CITRIX

NetScaler with Unified Gateway

Configuring Freshdesk

Contents

Disclaimer (Documentation)

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.

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

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 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/ your customer Instance is <*customer_domain*>.

  This is required for App Catalog creation in NetScaler.
- Admin account for NetScaler.

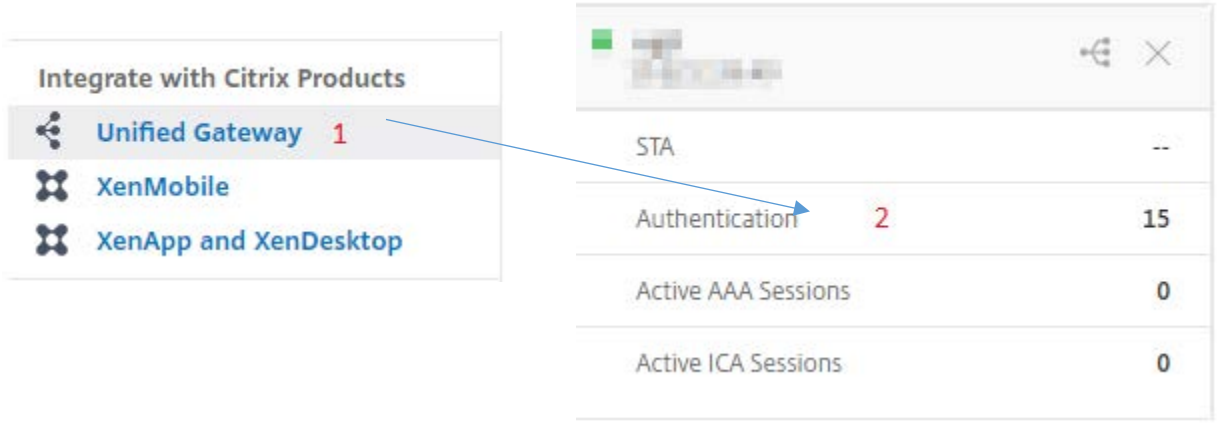
Freshdesk Configuration

The Freshdesk configuration steps are as follows:

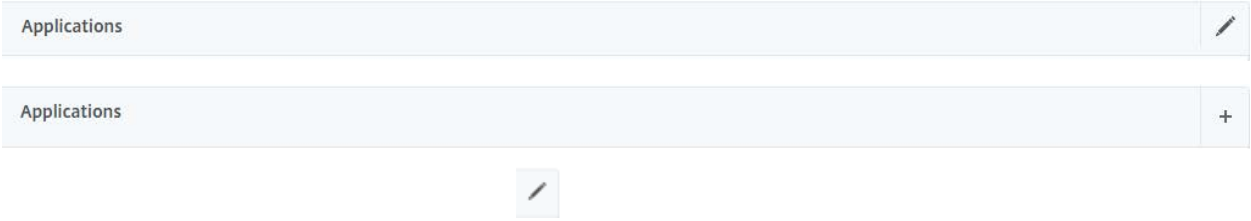
1. Configure Freshdesk with the App Catalog.
2. Configure SAML Setting into Freshdesk.

Step 1: Configure Freshdesk with App catalog

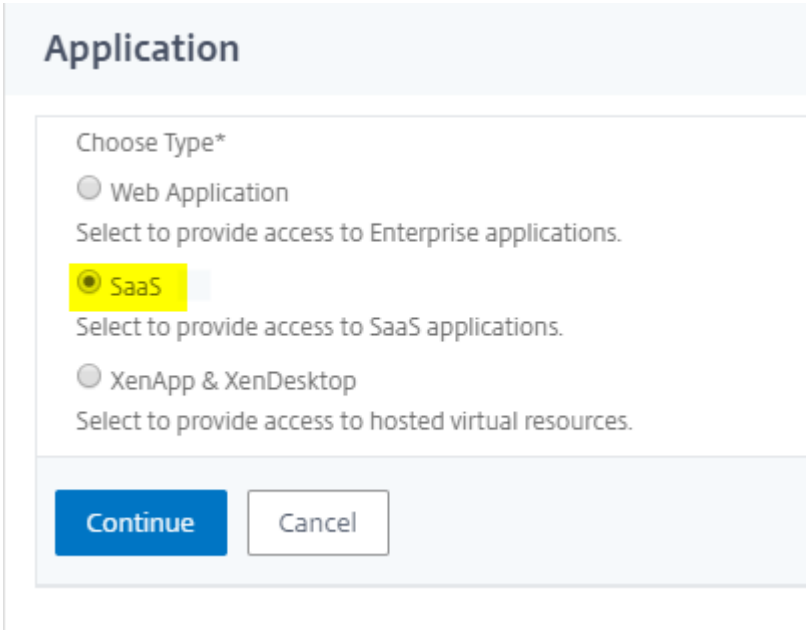
1. Click on Unified Gateway > Authentication



