Configuring Single Sign-On For Office 365 Services

docsys (en) 20 February 2013

NetIQ Access Manager is compatible with Microsoft 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 to access different services. You just need to sign in once with an existing password and Access Manager grants you 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 Office 365 to communicate with each other.

NOTE: Access Manager does not supports single sign-on to Microsoft Lync.

1 Configuring Access Manager

1.1 Prerequisite

Enable SAML 2.0 in Access Manager.

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

1.2 Adding Office 365 Metadata

1. In the Administration Console, go to *Identity Server* and then select an 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 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"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
login.microsoftonline.com/login.srf"/>
    <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: You can also access the SAML 2.0 Office 365 metadata from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml.

Here, 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) before the `</SPSSODescriptor>` XML tag.

5 Click *Next* to confirm the certificates.

6 Click *Finish* to save the metadata changes.

1.3 Configuring Federation Settings

1 In the Administration Console, go to *Identity Server* and select an Identity Server.

2 Select *SAML 2.0* and then select the service provider you created.

3 Select *Authentication Response*.

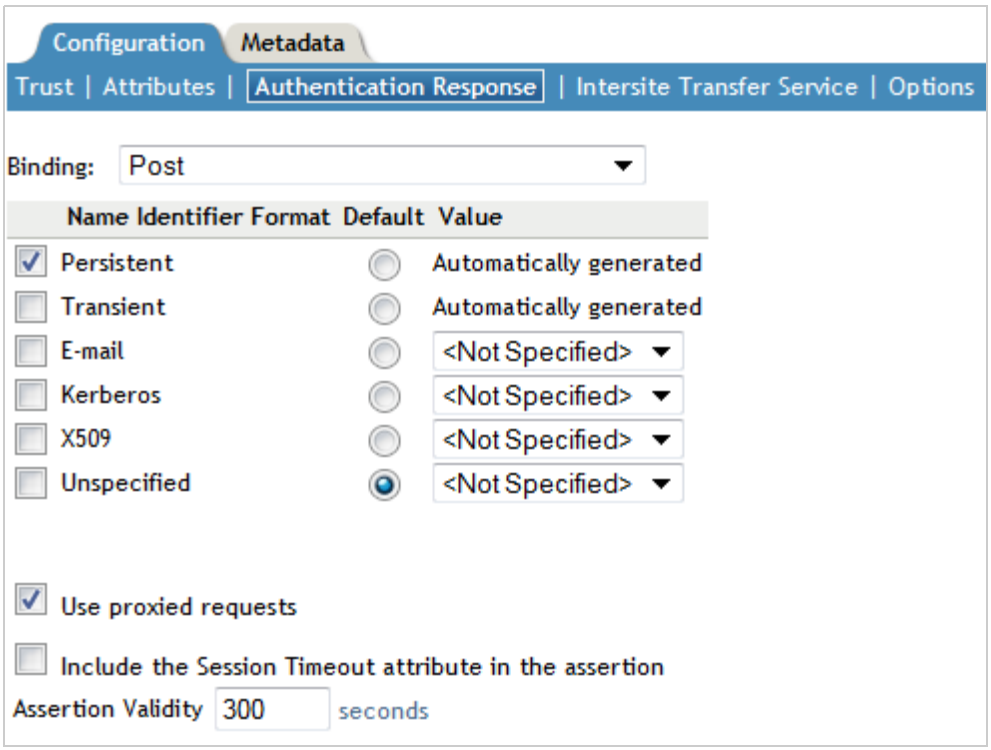
4 Change the default value of *Binding* from Artifact to Post.

5 Ensure that *Name Identifier Format* is Persistent. Deselect Transient.

6 Ensure that *Default value* is Not Specified. Do not select any value from the drop-down list.

This ensures that Access Manager does not automatically generate a random value for NameID. The NameID value is created based on the GUID value of the Access Manager user and is later used as the ImmutableID of the Office 365 user.

IMPORTANT: The GUID (global unique identifier) value differs depending on the user store of the user. For example, the GUID of an user on eDirectory will be different from the GUID of an user on Active Directory.



1.4 Configuring Attributes

The shadow account in Office 365 needs the following attributes:

- **ImmutableID:** Office 365 requires a 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, Access Manager includes this unique identifier in the assertion.

