CITRIX

NetScaler with Unified Gateway

Configuring Confluence

Abstract

Configuring Confluence 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.

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

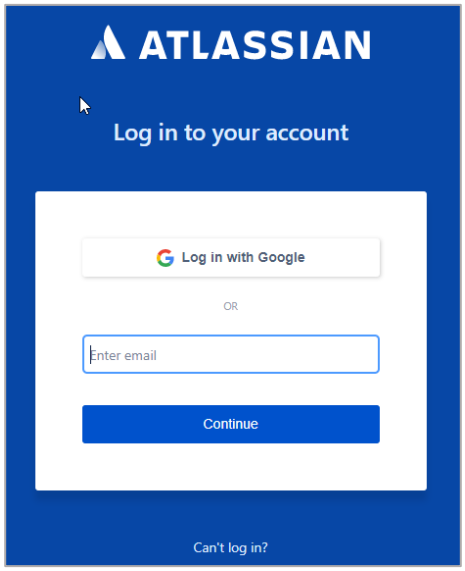
Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

Configuring Confluence for Single Sign-On

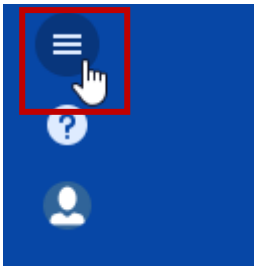
Configuring Confluence for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Confluence using their enterprise credentials.

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

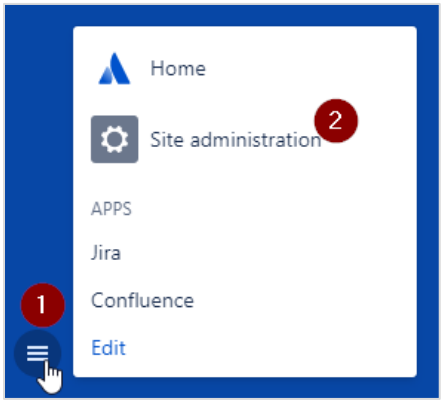
1. In a browser, type your organization's Atlassian cloud URL and press enter.
2. Log on to your Atlassian account.



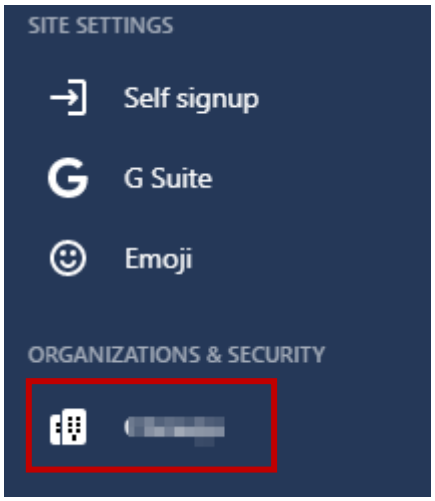
3. On the **Home** page, at the lower-left corner, click  .



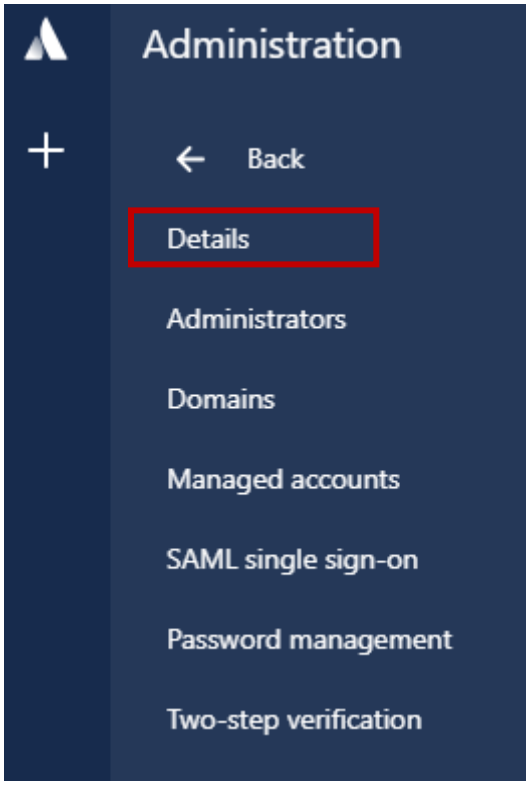
4. Click **Site administration**.



