



# NetScaler with Unified Gateway

## Configuring Jira

### Abstract

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

# Contents

- ABSTRACT .....0
- CONTENTS .....1
- DISCLAIMER (DOCUMENTATION) .....2
- PREFACE.....3
- OVERVIEW .....4
- CONFIGURING JIRA FOR SINGLE SIGN-ON.....5
- CONFIGURING NETSCALER FOR SINGLE SIGN-ON .....11
- TESTING THE CONFIGURATION.....17

# 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
<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.

Jira provides bug tracking, issue tracking, and project management functions that help software team to plan, track, and release software.

You can connect Jira with NetScaler by using your company's credentials to log on to your account via 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**

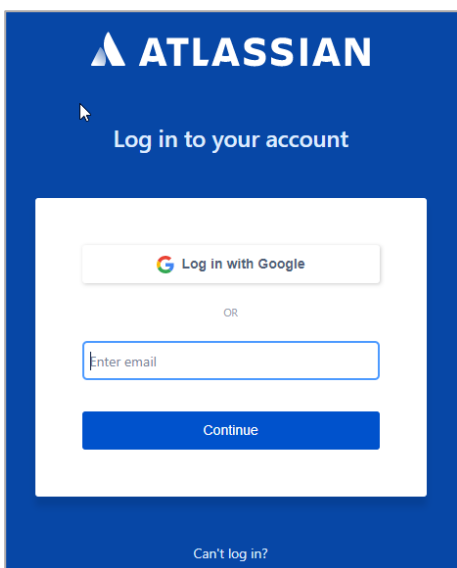
Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

# Configuring Jira for Single Sign-On

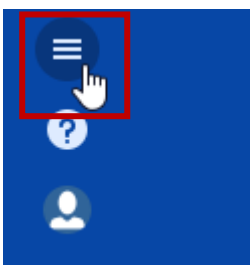
Configuring Jira for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Jira using their enterprise credentials.

To configure Jira for SSO through SAML, follow the steps below:

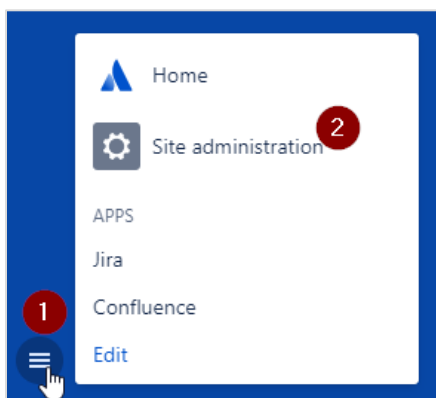
1. In a browser, type your organization's Atlassian cloud URL and press enter.
2. Log on to your Atlassian account.



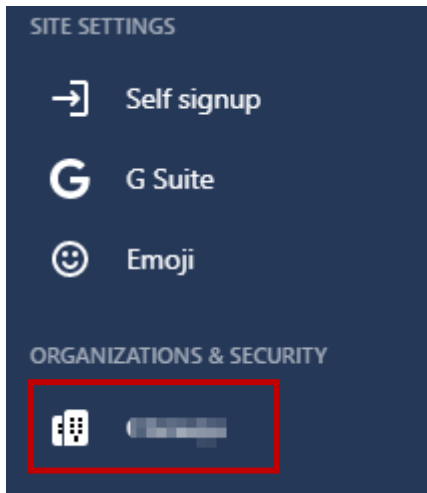
3. On the **Home** page, at the lower-left corner, click .



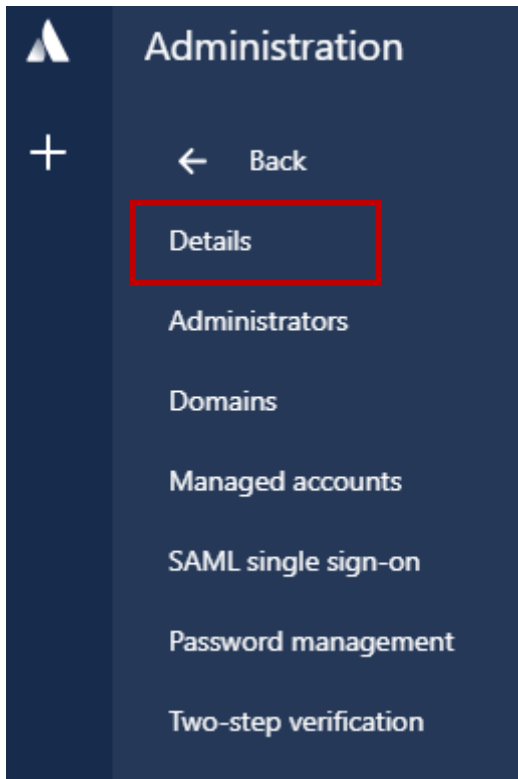
4. Click **Site administration**.