  IMPORTANT: The unique identifier should not be changed until the user exists in the system.

  The default value of ImmutableID is GUID. You can configure an existing attribute or a custom attribute to be sent as an unique identifier.

  Complete the following steps to configure an attribute:![bug 800158]

  1. Add the custom attribute in the office365 attribute set. If you want to configure an existing attribute, start from the step 2.
     a. In the Administration Console, click *Identity Server* > *Shared Settings* > *Custom Attributes*.
     b. In the *LDAP Attribute Names* section, click New. Specify a name for the attribute.

        If you want the attribute to return raw data instead of binary data, select *64-bit Encode Attribute Data*.

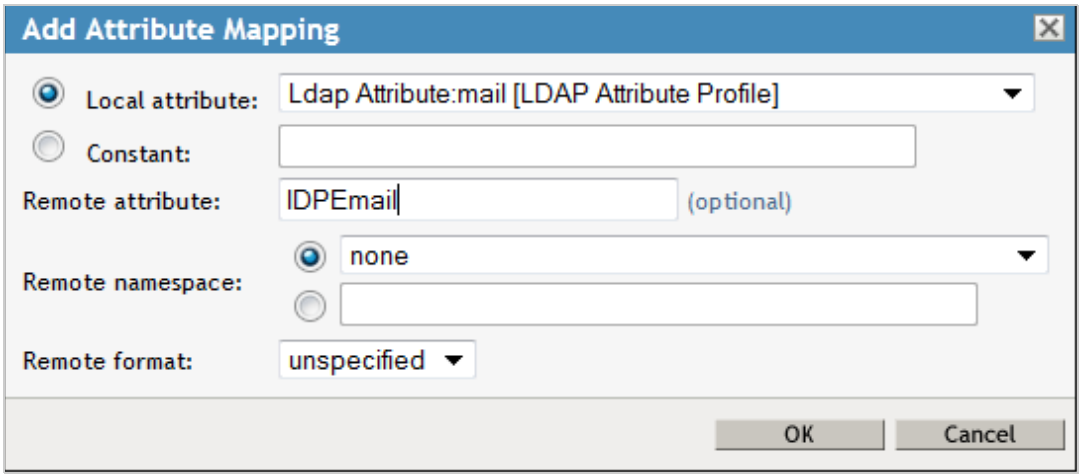
        For more information about attribute data encoding, see Section 6.4.2, "Creating LDAP Attribute Names," on page 137.
  2. Navigate to *Identity Server* > *Edit* > *SAML 2.0* and click the Office 365 service provider you configured.
  3. Select *Options*.
  4. Click *New* and specify the following:

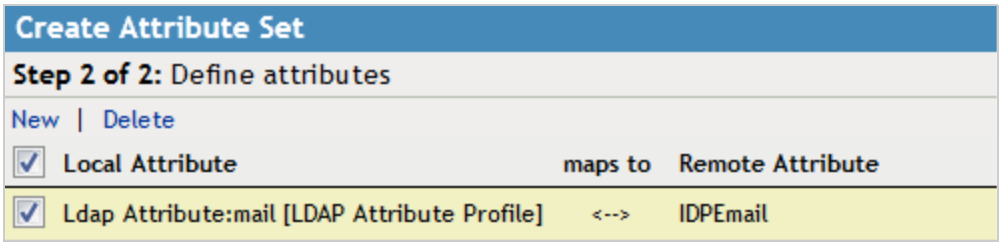
Property Name: SAML2_OFFICE365_NAMEID_ATTRIBUTE_NAME

