



# Integrating NetScaler with Microsoft Azure Active Directory

## Enterprise Use Case Guidelines

Enable NetScaler integration with Azure AD for XenApp and XenDesktop delivery as well as enterprise authentication into Azure AD driven cloud applications such as Office 365.

**Introduction** Here, an EPA check can also be run on the client

#### Overview

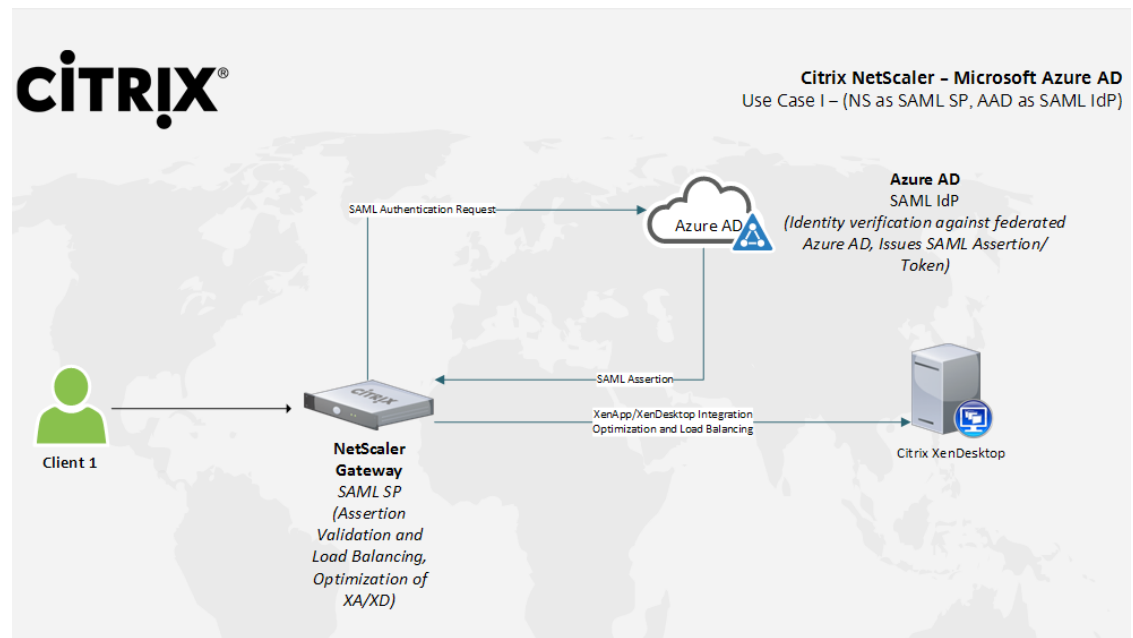
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications. Along with a core feature set supporting application delivery optimization, NetScaler also has a very diverse set of features supporting authentication for enterprise applications.

Microsoft Azure Active Directory (Azure AD) is a cloud based identity management platform that presents a large, growing set of capabilities for identity management. It integrates very well with Microsoft enterprise applications and Active Directory, and also with many other applications using popular protocols such as SAML.

This guide identifies two possible enterprise integration scenarios for NetScaler and Azure AD.

#### Solution Description

Use Case 1 - NetScaler as SAML SP, consuming SAML token from Azure AD for XenApp/XenDesktop



Here, the primary entities are –

- 1. NetScaler Gateway (VPN vserver)** – Acts as the SAML SP, requests for and validates the SAML assertion token sent from Azure AD.
- 2. Azure AD** – Acts as the SAML IdP. Provides user authentication SAML token and validates the user against a federated Azure AD.
- 3. XenApp/XenDesktop** – The XA/XD environment (StoreFront) is integrated with NSG, using NSG as the primary authentication mechanism; upon successful authorization, the user is given access to their apps and desktops.

**Note:** This approach can be used successfully with any enterprise application that is deployed with redundant AD environments on different cloud/on-premise environments. NetScaler can bring its significant application acceleration and optimization capabilities to work hand in hand with Azure AD's universal identity management for several applications.

### Typical Workflow

1. The user connects to the FQDN configured for the VPN vserver to access the XA/XD farm, upon which the user is redirected to Azure AD for authorization.
2. The user provides the authentication information as per their AD credentials, which Azure AD then validates and upon success, issues a token that can then be consumed by NetScaler Gateway (SAML SP)
3. NetScaler Gateway validates the assertion token sent from Azure AD and then provides access to the XA/XD farm. All NS optimization features (SmartAccess, SmartControl etc.) are available with this use case.

### Solution Configuration - Azure AD

#### Step 1 – Directory Integration

To integrate Azure AD with the on-premise directory, navigate to the Directory Integration section in the directory management screen (accessible at <http://manage.windowsazure.com> post login). Follow the steps here for directory integration.