5. On the **Administration** page, in the **ORGANIZATION & SECURITY** section, click the organization name for which you want to configure SAML authentication.

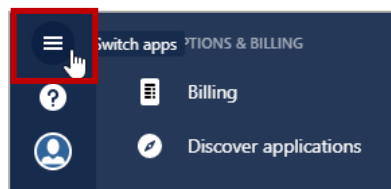


6. Click **Details** and verify the domain.

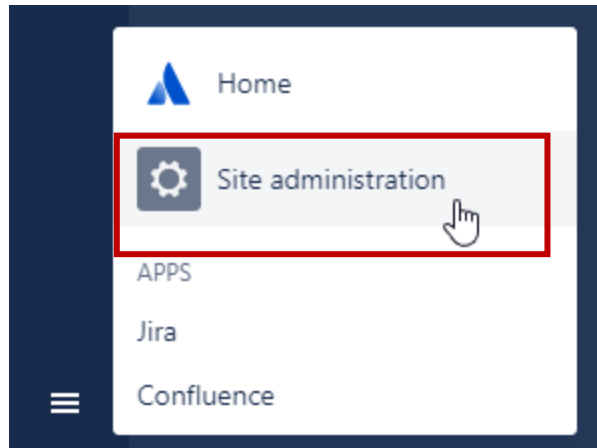


To verify the domain, follow the steps below:

- i. Click the **Switch apps** icon in the lower-left corner.



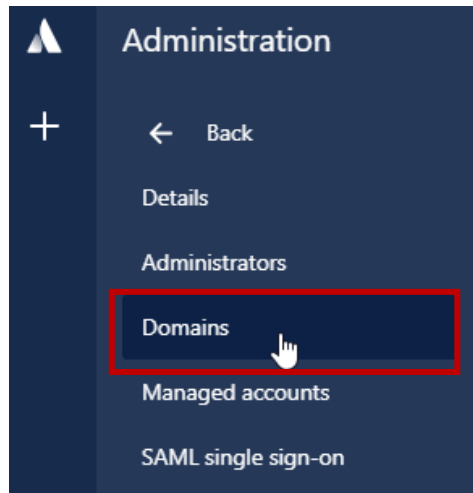
- ii. Click **Site administration**.



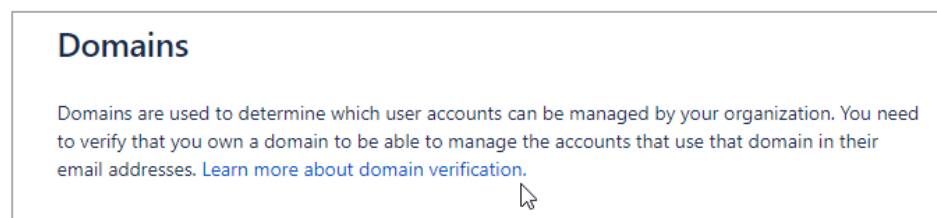
- iii. Click the organization name.



- iv. Click **Domains**.

