



# NetScaler with Unified Gateway

## Configuring Slack

### Abstract

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

# Contents

- ABSTRACT .....0
- CONTENTS .....1
- DISCLAIMER (DOCUMENTATION) .....2
- PREFACE.....3
- OVERVIEW .....4
- CONFIGURING SLACK FOR SINGLE SIGN-ON.....4
- CONFIGURING NETSCALER FOR SINGLE SIGN-ON .....9
- 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**

| <b>Convention</b> | <b>Description</b>  |
|-------------------|---|
| <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.

Slack provides cloud-based team collaboration tools and services that offer a platform that connects teams with the apps, services, and resources required to accomplish their work.

You can connect Slack with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

## Configuring Slack for Single Sign-On

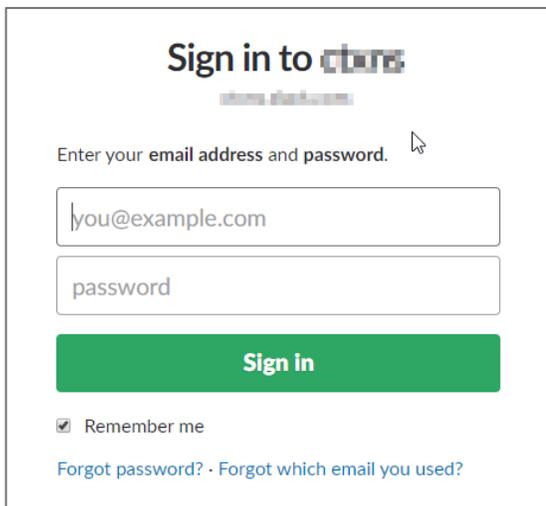
Configuring Slack for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Slack using their enterprise credentials.

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

1. In a browser, type <https://<your-organization>.slack.com> and press Enter.

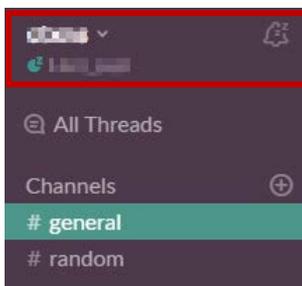
**Note:** For example, if the URL is <https://myserver.slack.com>, you must replace <your-organization> with myserver.

2. Log on to your Slack account.

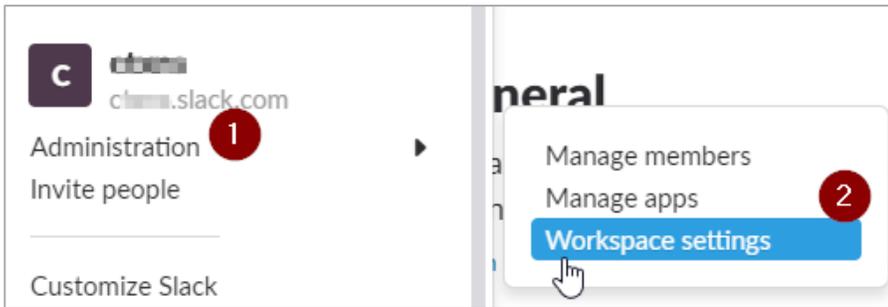


The screenshot shows the Slack sign-in interface for a workspace named 'ctars'. At the top, it says 'Sign in to ctars' with the URL 'ctars.slack.com' below it. A prompt asks the user to 'Enter your email address and password.' There are two input fields: the first contains 'you@example.com' and the second contains 'password'. Below the fields is a green 'Sign in' button. At the bottom, there is a checked 'Remember me' checkbox and two links: 'Forgot password?' and 'Forgot which email you used?'.