The screenshot displays the Windows Azure Directory Management console. The left sidebar shows the 'Citrix India' organization. The top navigation bar includes 'USERS', 'GROUPS', 'APPLICATIONS', 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', 'REPORTS', and 'LICENSES'. The 'DIRECTORY INTEGRATION' section is active, showing 'integration with local active directory'. It lists 'DOMAINS VERIFIED FOR DIRECTORY SYNC' as 2, 'DOMAINS PLANNED FOR SINGLE SIGN-ON' as 1, and 'DOMAINS CONFIGURED FOR SINGLE SIGN-ON' as 1. The 'DIRECTORY SYNC' toggle is set to 'ACTIVATED'. The 'LAST SYNC' occurred '6965 hours ago'. Below this, the 'deploy and manage' section lists three steps: 1. Add domains, 2. Install and run Azure AD Connect, and 3. Verify and manage directory sync. Step 3 is expanded, showing 'VERIFY INITIAL SYNC' with instructions to check the users page and 'ADD A NEW CUSTOM DOMAIN WITH SINGLE SIGN-ON' with instructions to use PowerShell cmdlets.

Integration Status	Count
DOMAINS VERIFIED FOR DIRECTORY SYNC	2
DOMAINS PLANNED FOR SINGLE SIGN-ON	1
DOMAINS CONFIGURED FOR SINGLE SIGN-ON	1

DIRECTORY SYNC: **ACTIVATED** (DEACTIVATED)

LAST SYNC: 6965 hours ago

#### deploy and manage

- 1 | Add domains
- 2 | Install and run Azure AD Connect
- 3 | Verify and manage directory sync
  - VERIFY INITIAL SYNC**: After the initial sync is complete, go to the users page to verify that your local directory data was successfully synchronized to Windows Azure AD.
  - ADD A NEW CUSTOM DOMAIN WITH SINGLE SIGN-ON**: Use Windows PowerShell cmdlets to add a custom domain for federation to Windows Azure AD. [Learn more](#)

*Step 2 – Add the NetScaler Gateway vserver as an application (SAML SP)*

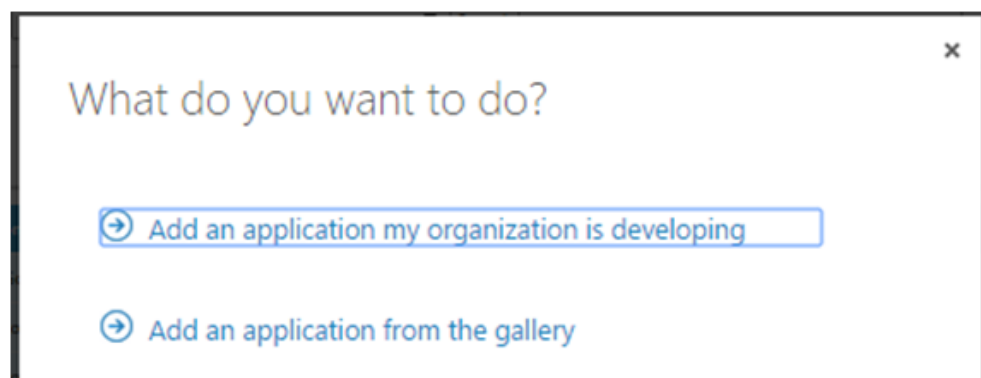
Navigate to the Application tab, then click on **Add** at the bottom of the page.

The screenshot shows the NetScaler management console with the 'APPLICATIONS' tab selected. At the top, there are navigation tabs: USERS, GROUPS, APPLICATIONS, DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, REPORTS, and LICENSES. Below these is a search bar with a dropdown menu showing 'Applications my company uses' and a search input field labeled 'Application name or Client ID'. The main area contains a table of applications:

NAME	PUBLISHER	TYPE	APP URL
Amazon.com	Amazon.com, Inc.	Web application	http://www.amazon.com
Citrix GoToMeeting	Citrix	Web application	http://www.gotomeeting.com
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com
Microsoft OneDrive	Microsoft Corporation	Web application	http://www.onedrive.com
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com
Office 365 Management APIs	Microsoft Corporation	Web application	http://office.microsoft.com
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com
Office 365 Yammer	Microsoft Corporation	Web application	http://office.microsoft.com
Salesforce	Salesforce.com	Web application	http://www.salesforce.com
Test	Citrix India	Web application	https://test.com/
Test NS XD	Citrix India	Web application	https://nsgtest.com/