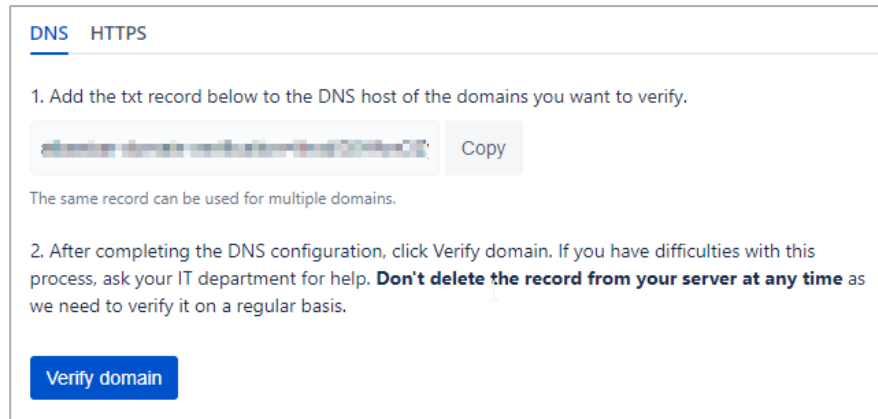


- v. You can verify a domain using DNS or HTTPS. For more information about the steps to verify a domain, in the right pane under **Domains** section, click the **Learn more about domain verification** link.



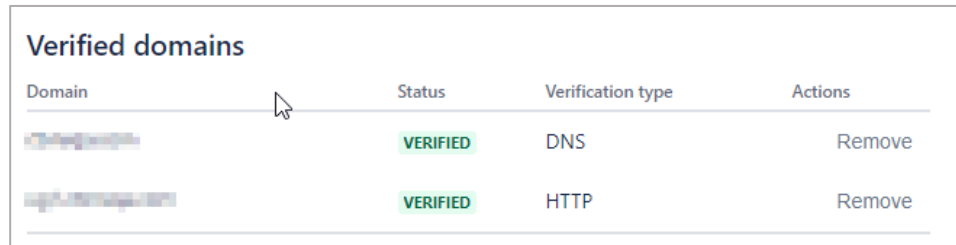


- vi. After completing the steps, click **Verify Domain**.



The screenshot shows a web interface with two tabs: "DNS" (selected) and "HTTPS". Under the "DNS" tab, there are two numbered instructions. Instruction 1 says to add a txt record to the DNS host of the domains to be verified. A text box contains a long alphanumeric string, and a "Copy" button is next to it. Below this, it says "The same record can be used for multiple domains." Instruction 2 says to click "Verify domain" after completing the DNS configuration, and to not delete the record from the server. At the bottom, there is a blue button labeled "Verify domain".

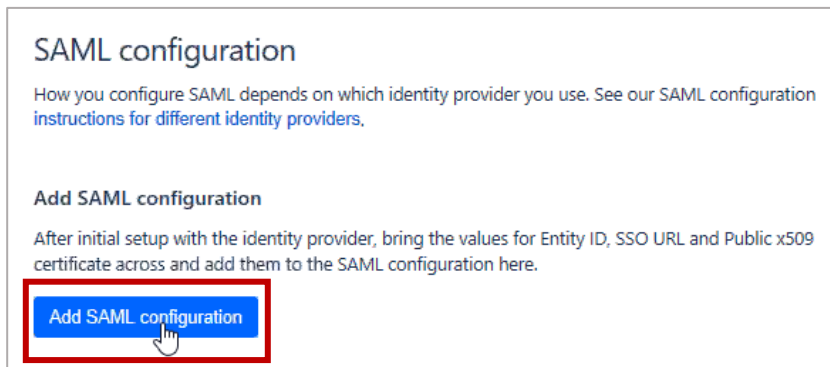
The **Status** column in the **Verified Domains** section displays **VERIFIED**.



The screenshot shows a table titled "Verified domains". The table has four columns: "Domain", "Status", "Verification type", and "Actions". There are two rows of data. The first row shows a domain with a status of "VERIFIED" (in a green box), a verification type of "DNS", and a "Remove" action. The second row shows a domain with a status of "VERIFIED" (in a green box), a verification type of "HTTP", and a "Remove" action.

Domain	Status	Verification type	Actions
[Redacted]	VERIFIED	DNS	Remove
[Redacted]	VERIFIED	HTTP	Remove

7. Click **SAML single sign-on**.
8. In the right pane, under **SAML Configuration**, click **Add SAML Configuration**.



The screenshot shows the "SAML configuration" page. It has a title "SAML configuration" and a subtitle "How you configure SAML depends on which identity provider you use. See our SAML configuration instructions for different identity providers." Below this, there is a section titled "Add SAML configuration" with a subtitle "After initial setup with the identity provider, bring the values for Entity ID, SSO URL and Public x509 certificate across and add them to the SAML configuration here." At the bottom of this section, there is a blue button labeled "Add SAML configuration" which is highlighted with a red box and a mouse cursor.