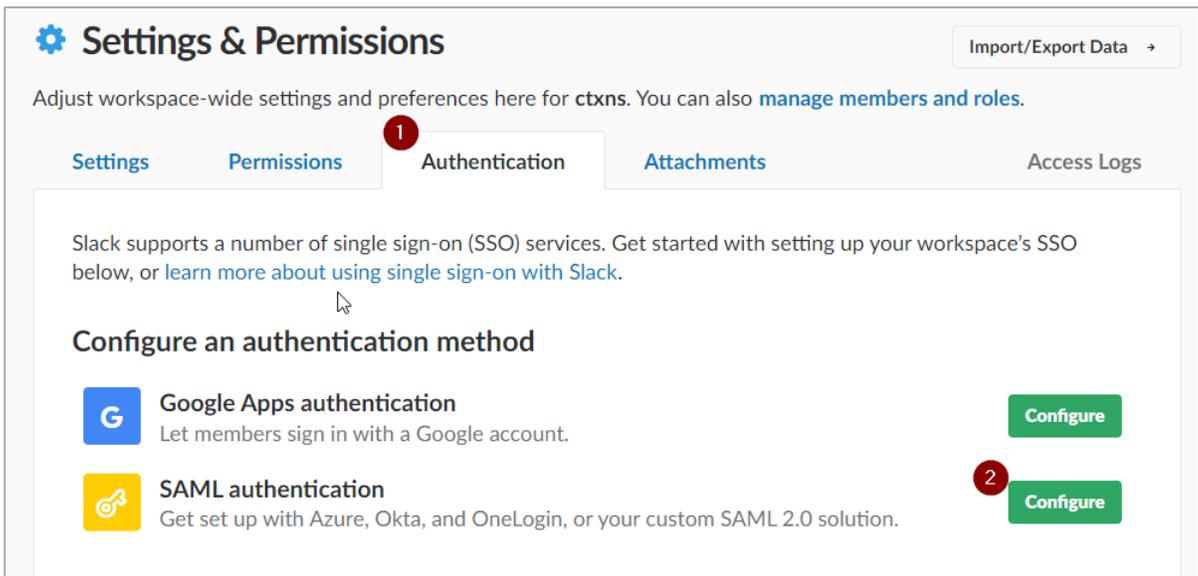
3. On the home page, in the upper left corner, click your workspace name.



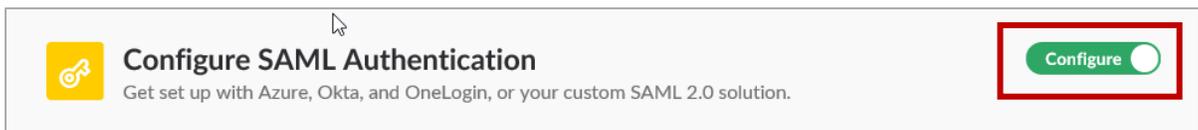
4. Click **Administration** > **Workspace Settings**.



5. Click **Authentication** > **Configure** next to SAML authentication.



6. To turn the test mode on to test and then save the configuration, click **Configure** next to **Configure SAML Authentication**.



The test button  appears indicating that the test mode is turned on.

7. In the **Configure SAML Authentication** section, specify the following information

**SAML 2.0 Endpoint (HTTP) 1**  
Enter your SAML 2.0 Endpoint. This is where you go when you try to login.  
Custom SAML Instructions  
https://ug3.slack.com/saml/login

**Identity Provider Issuer 2**  
The IdP Entity ID for the service you use.  
Slack\_2

**Public Certificate 3**  
\*.slack.com (Slack Systems, Inc.), expiring August 3, 2015 (edit)  
Copy and paste your entire x.509 Certificate here.  
-----BEGIN CERTIFICATE-----  
MIIFPzCCBCcCAwIBAgIQqjY189Tww/LWKRSSWOB2WZANdGqjRUCPw0BA  
QsF...  
wIQWDM3OBE+5F

