



NetScaler with Unified Gateway

Configuring Confluence

Abstract

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

Contents

- ABSTRACT0
- CONTENTS1
- DISCLAIMER (DOCUMENTATION)2
- PREFACE3
- OVERVIEW4
- CONFIGURING CONFLUENCE FOR SINGLE SIGN-ON5
- CONFIGURING NETSCALER FOR SINGLE SIGN-ON11
- TESTING THE CONFIGURATION17

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.

Confluence is a content collaboration software that provides functionalities to create, share, and collaborate on projects, maintain knowledge base and documentation, and track progress and team activities.

You can connect Confluence 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

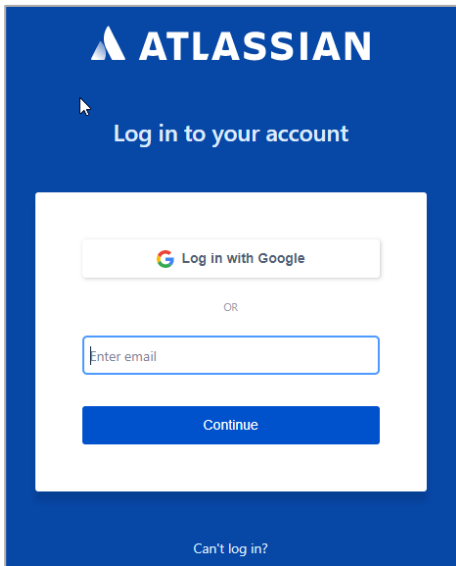
Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

Configuring Confluence for Single Sign-On

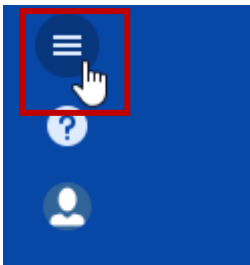
Configuring Confluence for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Confluence using their enterprise credentials.

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

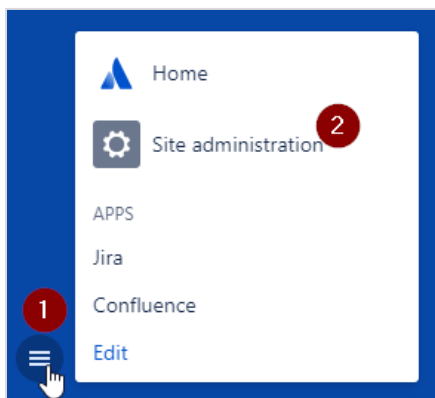
1. In a browser, type your organization's Atlassian cloud URL and press enter.
2. Log on to your Atlassian account.



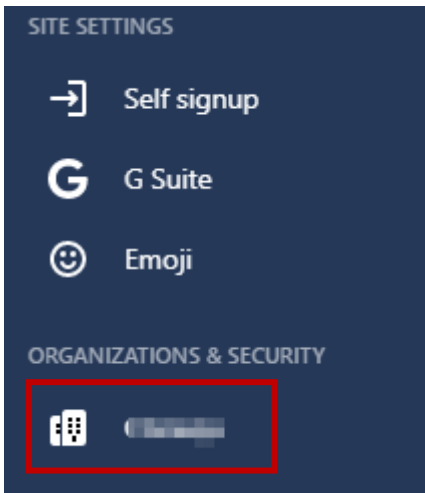
3. On the **Home** page, at the lower-left corner, click .



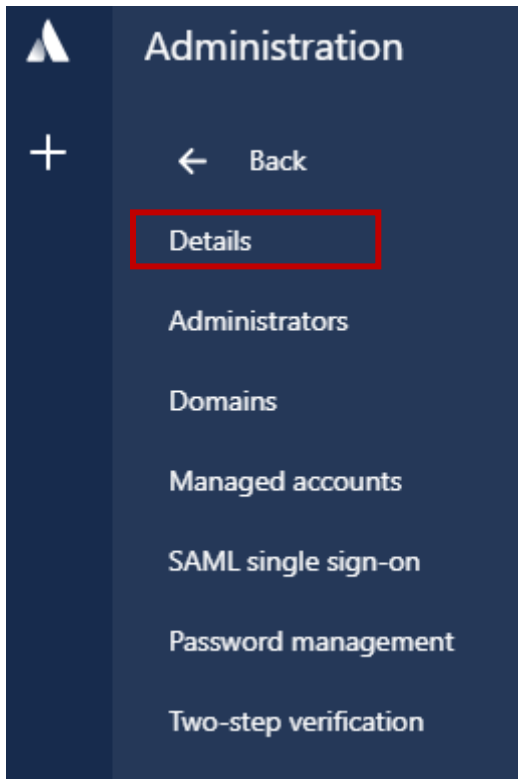
4. Click **Site administration**.