9. In the **Add SAML configuration** area, specify the following information:
- **Identity Provider Entity ID** - type a unique issuer ID. For example: yourcompany\_NS\_Jira
  - **Identity Provider SSO URL** - enter the IdP URL of your NetScaler app: https://<NetScaler Gateway FQDN>/saml/login

### Add SAML configuration

Identity provider Entity ID **1**  
  
 The URL your identity provider uses for SAML 2.0.

Identity provider SSO URL **2**  
  
 The SAML endpoint URL given to you by your identity provider.

Public x509 certificate **3**  
  
 Copy and paste the entire certificate.

**4**

- **Public x509 Certificate** – copy and paste the SAML IdP signing certificate.

To obtain the certificate, follow the steps below:

To obtain your IdP certificate, follow the steps below:

- Remotely access your NetScaler instance using PuTTY.
- Navigate to /nsconfig/ssl folder (using shell command `cd /nsconfig/ssl`) and press Enter.
- Type `cat <certificate-name>` and press Enter.

```

1  -----BEGIN CERTIFICATE-----
2  MIIFPzCCBCegAwIBAgIQApjY189Tw/6/mHRS5nGDuzAMBgqhkiG9w0BAQsFADBN
3  NQs=
4  allc
5  HTE
6  BAe
7  LJE
8  ADC
9  yVj
10 Kjf
11 vde
12 RK2
13 RYc
14 MBa
15 +Cc
16 Y2V
17 BBy
18 LyS
19 Ois
20 MDC
21 dCS
22 GGF
23 Y2V
24 dDa
25 PA6
26 +Xz
27 gSf
28 c+r
29 UOZLmrmuprexcnaJjor3rWILzckpubu9TqenWzWqLAdQ0aLz/m7az0qBzy4ND
30 6EDS
31  -----END CERTIFICATE-----
32

```

- Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
- Paste the text in a text editor and save the file in an appropriate format such as <your company name>.pem.

10. Click **Save Configuration**.

**Add SAML configuration**

Identity provider Entity ID  
UC\_...\_...  
The URL your identity provider uses for SAML 2.0.

Identity provider SSO URL  
https://ug2.blmwp.com/saml/login  
The SAML endpoint URL given to you by your identity provider.

Public x509 certificate  
UOZLmXmmUpFe1cHajjorJhwNCZCKpUou9TWqehWIwc  
M0QDa12/m7WZoQBA2y4NJ  
6ED5  
-----END CERTIFICATE-----  
Copy and paste the entire certificate.

**Save configuration** Cancel

The **SP Entity ID** and **SP Assertion Consumer Service URL** fields display values. Use these values while configuring NetScaler.

SP Entity ID  
https://auth.blmwp.com/saml/06000000-0000-0000-0000-000000000000 Copy

SP Assertion Consumer Service URL  
https://auth.blmwp.com/saml/06000000-0000-0000-0000-000000000000 Connection Copy

**Your current SAML configuration**

Identity provider Entity ID  
UC\_...\_...  
Identity provider SSO URL  
https://ug2.blmwp.com/saml/login  
Public x509 certificate  
-----BEGIN CERTIFICATE----- M... Show more

Edit configuration Delete configuration

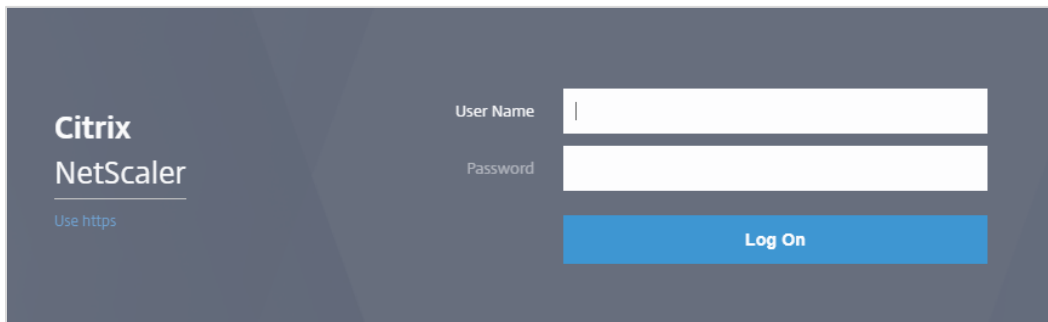
You have completed the required configuration on the service provider which is in this case – Jira.

