Single Sign On for Office 365 with NetScaler

Deployment Guide

This deployment guide focuses on defining the process for enabling Single Sign On into Microsoft Office 365 with Citrix NetScaler.
Table of Contents

Introduction 3
Configuration details 4
NetScaler features to be enabled 4
Solution description 5
Part 1: Configure Office 365 5
Part 2: Configure NetScaler 10
  Configure LDAP domain authentication 10
  To Configure the SAML IDP Policy and Profile 13
  To Configure your AAA Virtual Server 15
Validate the configuration 16
Troubleshooting 17
  Additional Resources 20
Conclusion 21
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications.

Microsoft Office 365 is a suite of cloud-based productivity and collaboration applications provided by Microsoft on a subscription basis. It includes Microsoft’s popular server-based applications such as Exchange, SharePoint, Office and Skype for Business. The apps are widely used by SMBs and enterprise customers alike to enable their business without significant capital investments.

Introduction

This guide focuses on enabling Microsoft Office 365 single sign on with Citrix NetScaler.
**Configuration Details**
The table below lists the minimum required software versions for this integration to work successfully. The integration process should also work with higher versions of the same.

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Required Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler</td>
<td>11.0, Enterprise/Platinum License</td>
</tr>
</tbody>
</table>

**NetScaler features to be enabled**
The essential NetScaler feature that needs to be enabled is explained below.

- **AAA-TM (Authentication, authorization and auditing - Traffic Management)**

**AAA-TM**
The AAA feature set controls NetScaler authentication, authorization, and auditing policies. These policies include definition and management of various authentication schemas. NetScaler supports a wide range of authentication protocols and a strong, policy-driven application firewall capability.
Solution description

Enabling SSO for Office 365 with NetScaler consists of two parts – configuring the Office 365 portal and the NetScaler appliance. Office 365 should be configured to use NetScaler as a third party SAML IDP (Identity Provider). The NetScaler is configured as a SAML IDP by creating the AAA Virtual Server that will host the SAML IDP policy.

The following instructions assume that you have already created the appropriate external and/or internal DNS entries to route authentication requests to a NetScaler-monitored IP address, and that an SSL certificate has already been created and installed on the appliance for the SSL/HTTPS communication. This document also assumes that a Microsoft Office 365 account has been created, the relevant domain has been added and domain verification for the same has been completed.

Part 1: Configure Office 365
Step 1: Confirm Microsoft Office 365 Portal Settings

1. In a web browser, log in to your Office 365 administration portal at https://login.microsoftonline.com using an account with administrative rights.

2. Confirm that the domain that is in use by your company for Office 365 has been verified by navigating to Domains in the left hand navigation bar.

Select the Domain Settings options in the Manage Domains section shown on the right after selecting the appropriate domain in the list –

![Office 365 admin center](https://login.microsoftonline.com)

- **Domain name**
- **Status**
  - Setup complete
  - Setup complete
  - Setup complete

Set as default
Step 2: Setup Federation Settings for Windows Azure AD

In order to complete single sign on configuration, you will need to complete the following steps –

1. Assuming that a local AD (Active Directory) server is used for validation of user credentials, the Microsoft Azure Active Directory Connect tool (formerly called DirSync) will need to be installed on a domain-joined computer. This tool is essential for configuring SSO for Office 365.

2. Complete the configuration for federation/establishing trust between Azure AD (Azure Active Directory) and NetScaler using the Azure AD Module for Windows Powershell

3. Setup Directory Synchronization using the Azure AD Directory Connect Tool to ensure that users in the local AD are replicated in Azure AD.

Before proceeding, you should verify that you have the signing certificate that NetScaler will use to sign the assertion. To get the verification certificate from the NetScaler appliance, follow these steps:

1. Login to your NetScaler appliance, then select the Configuration tab.

2. Select Traffic Management > SSL

3. Select Manage Certificates / Keys/ CSR's under the Tools section on the right as shown below

4. From the Manage Certificates window, browse to the certificate you will use for your AAA Virtual Server. Select the certificate and choose the Download button. Save the certificate to a location of your choice.
Step 2: Setup Federation Settings for Windows Azure AD

In order to complete single sign on configuration, you will need to complete the following steps –

The following tools should be installed before proceeding:

- REQUIRED: The Azure AD Module for Windows PowerShell is essential for this deployment. This module enables cmdlets to be run that completes the Azure AD administrative and configuration tasks for this deployment. Install the Microsoft Online Services Sign-In Assistant for IT Professionals RTW, then install the Azure Active Directory Module for Windows PowerShell (64-bit version). For the 32-bit version of the Azure Active Directory Module tool, refer to this link.

