

# Configure Freshservice

## Overview

Freshservice can be integrated with Identity Provider (IdP) for user authentication. This enable the user to sign into Freshservice using the same single sign on (SSO).

## Introduction

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

Before you start, you need the following:

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

## Freshservice Configuration

The Freshservice configuration steps are as follows:

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

### Step 1: Configure Freshservice with App catalog



1. Click on Unified Gateway > Authentication

The screenshot shows two parts of the Citrix NetScaler interface. On the left, a panel titled 'Integrate with Citrix Products' lists three options: 'Unified Gateway 1', 'XenMobile', and 'XenApp and XenDesktop'. A blue arrow points from the 'Unified Gateway 1' option to the right-hand panel. The right-hand panel is a window displaying authentication statistics for a specific gateway. It contains a table with the following data:

STA	--	
Authentication	2	15
Active AAA Sessions	0	
Active ICA Sessions	0	

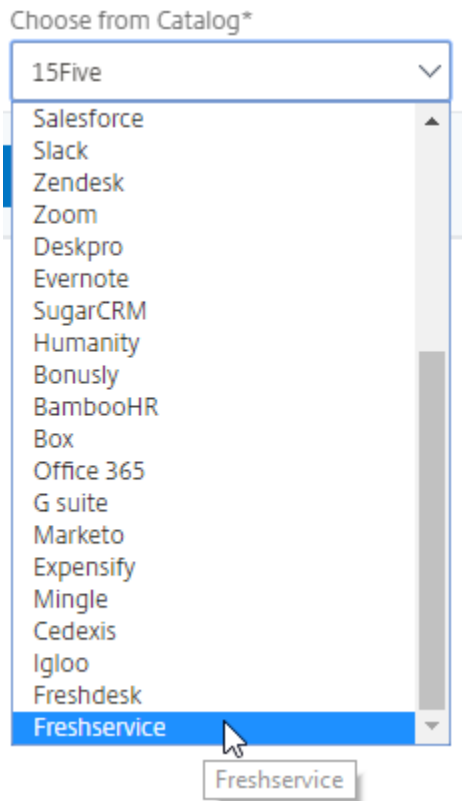
The Unified Gateway Configuration screen appears.



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

The screenshot shows the 'Application' configuration window. It has a title bar 'Application'. Below the title bar is a section titled 'Choose Type\*'. There are three radio button options: 'Web Application' (unselected), 'SaaS' (selected and highlighted in yellow), and 'XenApp & XenDesktop' (unselected). Below each option is a descriptive sentence: 'Select to provide access to Enterprise applications.' for Web Application, 'Select to provide access to SaaS applications.' for SaaS, and 'Select to provide access to hosted virtual resources.' for XenApp & XenDesktop. At the bottom of the window are two buttons: 'Continue' (blue) and 'Cancel' (white).

