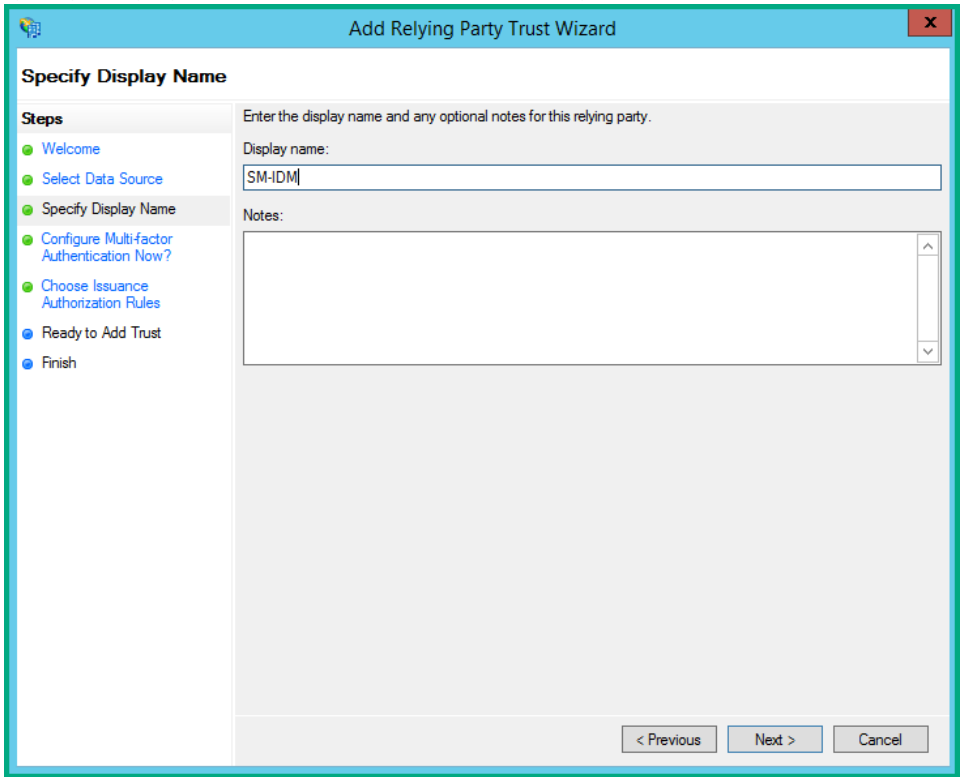
3. Select "Import data about the relying party from a file"
4. Select the spring_saml_metadata.xml file created in previous section
5. Select Next



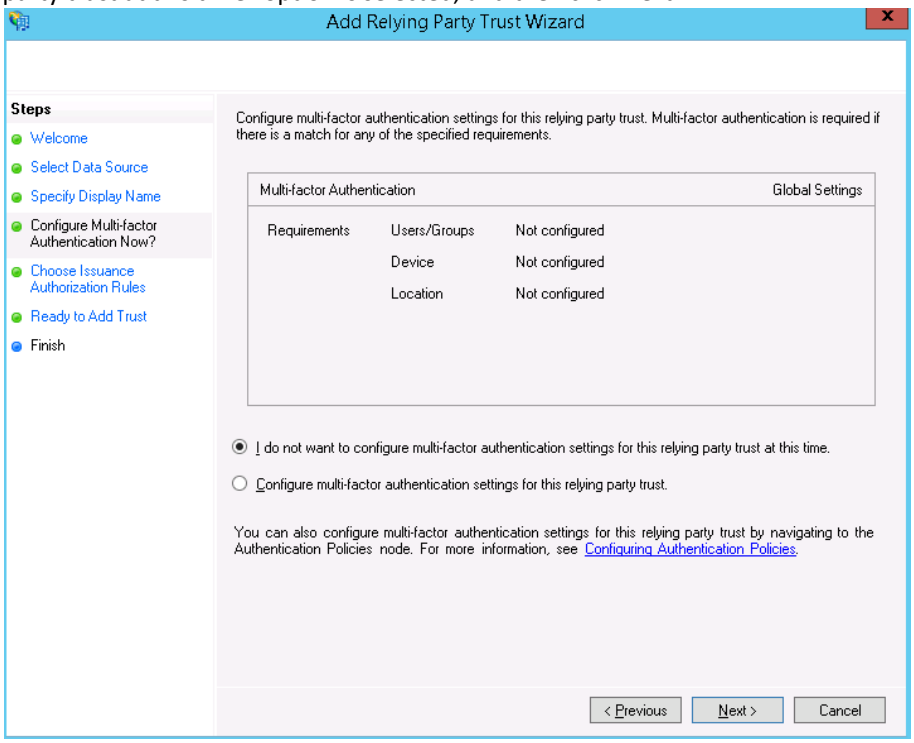
6. The wizard may complain that some content of metadata is not supported. You can safely ignore this warning