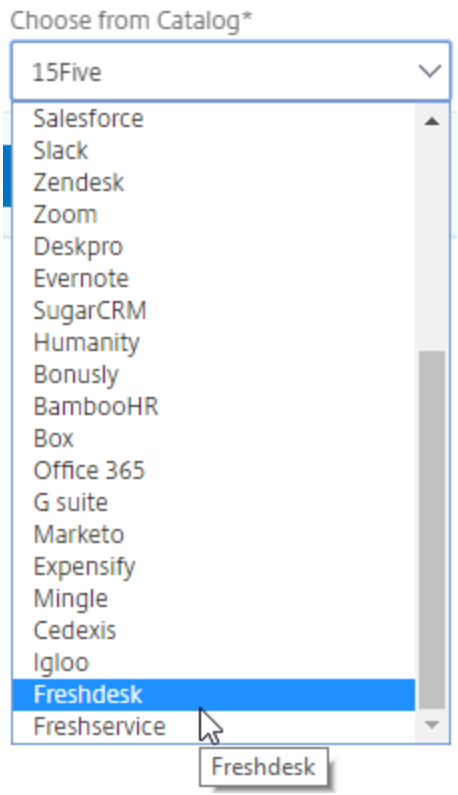
The Unified Gateway Configuration screen appears.



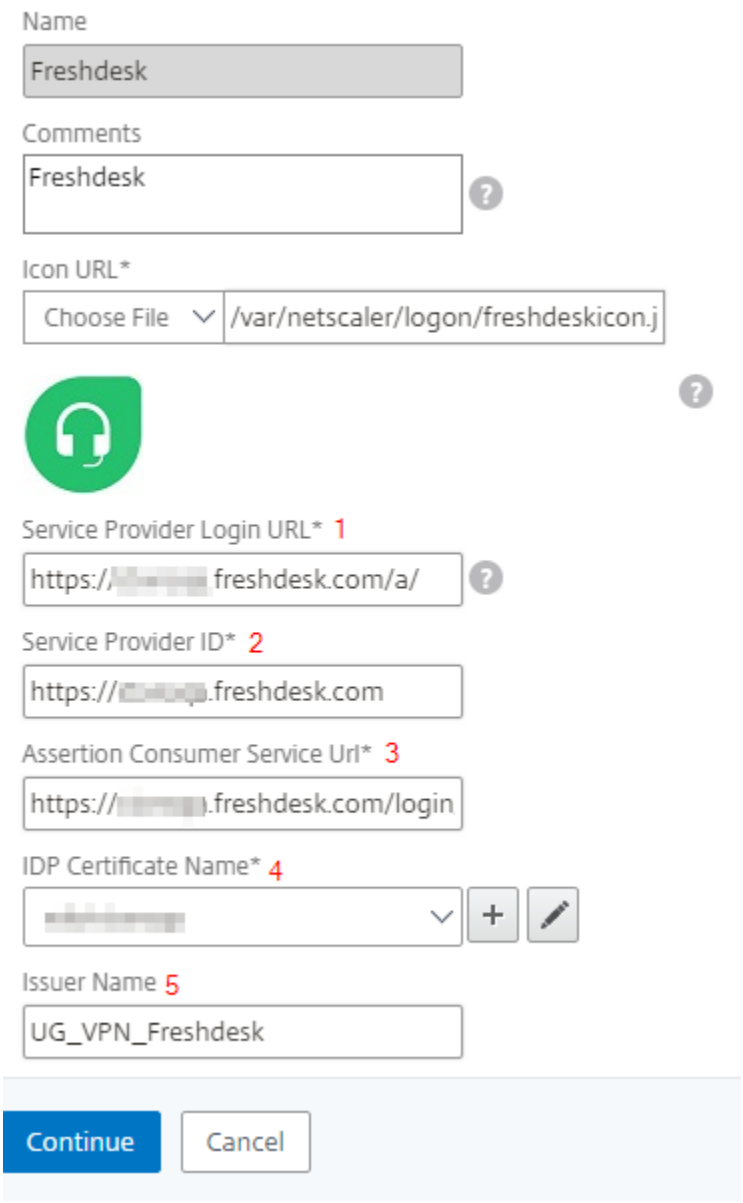
2. Go to **Application** section. Click on **icon**. Now you can see + **icon**. Click on it. The **Application** window appears.