# Configuring NetScaler for Single Sign-On

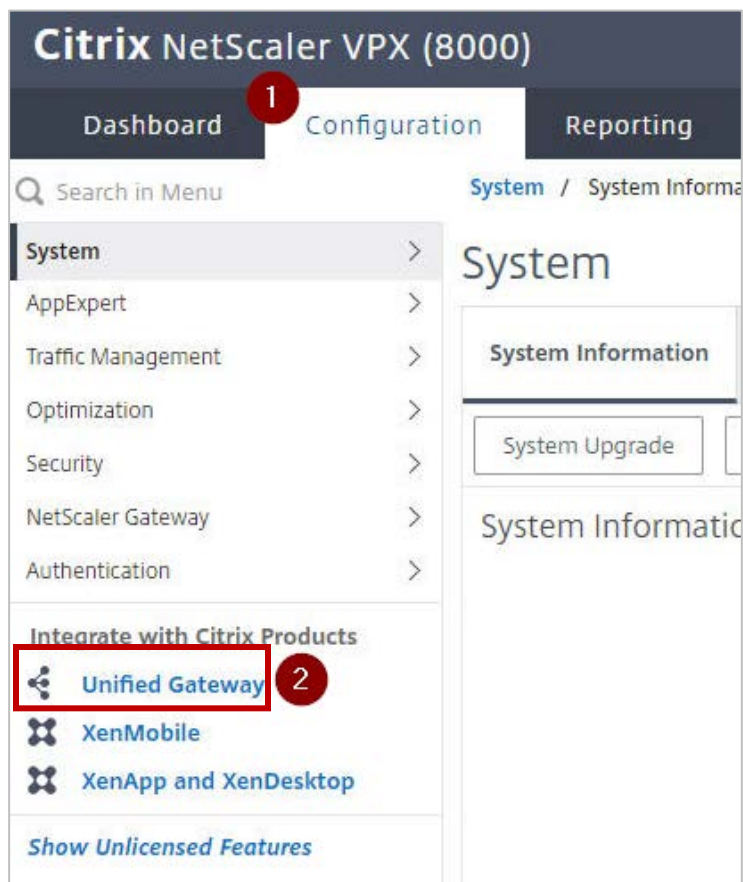
For configuring NetScaler for Jira, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

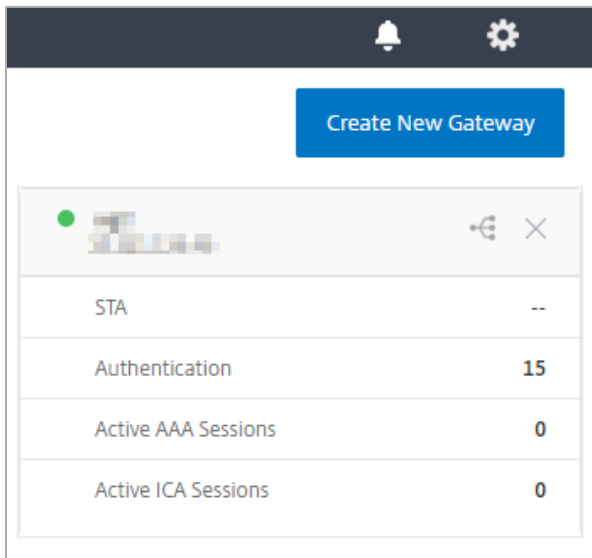
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



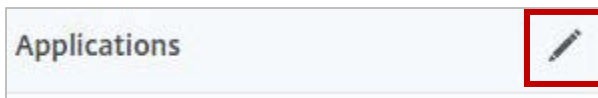
3. Click **Configuration > Unified Gateway**.



