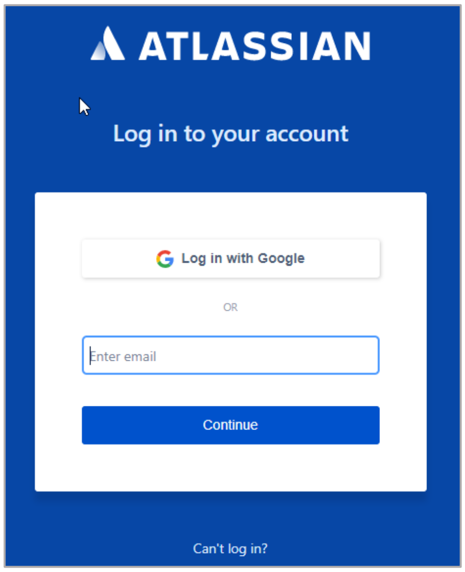
Configuring Confluence

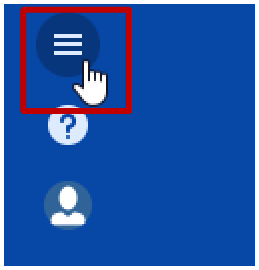
Configuring Confluence for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Confluence using their enterprise credentials.

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

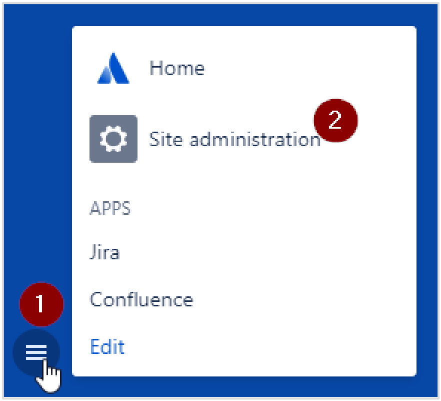
1. In a browser, type your organization's Atlassian cloud URL and press enter.
2. Log on to your Atlassian account.



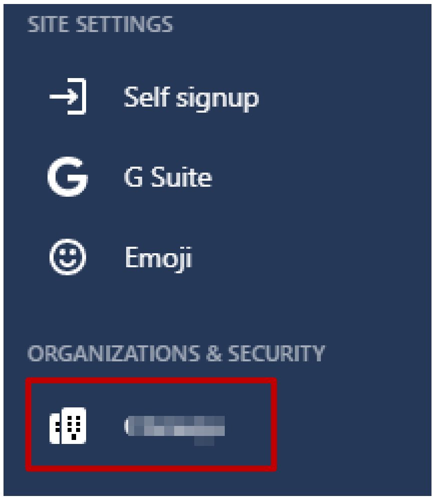
3. On the **Home** page, at the lower-left corner, click ☰.



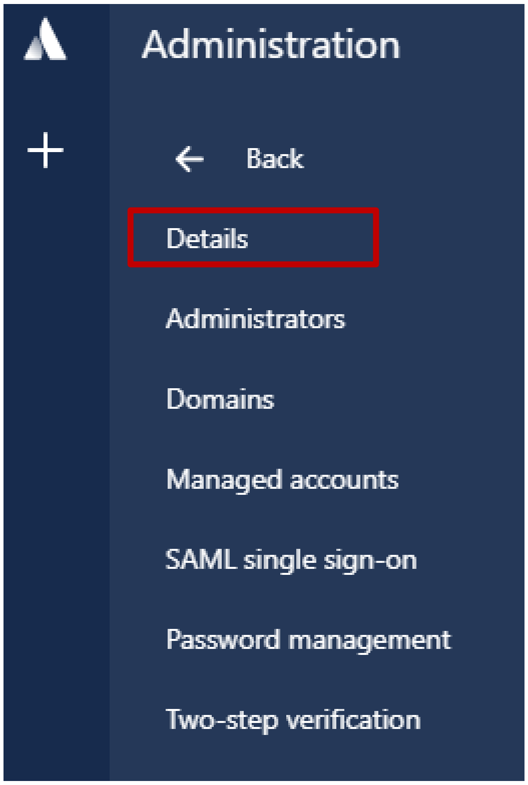
4. Click **Site administration**.



