

Azure Active Directory (AD)

This document is designed to assist with the setup of SAML federation between Nile, leveraging Okta as a Service Provider (SP), and Azure Active Directory (AD) as the Identity Provider (IdP).

Overview

This document is designed to assist with the setup of SAML federation between Nile, leveraging Okta as a Service Provider (SP), and Azure Active Directory (AD) as the Identity Provider (IdP).

Requirements

- Administrator rights to Nile Portal.
- Administrator rights to Azure AD.
- The same Nile Portal administrator needs to be a user in Azure AD

Azure AD Enterprise Application Setup

1. Sign in to the Microsoft Azure portal: <https://portal.azure.com>
2. Click the portal menu icon in the top left, and select **Azure Active Directory**
3. In the left pane, under **Manage**, click **“Enterprise applications”**
4. On the Enterprise applications page, click **“New application”**

one

5. On the “Browse Azure AD Gallery”, click **“Create your own application”**

ptwo

6. In the **Name** field, enter **“Nile”** or your preferred name for the application.

Select the radio button

“Integrate any other application you don’t find in the gallery (non-gallery)”.

pic

Click **Create**.

7. On the Nile **Overview** page:

three

Click **“Assign users and groups”**.

8. On the **Users and groups** page:

four

Click on **“Add user/groups”**.

9. **Select** user(s) to assign to the application:

five

Click **Assign**.

10. Click **Single sign-on** in the left menu

six

In **Select a single sign-on method**, click **SAML panel**.

11. On the **Set UP Single Sign-On with SAML** page, in the **Basic SAML Configuration** section

seven

Click **Edit**

12. Enter temporary values for **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** to generate the certificate for download.

eight

Click on **Save** (top bar) to save the changes.

13. Back on the **Set UP Single Sign-On with SAML** page, in the **Attributes & Claims** section, click Edit:

14. The **Attributes & Claims page** is presented

nine

Edit each claim one by one as follows:

a. Click on the user.mail claim line to open it for editing and delete the namespace URI. Change the Name to "mail".

eleven

Click **Save**

b. Similarly edit user.givenname by deleting the namespace URI and renaming givenname to **firstName**

twelve

Click **Save**

c. Edit user.userprinciplename by deleting the namespace URI.

thir

Click **Save**

d. Edit user.surname by deleting the namespace URI and renaming surname to **lastName**

fourteen

Click **Save**

e. Add a new claim for the **mobile** attribute:

fifteen

Click **Save**

f. Add a new claim for the **displayName** attribute

sixteen

Click **Save**

g. Add a group claim for the **memberOf** attribute as illustrated

seventeen

Click **Save**

15. Download the 'SAML Signing Certificate' (to be uploaded later to the Nile Portal when adding Azure AD as a provider):

Azure AD Identifier:

<https://sts.windows.net/f8b44d9b-778d-47da-9391-6249440b17a9/>

Login URL:

<https://login.microsoftonline.com/f8b44d9b-778d-47da-9391-6249440b17a9/saml2>
nine

Make a note of the **Azure AD Identifier** and the **Login URL**

(to be used on the Nile Portal provider setup):

eighteen

16. To be done after completing the next section:

Update the 'Identifier' and 'reply URL' in the 'Basic SAML Configuration' section of the Nile app from the metadata.xml file downloaded after completing the Nile Portal provider setup in the next section.

icon

NOTE

Note: After Azure AD is made an identity provider in the next section, the actual values for Identifier and Reply URL can be updated.

Nile Portal Identity Provider Setup

1. Login to the Nile Portal (<https://www.nile-global.cloud>) as an administrator.

2. Go to **Settings -> Global Settings -> Identity**

nine

Click on **ADD A NEW PROVIDER:**

3. Fill up the fields in the new provider window as follows:

Name: An appropriate string to name the provider.

IdP Issuer URI: Azure AD SAML app Identifier noted in step 15 of the previous section.

IdP SSO URL: Azure AD SAML app Login URL noted in step 15 of the previous section.

Destination URL: Azure AD SAML app Login URL noted in step 15 of the previous section.

SELECT CERTIFICATE: Upload the 'SAML signing certificate downloaded in step 15.