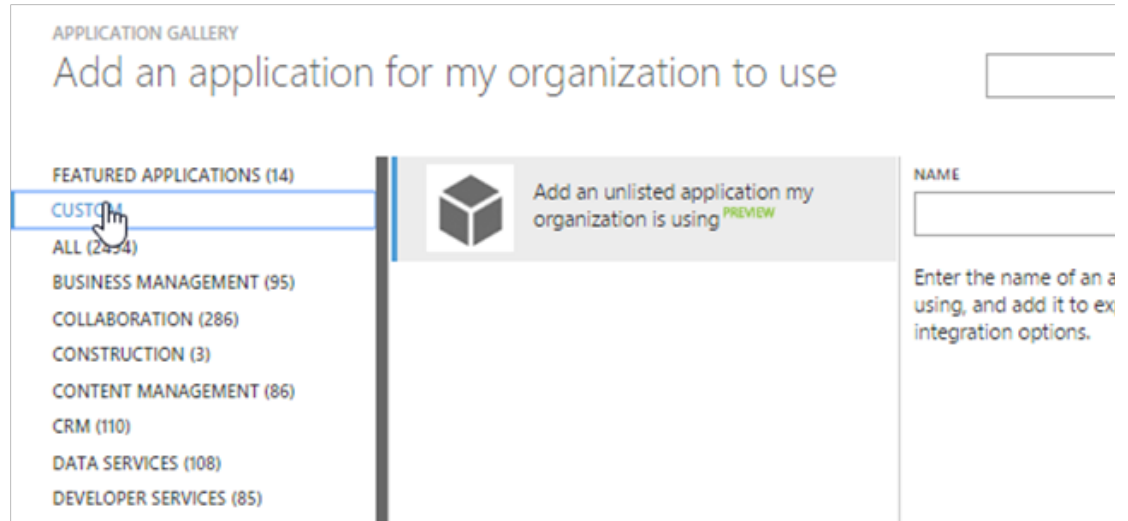
At the bottom of the table, there are two buttons: 'ADD' and 'DELETE'.

The next prompt asks you to choose where the app should be sourced from. Here, select **Add an application from the gallery**