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



5. Fill the Application template with appropriate values.



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

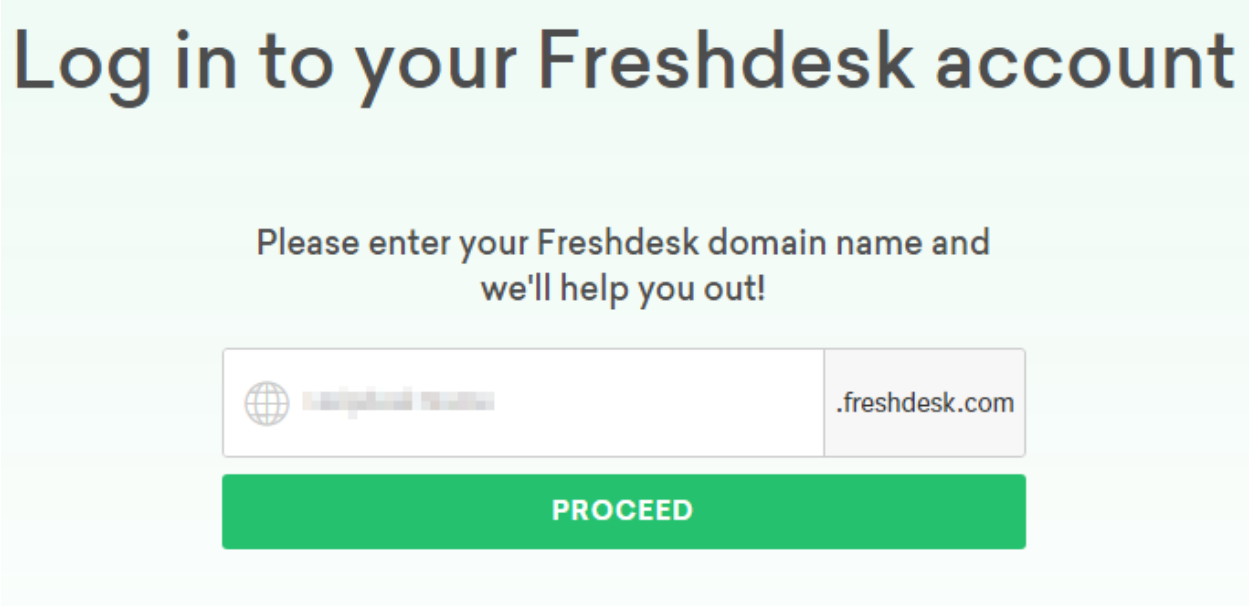
Field Name	Values

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

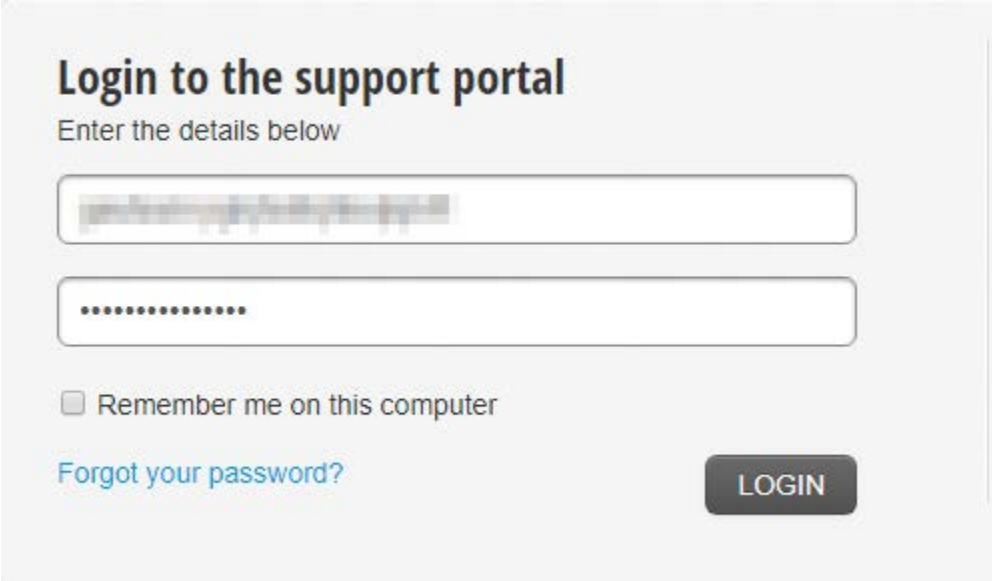
7. In place of <customer_domain>, enter your company domain name (See **Introduction** to know more about the <customer_domain> values).
8. After providing the required values, click **continue.** Click **done.**

