NetIQ Access Manager is compatible with Office 365 and provides single sign-on access to Office 365 services. Single sign-on access is supported for web-based clients such as Exchange Web Access and SharePoint Online. This means that you can use your existing LDAP credentials to access any of the Office 365 services without having to remember multiple passwords or sign in multiple times for accessing different services. All that you need to do is sign in once with an existing password and you are granted access to all the services.

This single sign-on access is achieved by implementing federated authentication through SAML 2.0 protocol. In this scenario, the Access Manager is configured as an identity provider and allows Office 365 to trust it for authentication. Office 365 is configured as a service provider that consumes authentication assertions from Access Manager. A trust model is set up for Access Manager and the Office 365 to communicate with each other.

- Section 1.1, “Configuring Access Manager,” on page 1
- Section 1.2, “Configuring the Service Provider Office 365,” on page 4

1.1 Configuring Access Manager

- Section 1.1.1, “Prerequisite,” on page 1
- Section 1.1.2, “Adding the Office 365 Metadata,” on page 1
- Section 1.1.3, “Configuring Federation Settings,” on page 2
- Section 1.1.4, “Configure Attributes,” on page 3

1.1.1 Prerequisite

Ensure that SAML 2.0 is enabled on the Identity Provider.

1 In the Administration Console, click Devices > Identity Servers > Edit.
2 In the Enabled Protocols section, verify if SAML 2.0 is selected.

1.1.2 Adding the Office 365 Metadata

1 In the Administration Console, go to Identity Server. Select the Identity Server.
2 Select SAML 2.0 > New Service Provider.
3 Specify the Source as Metadata text. Enter a name to identify the identity provider configuration.
4 In Text, copy paste the following metadata.
<?xml version="1.0" encoding="utf-8"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="urn:federation:MicrosoftOnline">
  <SPSSODescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    WantAssertionsSigned="true">
    <NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </NameIDFormat>
    <NameIDFormat>
      urn:mace:shibboleth:1.0:nameIdentifier
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:transient
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
    </NameIDFormat>
    <AssertionConsumerService isDefault="true" index="0"
    <AssertionConsumerService index="1"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
      Location="https://login.microsoftonline.com/login.srf"/>
  </SPSSODescriptor>
</EntityDescriptor>

**IMPORTANT:** The SAML 2.0 Office 365 metadata can also be accessed from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml.

In this, the AssertionConsumerService element appears at the start of the XML definition. If this metadata is pasted in the same format, it leads to an XML malformed error in the Identity Server.

To resolve this, move the AssertionConsumerService element (inclusive of opening and closing XML tags to appear before the </SPSSODescriptor> XML tag.

5 Click Next to confirm the certificates.
6 Click Finish to save the metadata changes.

### 1.1.3 Configuring Federation Settings

1 In the Administration Console, go to Identity Server. Select the Identity Server.
2 Select SAML 2.0. Select the service provider you created.
3 Select the Authentication Response.
4 Change the default value of Binding from Artifact to Post.
5 Make sure that the Name Identifier Format is Persistent. Deselect Transient.
6 Make sure that the Default value is Not Specified.
1.1.4 Configure Attributes

The following attributes in Access Manager are required to locate the shadow account in Office 365.

- **Immutable ID**: Office 365 requires an unique identifier for each user in the user store. This unique identifier attribute is sent for each federated login to Office 365 in the SAML2.0 NameID assertion. From 3.2 SP1 onwards, this unique identifier is included in the assertion sent by Access Manager.

  This identifier should not be changed over the lifetime of the user being in your system.

- **Office 365 User ID**: Office 365 requires you to sent the Office 365 User ID as IDPEmail attribute. To configure this, complete the following steps
  
  1. In the Administration Console, click *Identity Server > SAML 2.0*. Select the Office 365 Service Provider you configured.
  
  2. Select *Attributes*.
  
  3. Select a new *Attribute set*. Use None as the template.
  
  4. Add an Attribute mapping to establish a relation between the Local attribute and Remote Attribute. In Local Attribute, select Ldap Attribute:mail [LDAP Attribute Profile]. Specify the Remote Attribute as IDPEmail.
5. Make sure that this attribute is moved from the Available list to the Send with authentication list.

1.2 Configuring the Service Provider Office 365

- Section 1.2.1, “Prerequisite,” on page 4
- Section 1.2.2, “Establishing Trust Between Identity Provider and the Service Provider,” on page 5

1.2.1 Prerequisite

Ensure that you have Windows Powershell installed. This tool helps you manage many Microsoft Office 365 administrative tasks such as user management and domain management.

1.2.2 Establishing Trust Between Identity Provider and the Service Provider

Office 365 domains are federated using the Microsoft Online Services Module. You can use the Microsoft Online Services Module to run a series of cmdlets in the Windows PowerShell command-line interface to add or convert domains for single sign-on.

Each Active Directory domain that you want to federate using NetIQ Access Manager must either be added as a single sign-on domain or converted to be a single sign-on domain from a standard domain. Adding or converting a domain sets up a trust between NetIQ Identity Provider and Office 365.

To convert an existing standard domain to a federated domain, execute the following steps:

1. Open the Microsoft Online Services Module.
2. Run $cred=Get-Credential. Enter your cloud service administrator account credentials.
3. Run Connect-MsolService -Credential $cred. This cmdlet connects you to the cloud service. Creating a context that connects you to the cloud service is required before running any of the additional cmdlets installed by the tool.
4. For example: If the name of the domain you are converting to a single sign-on domain is acme.com, and the Base URL of the Identity Server is https://namtest.com:8443/nidp/, execute the following commands at the powershell prompt:

   $dom = “acme.com”
   $url = “https://namtest.com:8443/nidp/saml2/sso”
   $ecpUrl = “https://namtest.com:8443/nidp/saml2/sso”
   $uri = “https://namtest.com:8443/nidp/saml2/metadata”
   $logouturl = “https://namtest.com:8443/nidp/saml2/slo”
   $cert = “MIIFLDCCBBSgAwIBAgIkA........ww19yUoDRIo=”

   NOTE: Value of $cert indicates the signing certificate of Identity Server. Make sure that all the new line characters are removed from the certificate.

5. Use the following cmdlet to update the settings of the single sign-on domain:


1.3 Verifying Single Sign-On Access

You need at least one user in Office 365 to verify that single sign-on is set up. If you have an existing user, ensure that the Immutable ID matches with the GUID of the Access Manager user.

Existing Office 365 user:

For instance if your user store is eDirectory and want to retrieve the GUID of an existing Access Manager user, execute the following command on the eDirectory server terminal:

   ldapsearch -D cn=<context> -w <password> -b <search base> cn=<name of the user> GUID | grep GUID

The Office 365 user must be created with this GUID as the Immutable ID.
Creating a new Office 365 user:

Run the following command in Powershell to create an Office 365 user:

```powershell
new-msolUser -userprincipalName user1@domain name -immutableID immutableID of user1 - lastname lastname of user 1-firstname user1 -DisplayName "user1 users" - BlockCredential $false -LicenseAssignment testdomain:ENTERPRISEPACK -usageLocation IN -Password password of the user.
```

This command creates user1 in Office 365.

To verify that single sign-on has been set up correctly, perform the following procedure in a machine that has not added to the domain.

2. Log in with your corporate credentials (For example: user1@acme.com)
3. If single sign-on is enabled, the password field is dimmed. You will instead see the following message: You are now required to sign in at <your company>.
4. Select the Sign in at your company link.
   
   If you are able to sign in without errors, then single sign-on is successfully set up.