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

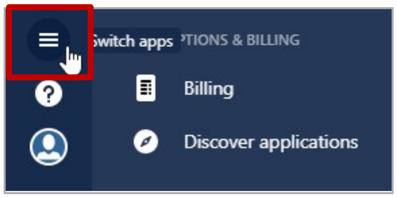


6. Click **Details** and verify the domain.

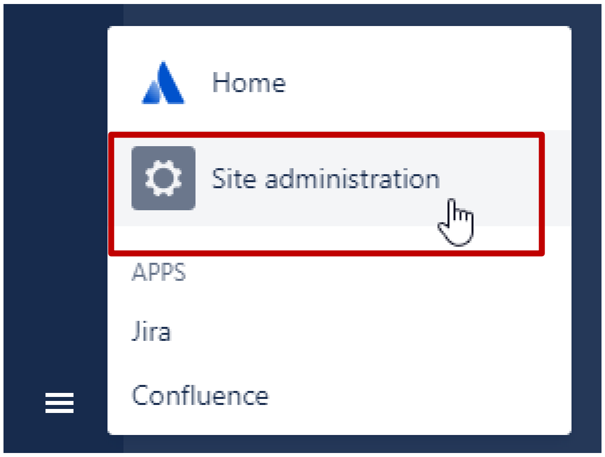


To verify the domain, follow the steps below:

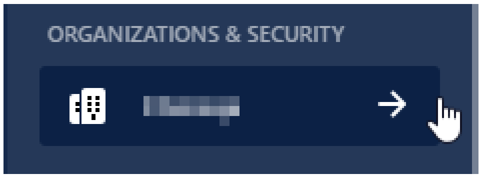
i. Click the **Switch apps** icon in the lower-left corner.



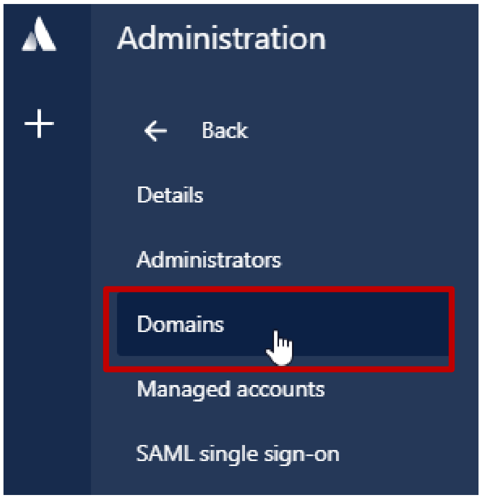
ii. Click **Site administration**.



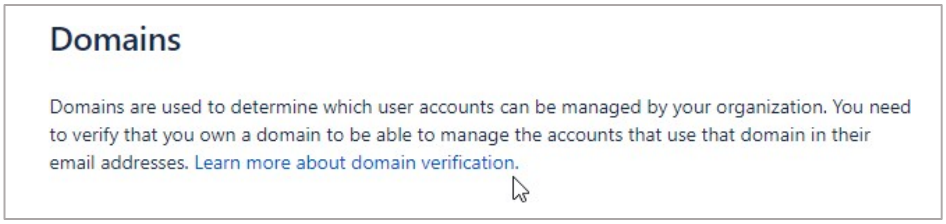
iii. Click the organization name.



iv. Click **Domains**.



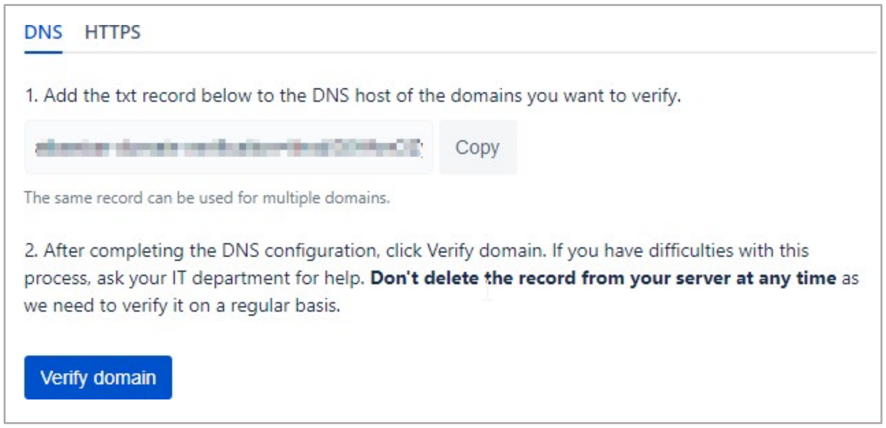
v. You can verify a domain using DNS or HTTPS. For more information about the steps to verify a domain, in the right pane under **Domains** section, click the **Learn more about domain verification** link.



Domains

Domains are used to determine which user accounts can be managed by your organization. You need to verify that you own a domain to be able to manage the accounts that use that domain in their email addresses. Learn more about domain verification.

