



# **NetScaler with Unified Gateway**

## **Configuring Freshdesk**

# Contents

- CONTENTS ..... 1
- DISCLAIMER (DOCUMENTATION) ..... 2
- PREFACE ..... 3
- OVERVIEW ..... 4
- CONFIGURING FRESHDESK 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.

Freshdesk 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**

<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 Freshdesk for Single Sign-On

Freshdesk supports SP/IdP initiated flow, which is supported in Netscaler (12.1).

Before you start, you need the following:

- Admin account for Freshdesk.
- Customer instance.  
For example, if your deployment URL is [https://<customer\\_domain>.freshdesk.com/](https://<customer_domain>.freshdesk.com/) your customer Instance is <customer\_domain>.
- This is required for App Catalog creation in NetScaler.
- Admin account for NetScaler.

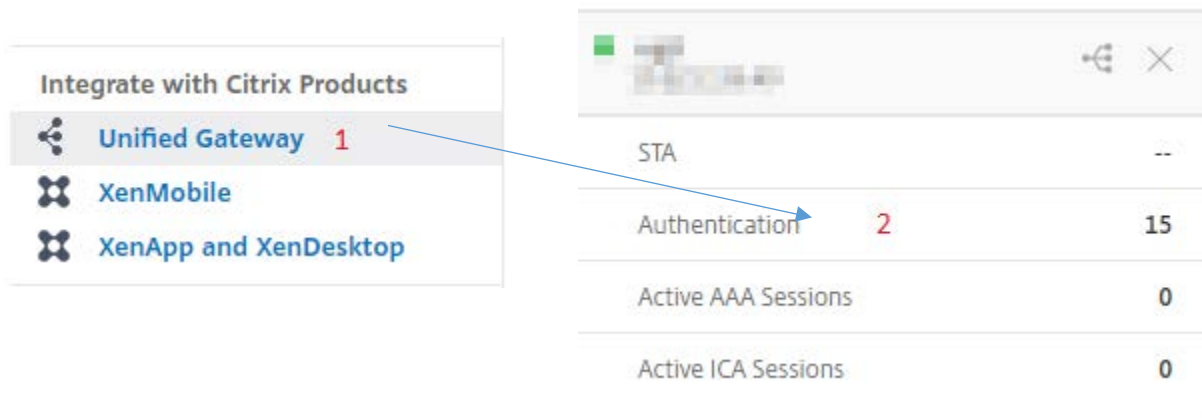
## Freshdesk Configuration

The Freshdesk configuration steps are as follows:

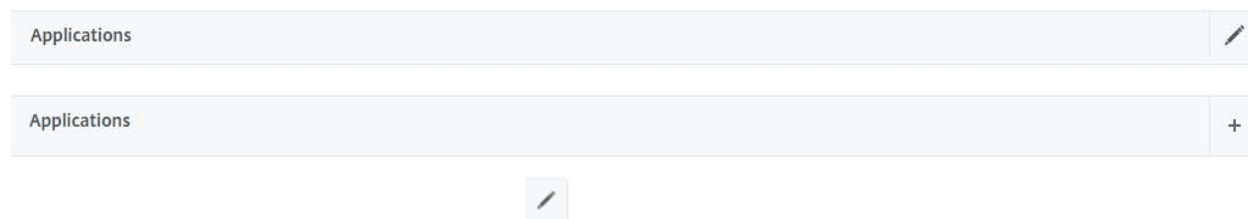
1. Configure Freshdesk with the App Catalog.
2. Configure SAML Setting into Freshdesk.

### Step 1: Configure Freshdesk 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.

The screenshot shows a dialog box titled "Application". Inside, there is a section "Choose Type\*" with three radio button options. The "SaaS" option is selected and highlighted with a yellow background. Below each option is a descriptive sentence. At the bottom of the dialog, there are two buttons: "Continue" (blue) and "Cancel" (white).

**Application**

Choose Type\*

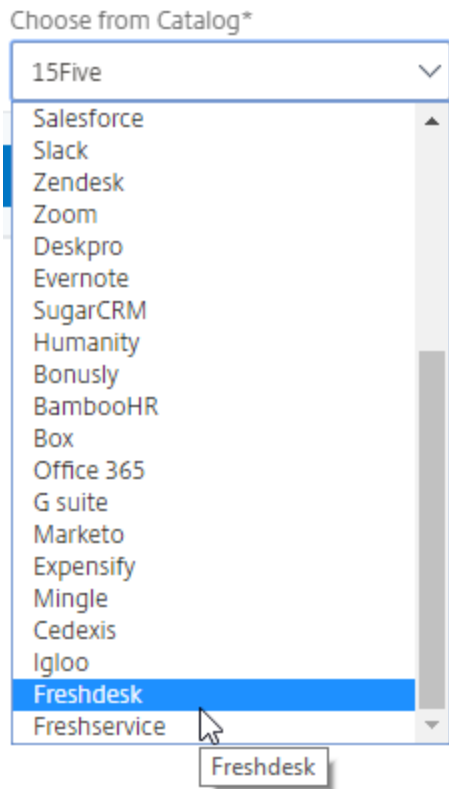
Web Application  
Select to provide access to Enterprise applications.

SaaS  
Select to provide access to SaaS applications.

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

**Continue** Cancel

3. Select **SaaS** from the Application type.
4. Select Freshdesk from the dropdown list.




5. Fill the Application template with appropriate values.



Name  
Freshdesk

Comments  
Freshdesk

Icon URL\*  
Choose File



Service Provider Login URL\* 1

Service Provider ID\* 2

Assertion Consumer Service Url\* 3

IDP Certificate Name\* 4

Issuer Name 5

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

Field Name	Values
------------	--------

URL	https://<customer_domain>.freshdesk.com/a/
Service Provider ID	https://<customer_domain>.freshdesk.com
ACS URL	https://<customer_domain>.freshdesk.com/login/saml
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

7. In place of <customer\_domain>, enter your company domain name (See **Introduction** to know more about the <customer\_domain> values).
8. After providing the required values, click **continue**. Click **done**.

## Step 2: Configure SAML Setting into Freshdesk

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

Log in to your Freshdesk account

Please enter your Freshdesk domain name and we'll help you out!

.freshdesk.com

**PROCEED**

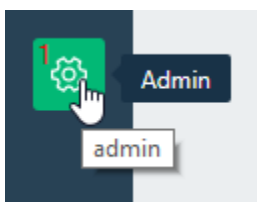
2. Enter your domain name and click on proceed, you will navigate to your domain login page.

## Login to the support portal

Enter the details below

  
  
 Remember me on this computer  
[Forgot your password?](#) 

3. Click on **Admin** tab in left side menu.



4. Admin window will appear, Inside **General Settings** click on **Security**.




Field Name	Values
SAML Login URL	https://ug1.<customer_domain>.com/saml/login
Logout URL	https://ug1.<customer_domain>.com/cgi/logout
Security Certificate Fingerprint	Generate the fingerprint of your IdP certificate and paste it in this section

- Select the Admin user to send the notification.

Admin Notifications

**Send notifications to**

 x 6

**Notification will be sent when**

- Agent is Added or Deleted

---

Password Policy

Changes you make to the password policy will be applicable within 8 hours. Your agents will be prompted to update their passwords during this time. If they fail to conform, they will be logged out of the support portal and will be forced to change their passwords the next time they try to log in.

**For Agents**

Default  Advanced

- Minimum of 8 characters
- Cannot contain username

**For Contacts**

Default  Advanced

- Minimum of 8 characters
- Cannot contain username

- Click on **SAVE**.