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




5. Fill the Application template with appropriate values.

Name  
Freshservice

Comments  
Freshservice

Icon URL\*  
Choose File ▾ /var/netScaler/logon/freshservice.pn



Service Provider Login URL\* 1  
https://[redacted].freshservice.com/lo

Service Provider ID\* 2  
https://[redacted].freshservice.com

Assertion Consumer Service Url\* 3  
https://[redacted].freshservice.com/lo

IDP Certificate Name\* 4  
[redacted] ▾ + ✎

Issuer Name 5  
UG\_VPN\_Freshservice

**Continue** Cancel

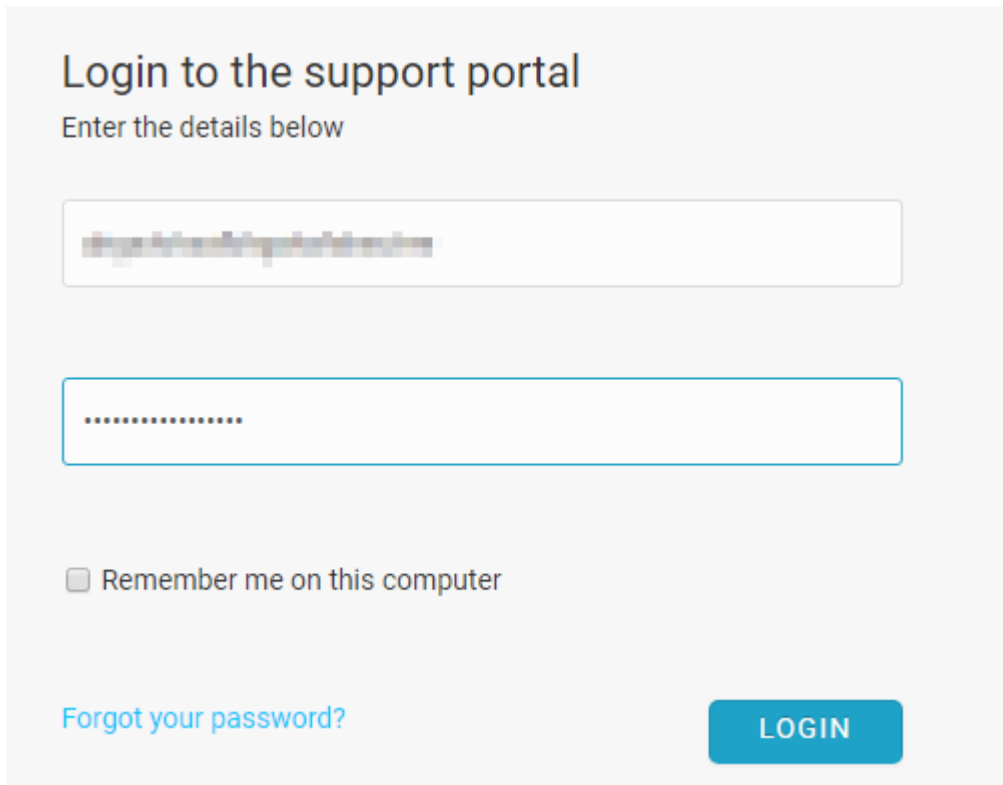
6. You must update the fields in Netscaler with the following values:

Field Name	Values
URL	https://<customer_domain>.freshservice.com/login/sso
Service Provider ID	https://<customer_domain>.freshservice.com
ACS URL	https://<customer_domain>.freshservice.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 Freshservice

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



Login to the support portal

Enter the details below

.....

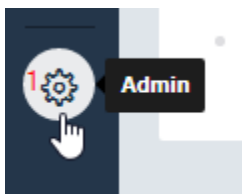
.....

Remember me on this computer

[Forgot your password?](#)

**LOGIN**

2. Click on Admin tab in left side menu.



3. Admin window will appear, click on **Helpdesk Security** under **General Settings**.

## Admin

### General Settings

Configure the basic settings that are necessary for your service desk



Helpdesk Rebranding



Helpdesk Security **2**



SLA Policies



Business Hours



Support Portal



Audit Logs **NEW**

4. Security window will appear, check on the **Single Sign On (SSO)** button and **SAML SSO** button and Complete all the field with appropriate values.

Security

#### 3 Single Sign On

##### 4 SAML SSO

SAML is an XML standard used for communicating identities between two web applications. You can use it to let large teams access your support portal easily using Single Sign On.

SAML Login URL

Freshservice will redirect users to this URL to login. You can get this from your SAML Identity Provider.

**5**

Logout URL

Optional logout URL to which users will be sent to when they logout of freshservice.

**6**

Security Certificate Fingerprint

Fingerprint (SHA256) of the SAML certificate provided by your SAML Provider. This will be used for encryption / validation

**7**

##### Simple SSO

Single Sign On allows you to use your own application or a centralized Server (like MS Active Directory) to authenticate agents and customers so that they can access Freshservice without entering a separate username and password.

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

5. Check **on** the **Secure connection using SSL** button and select the Admin user to send the notification.

customers so that they can access Freshservice without entering a separate username and password.

8  **Secure Connection using SSL**  
Secure Sockets Layer allows you to encrypt data that is transferred to and from Freshservice

Want to use Custom SSL for your support portal?

**IP Whitelisting**  
Restrict access to your support portal to only trusted locations and networks by defining the range of allowed IP addresses.

**Session Timeout**

Admin Notifications

Send notifications to

Admin  9

**Notification will be sent when**

- Agent is Added or Deleted
- IP Whitelisting is modified

6. Click on **Save** button.