CITRIX

NetScaler with Unified Gateway

Configuring Office 365

Contents

Disclaimer (Documentation)

This document is furnished "AS IS." Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix System, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

Citrix Systems, Inc., the Citrix logo, and Citrix Provisioning Services are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Preface

This section provides an overview about the information included in this guide.

Intended Audience

The information in this guide is intended for the System Administrators.

Document Conventions

The following table lists various conventions used in this guide.

Table 1: Document conventions used in this guide

Convention	Description
Bold	Used for names of interface elements (such as names of fields, panes, windows, menus, buttons, dialog boxes) and what the user specifically selects, clicks, presses, or types.
Note	Used to highlight information that is important.

Overview

The Citrix NetScaler application delivery controller (ADC) helps to load balance, accelerate, optimize, and secure enterprise applications.

Office 365 can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to office 365 using the same Single Sign On (SSO

Terminology

An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

The following table lists various terms that are used alternatively for completing configurations for service providers and identity providers.

Table 2: Terminology used for SP and IdP configurations

Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

Configuring Office 365 for Single Sign-On

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

Before you start, you need the following:

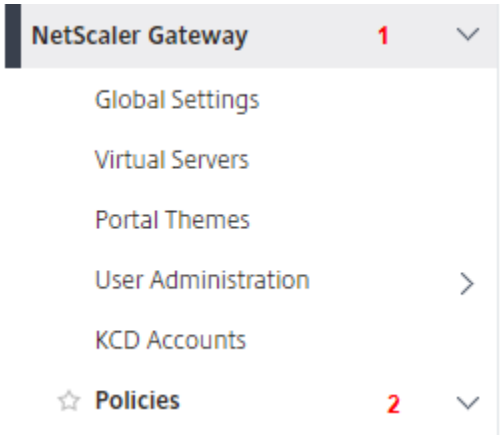
- Admin account for Office 365
- Admin account for NetScaler

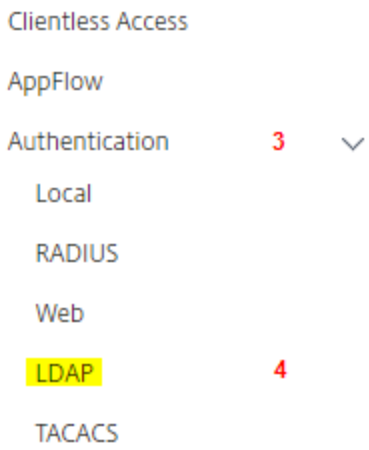
Office 365 Configuration

The Office 365 configuration steps are as follows:

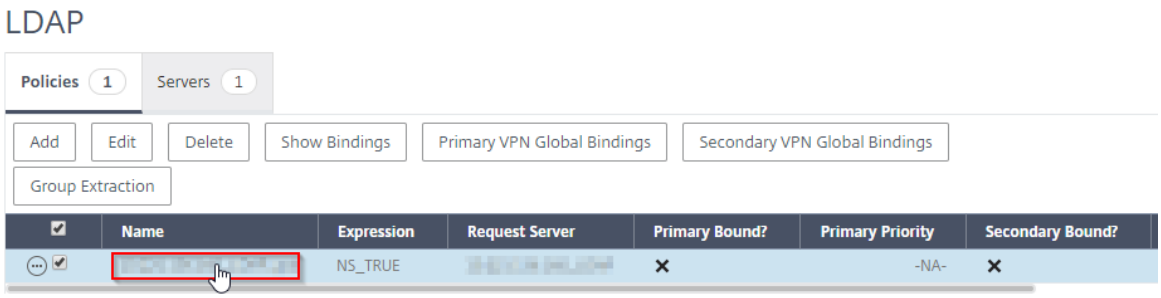
1. LDAP configuration in NetScaler
2. Configure Office 365 with the App Catalog.
3. NetScaler Configuration
4. Power Shell Configuration