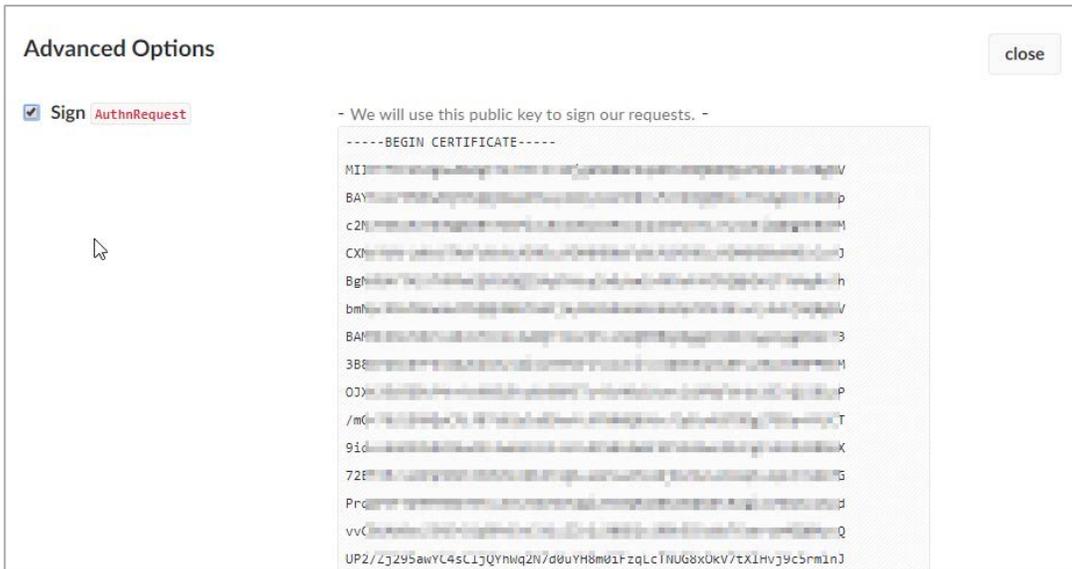
- i. **SAML 2.0 Endpoint (HTTP)** – type the log in URL.
- ii. **Identity Provider Issuer** – type IDP Entity ID.
- iii. **Public Certificate** - paste the identity provider certificate

To upload your IdP certificate, follow the steps below:

- i. Remotely access your NetScaler instance using PuTTY.
- ii. Navigate to /nsconfig/ssl folder (cd /nsconfig/ssl) and press Enter.
- iii. Type cat certificate-name.pem and press Enter.  
**Note:** This is your SAML IdP signing certificate.
- iv. Copy the text from -----BEGIN CERTIFICATE----- to-----END CERTIFICATE-----.

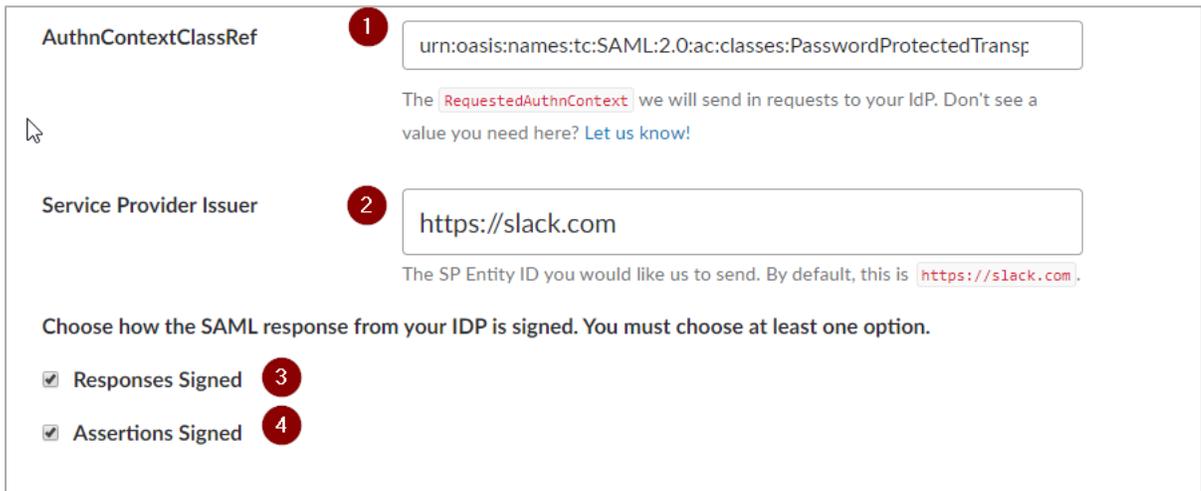
```
root@pers...# cd /nsconfig/ssl
root@pers...# cat certificate-name.pem
-----BEGIN CERTIFICATE-----
4IIC1zCCAkCgAwIBAgIGAWHYpNi8MA0GCSqGSIb3DQEEBQUAMIGuMQswCOYDVOQGEwJVUzETMBEG
A1... YTEU
4B... NDkl
f2... MDEx
q1... MRYw
FA... aWRl
cj... Bgkq
1k... 7aff
oC... 5OyZ
oa... FF3k
q+... H99Z
7x... hr8i
jPrC4ydcwMxqGdFFSQ/LHWUPGvG1pHzj47MzcN0EbdvVmKF61e4/fTkVz3ST3U=
-----END CERTIFICATE-----
root@pers...#
```

8. In the **Advanced Options** section, select the **Sign** check box.



The SP Signing Certificate appears. Copy and paste the value (end-to-end encryption key) in a notepad file and save the file in .pem format. For example: slack-sp.pem.