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

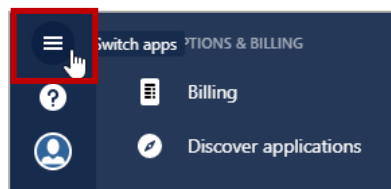


6. Click **Details** and verify the domain.

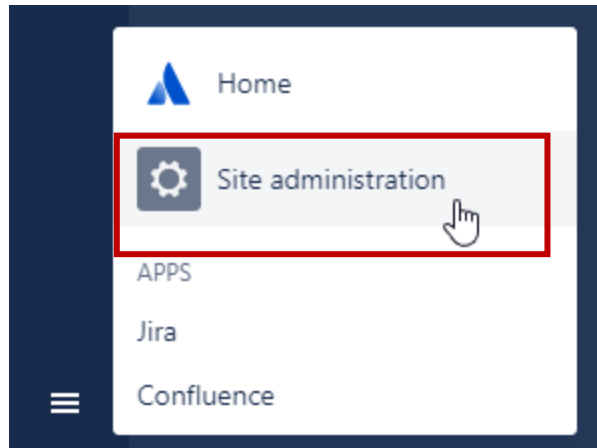


To verify the domain, follow the steps below:

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



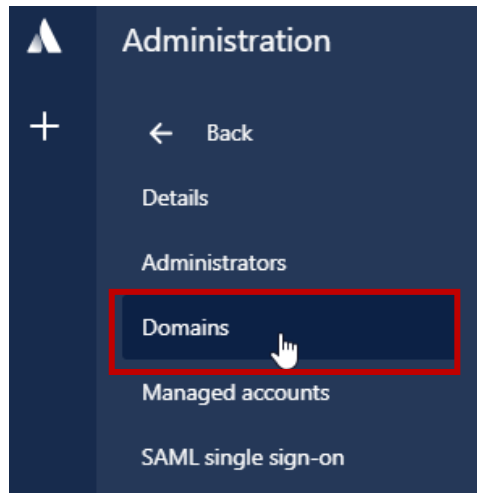
- ii. Click **Site administration**.



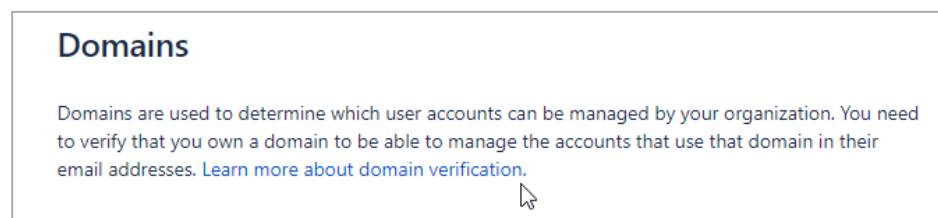
- iii. Click the organization name.



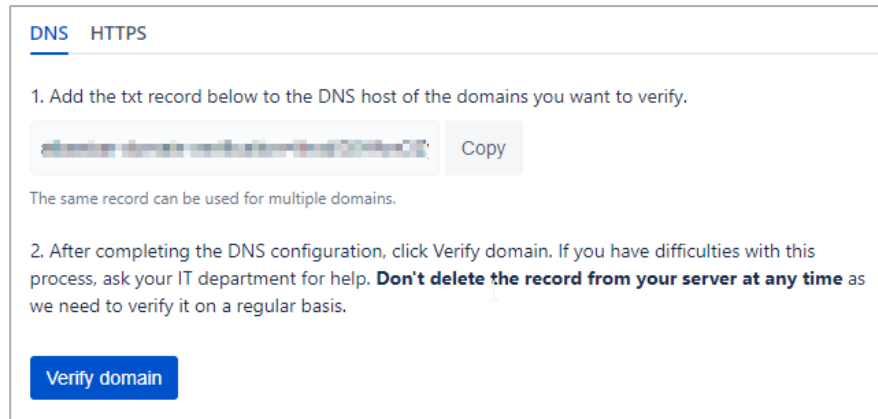
- iv. Click **Domains**.



- 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.