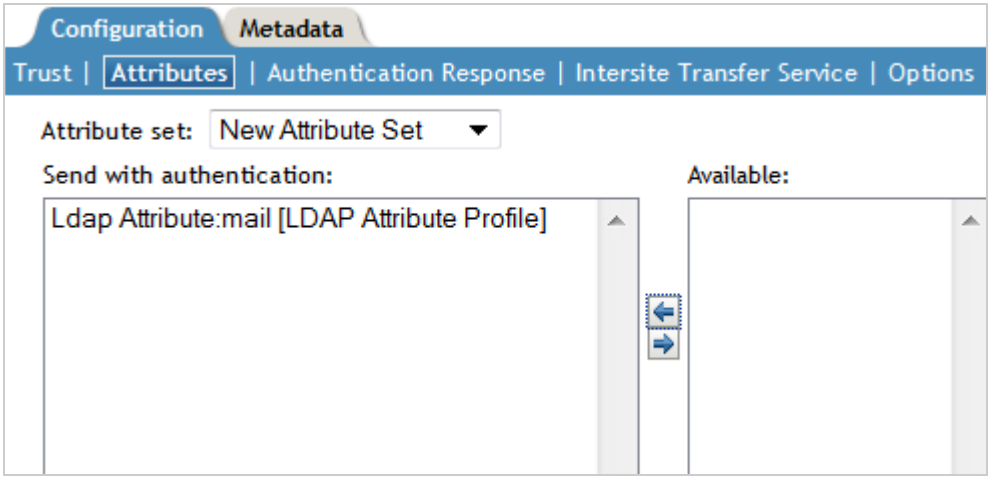
Property Value: Attribute name that you want to be sent as NameID in the assertion.

5. Update the Identity Server.

- **Office 365 User ID:** You must send the Office 365 User ID as an IDPEmail attribute. Complete the following steps to configure this attribute:
  1. In the Administration Console, click *Identity Server* > *SAML 2.0* and then 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].







5. Specify *Remote Attribute* as IDPEmail.
6. Ensure that LDAP Attribute:mail [LDAP Attribute Profile] attribute is moved from the *Available* list to the *Send with authentication* list.

2 Configuring Office 365

2.1 Prerequisite

- Install Windows Powershell on a Windows server. This tool helps you manage many Microsoft Office 365 administrative tasks such as user management and domain management. Ensure that this Windows server does not have the Active Directory Federation Service 2.0 snap-in installed.

  You can download the tool from Install Windows Powershell (http://technet.microsoft.com/en-us/library/jj205464.aspx).
- At least one user must already exist in Office 365 with an ImmutableID matching the GUID of Access Manager. To verify if the GUID of Access Manager user matches the Immutable ID of an Office 365 user, see “Existing Office 365 user:” on page 7.

  The users are not automatically provisioned during login.

2.2 Establishing Trust Between an Identity Provider and a Service Provider

You can configure Office 365 domains federations by 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 by using 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 Access Manager and Office 365.

To add a domain to Office 365, perform the following steps:

1. Log in to Office 365 as an administrator.
2. On the Admin page, click *Management* > *Domains* > *Add a domain*.
3. Specify the domain name that you want to add.
4. Click *Next*.
5. Verify the domain name.

   For more information about how to verify a domain, see Verify your domain and change name servers.
6. Select appropriate services.
7. Configure the DNS records on the domain registrar for other services.

NOTE: Do not configure the new domain to the primary domain. Using the `Set-MsolDomainAuthentication` command to set the domain as a federated domain results in an error if the domain is the default domain.

For more information, see Add a domain to Office 365.

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

1. Open the Microsoft Online Services Module from the Start menu.
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.

   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: The value of $cert indicates the signing certificate of Identity Server. Ensure that all the new line characters are removed from the certificate.

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

   ```
   Set-MsolDomainAuthentication -FederationBrandName $dom -Authentication
   Federated -PassiveLogOnUri $url -SigningCertificate $cert -IssuerUri $uri -
   ActiveLogOnUri $ecpUrl -LogOffUri $logouturl -PreferredAuthenticationProtocol
   SAMLP
   ```

2.3 Configuring Desktop Email Client to Access Office 365 Emails

You can configure your desktop email client to access Office 365 emails. The email clients must use a basic authentication and a supported exchange access method such as IMAP, POP, Active Sync, and MAPI.

The following is the list of email clients supported for this configuration:

- Microsoft Outlook 2007
- Microsoft Outlook 2010
- Thunderbird 8 and 9
- The iPhone (various iOS versions)
- Windows Phone 7

Complete the following steps:

1. Complete Step 1 through Step 4 in Section 2.2, “Establishing Trust Between an Identity Provider and a Service Provider,” on page 5.

   In Step 3, change $ecpUrl to `https://namtest.com:8443/nidp/smal2/sso`.