  Note: Support for the 32-bit version of this tool has ended, but it may still be used for this deployment. Additional information about this tool is available at the source link.

- OPTIONAL: Windows Azure AD Connect enables synchronization of directories between Azure AD and the local Active Directory. This tool simplifies user account setup in Office 365, eliminating the need to add them individually. For more information on directory synchronization using Azure AD Connect, refer to https://azure.microsoft.com/en-in/documentation/articles/active-directory-aadconnect/

  Note: Azure AD Connect is an optional installation, and this integration can be completed without it. However, in this instance you will need to ensure that the Azure AD tenant for your Office 365 account has all user accounts corresponding to the ones in your Active Directory (the user account login should be the same as the UPN for the user accounts in the local Active Directory)

PowerShell Commands

These commands are executed in the PowerShell after completing the Azure AD Directory Module installation. <your domain name> here refers to the domain name that your accounts are bound to – for example, for a user UPN (User Principal Name) of user1@company.com, <your domain name> will be “company.com.”

Step 1: Connect-MsolService will prompt for user credentials, provide an Office 365 administrative user’s credentials.

PS C:\Windows\system32> Connect-MsolService

Note: Steps 2 and 3 are necessary only if your domain has not already been added to Office 365. If it is already setup, you may skip to step 4.

Step 2: After connecting to the MS Online (Office 365) service, create a new domain. Ensure that the domain name matches with an existing public DNS record.

PS C:\Windows\system32> New-MsolDomain -name adfsns.citrix.com
Step 3: Get the DNS record information for the new domain with the following command:

PS C:\Windows\system32> Get-MsolDomainVerificationDns -DomainName <your domain name>
PS C:\Windows\system32> Confirm-MsolDomain -DomainName <your domain name>

Step 4: Provide a public certificate that will be used in SAML Signing. This is the certificate that was downloaded from the NetScaler device and bound to the AAA vserver.

PS C:\Users\administrator.CTXNS\Desktop\Certificates> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("<path to certificate, for example: C:\NS-IDP-Cert.cer>")
PS C:\Users\administrator.CTXNS\Desktop\Certificates> $certData = [system.convert]::tobase64string($cert.rawdata)

Step 5: Create variables and assign domain name and federation brand name.

The domain variable value should match with the domain created in Step 2.

PS C:\Users\administrator.CTXNS\Desktop\Certificates> $dom = "<your domain name>"
PS C:\Users\administrator.CTXNS\Desktop\Certificates> $fedBrandName = "<company brand name, for example: Citrix India>"

Step 6: Provide the URL for the SAML IdP (Identity Provider), in this case the FQDN (fully qualified domain name) for the AAA vserver that the SAML policies on the NetScaler appliance will be bound to. When NetScaler is acting as a SAML IdP the URL will be <aaavserver domain name>/saml/login.

Note: In the case of NetScaler Gateway acting as a SAML IDP the URL will be https://<NS Gateway domain name>/saml/login

In the case of AAATM, the SAML IDP URL will be https://<aaavserver domain name>/saml/login.

PS C:\Users\administrator.CTXNS\Desktop\Certificates> $url = "https://<aaavserver domain name>/cgi/tmlogout"
PS C:\Users\administrator.CTXNS\Desktop\Certificates> $uri = "https://<aaavserver domain name>/saml/login"
PS C:\Users\administrator.CTXNS\Desktop\Certificates> $ecpUrl = "https://<aaavserver domain name>/saml/login"

Note: The ECP protocol URL has been set to the same value as the login URL as there is no unique URL for ECP support.
Step 7: This is the critical step for configuration of SAML authentication in the Office 365 deployment.

```
PS C:\Users\administrator.CTXNS\Desktop\Certificates> Set-MsolDomainAuthentication -DomainName $dom -federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $url -SigningCertificate $certData -IssuerUri $uri -ActiveLogOnUri $ecpUrl -LogOffUri $url -PreferredAuthenticationProtocol SAMLP
```

If the domain being used has already been federated (for example, with ADFS), it needs to be converted to a standard domain before it can be used for federated authentication with NetScaler. Use the following command to convert it to a standard domain before setting new authentication parameters.

```
Convert-MsolDomainToStandard -DomainName <your domain name> -SkipUserConversion: $true -PasswordFile C:\userpasswords.txt
```

The userpasswords.txt file can be any path on the local hard drive; this command will dump all user passwords from the previously federated setup into this text file for reference. This will complete single sign-on configuration for Office 365 with NetScaler.