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



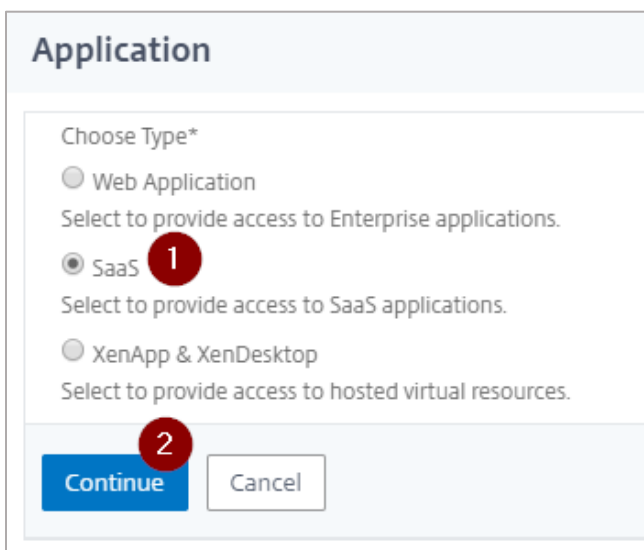
5. Click the edit icon for **Applications** section.



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 **Jira**.

The screenshot shows the 'Application' configuration dialog. At the top, it says 'Application'. Below that, there is a section 'Choose Type' with 'SaaS' selected. The main section is 'SaaS Application: Catalog vs. Customized'. It has two radio buttons: 'Choose from Catalog' (selected) and 'Customized Application'. Below the radio buttons is a dropdown menu labeled 'Choose from Catalog\*'. The dropdown menu is open, showing a list of applications: Ariba, Confluence, Creative Cloud, Docusign, Dropbox, GitHub, GoToMeeting, Jira (highlighted in blue), NewRelic, Oracle Cloud, PagerDuty, Service Now, Slack, Zendesk, and Zoom. There are red circles with numbers '1' and '2' next to the 'Choose from Catalog' radio button and the 'Jira' option in the dropdown menu, respectively.

10. Click **Continue**.

The screenshot shows the 'Application' configuration dialog. At the top, it says 'Application'. Below that, there is a section 'Choose Type' with 'SaaS' selected. The main section is 'SaaS Application: Catalog vs. Customized'. It has two radio buttons: 'Choose from Catalog' (selected) and 'Customized Application'. Below the radio buttons is a dropdown menu labeled 'Choose from Catalog\*'. The dropdown menu is open, showing a list of applications: Ariba, Confluence, Creative Cloud, Docusign, Dropbox, GitHub, GoToMeeting, Jira (highlighted in blue), NewRelic, Oracle Cloud, PagerDuty, Service Now, Slack, Zendesk, and Zoom. At the bottom of the dialog, there are two buttons: 'Continue' (highlighted with a red box) and 'Cancel'.

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

**Create Application from Template**

Name\* 1  
Jira ?

Comments 2  
Atlassian hosted Jira Cloud

11. In the **Add SAML configuration** area, specify the following information:

- **Enter URL** - enter the URL that you used for logging on to Jira.
- **Service Provider ID** - paste the SP Entity ID that you copied from the **SP Entity ID** box on the **SAML Single sign-on page** while configuring SAML for Jira.
- **Assertion Consumer Service Url\*** - replace <yourid> in the existing text <https://auth.atlassian.com/saml/<yourid>> with the value displayed by the **SP Assertion Consumer Service URL** box after saml-, on the **SAML Single sign-on page** while configuring SAML for Jira.  
**For example:** <https://auth.atlassian.com/login/callback?connection=saml-0653824d-3839-490b-9844-f82100811h7a>
- **Audience** - paste the SP Entity ID that you copied from the **SP Entity ID** box on the SAML Single sign-on page while configuring SAML for Jira.
- **Signing Certificate Name** - select an appropriate certificate that will be used for signing SAML requests and responses.