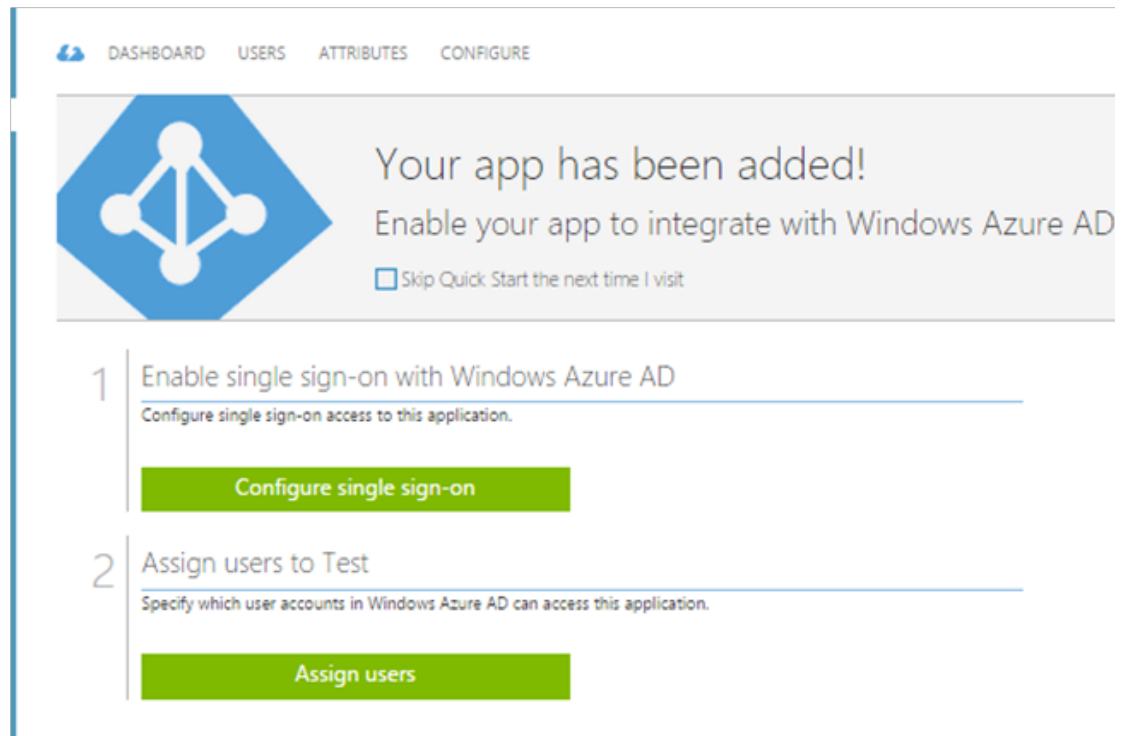




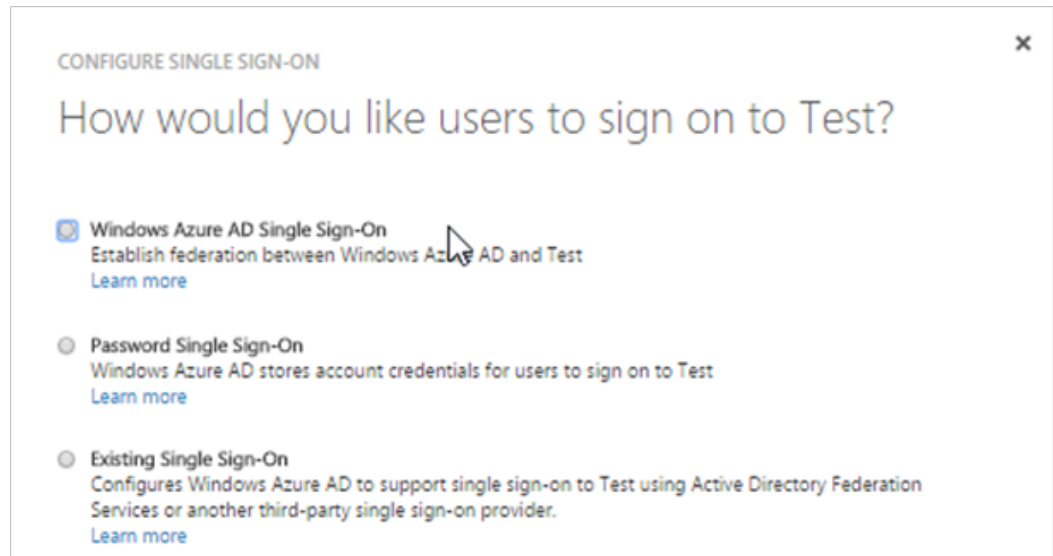
Next, you will be required to provide details about the application – in this screen, you are provided with a list of pre-integrated apps. Select the **Custom** option, then the **Add an unlisted application my organization is using** option.



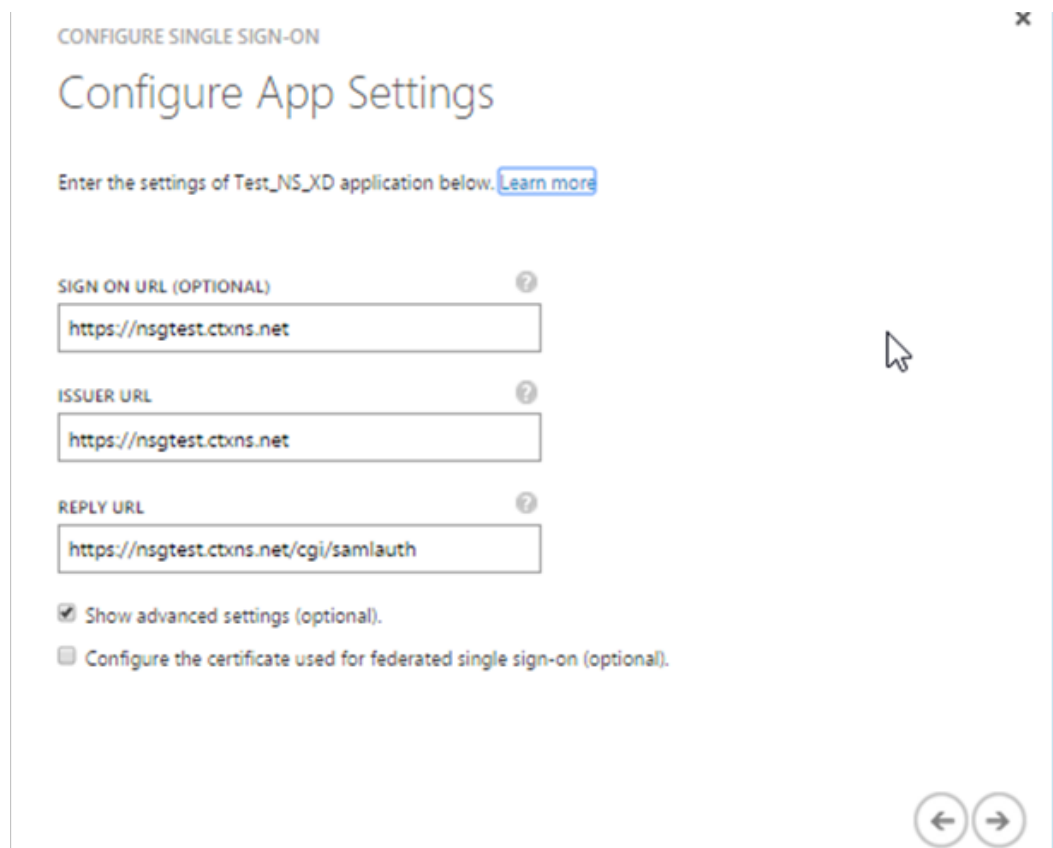
Here, you will also be required to provide a name for the application. After clicking on the tick-shaped icon at the bottom right of the screen, the application is added and the following screen is presented. This screen allows you to configure SSO.