Step 8: Convert the Domain to Federated.

```
PS C:\Users\administrator.CTXNS\Desktop\Certificates> Convert-MsolDomainToFederated -DomainName <your domain name>
```

If the command is successful, “Successfully updated <your domain name> domain” is shown at the PowerShell prompt.

Verify the federation settings by using the command Get-MsolDomainFederationSettings and confirm that the details are shown as entered (the command will prompt you to provide the domain name, provide <your domain name> as the value).
Part 2: Configure NetScaler

The following configuration is required on the NetScaler appliance for it to be supported as a SAML identity provider for Microsoft Office 365:

- LDAP authentication policy and server for domain authentication
- SSL certificate with external and internal DNS configured for the FQDN presented by the certificate (Wildcard certificates are supported.)
- SAML IDP policy and profile
- AAA virtual server

This guide covers the configuration described above. The SSL certificate and DNS configurations should be in place prior to setup.

Configuring LDAP domain authentication

For domain users to be able to log on to the NetScaler appliance by using their corporate email addresses, you must configure an LDAP authentication server and policy on the appliance and bind it to your AAA VIP address. (Use of an existing LDAP configuration is also supported)

1. In the NetScaler configuration utility, in the navigation pane, select Security > AAA – Application Traffic > Policies > Authentication > Basic Policies > LDAP.

2. To create a new LDAP policy: On the Policies tab click Add, and then enter Office365_LDAP_SSO_Policy as the name. In the Server field, click the ‘+’ icon to add a new server. The Authentication LDAP Server window appears.

3. In the Name field, enter Office365_LDAP_SSO_Server.

4. Select the bullet for Server IP. Enter the IP address of one of your Active Directory domain controllers. (You can also point to a virtual server IP for the purpose of redundancy if you are load balancing domain controllers)

5. Specify the port that the NetScaler will use to communicate with the domain controller. Use 389 for LDAP or 636 for Secure LDAP (LDAPS). Leave the other settings as they are.
6. Under Connection Settings, enter the base domain name for the domain in which the user accounts reside within the Active Directory (AD) for which you want to allow authentication. The example below uses cn=Users,dc=ctxns,dc=net.

7. In the Administrator Bind DN field, add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. A service account is advisable, so that there will be no issues with logins if the account that is configured has a password expiration.

8. Check the box for Bind DN Password and enter the password twice.

9. Under Other Settings: Enter samaccountname as the Server Logon Name Attribute.

10. In the SSO Name Attribute field, enter UserPrincipalName. Enable the User Required and Referrals options. Leave the other settings as they are.
11. Click on More at the bottom of the screen, then add mail as Attribute 1 in the Attribute Fields section. Leave Nested Group Extraction in the Disabled state (we are not going to be using this option for this deployment).

![Nested Group Extraction](image)

12. Click the Create button to complete the LDAP server settings.

13. For the LDAP Policy Configuration, select the newly created LDAP server from the Server drop-down list, and in the Expression field type ns_true.

![Expression](image)

14. Click the Create button to complete the LDAP Policy and Server configuration.
Configure the SAML IDP Policy and Profile

For your users to receive the SAML token for logging on to Microsoft Office 365, you must configure a SAML IDP policy and profile, and bind them to the AAA virtual server where users’ credentials are sent.

Use the following procedure:

1. Open the NetScaler Configuration Utility and navigate to Security > AAA – Application Traffic > Policies > Authentication > Basic Policies > SAML IDP
2. On the Policies Tab, select the Add button.
3. In the Create Authentication SAML IDP Policy Window, provide a name for your policy (for example – Office365_SSO_Policy).
4. To the right of the Action field, click the ‘+’ icon to add a new action or profile.
5. Provide a name (for example, Office365_SSO_Profile).
6. In the Assertion Consumer Service URL field, enter https://login.microsoftonline.com/login.srf
7. Leave the SP Certificate Name blank.
8. In the IDP Certificate Name field, browse to the certificate installed on the NetScaler that is will be used to secure your AAA authentication Virtual Server.
9. In the Issuer Name field enter https://nssaml.citrix.com/saml/login
10. Set the Encryption Algorithm to AES256 and leave the Service Provider ID field blank.
11. Set both the Signature and Digest algorithms to SHA-1.
12. Set the SAML Binding to POST.
13. Click on More, then put `urn:federation:MicrosoftOnline` in the Audience field.