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

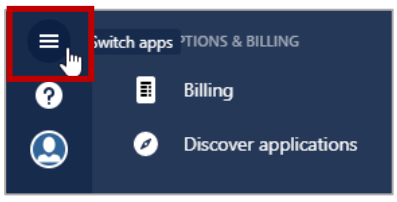


6. Click **Details** and verify the domain.

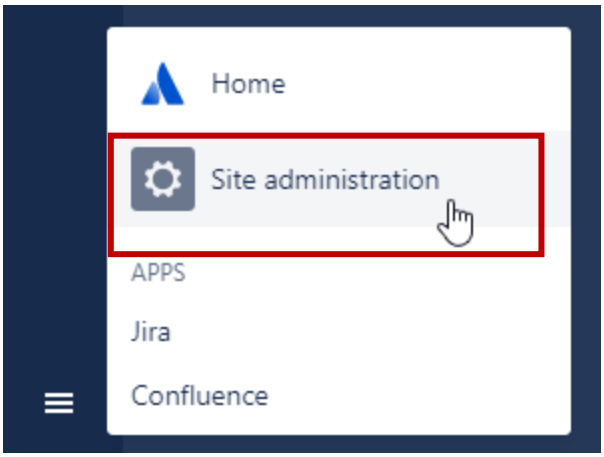


To verify the domain, follow the steps below:

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

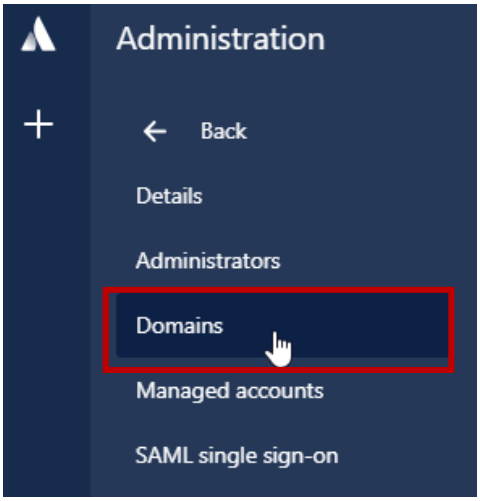


ii. Click **Site administration**.

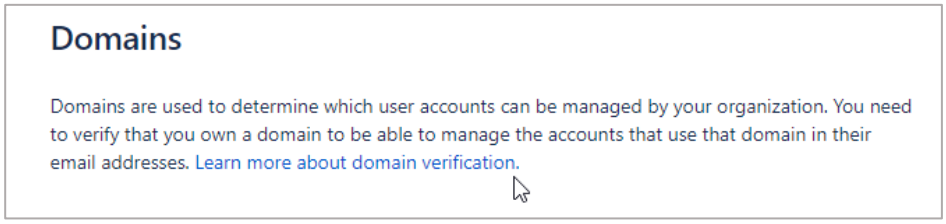


iii. Click the organization name.

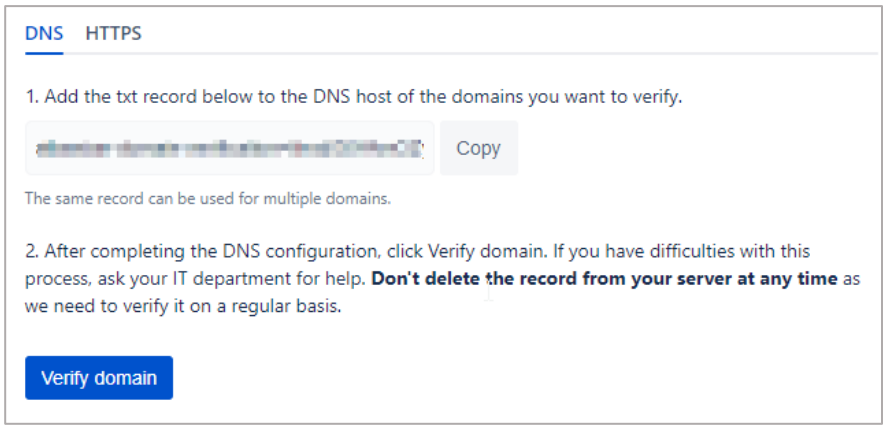
iv. Click **Domains**.