Step 2: Configure SAML Setting into Freshdesk

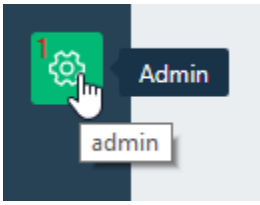
1. Login to **Freshdesk** as an Admin user.



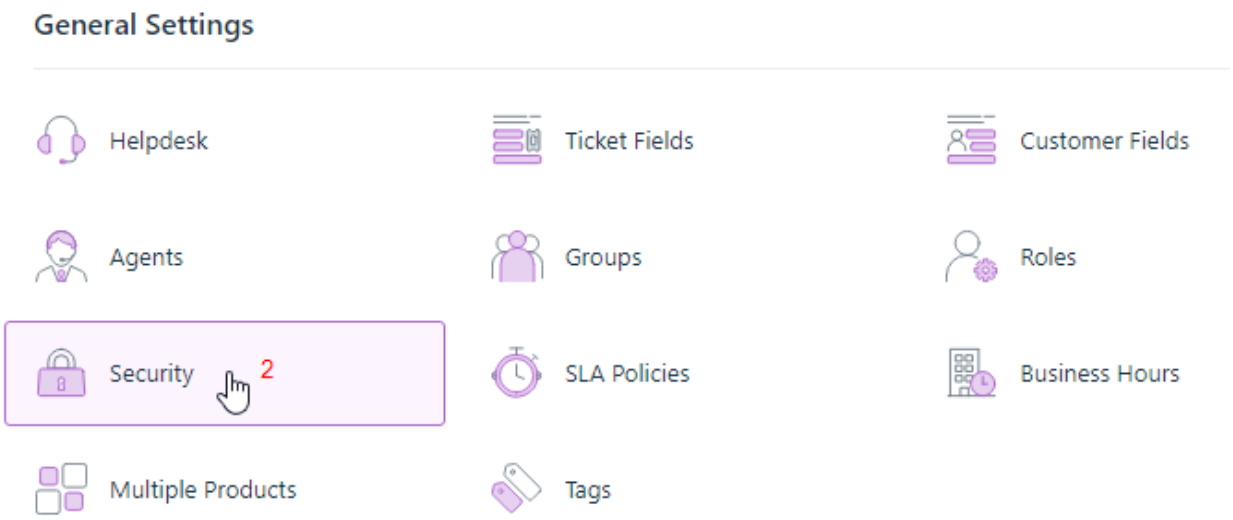
2. Enter your domain name and click on proceed, you will navigate to your domain login page.