Click on **Configure single sign-on** to begin SSO configuration. This gives you the following screen



Here, select **Windows Azure AD Single Sign-On**, then select the tick-shaped icon to the bottom right. The next screen requires you to present your application settings. The sign on and issuer URLs here are the FQDNs for the NetScaler Gateway, and the reply URL is the SAML authorization link for the NetScaler Gateway (`https://<gatewayFQDN>/cgi/samlauth` - here we use `nsgtest.ctxns.net` as the Gateway FQDN))



This next screen gives you the certificate that needs to be added into the SAML profile on NetScaler (discussed later), along with other necessary settings. This page needs confirmation at the bottom before you can go forward with the configuration.

To take the configuration forward or back, click on the arrowheads at the bottom right of the page.

**CONFIGURE SINGLE SIGN-ON**

## Configure single sign-on at Test\_NS\_XD

To accept the SAML token issued by Azure Active Directory, your application will need the information below. Refer to your application's SAML documentation or source code for details.

1. The following certificate will be used for federated single sign-on:  
Thumbprint: 3270bf5597004df339a4e6224731b6bd82810a6  
Expiry: 10/27/2016 00:00:00 UTC  
[Download certificate](#)
2. Configure the certificate and values in Test\_NS\_XD

**ISSUER URL**

is://sts.windows.net/c27e3447-787a-436e-a458-610124436854/

**SINGLE SIGN-ON SERVICE URL**

https://login.windows.net/c27e3447-787a-436e-a458-610124436854/

**SINGLE SIGN-OUT SERVICE URL**

https://login.windows.net/c27e3447-787a-436e-a458-610124436854/

☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.

This completes configuration, confirmed by the following screen –

**CONFIGURE SINGLE SIGN-ON**

## Single sign-on confirmation

Congratulations! You have successfully configured federated single sign-on.

**NOTIFICATION E-MAIL**

*Step 3 – Assign users*

Next, you should add the users who will have access to this application. Upon clicking on the next arrow in the last screen, you would be taken back to the application configuration screen shown earlier. Click on **Assign Users**. This gives you the screen shown above, that lists all the users defined in this Azure AD tenant.



Select a user, and click on the **Assign** User button in the bottom center of the screen. Do this for all the users who require access.

Exch Test2	No	Unassigned
Exch Test3	No	Unassigned
Exch Test4	No	Unassigned
Exch Test5	Yes	Direct
Exchange Online-Applicati...	No	Unassigned
Exchtest 8	No	Unassigned
Exchtest6	No	Unassigned
Exchtest7	No	Unassigned
Jayakumar K.	No	Unassigned
Mail 1	No	Unassigned
Mail 2	No	Unassigned
Mail 3	No	Unassigned
Mail 4	No	Unassigned
Netscaler	No	Unassigned
Power User	No	Unassigned

## Solution Configuration - NetScaler

### Step 1 - Integration Wizard

At the NetScaler GUI, click on the **XenApp and XenDesktop** option under **Integrate with Citrix Products** in the navigation panel to the left of the screen.

Configuration Item	Details
What is your deployment?	StoreFront
NS Gateway Settings	Provide the NSG IP address (10.105.157.171 in the test deployment), port and a name for the vserver that will be created by the wizard
Server Certificate	Either use an existing certificate (drop down list) or install a new one
Authentication	Here, use an available policy or create a new one. The wizard only supports LDAP/Radius/Client Certificate so the SAML policy will be added separately later. Select one of the three available options and continue configuration. The option chosen is irrelevant, as it will be modified later.
StoreFront	StoreFront FQDN: FQDN of the StoreFront server Site Path: Path to the StoreFront site (/Citrix/StoreWeb by default) Single sign-on domain: Provide the user domain for your LDAP server. Use only the domain and not the extension (.NET, .COM etc) Secure Ticketing Authority: STA Server (usually hosted at <StoreFront FQDN>/scripts/ctxsta.dll)
Xen Farm	Provide details of the XenApp/XenDesktop deployment