**Jira**

Enter URL\* 1  
<Your Org>.atlassian.net

Service Provider ID\* 2

Assertion Consumer Service Url\* 3  
<https://auth.atlassian.com/saml/<yo>

Audience 4  
<https://auth.atlassian.com/login/call>

SP Certificate Name 5

Signing Certificate Name\* 6

Issuer Name 7  
URL\_0000\_0002

8  
Continue Cancel

**Note:** For this configuration, SP certificate is not required hence the **SP Certificate Name** field does not require an entry.

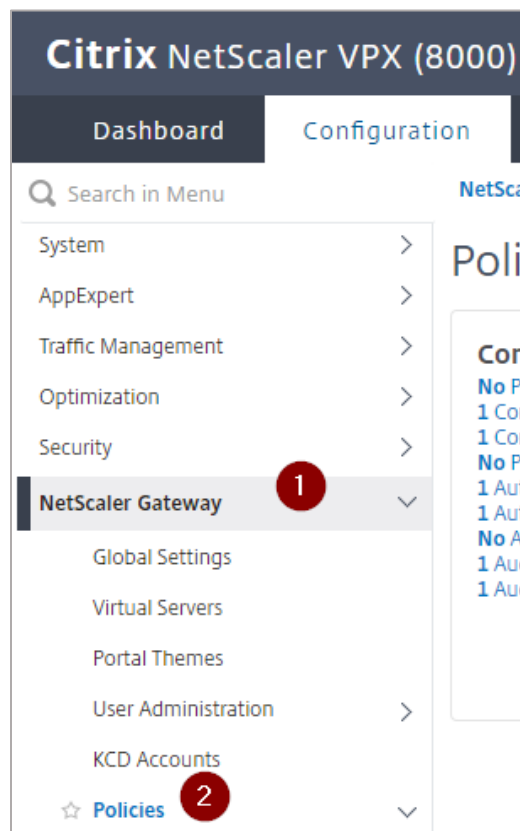
- **Signing Certificate Name** - click an appropriate certificate that will be used for signing SAML requests and responses.
- **Issuer Name** - type a unique issuer ID that you entered in the **Identity Provider Entity ID** box, while configuring SAML for Jira.

12. Click **Continue**.

13. Click **Done**.

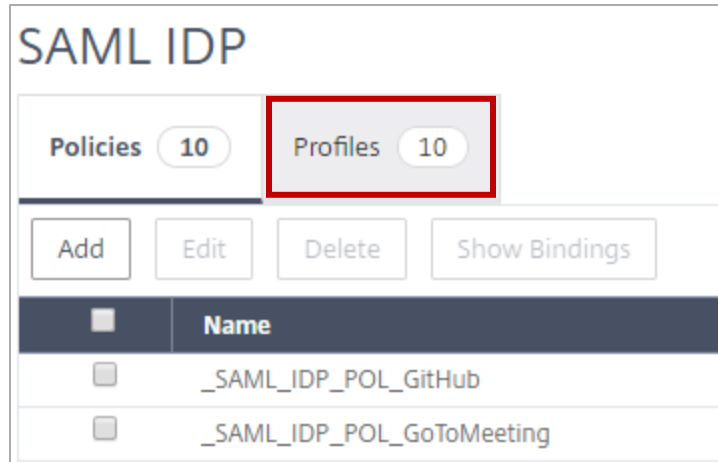
14. As Jira does not provide SP certificate, you must clear the **Reject Unsigned Requests** check box. To do so, follow the steps below:

- In Citrix NetScaler's **Configuration** tab, click **NetScaler Gateway** and then click **Policies**.




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





- iv. Select the check box for the SAML profile for Jira.
- v. On the Configure Authentication SAML IDP profile page, clear the **Reject Unsigned Requests** check box.



- vi. Click **OK**.
- vii. On the **Configure Authentication SAML IDP Policy** page, click **OK**.
- viii. On the **SAML IDP** page, in the upper right corner, click the **Save the running configuration(s)**  icon.

The Jira logo appears.

You have completed the NetScaler configuration for Jira.

# 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 **Jira**.  
Your Jira profile appears.  
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 organization's URL for Atlassian.
2. Type your organizational user name.  
You are redirected to NetScaler appliance's log in page.
3. Log on to NetScaler appliance using your enterprise credentials.  
  
Your Jira profile appears which indicates that you have successfully logged on to Jira.



#### 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).