   This URL should be https with valid certificate.

   Modify the ecp url parameter by running this command:

   ```
   Set-MsolDomainFederationSettings -DomainName namtest.com -ActiveLogOnUri
   "https://namtest.com/nidp/saml2/sso" -preferredauthenticationprotocol SAMLP
   ```

   You can download the email client from the download section of office 365.

2 Create a new email account in your email client and enter your Office 365 email ID.

NOTE: Configure Outlook related DNS settings before using email clients. You can configure these settings after adding the domain on the Office 365 port page.

3 The system prompts for specifying the basic authentication. Enter Access Manager credentials.

The email account is created after successful authentication.

NOTE: While logging in to the new email account, enter Access Manager credentials.

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 you 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
```

Create an Office 365 user 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:

```
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 "two letter country code[example: US,IN,DE,BE,GB etc]" -Password
"password of the user".
```

NOTE: Remove commas from values before running the command.

This command creates user1 in Office 365.

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

1 Go to Microsoft Online Services (http://login.microsoftonline.com/)

2 Log in with your corporate credentials. (For example : `user1@acme.com`)

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>`.

3 Select the *Sign in at your company* link.

If you are able to sign in without errors, single sign-on is set up successfully.

4 Troubleshooting

- Section 4.4, “Microsoft Online Services Sign-In Assistant Installation Fails If Microsoft Office Professional Plus Is Installed,” on page 9
- Section 4.5, “Active Profile Authentication Fails for Microsoft Exchange Clients,” on page 9

The following list includes few useful resources for troubleshooting:

- http://community.office365.com/en-us/tools/troubleshooting.aspx
- https://www.testexchangeconnectivity.com/
- http://office.microsoft.com/en-us/office365-suite-help/troubleshoot-sign-in-to-office-365-HA103737871.aspx
- http://support.microsoft.com/kb/2404500

4.1 Issue in Setting Up a Domain for Federation

If you try to set a primary domain for federation by running the `Set-MsolDomainAuthentication` command, it throws the following error:

```
Set-MsolDomainAuthentication: You cannot remove this domain as the default domain
without replacing it with another default domain. Use the Set-MsolDomain cmdlet to
set another domain as the default domain before you delete this domain.
```

To fix this issue, change the default domain by performing the following steps:

1. In the Office 365 portal, click *Organization Name* on the Admin page.
2. Click *Edit*.
3. Select a new default domain.

4.2 Issues with the Directory Synchronization Tool

- If the installation of the Directory Synchronization tool fails, check the Event Viewer. Installation may fail if the Microsoft Online Service Sign-In Assistant is already installed on the system.
- If you require to uninstall the Directory Synchronization tool, log off

  and then login. Otherwise, you may encounter issues.
- If the Directory Synchronization tool is slow, increase RAM of the server.

4.3 SSO to MicroSoft Services Fails

SSO fails at Microsoft with this error:

```
Your organization could not sign you in to this service
```

Perform the following steps to fix this issue:

- Verify that the attributes are configured properly. See Section 1.4, “Configuring Attributes,” on page 3.

  You can also use the SAML tracer plug-in Firefox to review the SAML assertion sent to office365.
- Verify that federation settings are using the `Get-MsolDomainFederationSettings -DomainName <YOUR DOMAIN>` command.

4.4 Microsoft Online Services Sign-In Assistant Installation Fails If Microsoft Office Professional Plus Is Installed

Manually install Microsoft Online Services Sign-In Assistant, if its installation fails after installing Microsoft Office Professional Plus with this message:

```
“The Microsoft Online Services Sign In Assistant has experience an error. The error
must be resolved before your subscription for this product can be verified. To
retry subscription verification, first resolve error message 800704DD or try to
manually install the Microsoft Online Services Sign In Assistant....”
```

You can download the installer from MicroSoft Download Center.

After installation is complete, relaunch the service to verify your Office 365 license. For more information, see Reactivate subscription license by using Osaui.exe.

4.5 Active Profile Authentication Fails for Microsoft Exchange Clients

If the active profile authentication fails for Microsoft Exchange (Outlook) clients, verify that the necessary DNS records have been added to your DNS. For more information, see Create DNS records at any DNS hosting provider for Office 365.