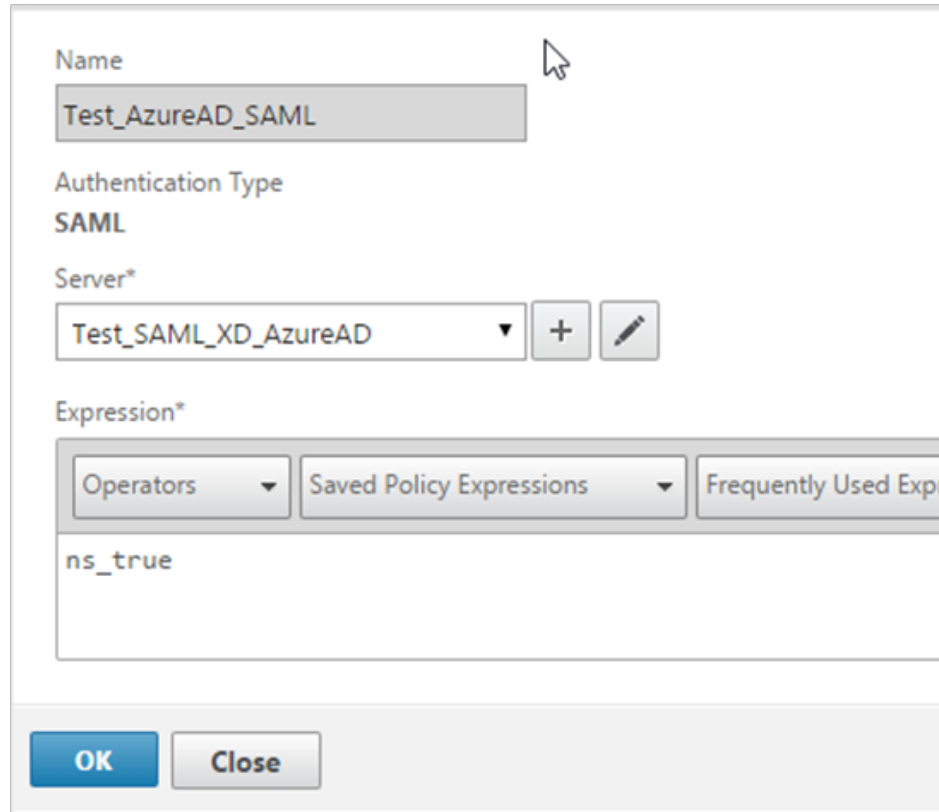
### Step 2 - SAML Configuration

Navigate to NetScaler Gateway>Virtual Servers and select the VPN virtual server created by the Wizard (typically named as \_XD\_<name given during configuration>)

Click on edit, then in the Basic Settings screen remove the LDAP/other policy configured when using the wizard. Click on the plus icon next to authentication, then select **SAML** and **Primary** on the **Choose Type** screen.



On the next screen, provide a name for the policy. Then, click on the plus or pencil (in case a SAML server is already configured) icon next to the server name. Put **ns\_true** as the expression as this policy is to be used for all authentication.



The screenshot shows a configuration window for a new policy. The 'Name' field contains 'Test\_AzureAD\_SAML'. The 'Authentication Type' is set to 'SAML'. The 'Server\*' dropdown menu is set to 'Test\_SAML\_XD\_AzureAD', with plus and edit icons to its right. The 'Expression\*' section has three tabs: 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions'. The 'Saved Policy Expressions' tab is active, showing 'ns\_true' in the text area. At the bottom are 'OK' and 'Close' buttons.

The next screen requires you to provide configuration settings. Here, for IDP certificate name, provide the certificate downloaded earlier in Step 2 when configuring Azure AD. The Redirect URL and the logout URL are the same and given by Single Sign-on Service URL and Single Sign-out service URL (on the same screen where the certificate above was available)

### Configure Authentication SAML Server

Name

Authentication Type  
**SAML**

IDP Certificate Name\*

Redirect URL\*

Single Logout URL

User Field

Signing Certificate Name

Issuer Name

Reject Unsigned Assertion\*

SAML Binding\*

The signing certificate should be the NS server certificate and the issuer name is the FQDN for the NS gateway. For this basic configuration, we have Reject Unsigned Assertion set to off.

Now, click on More. In the additional settings that come up, change the signature algorithm and digest method to SHA256 as shown below –

Signature Algorithm\*

☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method\*

☐ SHA1 ☒ SHA256

This completes configuration for SAML.

*Step 3 – StoreFront Configuration*

On the StoreFront Server, the following needs to be done –

- Enable the pass-through authentication from NetScaler Gateway on StoreFront. For more information, refer to Citrix eDocs - Create and configure the authentication service.

Note: StoreFront must trust the issuer of the NetScaler Gateway virtual server's bound certificate (Root and/or Intermediate certificates) for the Authentication Callback service.

- Add NetScaler Gateway to StoreFront. For more information, refer Citrix eDocs - Add a NetScaler Gateway connection.

Note: The Gateway URL must match exactly what the users are typing into the web browser address bar. The NetScaler Gateway uses passthrough authentication to StoreFront.

- Enable remote access on the StoreFront store. For more information, refer Citrix eDocs - Manage remote access to stores through NetScaler Gateway

## Use Case 2 - NetScaler as SAML IdP, providing SAML token to Azure AD for Microsoft Applications

Here, the primary entities are –

**NetScaler AAA Vserver** – Acts as the SAML IdP, processes requests from Office 365 and other Azure AD enabled applications and sends the SAML assertion token to Azure AD.