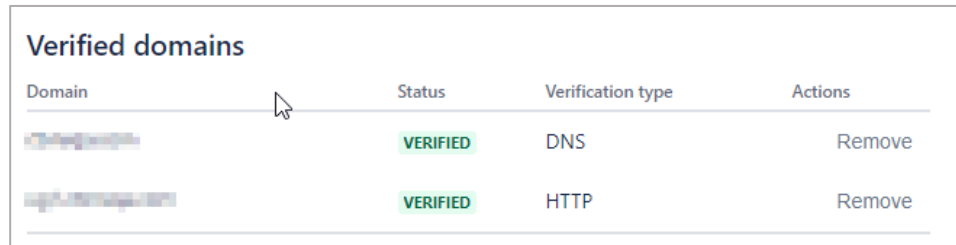


- vi. After completing the steps, click **Verify Domain**.



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. Below this is a text box containing a long alphanumeric string and a "Copy" button. A note below states, "The same record can be used for multiple domains." Instruction 2 says to click "Verify domain" after DNS configuration, and to ask the IT department for help if there are difficulties, warning not to delete the record. At the bottom of the instructions is a blue button labeled "Verify domain".

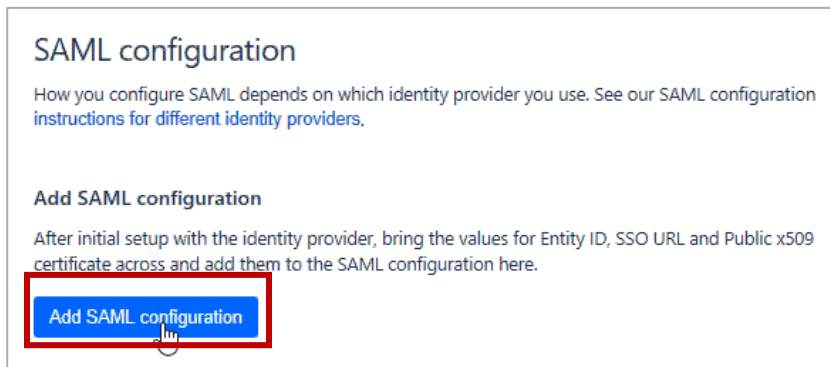
The **Status** column in the **Verified Domains** section displays **VERIFIED**.



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 (partially obscured), a status of "VERIFIED" in a green box, a verification type of "DNS", and a "Remove" action. The second row shows another domain (partially obscured), 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 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 is a blue button labeled "Add SAML configuration", which is highlighted with a red rectangular box.

9. In the **Add SAML configuration** area, specify the following information:
- **Identity Provider Entity ID** - type a unique issuer ID. For example: yourcompany_NS_Confluence
 - **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 BAc
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 UOZLmrmuprexcnAjJorJiWILzckpubu9TqenWzWqLAdQ0aLz/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

The URL your identity provider uses for SAML 2.0.

Identity provider SSO URL

The SAML endpoint URL given to you by your identity provider.