14. Set the Skew Time to an appropriate value. This is the time difference that will be tolerated between the NetScaler appliance and the Office 365 server for the validity of the SAML assertion.

15. Set the Name ID Format to Persistent, and put `http.req.user.name.b64encode` in the Name ID Expression field. This directs NetScaler to provide the SSO username attribute (UserPrincipalName) that was defined earlier during LDAP configuration as the user ID for Office 365.

16. Type `IDPEmail` in the Attribute1 field, then `HTTP.REQ.USER.ATTRIBUTE(1)` in the Attribute1 Expression field. This will provide the mail attribute added earlier as the email ID used by Office 365. This is useful when the email ID for a user is different from the User Principal Name listed in Active Directory.

17. Click Create to complete the SAML IDP profile configuration and return to the SAML IDP Policy creation window.
18. In the Expression field, add the following expression: \texttt{HTTP.REQ.HEADER("Referer").CONTAINS("microsoft")}

19. Click Create to complete the SAML IDP Configuration.

**To Configure your AAA Virtual Server**

An employee trying to log in to Office 365 is redirected to a NetScaler AAA virtual server which validates the employee’s corporate credentials. This virtual server listens on port 443, which requires an SSL certificate, in addition to external and/or internal DNS resolution of the virtual server’s IP address on the NetScaler appliance. The following steps require a pre-existing virtual server to be in place and assume that the DNS name resolution is already in place, and that the SSL certificate is already installed on your NetScaler appliance.

1. In the NetScaler Configuration tab navigate to Security > AAA – Application Traffic > Virtual Servers and click the Add button.

2. In the Authentication Virtual Server window, enter the virtual server’s name and IP address. (av1 and 10.105.157.62 in this example)

3. Scroll down and make sure that the Authentication and State check boxes are selected.

4. Click Continue.

5. In the Certificates section, select No Server Certificate.

6. In the Server Cert Key window, click Bind.

7. Under SSL Certificates, choose your AAA SSL Certificate and select Insert. (Note – This is NOT the Office 365 SP certificate.)

8. Click Save, then click Continue.

9. Click Continue again to bypass the Advanced Policy creation option, instead opting to add a Basic Authentication Policy by selecting the ‘+’ icon on the right side of the window.

10. From the Choose Type window, select Choose Policy from the drop-down list, select LDAP, leaving Primary as the type, and select Continue.

11. Select Bind and from within the Policies window select the Office 365_LDAP_SSO_Policy created earlier.

12. Click OK to return to the Authentication Virtual Server screen.

13. Under Basic Authentication Policies click the ‘+’ icon on the right to add a second Basic Policy.

14. From the Choose Policy drop-down list, select SAMLIDP, leave Primary as the type, and click Continue.

15. Under Policies select Bind, select your Office 365_SSO_Policy, and click Insert and OK.

16. Click Continue and Done.
After completing the AAA configuration above, this is how the Basic Settings screen of the AAA vserver will look:

![Authentication Virtual Server](image)

**Validate the configuration**

Point your browser to https://login.microsoftonline.com. In the email or phone field, provide the UPN (which serves as the user ID for Office 365) for your enterprise user account. Upon typing the same and switching to the password field, you should be redirected to the NetScaler AAA logon form.

Log in with user credentials that are valid for the NetScaler environment you just configured. Your Office 365 folders and applications should appear.
Troubleshooting

In order to help while troubleshooting, here is the list of entries that will be observed in the ns.log file (located at /var/log on the NetScaler appliance) for a successful SAML login (note that some of the entries such as encrypted hash values etc. will vary) –

Section 1: The NetScaler receives the authentication request from Office 365


Jan 18 02:14:21 <local0.info> 10.105.157.60 01/18/2016:02:14:21 GMT 0-PPE-0 : default AAATM Message 6187 0 : “Parse SAML authn_request: couldn’t find ACS after finding AuthnRequest tag, ignoring”
(Note: this is not an error, the authentication will proceed normally)

Section 2: Messages indicating successful authentication and extraction of parameters from the back-end LDAP server.

