How to Configure Symantec Mobility Suite with onelogin™

Note: An Enterprise onelogin™ account is required for AD integration. The below article assumes that AD integration has already been performed. For more information see https://support.onelogin.com/hc/en-us/articles/202361690-Installing-an-Active-Directory-Connector-ADC- or contact onelogin™ support.

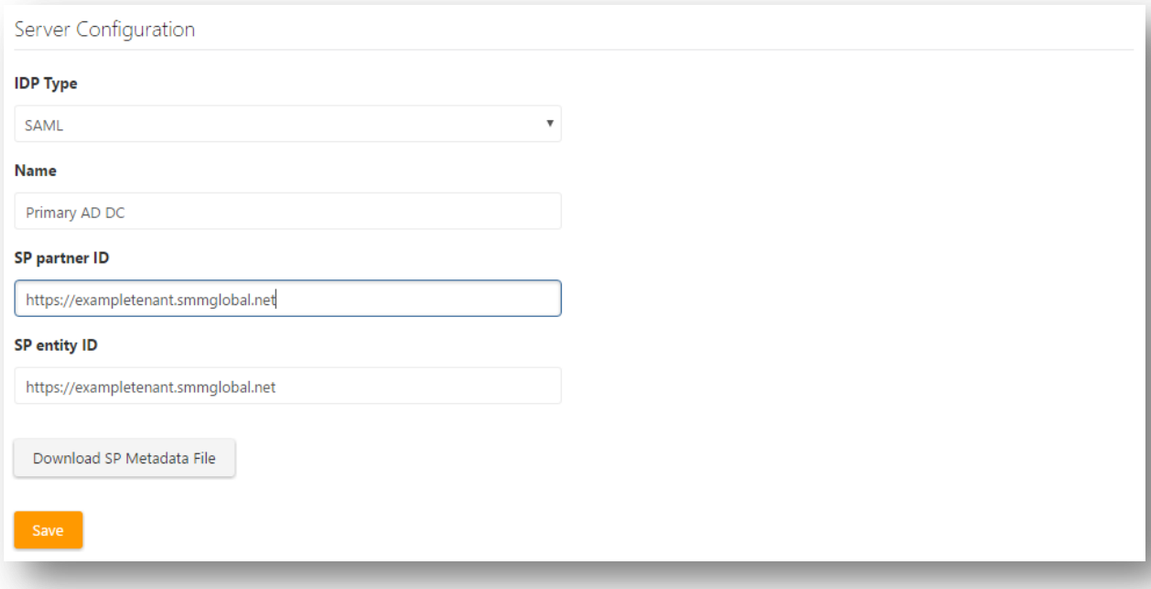
1. Log into the https://admin.us.onelogin.com
2. At the top **Click Apps > Add App**.
3. In the search area enter **Symantec Mobility**.
4. Click on **Symantec Mobility Suite**:

5. Under configuration enter the desired display name and **Save**.
6. Click the configuration tab and enter the FQDN of the Mobility tenant for both the SAML Audience and SAML Consumer URL.
7. Download the onelogin™ Metadata file by clicking **MORE ACTIONS > SAML Metadata**.
8. Open the metadata file in a text editor and add the following lines above the "</IDPSSODescriptor>" directive:

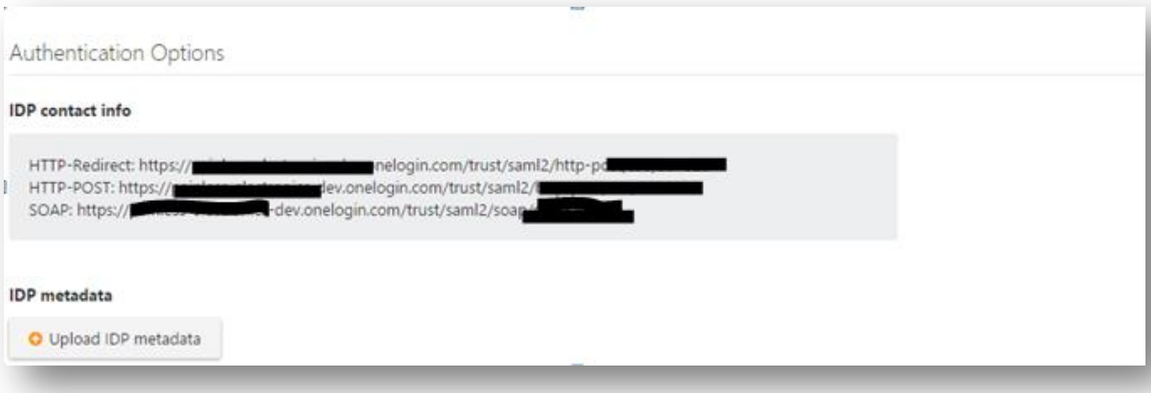
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="First Name" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="Last Name" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="Email" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="Username" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="MemberOf" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>

For Example:

9. Save the Metadata file.
10. Navigate to the **Mobility Admin Console > Settings > External IDP**.
11. Under IDP Type Select **SAML** and enter the FQDN (ie https://example.symantec.com) for SP partner ID and SP entity ID:



12. Click **Save**.
13. Under **IDP metadata** click **Upload IDP metadata** and browse to the metadata file created from step 9:



14. Configure each attribute as follows:

User name → Username
First name → First Name
Last name → Last Name
Email → Email
Group → memberOf

15. Enable the IDP and finally **save**.
16. Test the configuration using a browser in incognito mode (Ctrl + Shift + N) by browsing to the Mobility FQDN and clicking Signing using SSO.

Note: If no access policy is created the following error will appear after successfully logging into the console. Contact onelogin™ support for more information on how to assign applications to users: