



# **NetScaler with Unified Gateway**

## **Configuring Zoho**

# Contents

CONTENTS .....	1
DISCLAIMER (DOCUMENTATION) .....	2
PREFACE.....	3
OVERVIEW .....	4
CONFIGURING ZOHO FOR SINGLE SIGN-ON .....	5

# 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
<b>Bold</b>	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.
<b>Note</b>	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.

Zoho can be integrated with Identity Provider (IdP) for user authentication. This enable the user to sign into Zoho 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**

<b>Service Provider (SP)</b>	<b>Identity Provider (IdP)</b>
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

# Configuring Zoho for Single Sign-On

Zoho has IdP initiated flow, which is supported in Netscaler (12.1).

Before you start, you need the following:

- Admin account for Zoho.
- Customer Domain.  
For example if your IdP deployment URL is [https://ug1.<customer\\_domain>.com/logon/LogonPoint/index.html](https://ug1.<customer_domain>.com/logon/LogonPoint/index.html) , your Customer domain will be <customer\_domain>.
- Admin account for NetScaler.

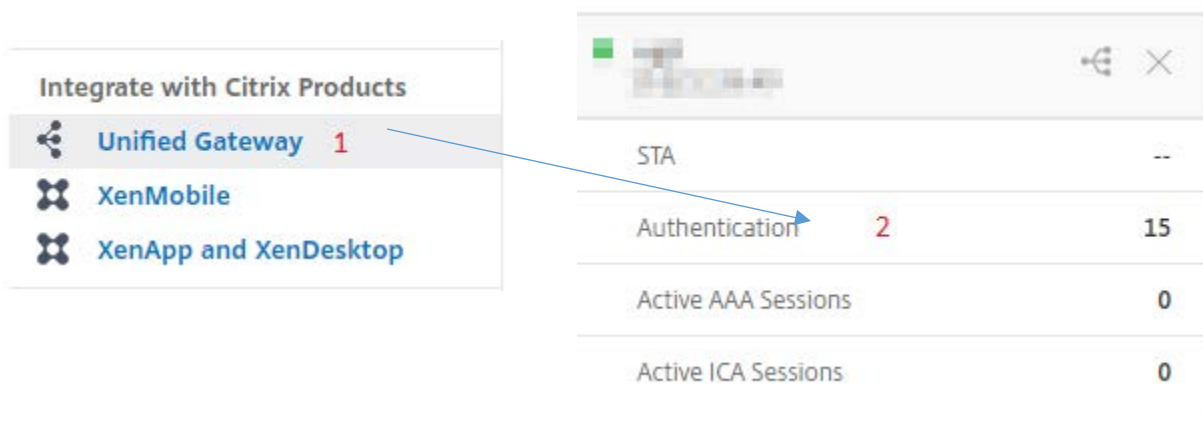
## Zoho Configuration

The Zoho configuration steps are as follows:

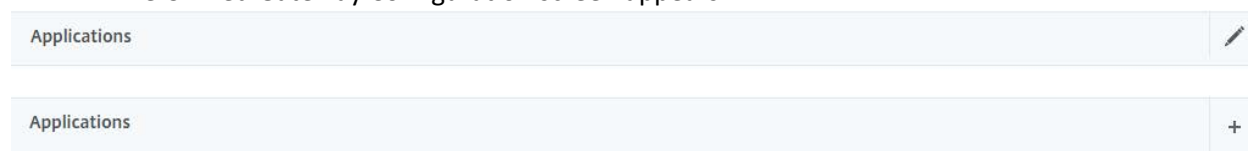
1. Configure Zoho with the App Catalog.
2. Configure SAML Setting into Zoho.


### Step 1: Configure Zoho with App catalog

1. Click on Unified Gateway > Authentication



The Unified Gateway Configuration screen appears.



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

### Application

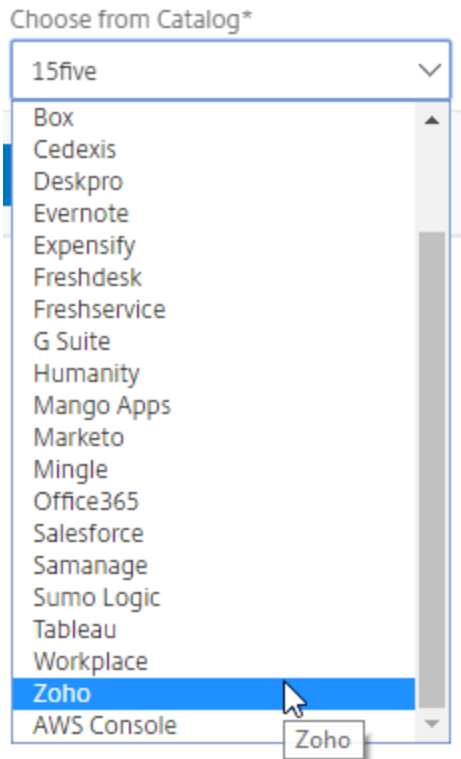
Choose Type\*

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 Zoho from the dropdown list.




5. Fill the Application template with appropriate values.



Name  
Zoho

Comments  
Zoho

Icon URL\*  
Choose File ▾ /var/netScaler/logon/zoho.png



Service Provider Login URL\*  
https://www.zoho.com/accounts/

Service Provider ID\* 1  
https://accounts.zoho.com/

Assertion Consumer Service Url\* 2  
https://accounts.zoho.com/samlres

IdP Certificate Name\* 3  
[blurred] ▾ + ✎

Issuer Name 4  
UG\_VPN\_Zoho

**Continue** Cancel

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

Field Name	Values
Service Provider ID	https://accounts.zoho.com/
ACS URL	https://accounts.zoho.com/samlresponse/<customer_id>
IdP Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

7. In place of <customer\_id>, enter your company Id (Follow **step 2** to get the customer id).
8. After providing the required values, click **continue**. Click **done**.

## Step 2: Configure SAML Setting into Zoho

1. Login to **Zoho** as an Admin user.



One account. Access all services.

Sign In to access Accounts

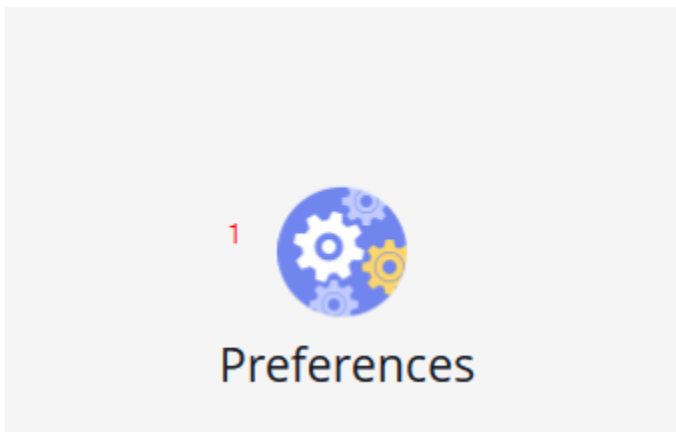
Email Address

Password

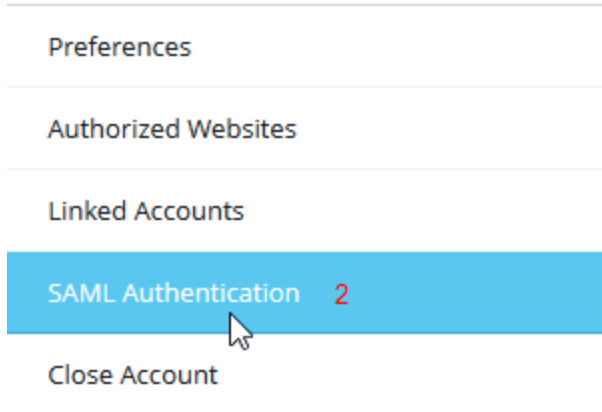
Keep me signed in    [Forgot Password?](#)

**Sign In**

2. To get SAML Authentication page, you need to sign into **Zoho mail** and verify your account then login into **Zoho Account** again.
3. Zoho Accounts window will appear, click on **Preferences**.



4. Settings window will appear, click on **SAML Authentication**.



5. SAML Authentication window will appear, click on **Setup Now**.



6. Complete all the fields with appropriate values and click on **get key from file** and upload your **IdP certificate**.

## SAML Authentication

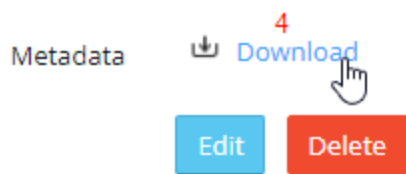
SAML is an XML-based framework for exchanging user authentication, entitlement, and attribute information.

Login URL	https://ug1.<customer_domain>.com/saml/login
Logout URL	https://ug1.<customer_domain>.com/cgi/logout
	<input type="checkbox"/> Do you need Logout Response?
Change Password URL	https://ug1.<customer_domain>.com/cgi/logout
PublicKey	Update IdP Certificate <a href="#">Get key from file</a> <sup>4</sup>
Algorithm	RSA <span>▼</span>
	<input type="checkbox"/> Just In Time Provisioning
Zoho Service	Accounts <span>▼</span>
	<sup>5</sup> Add Cancel

- Update all the fields in SAML authentication page and click on **Add**.

Field Name	Values
Login URL	https://ug1.<customer_domain>.com/saml/login
Logout URL	https://ug1.<customer_domain>.com/cgi/logout
Change password URL	https://ug1.<customer_domain>.com/cgi/logout
Public Key	Update IdP Certificate

- In place of <customer\_domain>, enter your customer domain name (See **Introduction** to know more about the <customer\_domain> values).
- SAML Authentication window will appear, click on **download metadata**.



10. Copy **customer id** from your metadata.

```
<md:AssertionConsumerService  
  Location="https://accounts.zoho.com/samlresponse/[redacted]  
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
  isDefault="true" index="0"/>
```

Customer id

Default authentication type for embedded views

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