9. **AuthnContextClassRef** displays the following value by default:  
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport



10. In the **Service Provider Issuer** box, type <https://slack.com>.  
**Note:** If you change the Service Provider Issuer name, ensure that you note it.
11. To specify how the SAML response from your IdP is signed, select the check boxes named **Responses Signed** and **Assertions Signed**.

12. In the **Settings** area, define if the users can edit their profile information such as email address and display name. You can also define if SSO authentication must be optional or required.

### Settings

- Update profile each time a user logs in**  
Available user profile fields will be synced from your identity provider every time a user logs in.
- Allow users to change their email address**  
Users will be able to change their email address to something other than the one from their SAML account. They'll still log in with SAML.
- Allow users to choose their own display name**  
Users will be able to change their display name to something other than the one from their SAML account.

**Authentication for your workspace must be used by:**

- All workspace members
- All workspace members, except guest accounts
- It's optional

13. In the **Customize** area you can type a label for the Sign in button.

### Customize

**Sign In Button Label**

Do you have a nickname for your SSO system? Add it to the Sign In Button!

**Button Preview**



This is what your Sign In Button will look like.

14. To test the configuration, click **Test Configuration**.

### Test and Save

**Test Configuration**

This will only test your changes.

**Save Configuration**

Emails will be sent to workspace members who have not set up SSO for their Slack accounts.

If the configuration is appropriate, a confirmation message appears.

✔ Your test has passed! Save below.

15. Click **Save Configuration**.

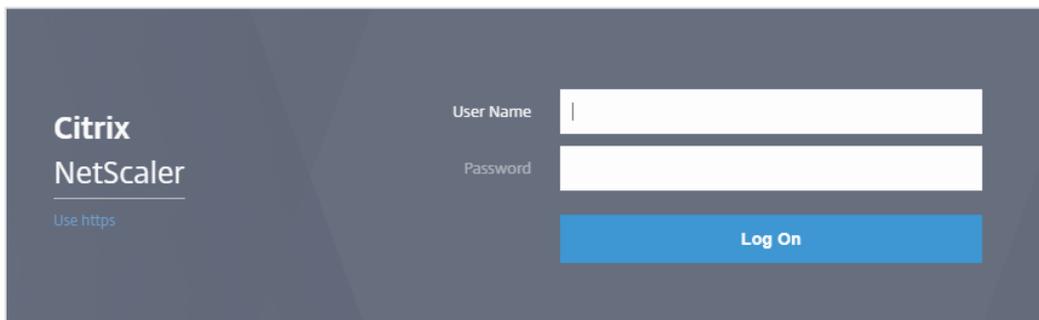
You have completed the required configuration on the service provider which is in this case – Slack.

# Configuring NetScaler for Single Sign-On

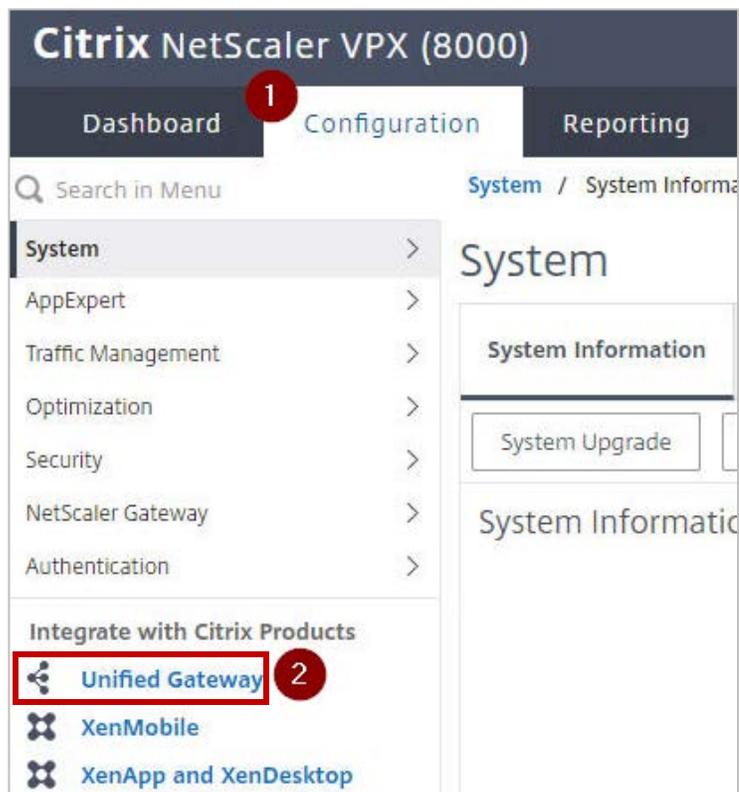
For configuring NetScaler for Slack, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