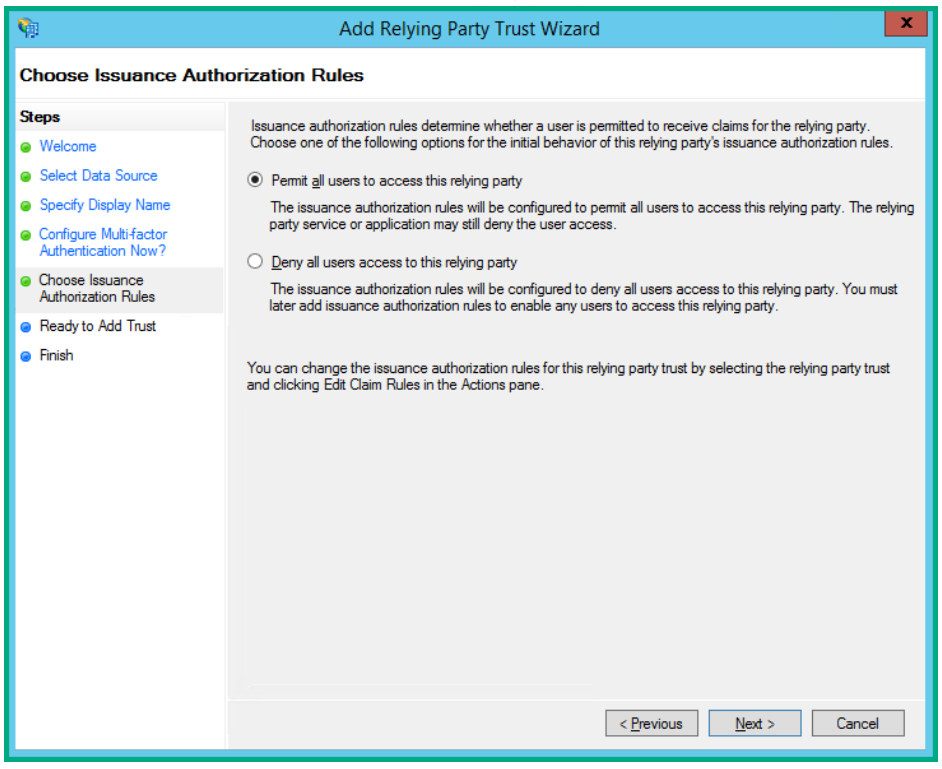
7. Specify a display name for the IdM service, and add optional notes. Click **Next**:



8. Make sure that the “I do not want to configure multi-factor authentication setting for this relying party trust at this time” option is selected, and then click Next