Jan 18 02:14:32 <local0.info> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
AAA Message 6193 0 : “In update_aaa_cntr: Succeeded policy for user administrator = ldap2”

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
AAATM Message 6194 0 : “extracted SSOusername: Administrator@CTXNS.net for user administrator”

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
SSLVPN Message 6195 0 : “sslvpn_extract_attributes_from_resp: attributes copied so far are Administrator@ctxns.com ”

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
SSLVPN Message 6196 0 : “sslvpn_extract_attributes_from_resp: total len copied 28, mask 0x1 ”

Section 3: Messages verifying SAML transaction and sending of SAML assertion with signature

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
AAATM Message 6197 0 : “SAMLIDP: Checking whether current flow is SAML IdP flow, input U0ZEQ19TQU1MAElEPV84MzZiNGE5Mi01OWU1LTRmZDEtYjRmOS05NjBiZWMxMTY0YjAmYmluZD1wb3N0JkF4N2tWTEphWGc5MEhHT1pnakhSN0RSbE9tYkU=”

Jan 18 02:14:32 <local0.info> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
AAA EXTRACTED_GROUPS 6198 0 : Extracted_groups “ADSyncAdmins,ReportingGroup {133115cb-a0b1-4a96-83db-2f4828balecf},SQLAccessGroup {133115cb-a0b1-4a96-83db-2f4828balecf},PrivUserGroup {133115cb-a0b1-4a96-83db-2f4828balecf},VPN-USER,RadiusUser,LyncDL,ContentSubmitters,Organization Management,CSAdministrator,RTCUniversalUserAdmins,RTCUniversalServerAdmins,Group Policy Creator Owners,Domain Admins,Enterprise Admins,Schema Admins,Administrators”

Jan 18 02:14:32 <local0.info> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
AAATM LOGIN 6199 0 : Context administrator@116.202.78.57 - SessionId: 34- User administrator - Client_ip 116.202.78.57 - Nat_ip “Mapped Ip” - Vserver 10.105.157.62:443 - Browser_type “Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko” - Group(s) “N/A”
Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
AAATM Message 6200 0 : "SAMLIDP: Checking whether current flow is SAML IdP flow, input
U0ZEQ19TQU1MAElEPV84MzZiNGE5Mi010WUl
TRm2ZETYjRmOS5NjBiZWMxNTY0YjAmYmluZD1wbnVsbWNvbmhyb2Nob29sbC9w
Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
SSLVPN Message 6201 0 : "UnifiedGateway: SSOID update skipped due to StepUp or
LoginOnce OFF, user: administrator"

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
tion:MicrosoftOnline</saml:Audience></saml:Conditions>

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 : default
AAATM Message 6204 0 : "SAMLIDP: SendAssertion: Copying attribute Administrator@ctxns.com to response"
Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 :
default AAATM Message 6205 0 : “SAML: SendAssertion, Digest Method SHA1, SignedInfo
used for digest is <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:Canoni
calizationMethod>http://www.w3.org/2001/10/xml-exc-c14n#"</ds:CanonicalizationMethod>
<ds:SignatureMethod>http://www.w3.org/2000/09/xmldsig#rsa-sha1"</ds:SignatureMethod>
<ds:Reference URI="#_eb2de2e7d944c358296c3789aec309"/><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>tTfFyb7MaMq4nVR/AIBXN9WGyq8g=</ds:DigestValue></ds:Reference></ds:SignedInfo>"

Jan 18 02:14:32 <local0.debug> 10.105.157.60 01/18/2016:02:14:32 GMT 0-PPE-0 :
default AAATM Message 6206 0 : "SAML: SendAssertion, Signature element is
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"</ds:CanonicalizationMethod>
<ds:SignatureMethod>http://www.w3.org/2000/09/xmldsig#rsa-sha1"</ds:SignatureMethod>
<ds:Reference URI="#_eb2de2e7d944c358296c3789aec309"/><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>tTfFyb7MaMq4nVR/AIBXN9WGyq8g=</ds:DigestValue></ds:Reference></ds:SignedInfo>"

Jan 18 02:14:33 <local0.debug> 10.105.157.60 01/18/2016:02:14:33 GMT 0-PPE-0 :
default SSLVPN Message 6207 0 : "core 0: initClientForReuse: making aaa_service_
fqdn_len 0 "

Additional Resources

Microsoft lists the generic required configuration for SAML 2.0 compliant identity providers to
.aspx
Conclusion
NetScaler provides a secure and seamless experience with Office 365 by enabling single sign-on into Office 365 accounts, avoiding the need for users to remember multiple passwords and user IDs, while reducing the administrative overhead involved in maintaining these deployments.