

Configuring Office 365

Office 365 has SP/IdP initiated flow, which is supported in NetScaler (12.1.).

Before you start, you need the following:

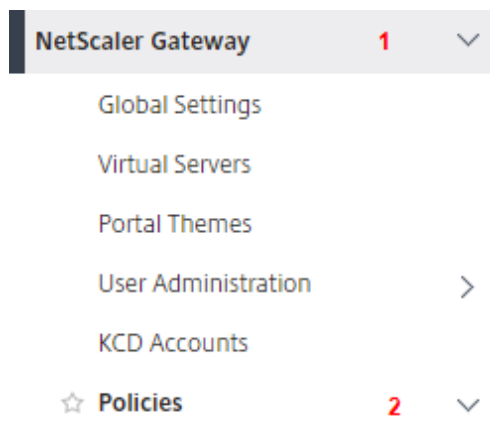
- Admin account for Office 365
- Admin account for NetScaler

Office 365 Configuration

The Office 365 configuration steps are as follows:

1. LDAP configuration in NetScaler
2. Configure Office 365 with the App Catalog.
3. NetScaler Configuration
4. Power Shell Configuration

Step 1: LDAP configuration in NetScaler



- Clientless Access
- AppFlow
- Authentication 3 ▾
- Local
- RADIUS
- Web
- LDAP** 4
- TACACS

1. Click on **NetScaler Gateway > Policies > Authentication > LDAP**

LDAP

Policies 1		Servers 1									
Add		Edit		Delete		Show Bindings		Primary VPN Global Bindings		Secondary VPN Global Bindings	
Group Extraction											
<input checked="" type="checkbox"/>	Name	Expression	Request Server	Primary Bound?	Primary Priority	Secondary Bound?					
<input checked="" type="checkbox"/>	NS_LDAP	NS_TRUE		×	-NA-	×					

2. **LDAP** window will open > Click on it.

Name

Server*

+ ?

Expression*

Edit

NS_TRUE

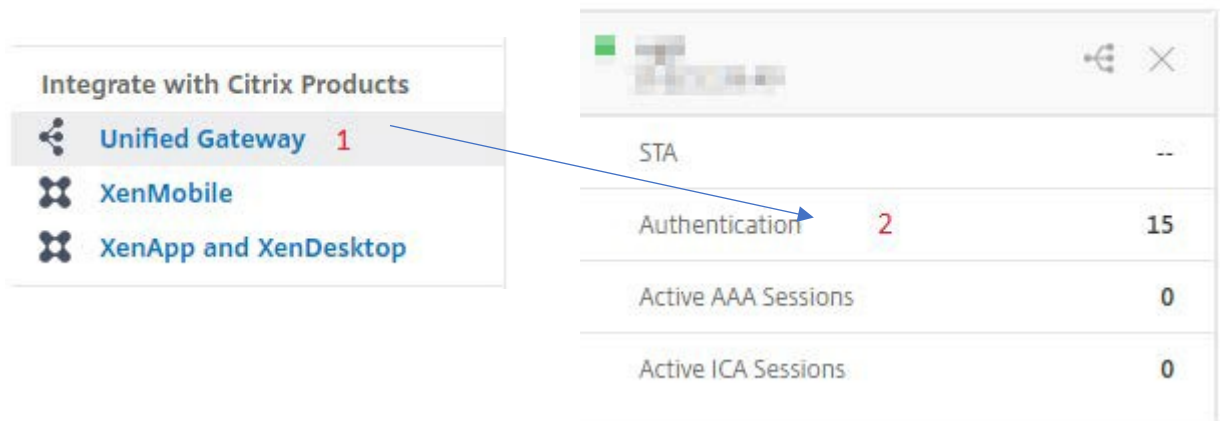
3. **Configure Authentication LDAP Policy** window will open > Click on edit, of the field **Server**.



4. **Configure Authentication LDAP Server** pop-up will open > Scroll down and add **objectGUID** in the **Attributes** field using comma in between.
5. Click **OK**.



Step 2: Configure Office 365 with App Catalog

1. Click on **Unified Gateway > Authentication**.



The **Unified Gateway Configuration** screen appears.



2. Go to **Applications** section. Click on  icon. Now, you can see  icon. Click on it. The **Application** window appears.

Application

Choose Type*

Web Application
Select to provide access to Enterprise applications.

SaaS
Select to provide access to SaaS applications.

XenApp & XenDesktop
Select to provide access to hosted virtual resources.

3. Select **SaaS** from the Application type.
4. Select **Office 365** from the drop-down list.

Choose from Catalog*

15Five

Creative Cloud
DocuSign
Domo
Dropbox
GoToMeeting
Jira
PagerDuty
Service Now
Salesforce
Slack
Zendesk
Zoom
Deskpro
Evernote
SugarCRM
Humanity
Bonusly
BambooHR
Box
Office 365


Office 365

5. Fill the application template with the appropriate values.

Name
Office 365 NS

Comments
Single-Sign on into Office 365 apps ?

Icon URL*
Choose File ▾ /var/netScaler/logon/Office 365 Nev



Service Provider Login URL* **1**
https://login.microsoftonline.com/lc

Service Provider ID* **2**
urn:federation:MicrosoftOnline

IDP Certificate Name* **3**
[Redacted] ▾ + ✎

Issuer Name **4**
https://ug3.[Redacted].com/saml/login

Attribute1 **5**
IDPEmail

6. You must update the fields in NetScaler with the following values:

Field Name	Values
Service Provider ID	urn:federation:MicrosoftOnline
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

7. After providing the required values, click **Continue**. Click **Done**.

Step 3: Office 365 Power Shell Configuration

Below Power Shell commands needs to be executed to complete the office 365 SSO setup.

1. Connect-MSolService will prompt for user credentials, provide an Office 365 administrative user's credentials.

```
PS C:\Windows\system32> Connect-MsolService
```

2. Set the attributes for office 365

```
PS C:\Windows\system32> $dom = "Domain Name"
```

```
PS C:\Windows\system32> $fedBrandName = "Matched as of domain name"
```

```
PS C:\Windows\system32> $url = "IdP logout url"
```

```
PS C:\Windows\system32> $uri = "IdP saml login url"
```

```
PS C:\Windows\system32> $ecpUrl = "IdP saml login url"
```

```
PS C:\Windows\system32> $cert = New-Object  
System.Security.Cryptography.X509Certificates.X509Certificate2("<IdP public certificate  
location")
```

```
PS C:\Windows\system32> $certData = [system.convert]::tobase64string($cert.rawdata)
```

3. Domain needs to be federated in order to enable SSO for office 365. Use below command to make the domain federated.

```
PS C:\Windows\system32> Set-MsolDomainAuthentication -DomainName $dom -  
federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri  
-SigningCertificate $certData -IssuerUri $uri -ActiveLogOnUri $ecpUrl -LogOffUri $url -  
PreferredAuthenticationProtocol SAML
```

Default authentication type for embedded views

- Allow users to choose their authentication type
- Tableau
- [redacted].com (SAML)