Add a new provider

General Settings

Name*

MMOUSSA Azure AD

Protocol

SAML2

SAML Settings

IdP Issuer URI*

Azure AD identifier

<https://sts.windows.net/f8b44d9b-778d-47da-9391-6249440b17a9/>

IdP SSO URL*

Azure AD Login URL

<https://login.microsoftonline.com/f8b44d9b-778d-47da-9391-6249440b>

Destination URL*

Azure AD Login URL

<https://login.microsoftonline.com/f8b44d9b-778d-47da-9391-6249440b>

SELECT CERTIFICATE

691fed9d-e402-4055-90f8-beee5839d02f

Uploaded Cert

CANCEL

SUBMIT

Click the **SUBMIT** button to save the changes and add the new Azure AD provider

Click the **METADATA** button to download the file.

4. Open the downloaded file with a text editor, and search for the 'entityID' and 'Location' strings.

NOTE: Save the **entityID** and **Location** values. Those values are used later to complete the Azure AD enterprise application configuration

For illustration purposes only, the values used in this example:

entityID:

<https://www.okta.com/saml2/service-provider/spchehmcqiyIhitxumru>

Location:

<https://login.u1.nile-global.cloud/sso/saml2/0oah83qpuT5TRtMY5d7>

5. Go back to the enterprise app (Nile) created on Azure AD to edit the 'Basic SAML Configuration':

Click on **Edit**

6. Replace the temporary values of **Entity ID** and **Reply URL** with the values of **entityID** and **Location** collected earlier in step 4:

tthree

Click the Save button to save the changes and thus complete the Azure AD enterprise app (Nile) configuration.

7. Verify your changes:

tfour

icon

NOTE

Note: it is assumed that the administrator credentials belong to a domain in Azure AD. This domain would already be an Allowed domain on the Nile Portal.

Note: The Azure AD provider configuration is completed for SSO users to gain Internet access after signing-in using their AD credentials.

Group Mapping

The group mapping is used to map a designated Azure AD admin group to the Nile Portal Administrator group. A **Group** rule is needed and can be added on the Nile Portal as illustrated in the following steps.

The example that follows maps an AD admin group “NileAdmin” to the Nile Portal Administrator group, and a ‘NileMonitor’ group to the Nile Portal Monitor Admin group

1. Click the **Group Rules** tab:

tfive

2. Click “ADD GROUP MAPPING”:

tsix

Add the group name to the “Friendly name” and “External name” fields.

Press SAVE.

3. Click the **ADD GROUP RULE**:

tseven

4. Add two group rules to map AD users members of two AD groups (NileAdmin and NileMonitor in this example) to the Nile Portal Administrator and Monitor groups respectively, by evaluating the ‘memberOf’ attribute value coming in the SAML assertion from Azure AD:

Name: An appropriate rule name

Mapping Value: Azure AD Group object ID

Assigned groups: Select the appropriate Nile group from the drop-down list

teight

Click SAVE.

tnine

Click SAVE.

5. After adding the two rules, this pane is displayed:

thirty

6. Activate the two rules by clicking on the **INACTIVE** button to change the state to **ACTIVE**:

thir

PSK-SSO SSID Setup

1. Log back in to the Nile Portal

1. Go to the **Settings ? Segments** page to create the PSK SSO Segment:

a. Click on the ? to add a new segment

b. Type a meaningful segment name (Demo PSK SSO)

ttwo

c. Go to the 'Service area' tab to select the DHCP server and scope:

tthree

d. Go to the 'Advanced' tab and check off the 'URL Allow List' and click on to add the following DNS names one at a time:

azure.microsoft.com

amp.azure.net

dev.azure.com

***.amcdn.msftauth.net**

***.trafficmanager.net**

***.omegacdn.net**

***.azureedge.net**

***.aadcdn.msftauth.net**

***.msidentity.com**

***.dev.azure.com**

***.aadcdn.msauth.net**

tfour

e. Click SAVE to complete the addition of the new segment

3. Go to the **Settings ” Wireless** page to create the PSK SSO SSID:

1. Select the '**Personal**' radio button

2. Type the desired SSID name

3. Select the **Security** option

4. Check off the '**Enable SSO**' box

5. Enter the Pre-shared key

6. Select the previously created PSK-SSO segment

tfive

g. Click the SAVE button to complete the PSK-SSO SSID creation.