Public x509 certificate

```
UOZLmXmmUpFe1cHajjorJhwNCZCKpUou9TWqehWIwc
M0QDai2/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

[Copy](#)

SP Assertion Consumer Service URL

[Copy](#)

Your current SAML configuration

Identity provider Entity ID

UC_12345678901234567890

Identity provider SSO URL

https://ug2.confluence.com/saml/login

Public x509 certificate

-----BEGIN CERTIFICATE----- MIIEPjCCBjgCAQAw... Show more

[Edit configuration](#) [Delete configuration](#)

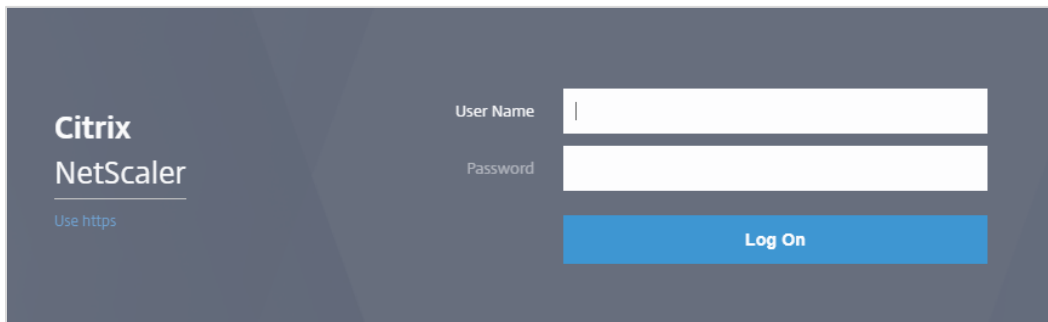
You have completed the required configuration on the service provider which is in this case – Confluence.

Configuring NetScaler for Single Sign-On

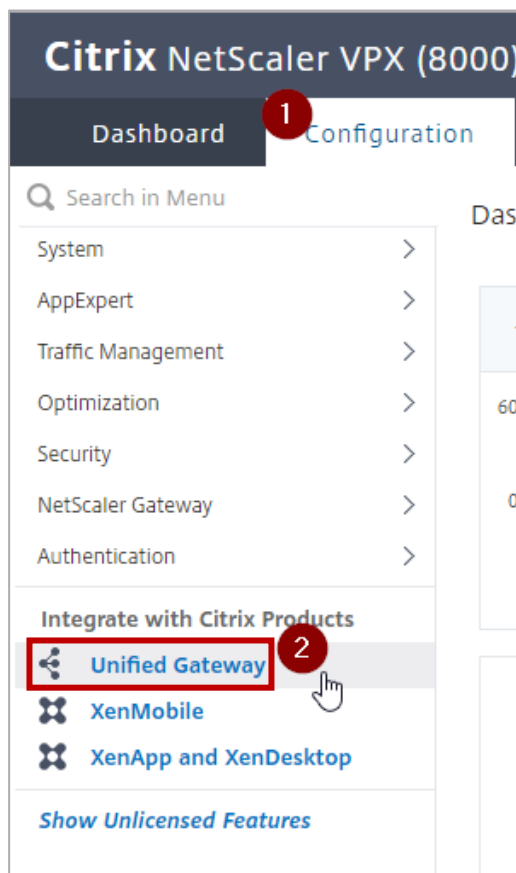
For configuring NetScaler for Confluence, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

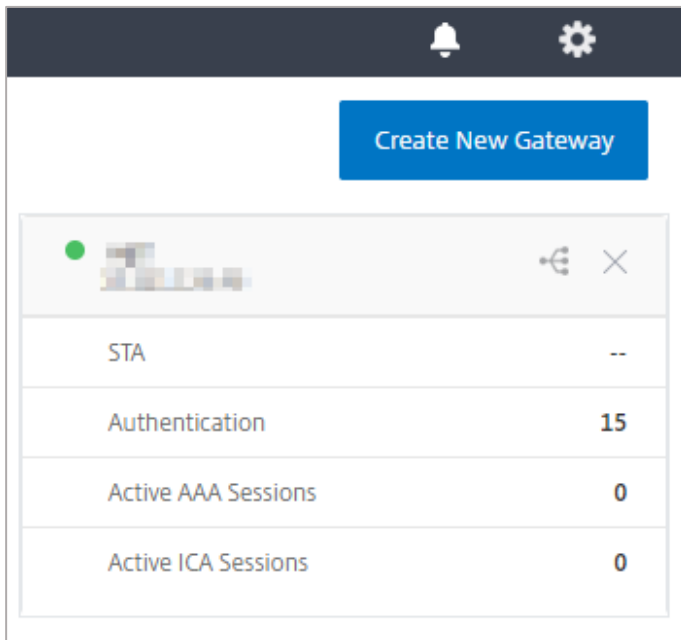
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



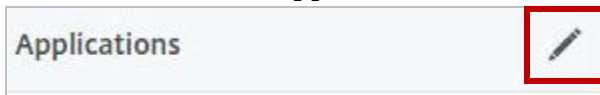
3. Click **Configuration > Unified Gateway**.



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



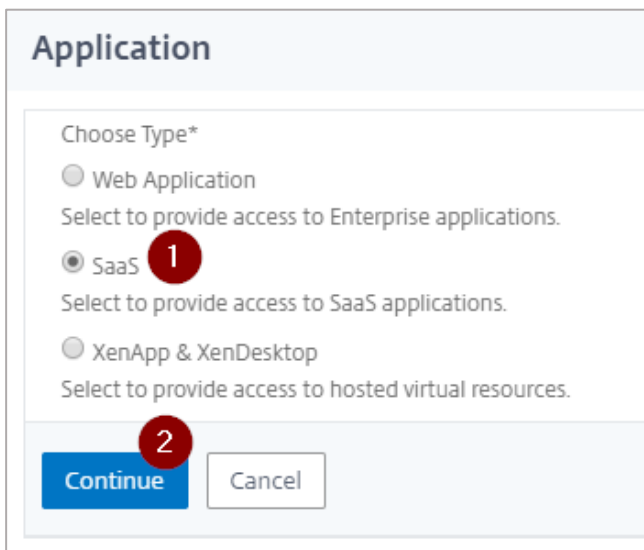
5. Click the edit icon for **Applications** section.



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 **Confluence**.

The screenshot shows the 'Application' configuration page. At the top, there is a 'Choose Type' section with 'SaaS' selected. Below this is a section titled 'SaaS Application: Catalog vs. Customized'. In this section, the 'Choose from Catalog' radio button is selected, indicated by a red circle with the number '1'. Below the radio buttons is a dropdown menu labeled 'Choose from Catalog*'. The dropdown menu is open, showing a list of application names: Ariba, Ariba, Confluence, Creative Cloud, Docusign, Dropbox, GitHub, GoToMeeting, Jira, NewRelic, Oracle Cloud, PagerDuty, Service Now, Slack, Zendesk, Zoom, and webex. The 'Confluence' option is highlighted in blue, and a mouse cursor is pointing at it, indicated by a red circle with the number '2'.

10. Click **Continue**.

The screenshot shows the 'Application' configuration page after the 'Confluence' selection. The 'Choose from Catalog*' dropdown menu now displays 'Confluence'. At the bottom of the page, there are two buttons: 'Continue' (a blue button) and 'Cancel' (a white button with a grey border). A mouse cursor is pointing at the 'Continue' button.

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

Create Application from Template

Name* **1**
Confluence ?

