



NetScaler with Unified Gateway

Configuring Zendesk

Abstract

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

Contents

- ABSTRACT0
- DISCLAIMER (DOCUMENTATION)2
- PREFACE3
- OVERVIEW4
- CONFIGURING ZENDESK FOR SINGLE SIGN-ON4
- CONFIGURING NETSCALER FOR SINGLE SIGN-ON8
- TESTING THE CONFIGURATION.....14

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
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.

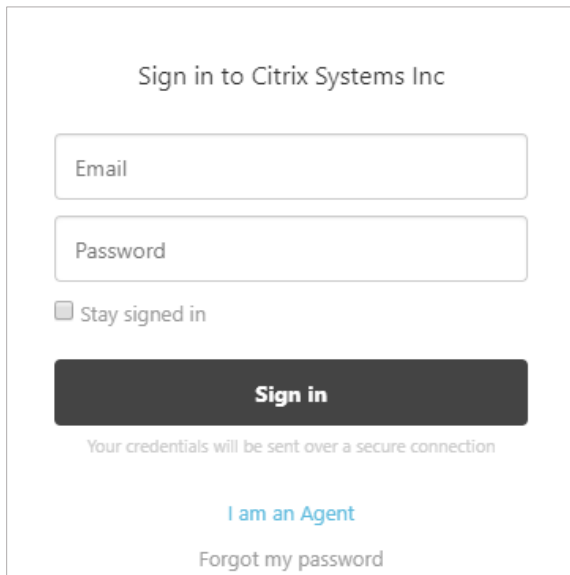
Zendesk provides customer service software and support ticketing system which is a cloud-based help desk solution.

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

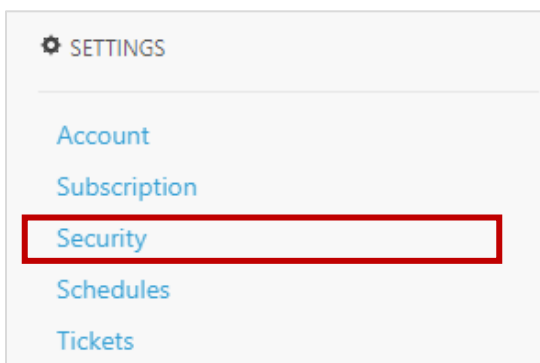
To configure Zendesk for single sign-on through SAML, follow the steps below:

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



The screenshot shows the sign-in page for Citrix Systems Inc. It features a title "Sign in to Citrix Systems Inc" at the top. Below the title are two input fields: "Email" and "Password". Underneath the "Password" field is a checkbox labeled "Stay signed in". A prominent black "Sign in" button is centered below the checkbox. Below the button, a message states "Your credentials will be sent over a secure connection". At the bottom of the form, there are two links: "I am an Agent" in blue text and "Forgot my password" in a smaller, grey font.

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



The screenshot displays the "SETTINGS" menu in the Zendesk interface. The menu is titled "SETTINGS" with a gear icon. Below the title, there is a list of settings categories: "Account", "Subscription", "Security", "Schedules", and "Tickets". The "Security" option is highlighted with a red rectangular border.

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





The screenshot shows the 'Security' configuration page for 'Admins & Agents'. It features a navigation bar with 'Admins & Agents', 'End-users', 'SSL', and 'Global'. The main heading is 'Administrator and agent sign-in authentication'. Below this, a paragraph explains that by default, users are authenticated with Zendesk accounts, but can be configured to use Google, Microsoft, or SAML. A list of four authentication methods is provided, each with a radio button and a description. The 'Single sign-on (SSO)' option is selected, indicated by a green checkmark and a red rectangular highlight.

Security

Admins & Agents End-users SSL Global


Administrator and agent sign-in authentication

By default, your administrators and agents are authenticated and signed in using Zendesk user accounts. You can configure your administrators and agents to sign in using Google, Microsoft, or a single sign-on solution using SAML (Professional and Enterprise).

-  **Zendesk**
Admins and agents sign in with their Zendesk accounts.
-  **Google**
Admins and agents use Google authentication to sign in to Zendesk.
-  **Microsoft**
Admins and agents use Microsoft authentication to sign in to Zendesk.
-  **Single sign-on (SSO)**
Admins and agents use your SSO service to sign in to Zendesk. Requires configuration.


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

The screenshot shows the 'End-users' section of the configuration page. It contains a single radio button option for 'Single sign-on (SSO)', which is currently unselected. The description states that customers use the SSO service to sign in to Zendesk, and that configuration is required.