**Office 365** – Client Azure AD application.

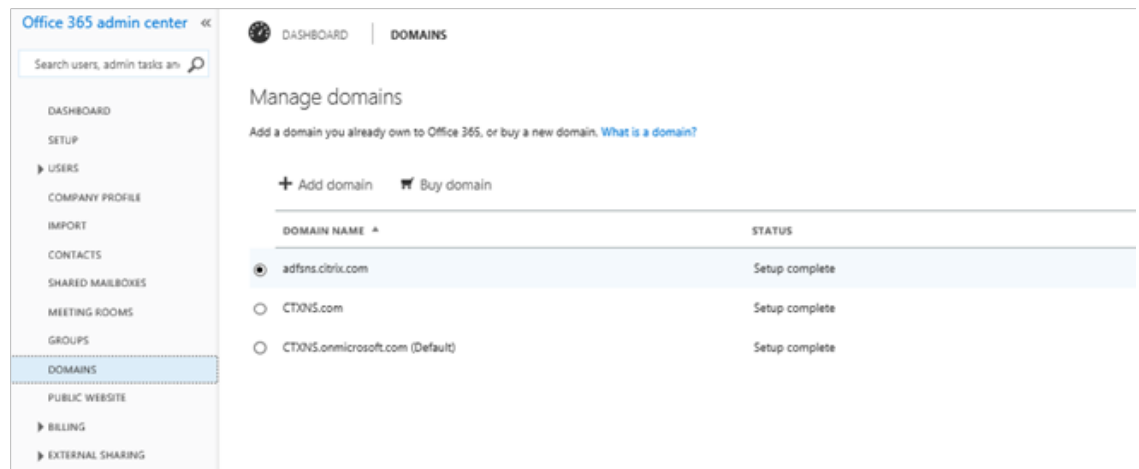
### Typical Workflow

1. The user connects to Office 365, provides his corporate credentials.
2. The Office 365 login page automatically redirects the user to the NetScaler AAA vserver SAML login page.
3. The user provides the authentication information as per their AD credentials, which NetScaler then validates and upon success, issues a token that can then be consumed by Azure AD (SAML SP)
4. Office 365/Azure AD validates the assertion and then provides access to Office 365.

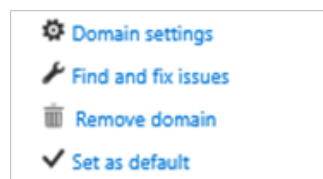
### Part 1: Configure Office 365

#### Step 1 - Confirm Microsoft Office 365 Portal Settings

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



Selecting the domain settings view will show you details about the configured domain, including the current single sign on configuration, if any.

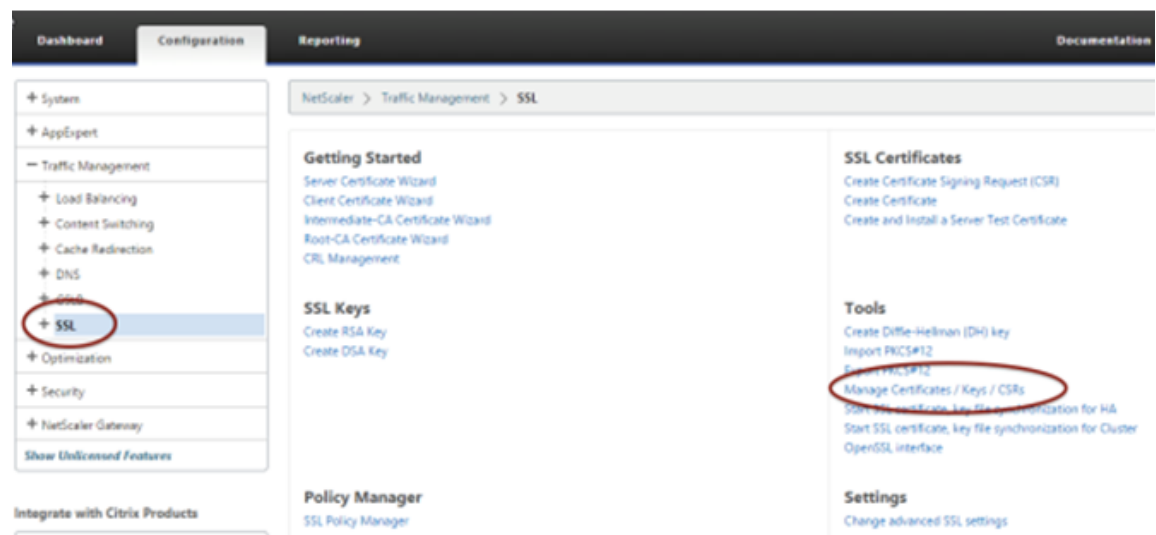
*Step 2: Setup Federation Settings for Windows Azure AD*

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.
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. In 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.



*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 <your domain name>
```

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 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 SAMLIdP (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 Office365 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 SAML
```

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 logon to the NetScaler appliance with their corporate email addresses, you must configure an LDAP authentication server and policy on the appliance that is bound to your AAA VIP address. (Use of an existing LDAP configuration is also supported)

1. In the NetScaler Configuration tab, select Security > AAA – Application Traffic > Policies > Authentication > Basic Policies > LDAP.
2. Create a new LDAP policy: On the Policies tab click Add, and 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 Server IP radio button. 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 is

The screenshot shows the 'Configure Authentication LDAP Server' configuration window. The 'Name' field is set to 'Office365\_SSO\_LDAP\_Server'. Under the 'Server' section, 'Server IP' is selected. The 'IP Address' is '192.168.1.15' with an 'IPv6' checkbox. 'Security Type' is set to 'PLAINTEXT' and 'Port' is '389'. On the right, 'Server Type' is 'AD', 'Time-out (seconds)' is '3', and the 'Authentication' checkbox is checked.