Step 1: LDAP configuration in NetScaler

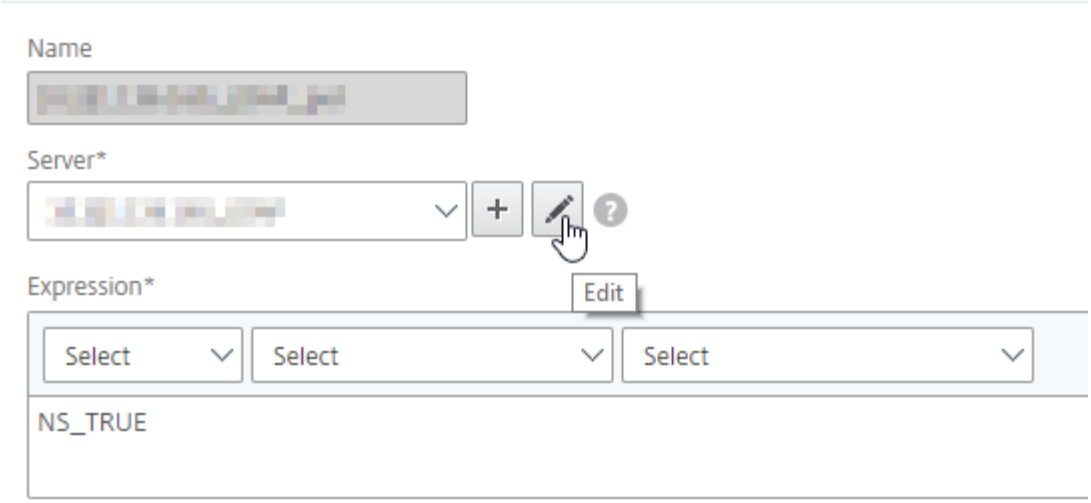




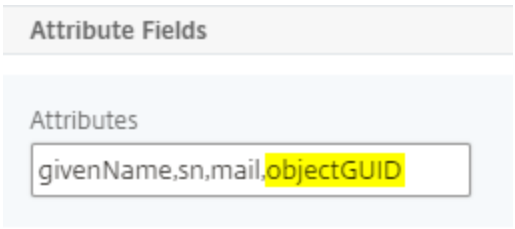
1. Click on **NetScaler Gateway > Policies > Authentication > LDAP**



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



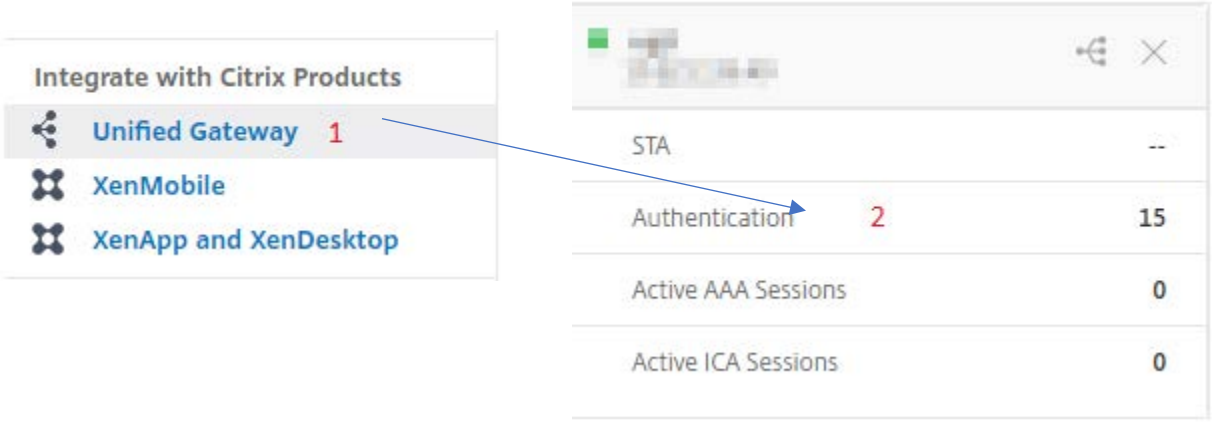
3. **Configure Authentication LDAP Policy** window will open **>** Click on edit, of the field **Server**.



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.**

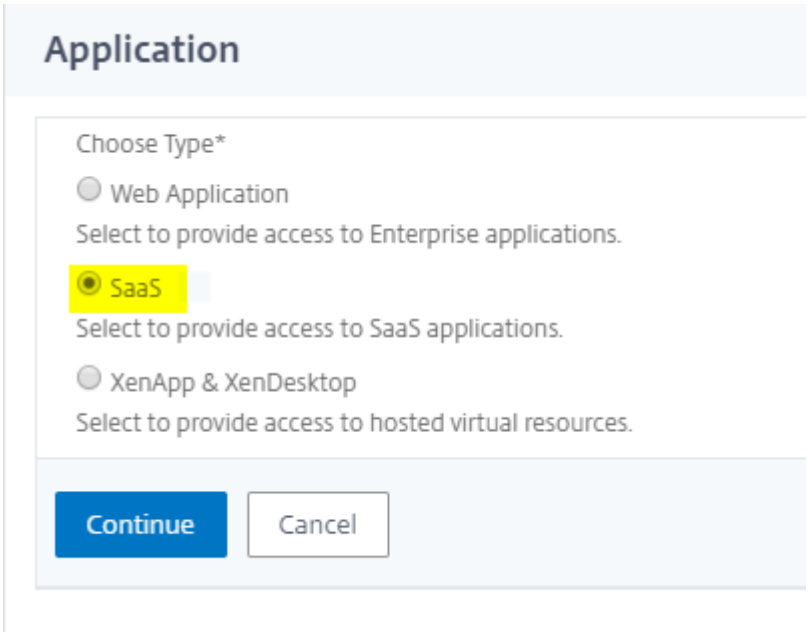
Step 2: Configure Office 365 with App Catalog