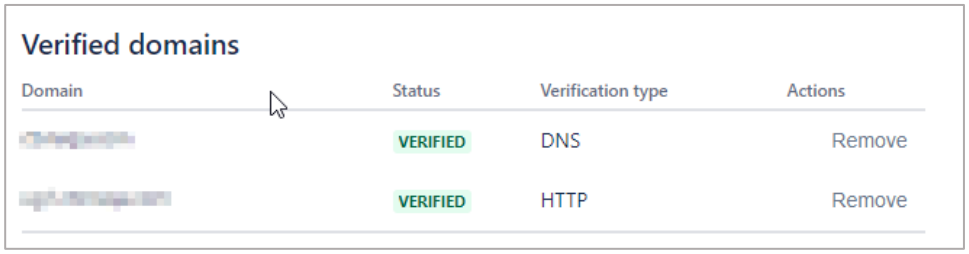
v. You can verify a domain using DNS or HTTPS. For more information about the steps to verify a domain, in the right pane under **Domains** section, click the **Learn more about domain verification** link.



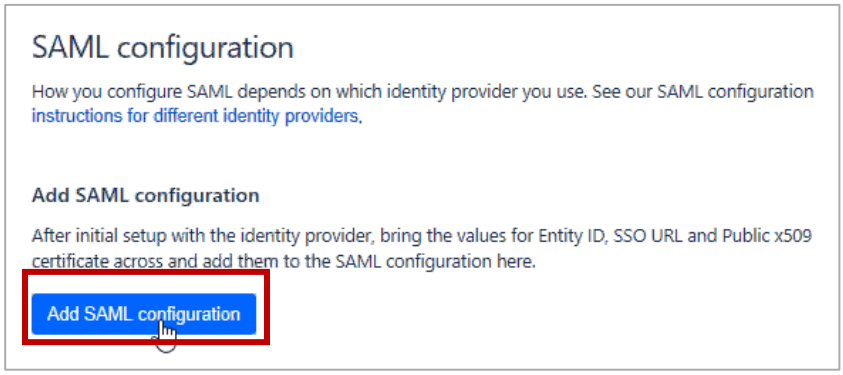
vi. After completing the steps, click **Verify Domain**.



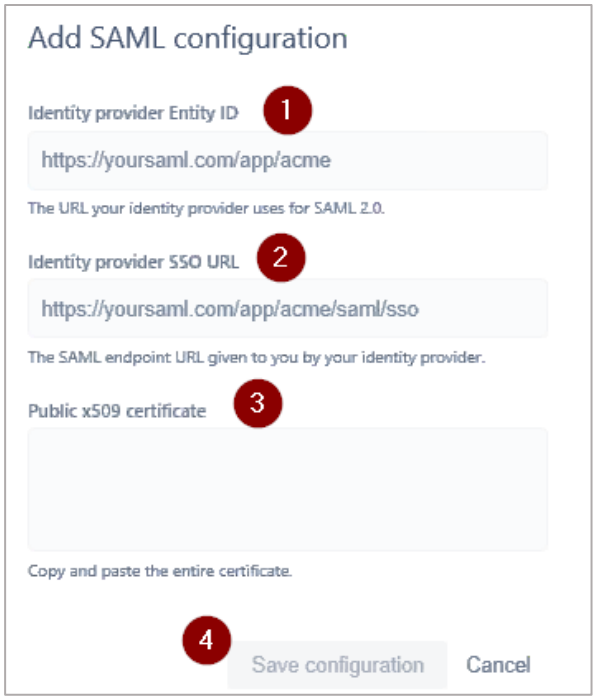
The **Status** column in the **Verified Domains** section displays **VERIFIED**.