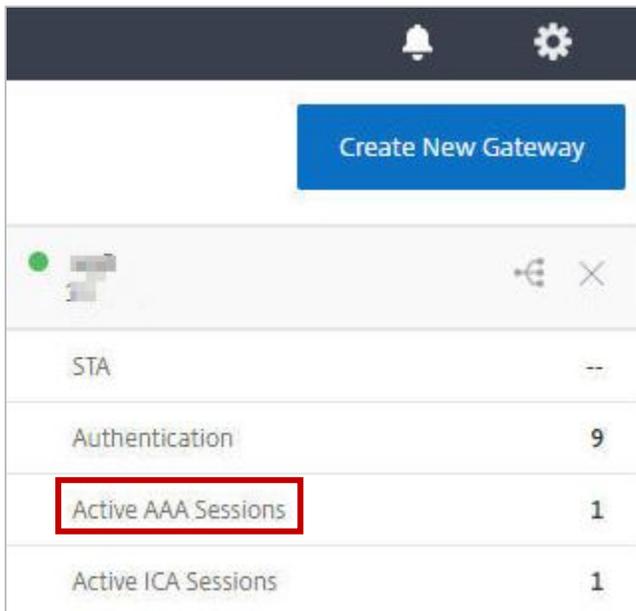
1. Connect to VPN using NetScaler with Unified Gateway.  
**Note:** Ensure that you obtain SP certificate before you start with the configuration. For more information refer: [Obtaining SP Certificate](#).
2. Log on to NetScaler using your user name and password.



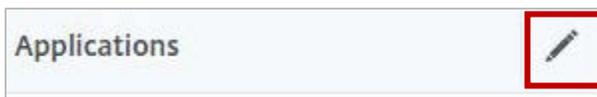
3. Click the **Configuration > Unified Gateway**.



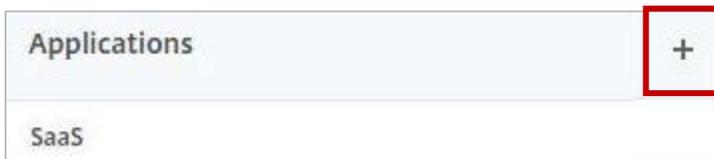
4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



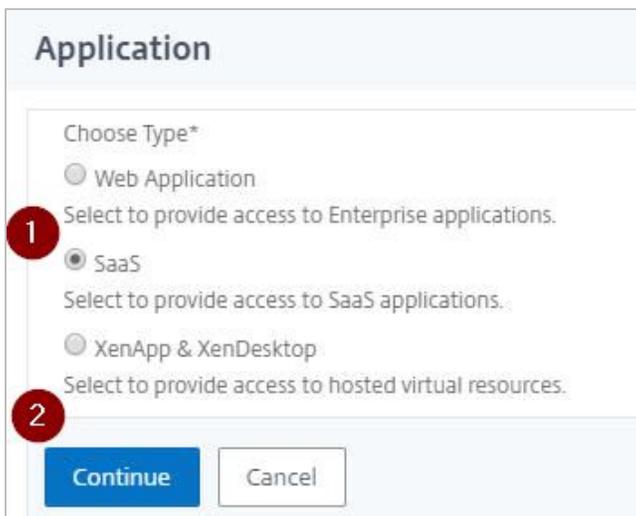
5. Click the edit icon for **Applications** section.



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 **Slack**.