 **Single sign-on (SSO)**
Your customers use your SSO service to sign in to Zendesk. Requires configuration.

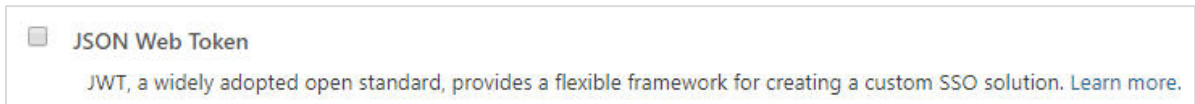
7. Select the **SAML** check box.

This screenshot shows the configuration details for the 'Single sign-on (SSO)' option. It includes a green checkmark and a lock icon. Below the main heading, there is a checkbox for 'SAML' which is checked and highlighted with a red box. A descriptive paragraph explains that SAML is an industry standard SSO framework used by large enterprises for communicating identities across the internet, with a link to 'Learn more'.

 **Single sign-on (SSO)**
Admins and agents use your SSO service to sign in to Zendesk. Requires configuration.

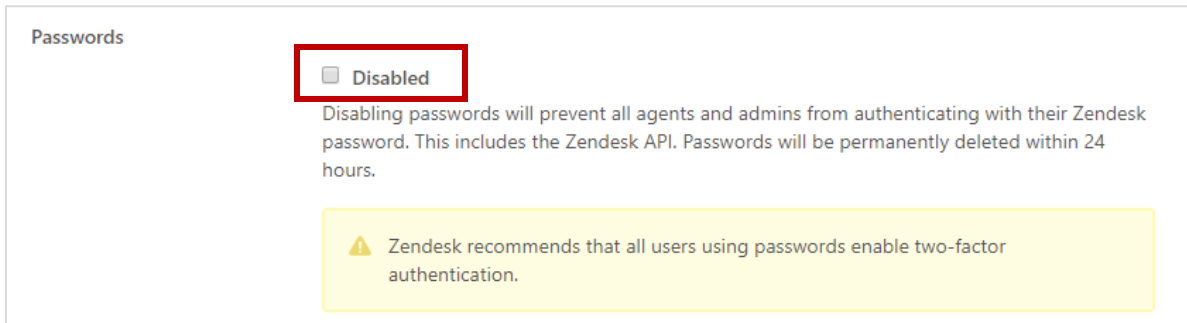
SAML
SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet. [Learn more.](#)

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



JSON Web Token
JWT, a widely adopted open standard, provides a flexible framework for creating a custom SSO solution. [Learn more.](#)


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



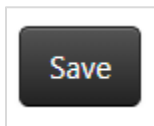
Passwords

Disabled

Disabling passwords will prevent all agents and admins from authenticating with their Zendesk password. This includes the Zendesk API. Passwords will be permanently deleted within 24 hours.

 Zendesk recommends that all users using passwords enable two-factor authentication.

15. Click **Save**.



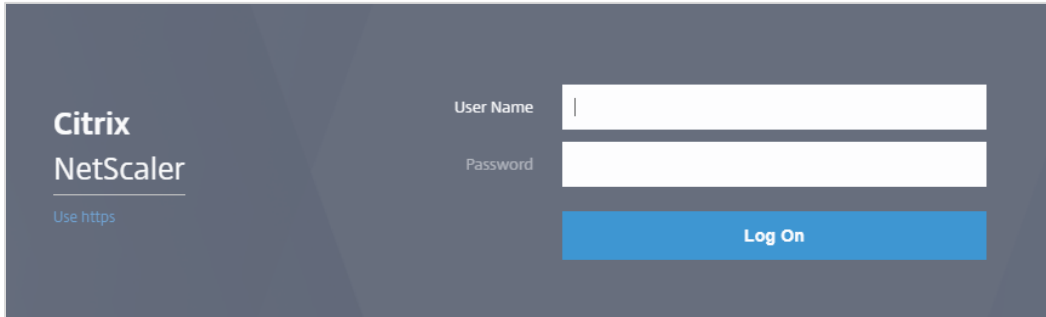
You have completed the required configuration.

