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 <u>https://support.onelogin.com/hc/en-us/articles/202361690-Installing-an-Active-Directory-Connector-ADC-</u> or contact onelogin[™] support.

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

Symantec Mobility Suite Symantec Corporation SAML2.0

- 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:

 \odot

	<nameidformat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</nameidformat>
	<singlesignonservice binding="urn:oasis:names:tg:SAML:2.0:bindings:HTTP-Redirect" location="https://herearchites.com/trust/saml2/soap/s</td></tr><tr><td></td><td><saml:Attribute NameFormat=" name="First Name" urn:oasis:names:tc:saml:2.0:bindings:soap"="" urn:oasis:names:tg:saml:2.0:attrname-format:basic"="" urn:oasis:names:tg:saml:2.0:bindings:http-post"="" xmlns:saml="urn:oasis:names:tg:SAML:2.0:assertion"></singlesignonservice>
	<saml:attribute name="Last Name" nameformat="urn:oasis:names:tg:SAML:2.0:attrname-format:basic" xmlns:saml="urn:oasis:names:tg:SAML:2.0:assertion"></saml:attribute>
	<saml:attribute name="Email" nameformat="urn:oasis:names:to:SAML:2.0;attrname-format:basic" xmlns:saml="urn:oasis:names:to:SAML:2.0;assertion"></saml:attribute>
	<saml:attribute name="Username" nameformat="urn:oasis:names:tg:SAML:2.0;attrname-format:basic" xmlns:saml="urn:oasis:names:tg:SAML:2.0;assertion"></saml:attribute>
	<pre><saml:attribute name="MemberOf" nameformat="urn:oasis:names:jg:SAML:2.0;attrname_format:basic" xmlns:saml="urn:oasis:names:jg:SAML:2.0;assertion"></saml:attribute></pre>
	/TDD250/Dagatistat
1	IDESSONESCTIP.COT>

- 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 <u>https://example.symantec.com</u>) for SP partner ID and SP entity ID:

erver Configuration	
РР Туре	
SAML	•
ame	
Primary AD DC	
P partner ID	
https://exampletenant.smmglobal.net	
P entity ID	
https://exampletenant.smmglobal.net	
Download SP Metadata File	

12. Click Save.

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

Authentication Options		
DP contact info		
HTTP-Redirect: https:// HTTP-POST: https:// SOAP: https://	nelogin.com/trust/saml2/http-pd lev.onelogin.com/trust/saml2/l elogin.com/trust/saml2/soap	•
IDP metadata		
O Linload IDP metadata		

14. Configure each attribute as follows:

User name \rightarrow Username First name \rightarrow First Name Last name \rightarrow Last Name Email \rightarrow Email Group \rightarrow 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:

SOMETHING WENT WRONG You do not have access to this application. Please contact your administrator.	
You do not have access to this application. Please contact your administrator.	SOMETHING WENT WRONG
	You do not have access to this application. Please contact your administrator.