The screenshot shows a form titled "Application". Under the heading "Choose Type", the value "SaaS" is selected. Below this is a section titled "SaaS Application: Catalog vs. Customized". It contains two radio buttons: "Choose from Catalog" (which is selected) and "Customized Application". Under "Choose from Catalog\*", there is a dropdown menu. The menu is open, showing a list of application names: Confluence, Creative Cloud, Docusign, Dropbox, GitHub, GoToMeeting, Jira, Oracle Cloud, PagerDuty, Service Now, Slack, Zendesk, Zoom, WebEx, and Domo. The "Slack" option is highlighted with a blue bar. Red circles with numbers "1" and "2" are overlaid on the image. Circle "1" is positioned over the "Choose from Catalog" radio button, and circle "2" is positioned over the "Slack" option in the dropdown menu.

10. Click **Continue**.
11. In the **Create Application from Template** section, type the name of your SaaS application, in this case Slack, and relevant comments.

The screenshot shows a form titled "Create Application from Template". It has two input fields. The first field is labeled "Name\*" and contains the text "Slack". To the right of this field is a small grey circle with a question mark. The second field is labeled "Comments" and is currently empty. To the right of this field is also a small grey circle with a question mark.

**Note:**

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 the SAML values that you need to copy while configuring SSO for SP and paste the values to appropriate fields while configuring SSO for IdP NetScaler.

Table 2: SSO field values used for SP and IdP configurations

| Service Provider (SP) Slack | Identity Provider (IdP) NetScaler |
|-----------------------------|-----------------------------------|
| Service Provider Issuer     | Service Provider ID               |
| Identity Provider Issuer    | Issuer Name                       |

12. In the area below the logo, specify the following information:

The screenshot shows a configuration form with the following fields and labels:

- 1. Service Provider Login URL\* (text input: https://<your-organization>.slack.co)
- 2. Service Provider Log Out URL\* (empty text input)
- 3. Service Provider ID\* (empty text input)
- 4. Assertion Consumer Service Url\* (text input: https://<your-organization>.slack.co)
- 5. SP Certificate Name (dropdown menu, empty)
- 6. Sign Assertion (dropdown menu, value: ASSERTION)
- 7. IDP Certificate Name\* (dropdown menu, value: ns-sftrust-certificate)
- 8. Issuer Name (text input: U\_...\_...\_2)
- 9. Continue (blue button)
- Cancel (white button)

- i. **Service Provider Login URL** - enter the URL that you use to access Slack in https://<your-organization>.slack.com format.

- Note:** For example, if the URL is <https://myserver.slack.com>, you must replace <your-organization> with myserver.
- ii. **Service Provider Log Out URL** – enter the URL that you use to access Slack in <https://<your-organization>.slack.com> format.  
**Note:** For example, if the URL is <https://myserver.slack.com>, you must replace <your-organization> with myserver.
  - iii. **Service Provider ID** – type the URL that you entered for Service Provider Issuer while configuring Slack.
  - iv. **Assertion Consumer Service Url\*** – enter the URL that you use to access Slack in <https://<your-organization>.slack.com> format.  
**Note:** For example, if the URL is <https://myserver.slack.com>, you must replace <your-organization> with myserver.
  - v. **SP Certificate Name** – click the appropriate certificate name.  
To obtain the SP certificate follow the steps below:
    - a. Copy the file that you saved in pem format while configuring Slack for SSO and paste it to NetScaler I.P. at /nsconfig/ssl using WinSCP or similar tool.
    - b. Remotely access your NetScaler instance using PuTTY.
    - c. Run the following command:  
add ssl certkey slack-sp -cert slack-sp.pem
  - vi. **IDP Certificate Name** – click the appropriate certificate name.
  - vii. **Issuer Name** – type the issuer ID that you entered for Identity Provider Issuer while configuring Slack.

13. Click **Continue**.

14. Click **Done**.

The Slack appears.

15. Click **Done**.

You have completed the NetScaler configuration for Slack.

# 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 **Slack**.  
Your Slack profile is displayed.  
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 vanity URL/signin.
2. You are redirected to NetScaler appliance's log in page.
3. Log on to NetScaler appliance using your enterprise credentials.  
  
Your Slack profile is displayed which indicates that you have successfully logged on to Slack.



**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).