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

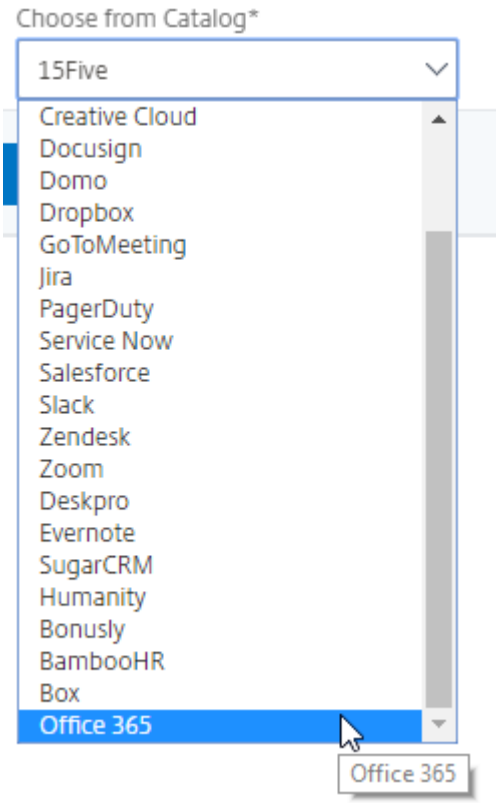


The **Unified Gateway Configuration** screen appears.

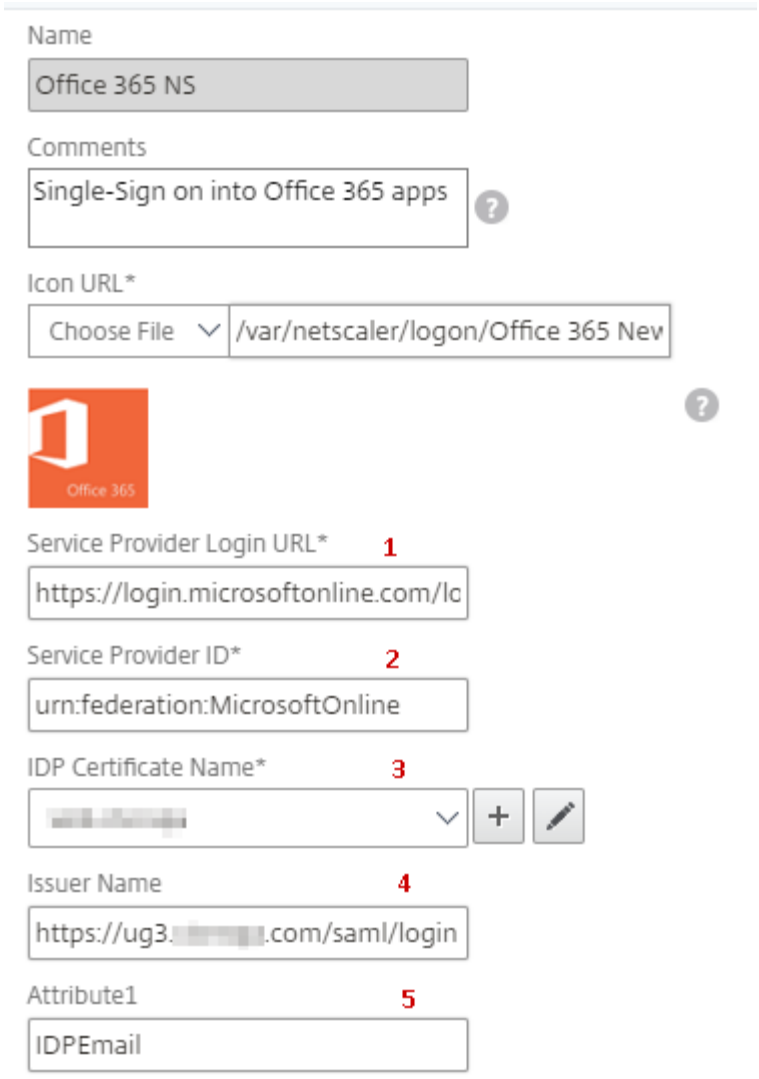
2. Go to **Applications** section. Click on icon. Now, you can see **+ icon.** Click on it.
The **Application** window appears.



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



5. Fill the application template with the appropriate values.



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 SAMLP