Comments **2**
Atlassian hosted Confluence

11. In the section next to the icon, specify the following information:

- **Enter URL** - enter the URL that you used for logging on to Confluence.
- **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 Confluence.
- **Assertion Consumer Service Uri*** - 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 Confluence.
For example: <https://auth.atlassian.com/login/callback?connection=saml-0653824d-3839-490b-9844-aa1134p1111e>
- **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 Confluence.
- **Signing Certificate Name** - select an appropriate certificate that will be used for signing SAML requests and responses.

Confluence

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

Service Provider ID* **2**

Assertion Consumer Service Uri* **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**

8 Continue Cancel

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

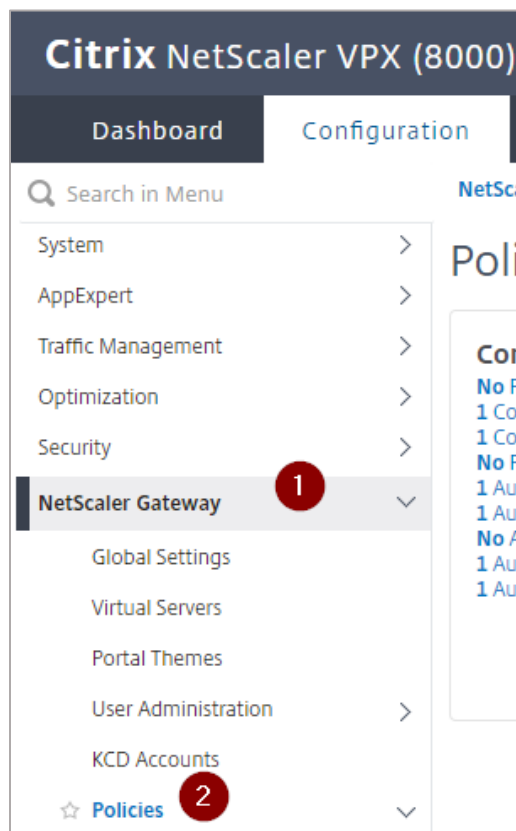
- **Signing Certificate Name** - click an appropriate certificate that will be used for signing SAML requests and responses.
- **Issuer Name** - type a unique issuer ID that you entered in the **Identity Provider Entity ID** box, while configuring SAML for Confluence.

12. Click **Continue**.

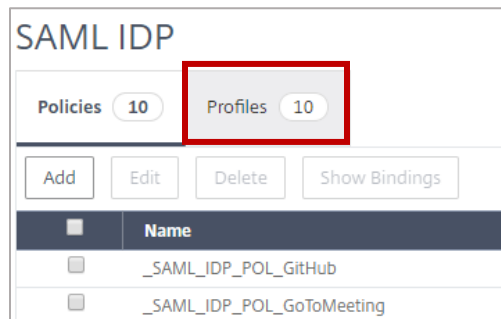
13. Click **Done**.

14. As Confluence 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 checkbox for the SAML profile for Confluence.
- v. On the **Configure Authentication SAML IDP Profile** page, clear the **Reject Unsigned Requests** check box.



The screenshot shows a configuration form for a SAML IDP profile. It includes a text field for 'Service Provider ID' containing a URL. Below it is a checkbox labeled 'Reject Unsigned Requests', which is highlighted with a red rectangular box. Underneath are radio buttons for 'Signature Algorithm*' with options 'RSA-SHA1' (selected) and 'RSA-SHA256'. At the bottom, there is a label for 'Digest Method*'. The entire form is enclosed in a light gray border.

- 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 Confluence logo appears.

You have completed the NetScaler configuration for Confluence.

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 **Confluence**.
Your Confluence 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 Confluence profile appears which indicates that you have successfully logged on to Confluence.



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).