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 recommended to eliminate any issues with logins if the account that is configured includes a password expiration.
8. Check the box for Bind DN Password and enter the password twice.

**Connection Settings**

Base DN (location of users)

Administrator Bind DN

☒ BindDN Password  
 Administrator Password

Confirm Administrator Password

[Retrieve Attributes](#)

9. Under Other Settings: Enter samaccountname (or UserPrincipalName, based upon your LDAP configuration) 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.

**Other Settings**

Server Logon Name Attribute

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute

Default Authentication Group

☒ User Required  
☒ Referrals  
 Maximum Referral Level

Referral DNS Lookup

☐ Validate LDAP Server Certificate  
 LDAP Host Name

11. Click More at the bottom of the screen, and add mail as Attribute 1 in the Attribute Fields section. Leave Nested Group Extraction in the Disabled state (this deployment does not include this option)

**Nested Group Extraction**

☐ Enabled ☒ Disabled

Maximum Nesting Level

Group Search Filter

Group Name Identifier\*

Group Search Attribute\*

Group Search Sub-Attribute

**Attribute Fields**

Attribute 1

Attribute 2

Attribute 9

Attribute 10



11. Click the **Create** button to complete the LDAP server settings.
12. 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`. Click the **Create** button to complete the LDAP Policy and Server configuration.

Expression\*

Operators Saved Policy Expressions Frequently Used Expressions

ns\_true

Create Close

#### *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. Select the NetScaler Configuration tab and navigate to Security > AAA – Application Traffic > Policies > Authentication > Basic Policies > SAML IDP
  2. In the Policies tab, select the Add button.
  3. In the Create Authentication SAML IDP Policy window, create a name for your policy (for example – Office365\_SSO\_Policy).
  4. Click the '+' icon next to the Action field to add a new action or profile.
  5. Create an action 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 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.
- (Screenshot on the next page)

**Configure Authentication SAML IDP Pro**

Assertion Consumer Service Url  
 ?

IDP Certificate Name  
 +

SP Certificate Name  
 +

Encryption Algorithm

☐ Send Password

Issuer Name

Service Provider ID

☐ Reject Unsigned Requests

Signature Algorithm\*  
☒ RSA-SHA1 ☐ RSA-SHA256

Digest Method\*  
☒ SHA1 ☐ SHA256

SAML Binding\*

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.

Audience  
urn:federation:MicrosoftOnline

Skew Time(mins)  
5

Name ID Format  
Persistent

Name ID Expression  
http.req.user.name.b64encode

Attribute 1  
IDPEmail

Attribute1 Expression  
HTTP.REQ.USER.ATTRIBUTE(1)

16. Click on More, then put urn:federation:MicrosoftOnline in the Audience field.
17. 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.
18. 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.
19. 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.
20. Click Create to complete the SAML IDP profile configuration and return to the SAML IDP Policy creation window.
21. In the Expression field, add the following expression: `HTTP.REQ.HEADER("Referer").CONTAINS("microsoft")`
22. Click Create to complete the SAML IDP Configuration.

*To Configure your AAA Virtual Server*

An employee trying to login 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, this is how the Basic Settings screen of the AAA vserver should look:

Authentication Virtual Server	
<b>Basic Settings</b>	
Name	av1
Authentication Domain	-
IP Address	10.105.157.62
Port	443
<b>Certificates</b>	
1 Server Certificate	
No CA Certificate	
<b>Advanced Authentication Policies</b>	
No Authentication Policy	
<b>Basic Authentication Policies</b>	
Primary Authentication	
1 LDAP Policy	
1 SAML IDP Policy	

#### *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.



## Conclusion

NetScaler enables seamless integration with Azure Active Directory, enabling user authentication into Office 365 and other Microsoft applications along with optimization for key applications such as XenApp and XenDesktop while using Azure Active directory for authentication .

**Corporate Headquarters**  
Fort Lauderdale, FL, USA

**Silicon Valley Headquarters**  
Santa Clara, CA, USA

**EMEA Headquarters**  
Schaffhausen, Switzerland

**India Development Center**  
Bangalore, India

**Online Division Headquarters**  
Santa Barbara, CA, USA

**Pacific Headquarters**  
Hong Kong, China

**Latin America Headquarters**  
Coral Gables, FL, USA

**UK Development Center**  
Chalfont, United Kingdom



### About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2015 of \$3.28 billion, Citrix solutions are in use at more than 400,000 organizations and by over 100 million users globally. Learn more at [www.citrix.com](http://www.citrix.com).

Copyright © 2016 Citrix Systems, Inc. All rights reserved. Citrix and other marks appearing herein are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names are trademarks of their respective owners.