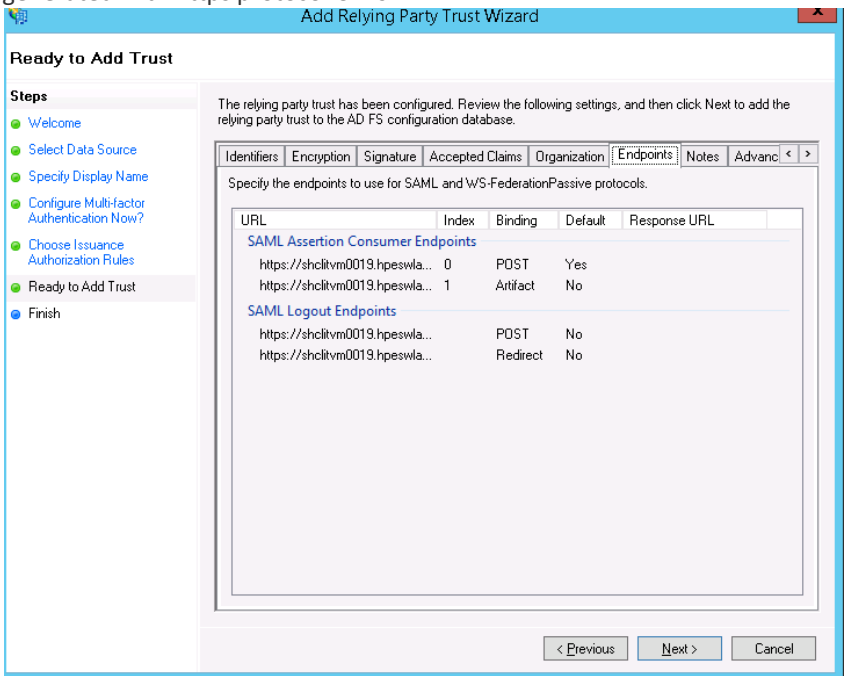


9. Select the **Permit all users to access this relying party** issuance authorization rule.

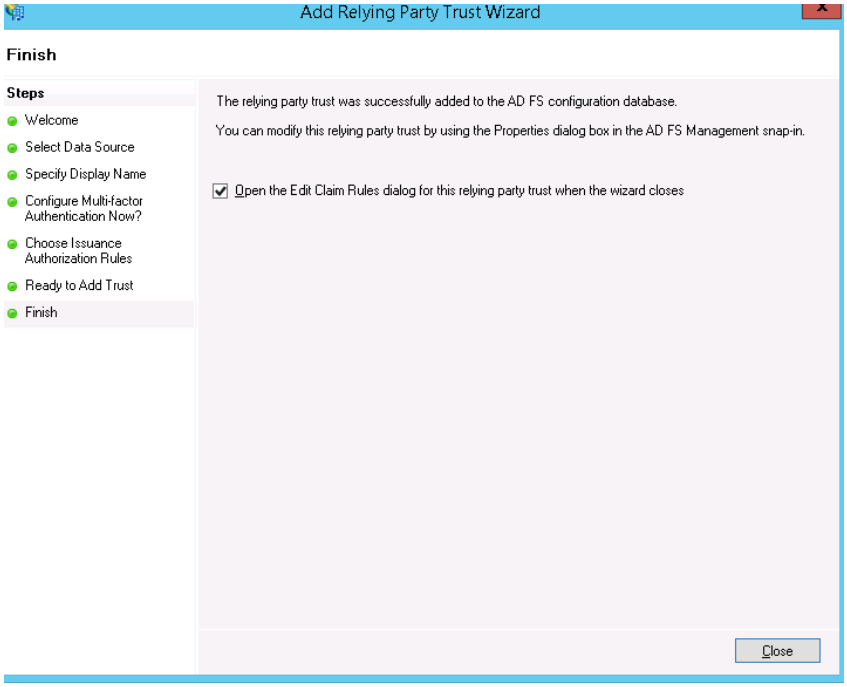


10. You are now in the **Ready to Add Trust step**.

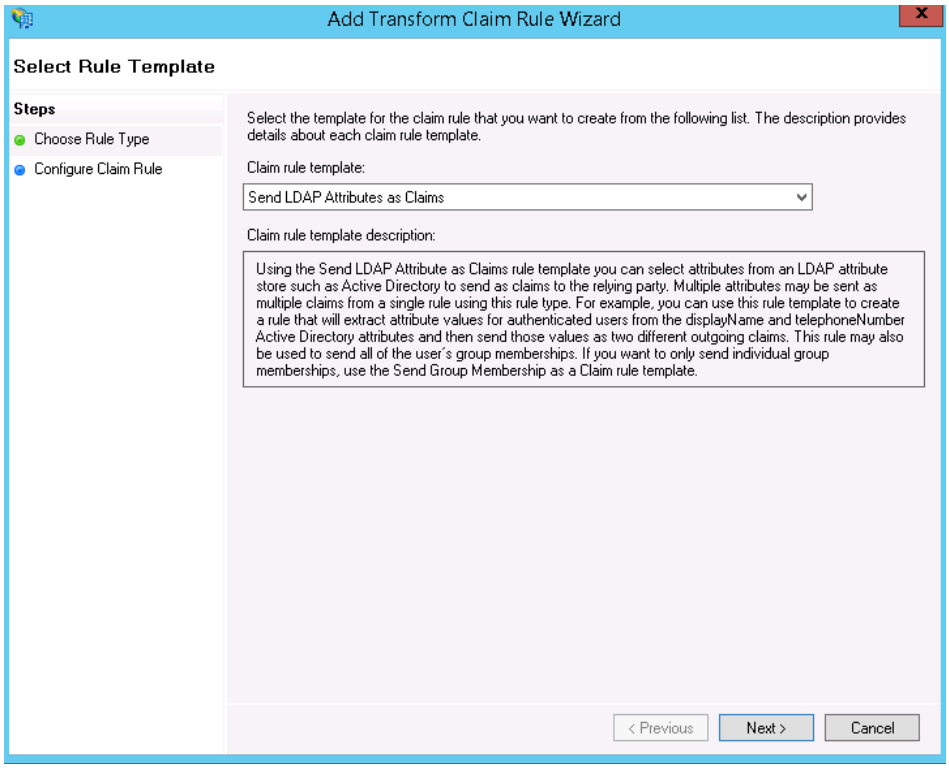
11. Check that the **Endpoints** tab contains multiple endpoint values. If not, verify that your metadata was generated with https protocol URLs