Configuring NetScaler for Single Sign-On

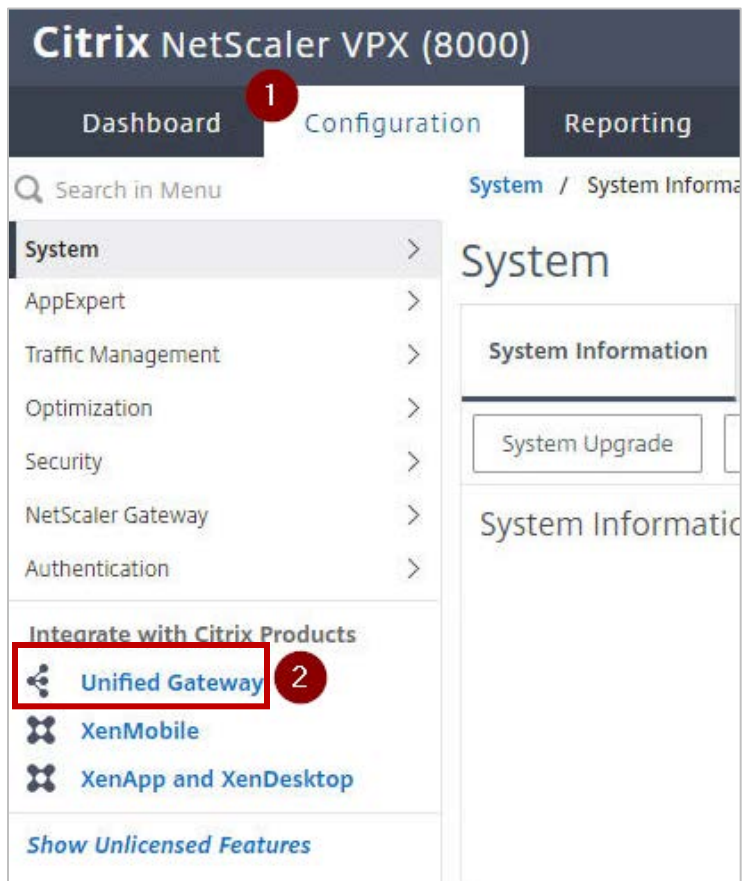
For configuring NetScaler for Zendesk, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

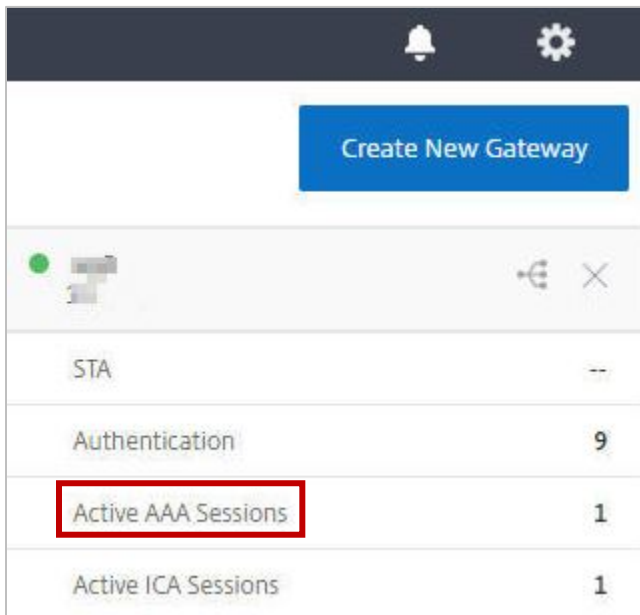
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



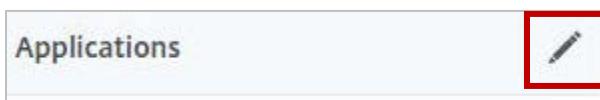
3. Click **Configuration > Unified Gateway**.



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



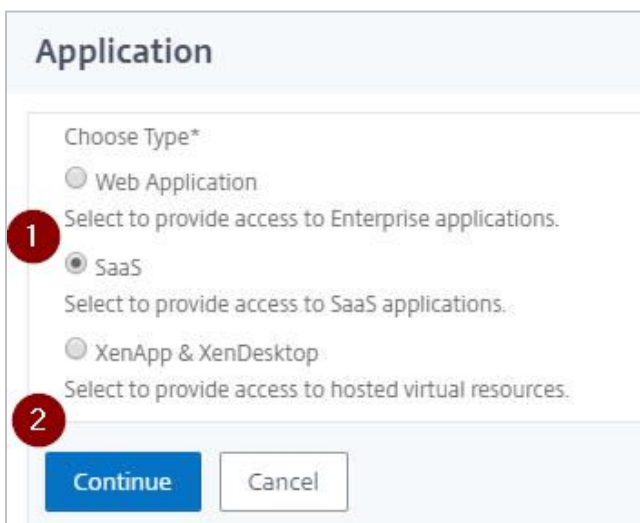
5. Click the edit icon for **Applications** section.



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**.