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



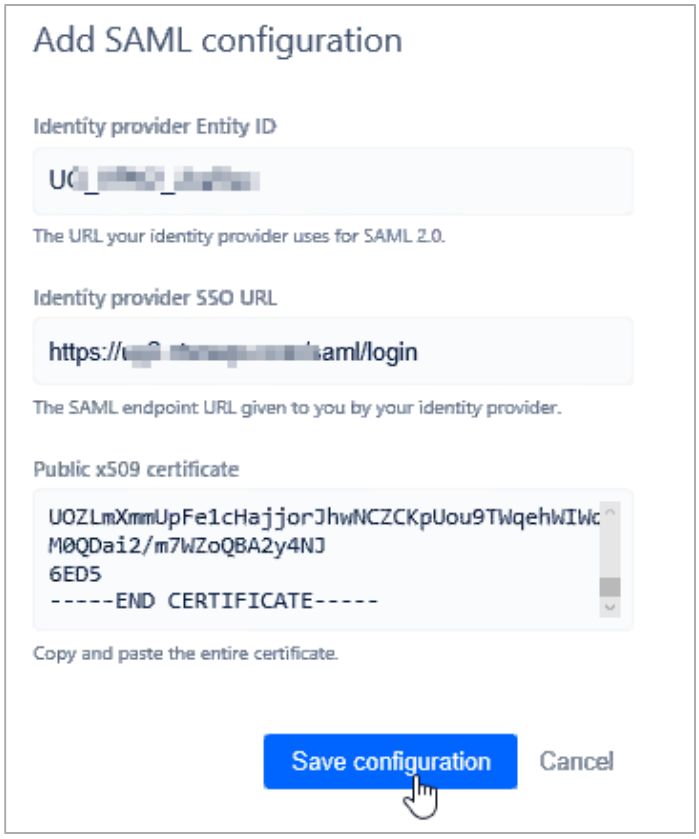
9. In the **Add SAML configuration** area, specify the following information:
   - **Identity Provider Entity ID** - type a unique issuer ID. For example: yourcompany_NS_Confluence
   - **Identity Provider SSO URL** - enter the IdP URL of your NetScaler app: https://<Netscaler Gateway FQDN>/saml/login



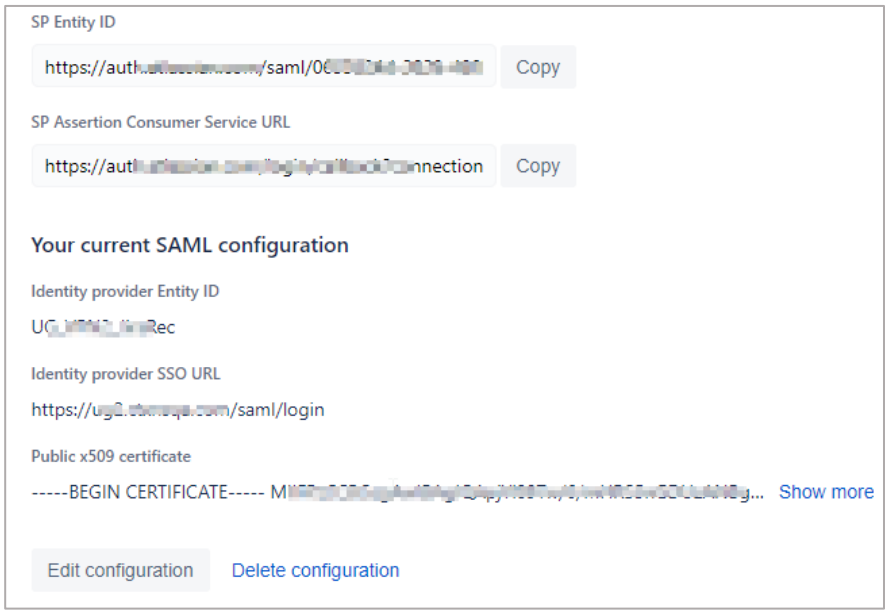
- **Public x509 Certificate** – copy and paste the SAML IdP signing certificate.
  To obtain the certificate, follow the steps below:
  To obtain your IdP certificate, follow the steps below:
  i. Remotely access your NetScaler instance using PuTTY.
  ii. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.
  iii. Type cat <certificate-name> and press Enter.

  iv. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
  v. 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**.



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



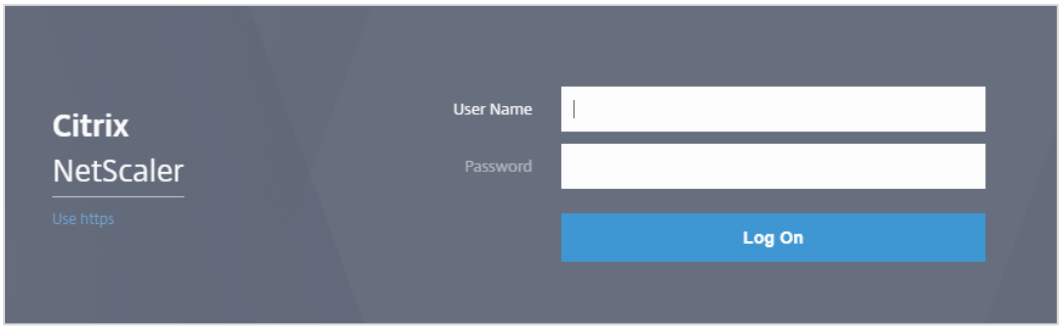
You have completed the required configuration on the service provider which is in this case – Confluence.

Configuring NetScaler for Single Sign-On

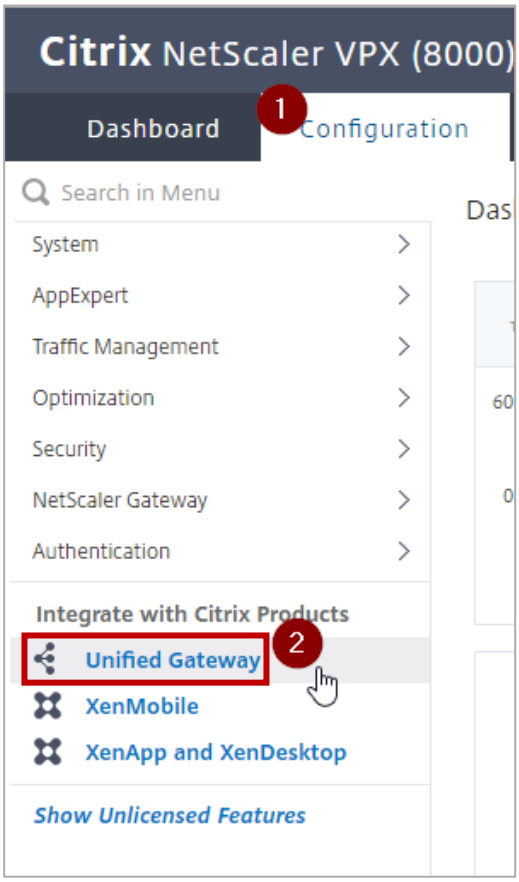
For configuring NetScaler for Confluence, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

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

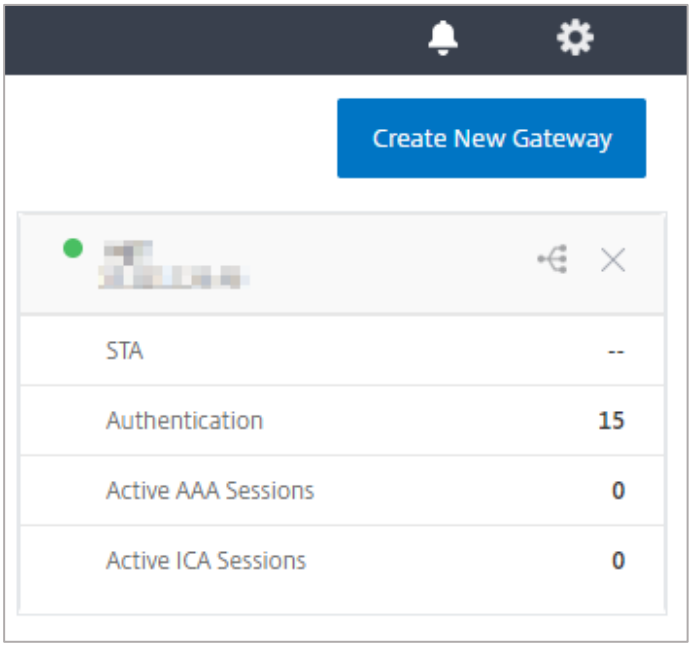
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



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



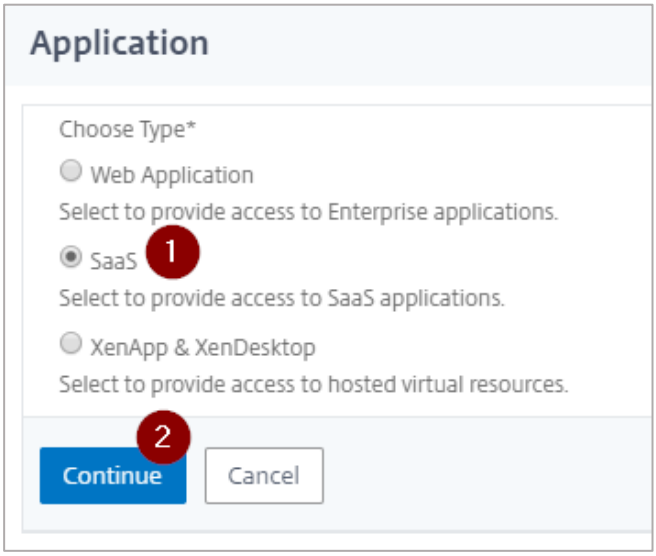
4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



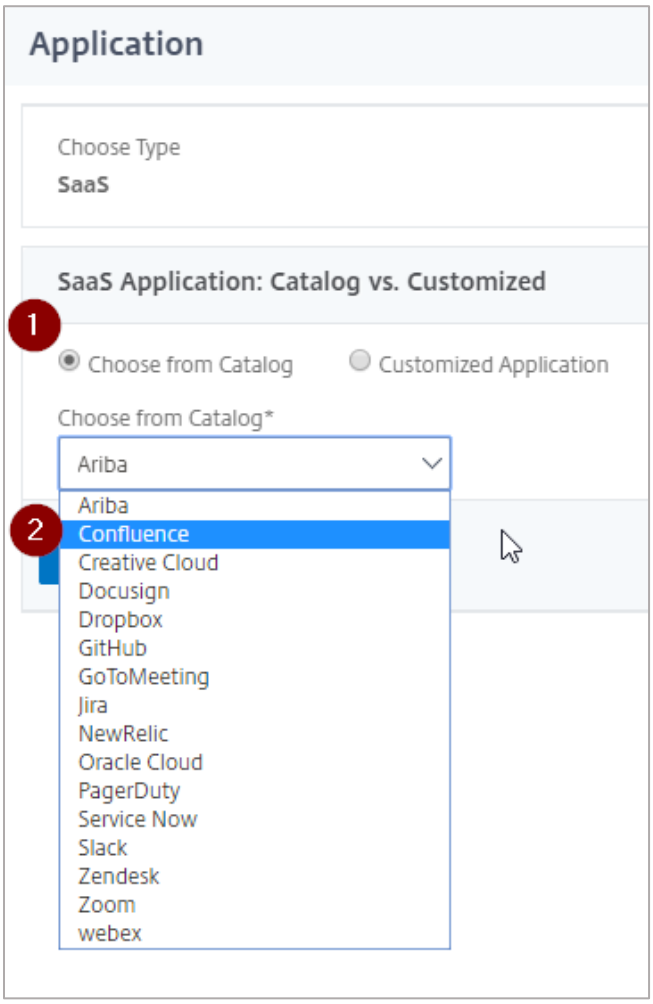
5. Click the edit icon for **Applications** section.

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

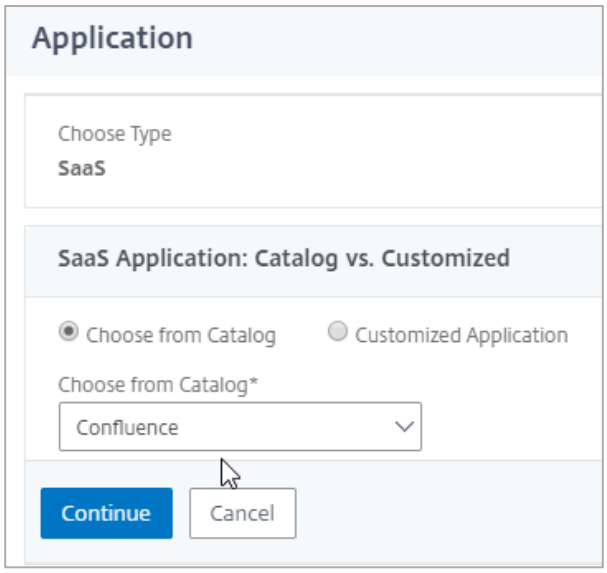
7. Click **SaaS** > **Continue**.