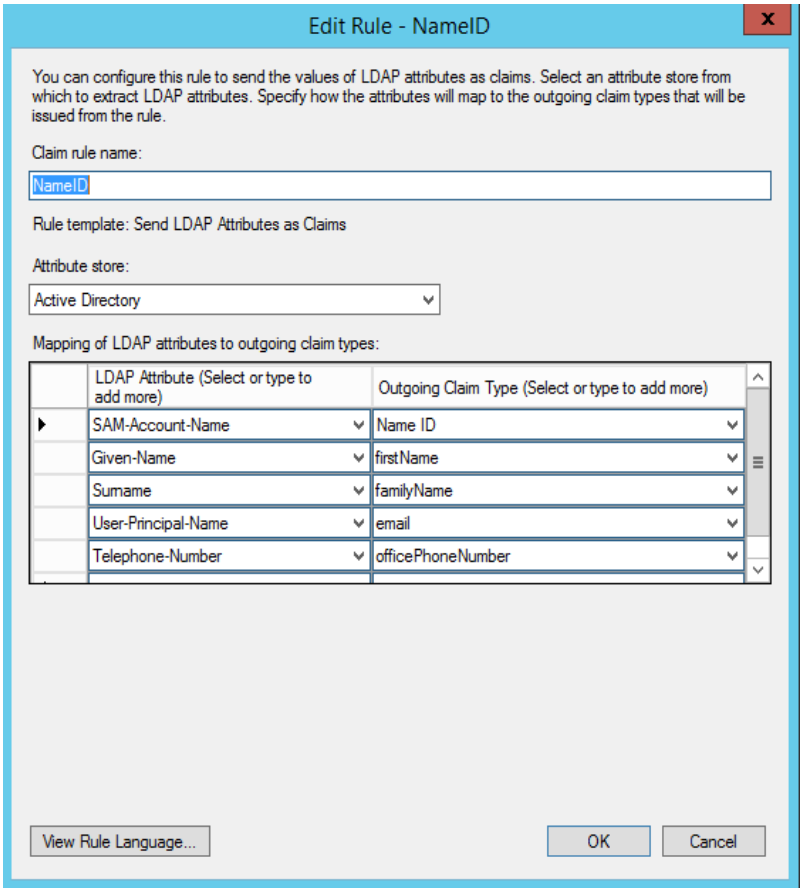


12. Leave the **Open the Edit Claim Rules dialog** checkbox selected, and then click **Close** to close the wizard



13. The Add Transform Claim Rule wizard opens
14. Under the tab "Issuance transform rules", Select "Add Rule", choose "Send LDAP Attributes as Claims" and click Next


Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Claim rule template:
Send LDAP Attributes as Claims
Claim rule template description:
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
< Previous
Next >
Cancel


Edit Rule - NameID
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:
NameID
Rule template: Send LDAP Attributes as Claims
Attribute store:
Active Directory
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)
SAM-Account-Name
Name ID
Given-Name
firstName
Surname
familyName
User-Principal-Name
email
Telephone-Number
officePhoneNumber
View Rule Language...
OK
Cancel

The full list of available fields for the outgoing claim type are listed here with example LDAP attributes:

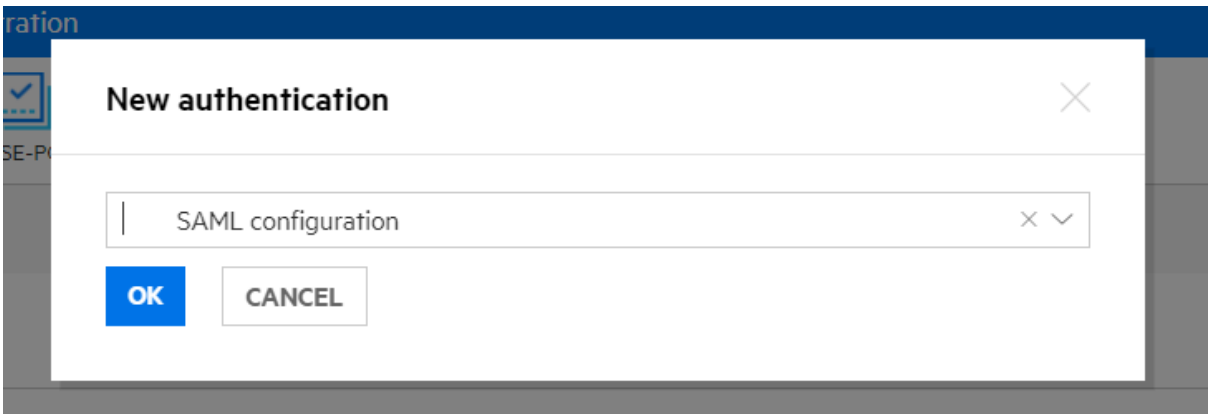
LDAP Attributes	Outgoing claim type
Login name	Name ID
First name	firstName
Middle name	middleName
Last name	familyName
Full name	fullName
Office phone number	officePhoneNumber
Home phone number	homePhoneNumber
Mobile phone number	mobilePhoneNumber
Language	Language
Location	location
Zip code	zipCode

Note: in case of errors, these can be changed in ADFS and will automatically be used to test against.

Once this is completed you can now update Back Office with the SAML Authentication details.

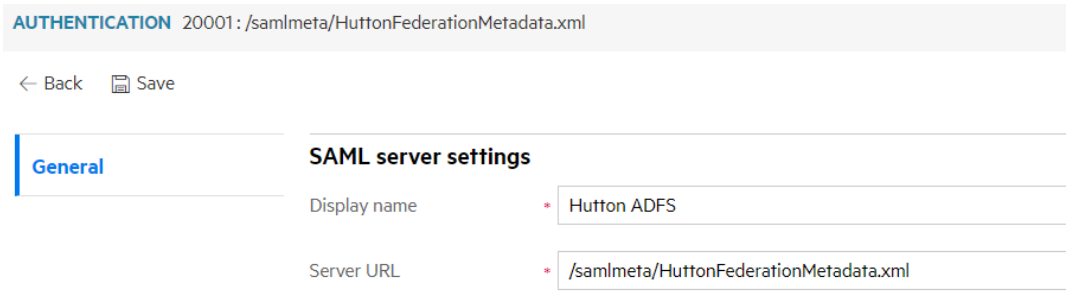
Back Office Instructions

1. Click on Accounts
2. Select the Account that you want to add the SAML Authentication to.
3. On the Account Screen, Click on the Authentications Tab
4. Click New
5. In the pop up box, select SAML Authentication from the drop down list and click OK



6. On the next screen you will be presented with 2 fields to populate:
   Display Name: enter a suitable value to identify the authentication (free text)
   Server URL:
   Note: If the mutual trust is established via https, enter the https URL of the external IdP metadata.

If the mutual trust is not established via https, enter this URL: /samlmeta/<external IdP metadata.xml>



7. Click Save

If SAML Authentication is set up correctly, you should now be able to login to your tenants for that account.

Federated IdP users can access the tenant after the configurations are completed. The user profile is synced to Suite Administration after the user logs in for the first time.

Troubleshooting / Common Issues

After Migration from SAW, user is able to login but does not have correct permissions

- Look for the Person record in the SMA-X tenant, it is likely that it has created a new person record and not linked it to an existing person record. If this is the case the Name ID field (which links to the UPN in SMA-X / SAW Person record) is not mapped correctly in the meta-data file. Update the meta-data file settings on the ADFS to reflect the correct values.