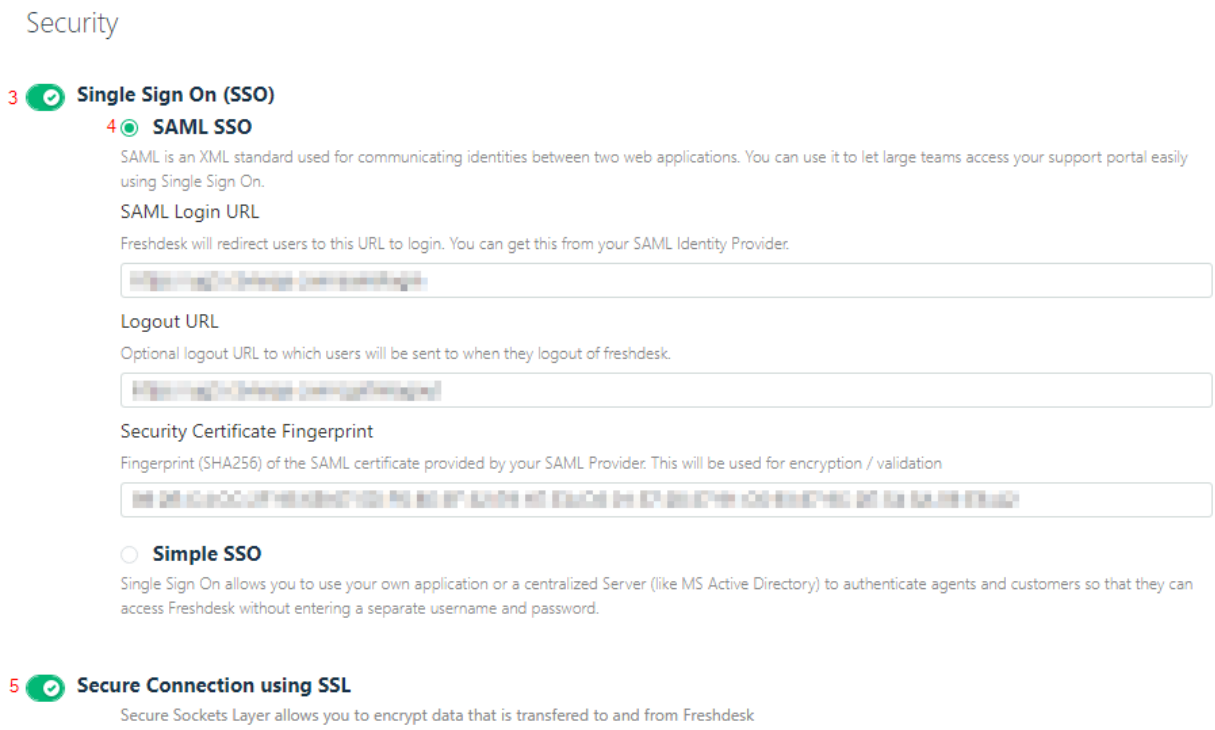
3. Click on **Admin** tab in left side menu.



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

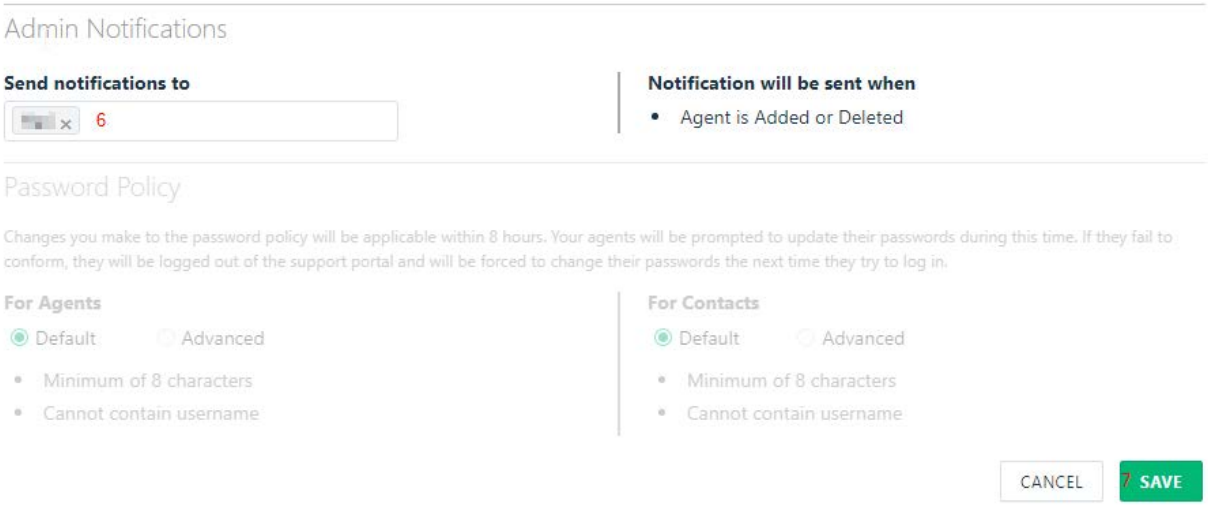


5. Security window will appear, check on the **Single Sign On** (**SSO**), **SAML SSO** and **Secure connection using SSL** buttons and Complete all the field with appropriate values.



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

6. Select the Admin user to send the notification.



7. Click on **SAVE**.