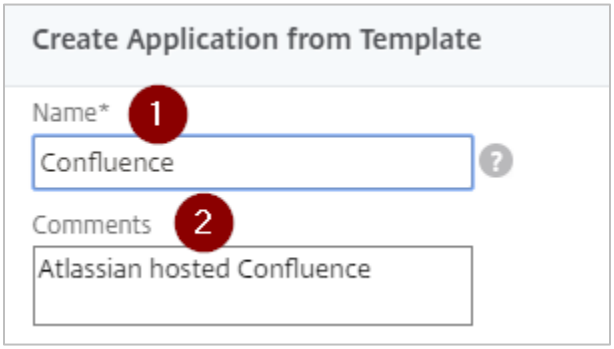
8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **Confluence**.



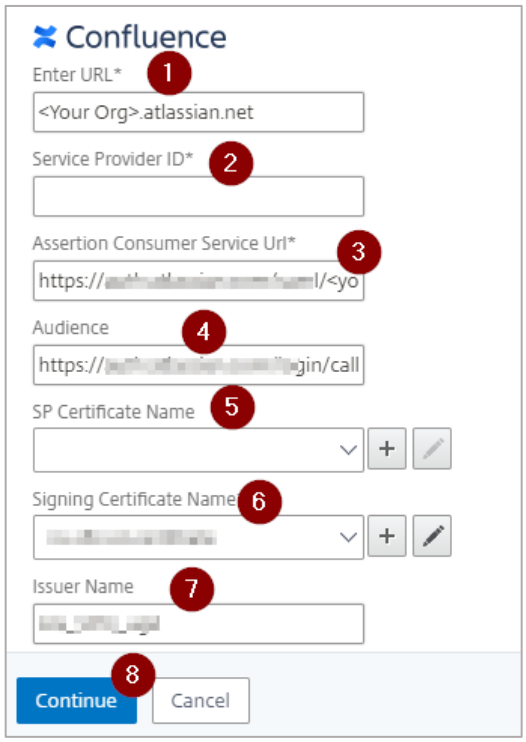
10. Click **Continue**.



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



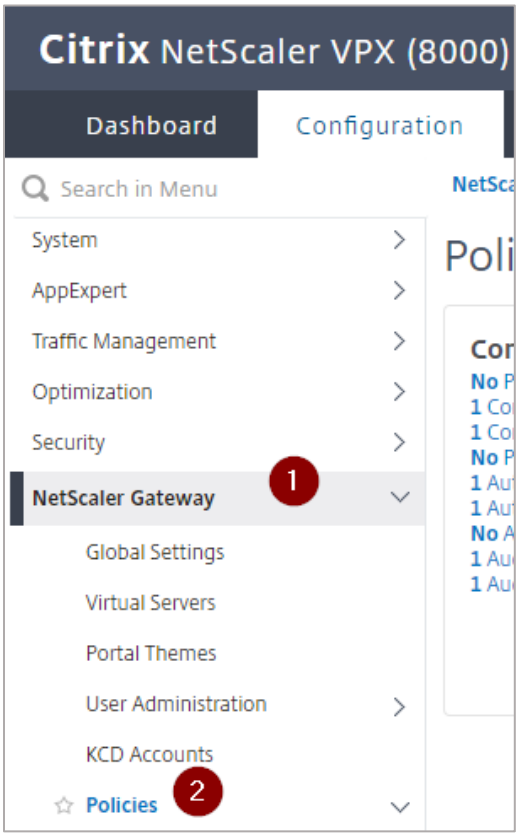
11. In the section next to the icon, specify the following information:
    - **Enter URL** - enter the URL that you used for logging on to Confluence.
    - **Service Provider ID** - paste the SP Entity ID that you copied from the **SP Entity ID** box on the **SAML Single sign-on page** while configuring SAML for Confluence.
    - **Assertion Consumer Service 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 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.



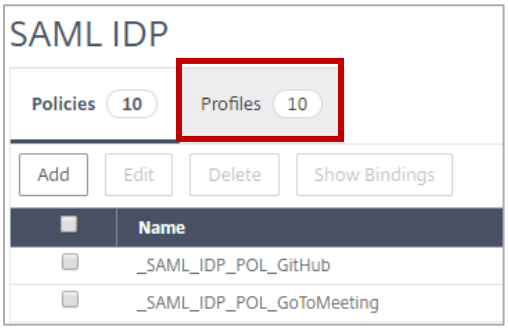
Note: For this configuration, SP certificate is not required hence the **SP Certificate Name** field does not require an entry.

- **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:
    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. 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.

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