Application

Choose Type
SaaS

SaaS Application: Catalog vs. Customized

Choose from Catalog Customized Application

Choose from Catalog*

Ariba

Ariba
Confluence
Creative Cloud
Docusign
Dropbox
GitHub
GoToMeeting
Jira
NewRelic
Oracle Cloud
PagerDuty
Service Now
Slack
Zendesk
Zoom

10. Click **Continue**.

SaaS Application: Catalog vs. Customized

Choose from Catalog Customized Application

Choose from Catalog*

Zendesk

Continue Cancel

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

The screenshot shows the 'Create Application from Template' form for Zendesk. It includes the following fields and callouts:

- 1**: Enter URL* (https://<customer>.zendesk.com/)
- 2**: Service Provider ID* (empty)
- 3**: Assertion Consumer Service Url* (https://<customer>.zendesk.com/ac)
- 4**: Audience (<customer>.zendesk.com)
- SP Certificate Name (dropdown menu)
- Signing Certificate Name* (ns-sftrust-certificate)
- 5**: Issuer Name (UG_VPN_ug2)
- 6**: Buttons for Continue and Cancel

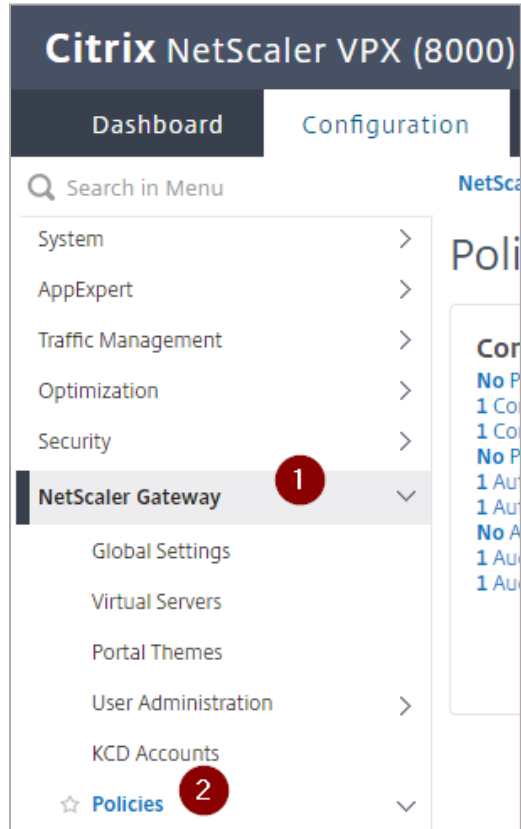
- **Assertion Consumer Service URL** - type the appropriate URL based on the format: https://<customer>.zendesk.com/access/saml/
- **Audience** - type the appropriate ULR based on the format: https://<customer>.zendesk.com/access/saml/
- **Issuer Name** - type the service provider ID

12. Click **Continue**.

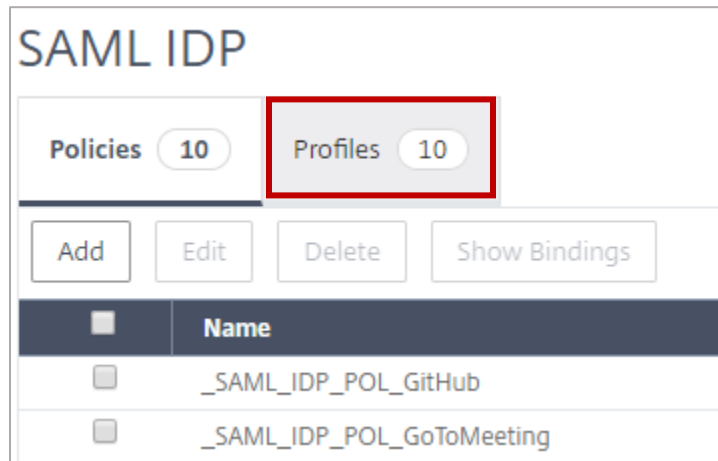
13. Click **Done**.

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.

The screenshot shows the 'Configure Authentication SAML IDP Profile' configuration page. The page contains several fields and options:

- Name:**
- Assertion Consumer Service Url:**
- Service Provider Logout URL:**
- IDP Certificate Name:**
- SP Certificate Name:**
- Sign Assertion*:**
- Issuer Name:**
- Service Provider ID:**
- Reject Unsigned Requests:** (highlighted with a red box)
- Signature Algorithm*:** RSA-SHA1 RSA-SHA256
- Digest Method*:**

- 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

© 2018 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).