CITRIX

# NetScaler with Unified Gateway

## Configuring Zendesk


## Abstract

Configuring Zendesk for SSO enables administrators to manage their users using NetScaler.

# 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.

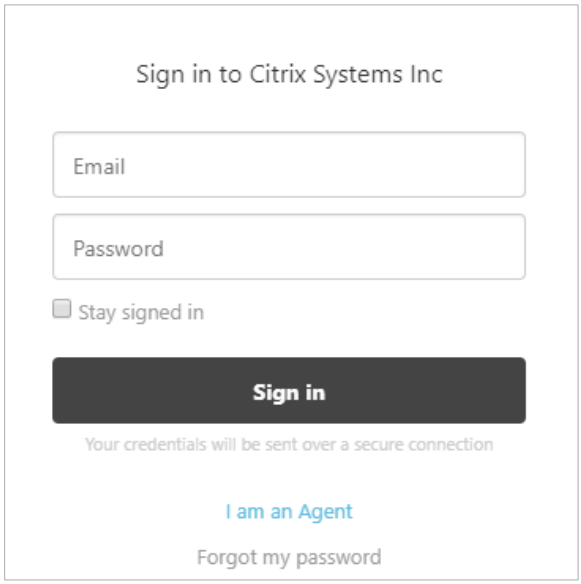
Zendesk provides customer service software and support ticketing system which is a cloud-based help desk solution.

You can connect Zendesk with NetScaler by using your company's credentials to log on to your account via SSO.

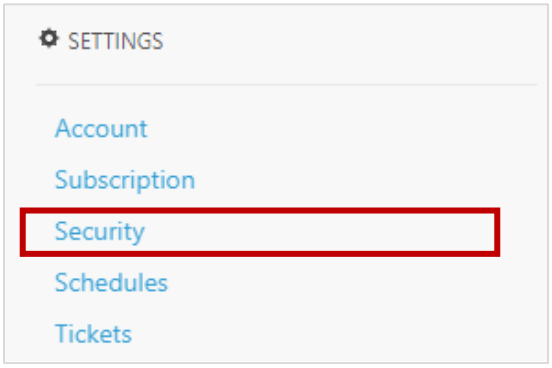
# Configuring Zendesk for Single Sign-on

To configure Zendesk for single sign-on through SAML, follow the steps below:

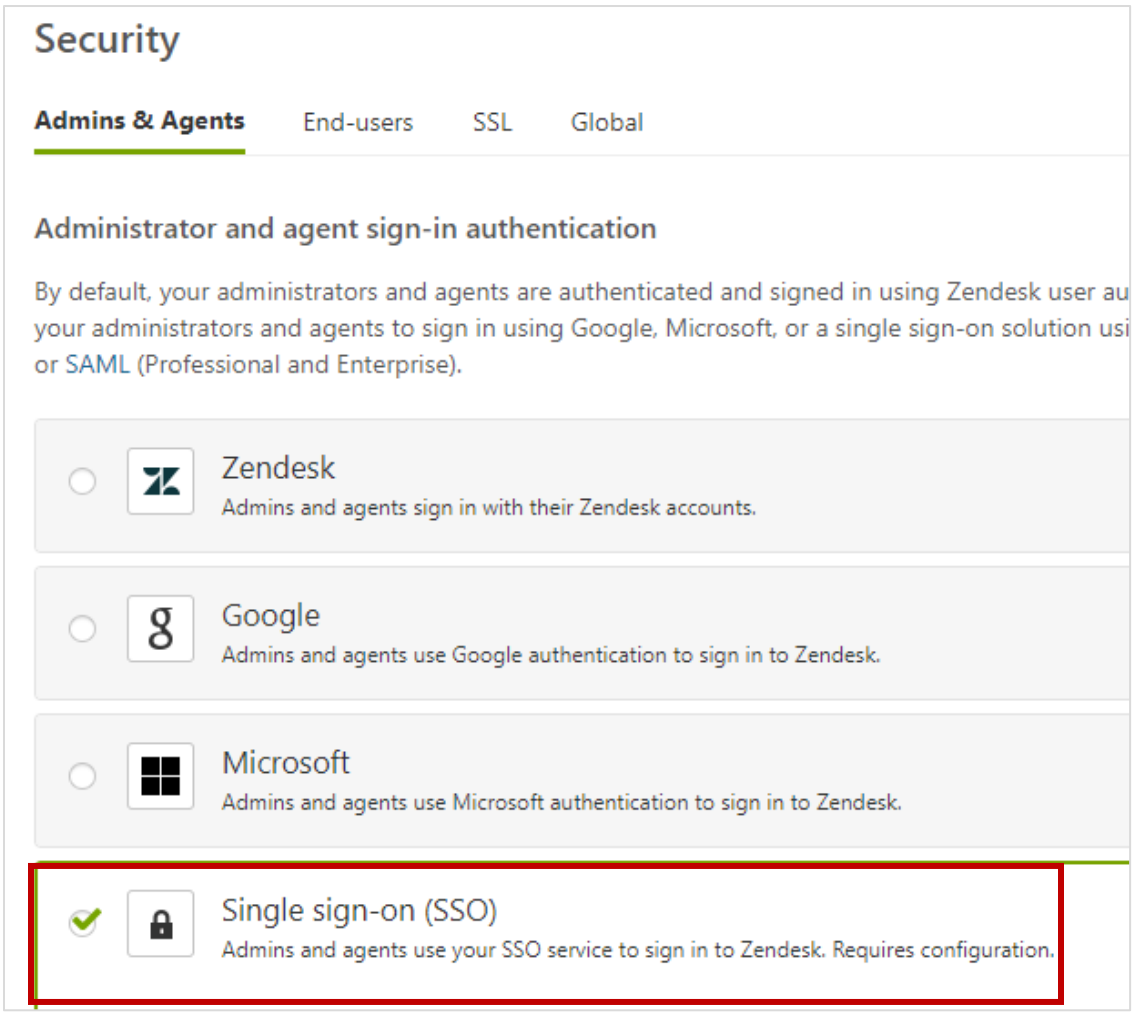
1. In a browser, type https://<customer>.zendesk.com and press enter.
2. Log on to your Zendesk account as an administrator.



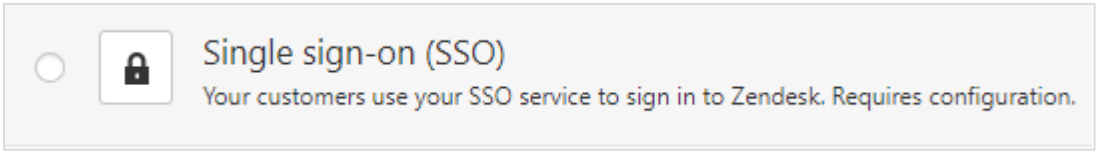

3. On the **Support** page, in the left pane, click the **Admin** icon .
4. In the **Setting** section, click **Security**.



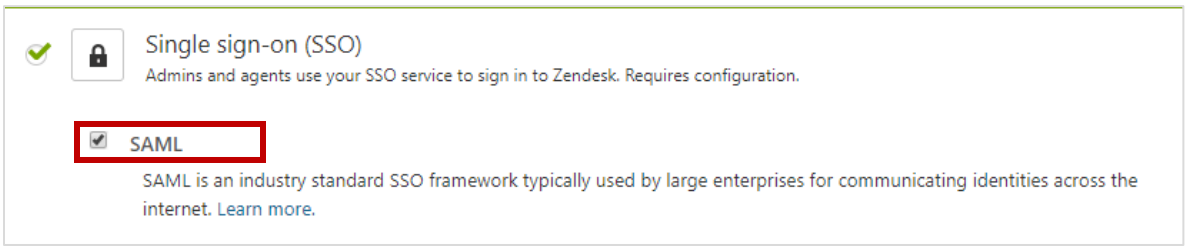
5. In the **Security** area, to enable single sign on for administrators and agents, in the **Admin & Agents** section, click **Single sign-on (SSO)**.



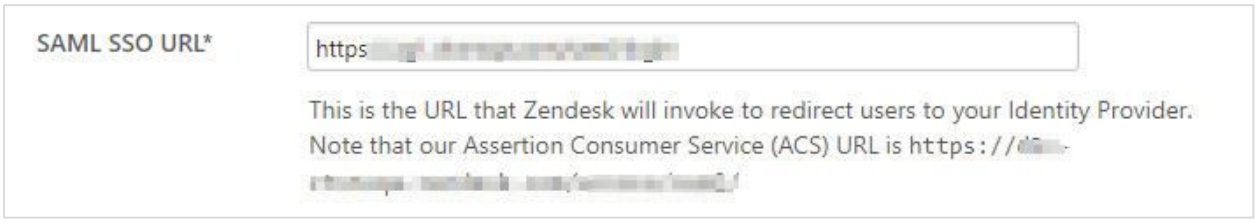

6. To enable single sign on for end users, in the **End-users** section, click **Single sign-on (SSO)**.



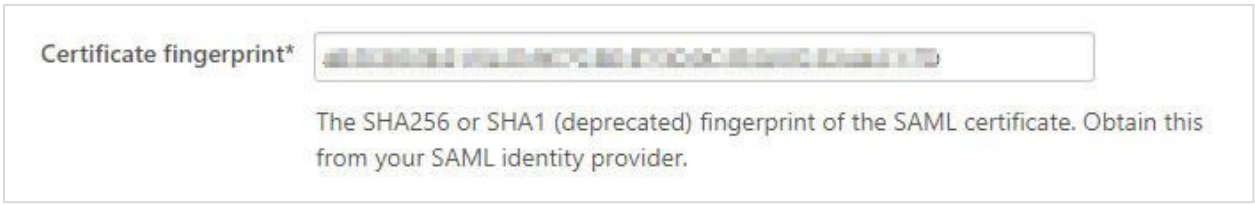

7. Select the **SAML** check box.



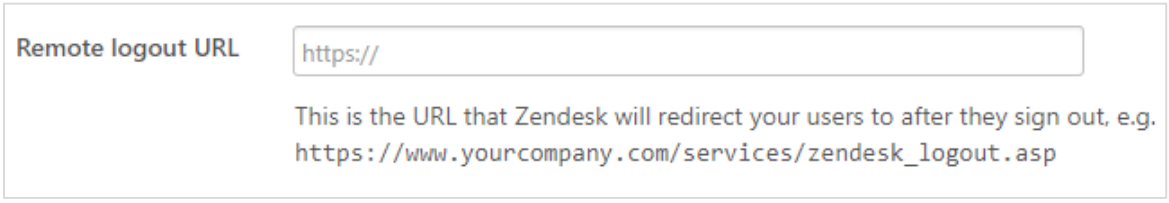
8. Enter the SAML SSO URL for example: https://<Netscaler FQDN>/saml/login.



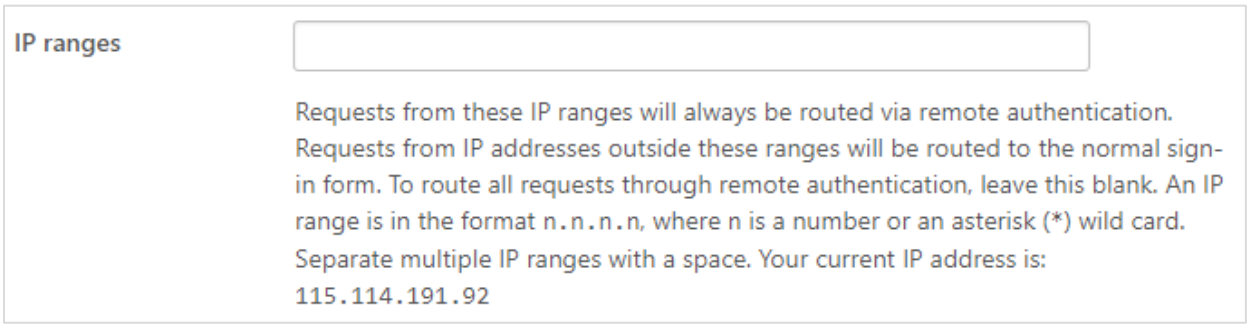

9. In the **Certificate fingerprint*** box, you must paste the Certificate fingerprint.



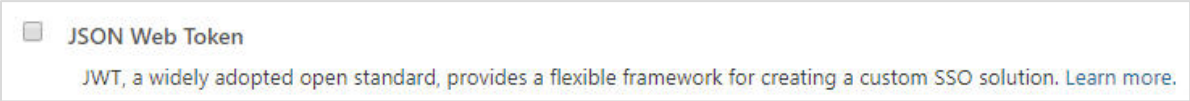

10. To add fingerprint of the NetScaler IDP SAML Signing certificate, follow the steps below:
    i. Remotely access your NetScaler instance using PuTTY.
    ii. Log on to Shell by typing Shell.
    iii. Navigate to /nsconfig/ssl folder (cd /nsconfig/ssl) and press Enter.
    iv. Type *openssl x509 -in certificatename shell.pem -fingerprint –noout* and press Enter.
    v. Copy the fingerprint that has been generated and paste that in the **Certificate fingerprint*** box.
11. If you want the users to redirect to a specific site after logging out, in the **Remote logout URL** box, enter the specific URL. For example: www.yourcompany.com/zendesklogout.



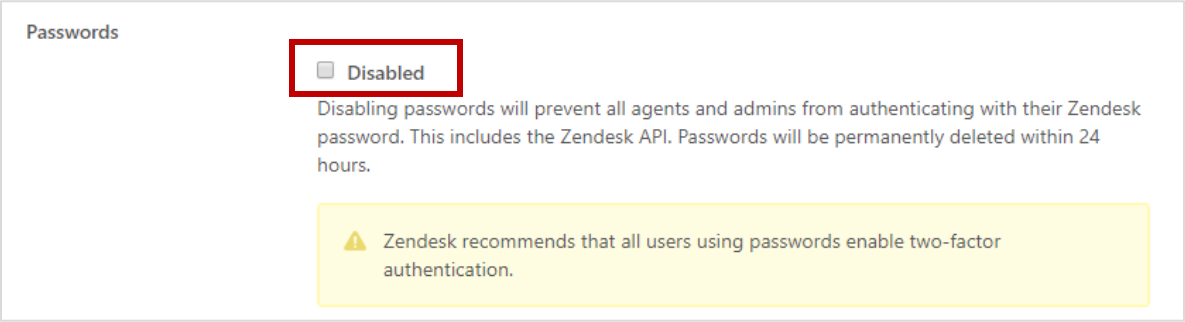

12. Type the IP ranges if required.



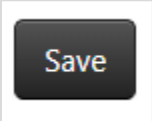
13. Keep the **JSON Web Token** check box unchecked.




14. If you don't want to necessitate the agents and administrators to enter passwords, select the **Disabled** check box.




15. Click **Save**.



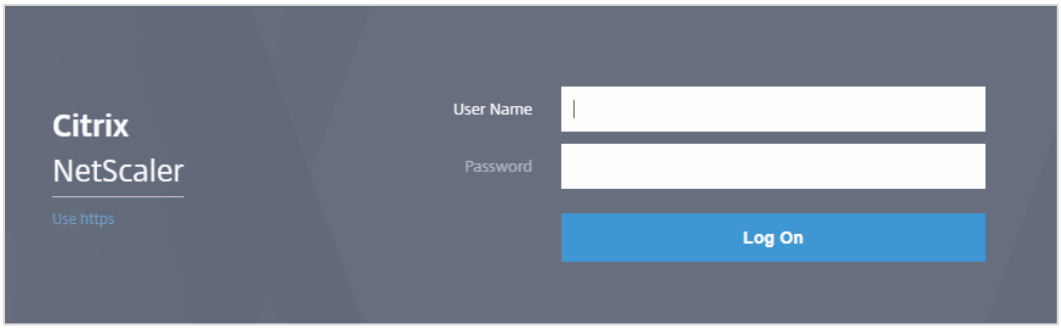

You have completed the required configuration.

# Configuring NetScaler for Single Sign-On

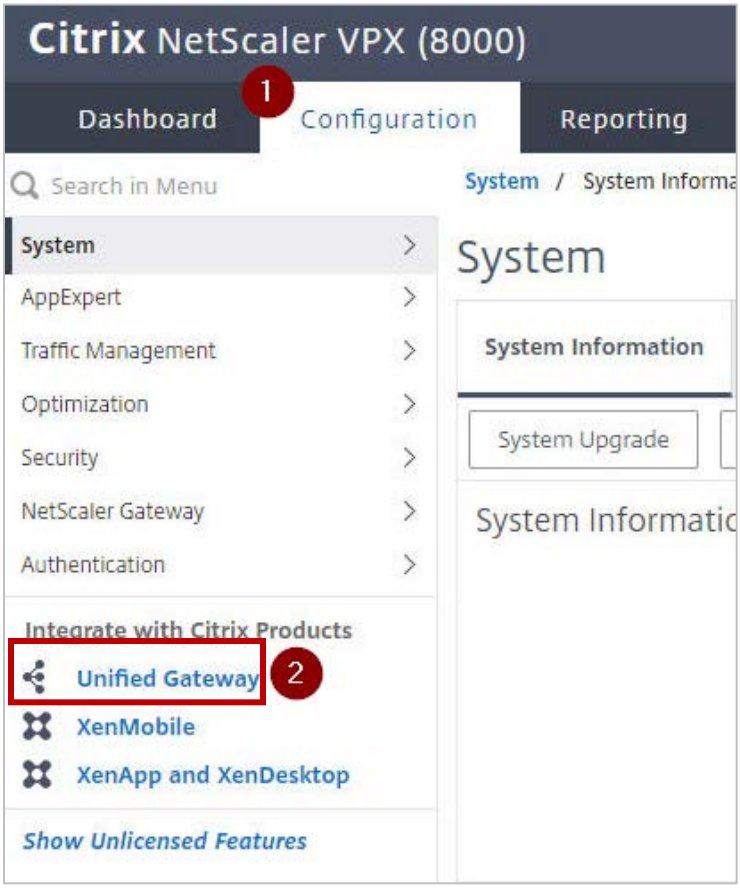
For configuring NetScaler for Zendesk, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

To configure NetScaler for single sign on through SAML, complete the following steps:

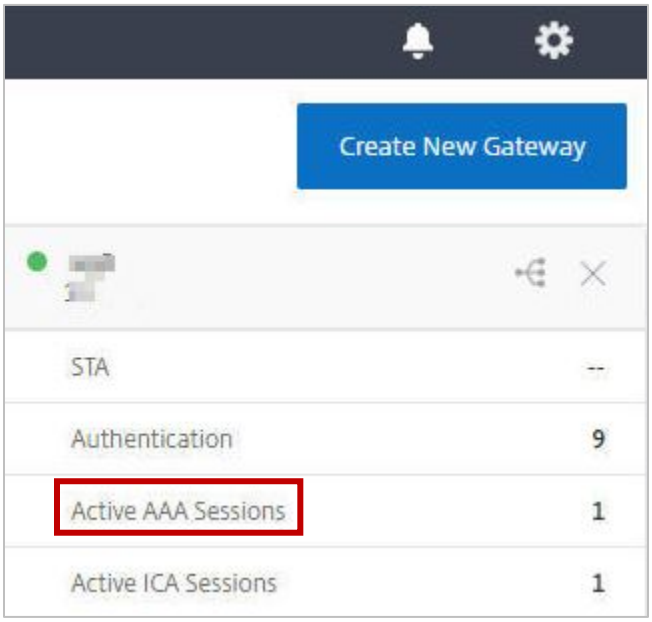
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.




3. Click **Configuration** > **Unified Gateway**.



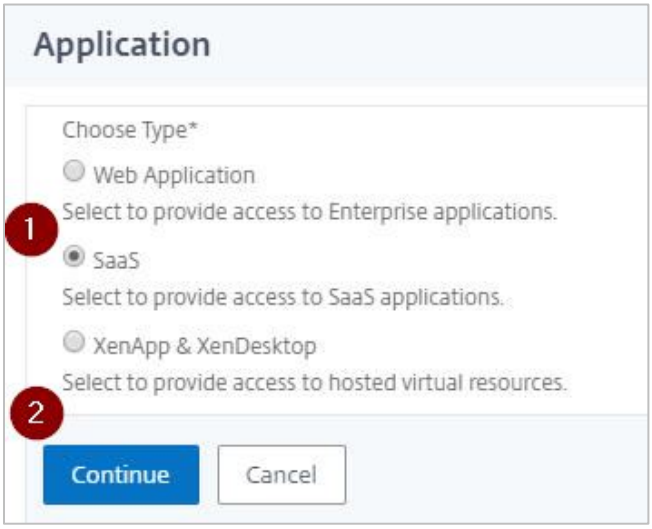
4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



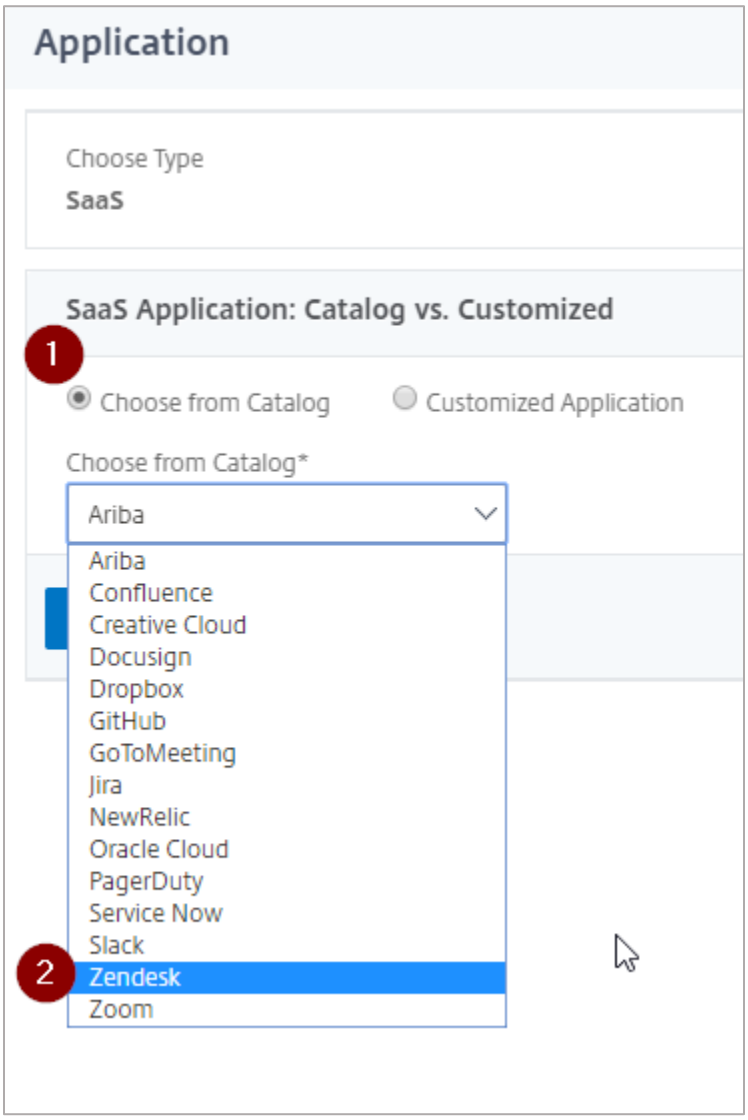

5. Click the edit icon for **Applications** section.


6. For adding a SaaS application, click the plus icon ⊞ that appears in the edit mode.

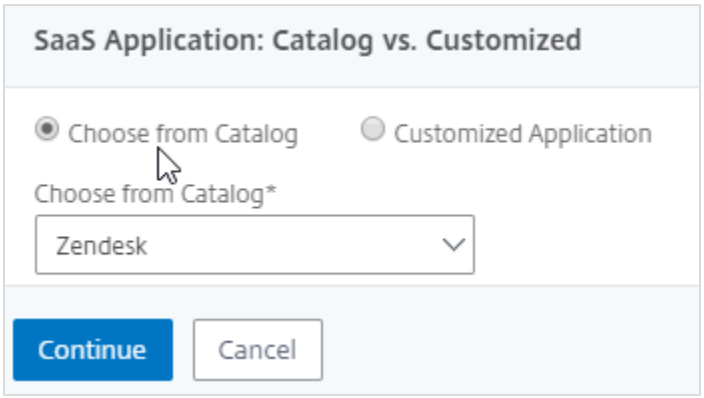

7. Click **SaaS** > **Continue**.



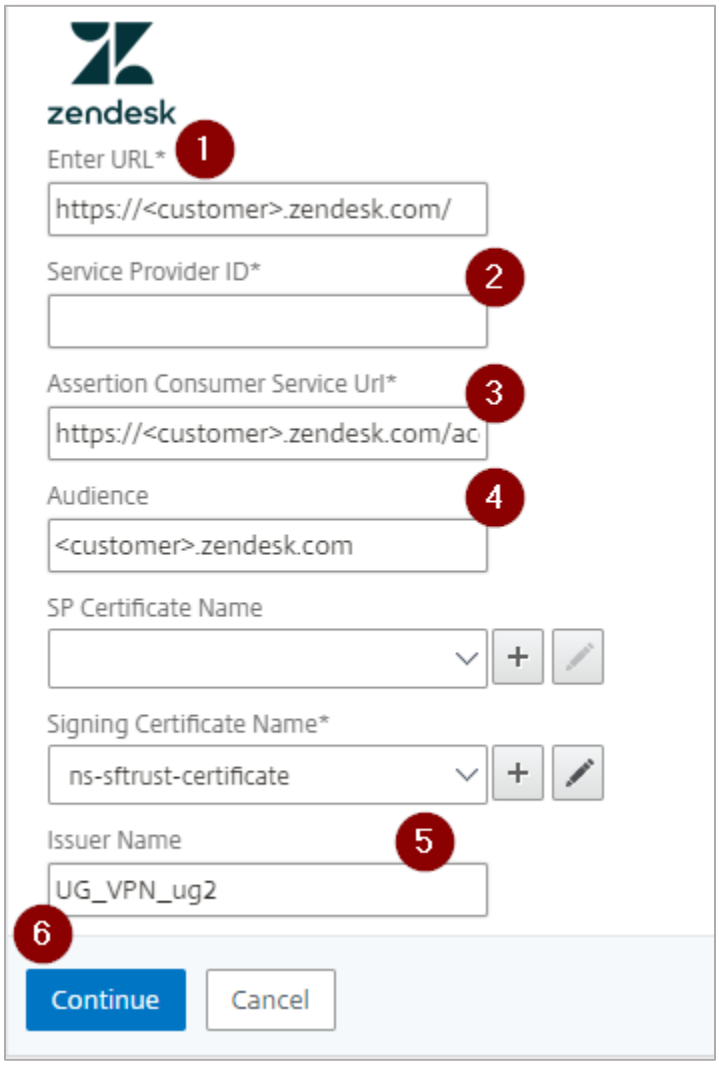
8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **Zendesk**.




10. Click **Continue**.

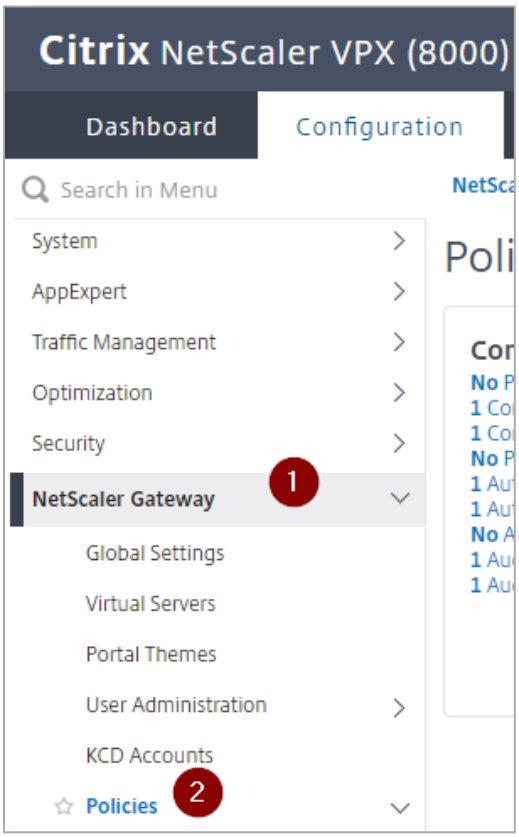


11. In the **Application** area, under **Create Application from Template** section, specify the following information:
    - **Enter URL** - enter your Zendesk URL that you use for accessing Zendesk
    - **Service Provider ID** - type the Zendesk URL that you use for accessing Zendesk without a trailing slash

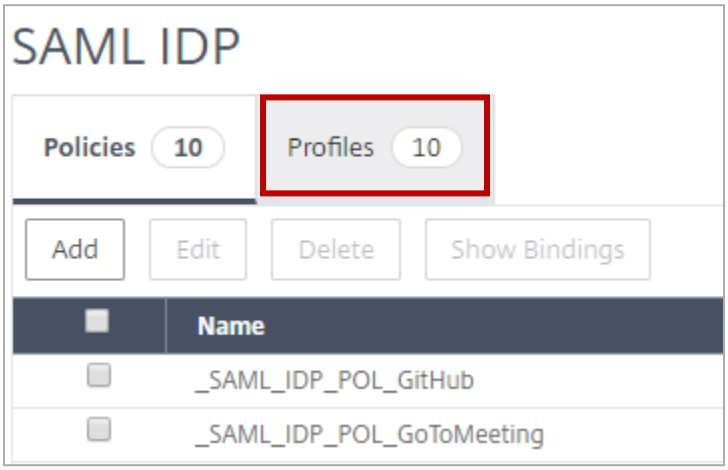



    - **Assertion Consumer Service URL** - type the appropriate URL based on the format: https://<customer>.zendesk.com/access/saml/
    - **Audience** - type the appropriate ULR based on the format: https://<customer>.zendesk.com/access/saml/
    - **Issuer Name** - type the service provider ID
12. Click **Continue**.
13. Click **Done**.

14. As Zendesk does not provide SP certificate, you must clear the **Reject Unsigned Requests** check box. To do so, follow the steps below:
    i. In Citrix NetScaler's **Configuration** tab, click **NetScaler Gateway** and then click **Policies**.

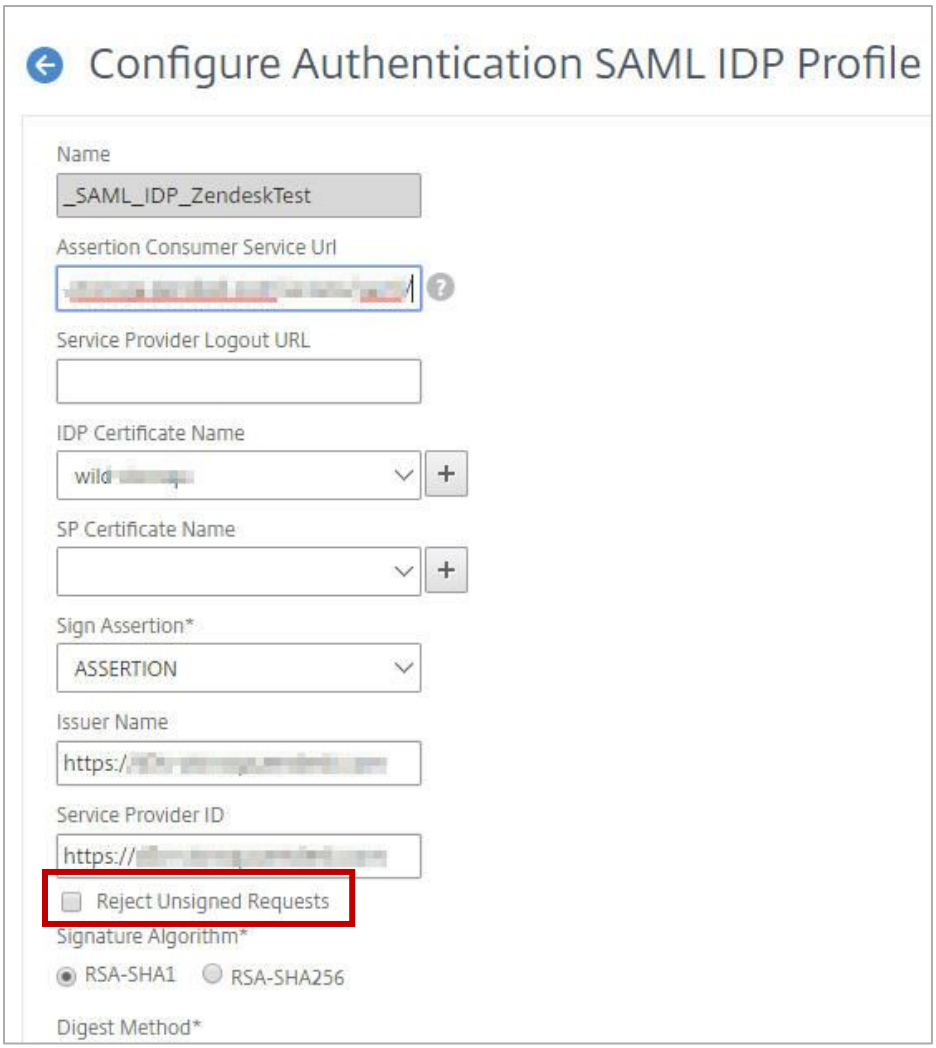



    ii. Click **Authentication** > **SAML IDP**.
    iii. In the **SAML IDP** area, click the **Profiles** tab.




    iv. Click the SAML profile for Zendesk.

v. Clear the **Reject Unsigned Requests** check box.




vi. Click **OK.**

You have completed the NetScaler configuration for Zendesk.

# Testing the Configuration

## Testing the IdP Initiated Flow

To test the IdP initiated configuration, follow the steps below:

1. Access the IdP URL.
2. Log on to NetScaler appliance using your enterprise credentials.
3. Click **Clientless Access**.
4. On the home page, click **Apps** tab.
5. Click **Zendesk**.
   You are logged on to Zendesk.
   You have completed testing the IdP initiated flow.

## Testing the SP Initiated Flow

To test the SP initiated configuration, follow the steps below:

1. Access the Zendesk instance.
2. If you are an administrator or an agent, click **I am an Agent**.
3. You are redirected to NetScaler appliance's log in page.
4. Log on to NetScaler appliance using your enterprise credentials.
   You are logged on to Zendesk.
   You have completed testing the SP initiated flow.

**Locations**

**Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States**