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



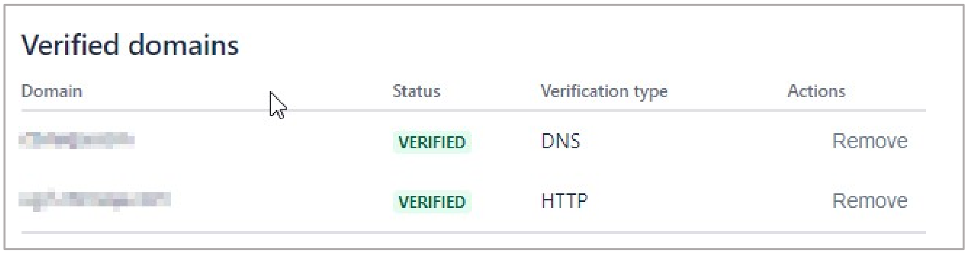
1. Add the txt record below to the DNS host of the domains you want to verify.

[redacted]

The same record can be used for multiple domains.

2. After completing the DNS configuration, click Verify domain. If you have difficulties with this process, ask your IT department for help. **Don't delete the record from your server at any time** as we need to verify it on a regular basis.

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

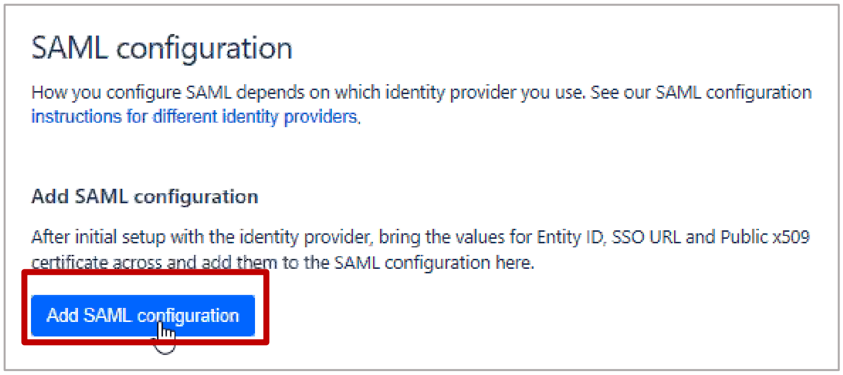


Verified domains

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**.



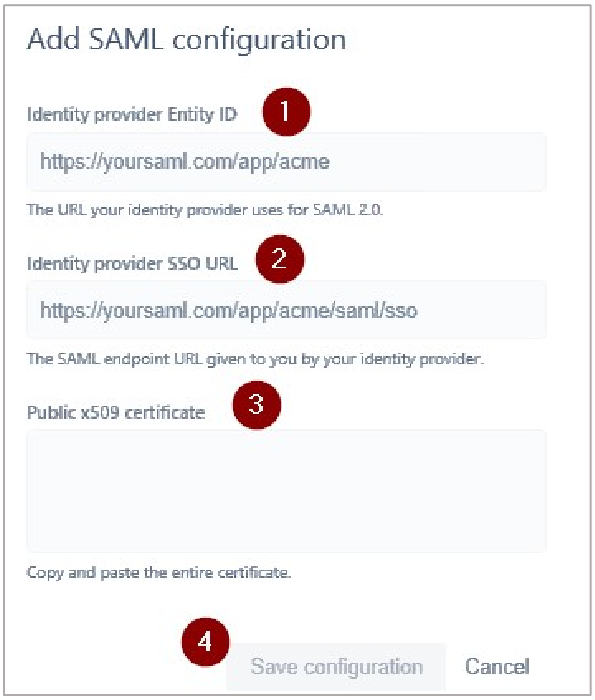
SAML configuration

How you configure SAML depends on which identity provider you use. See our SAML configuration instructions for different identity providers.

Add SAML configuration

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.

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

https://yoursaml.com/app/acme

The URL your identity provider uses for SAML 2.0.

Identity provider SSO URL

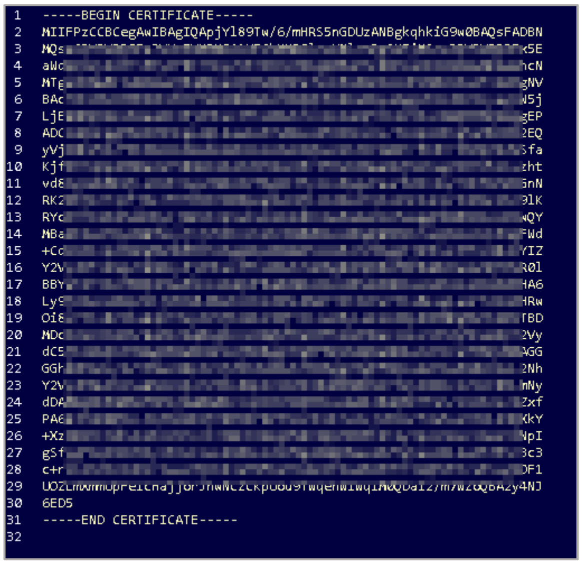
https://yoursaml.com/app/acme/saml/sso

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

Public x509 certificate

Copy and paste the entire certificate.

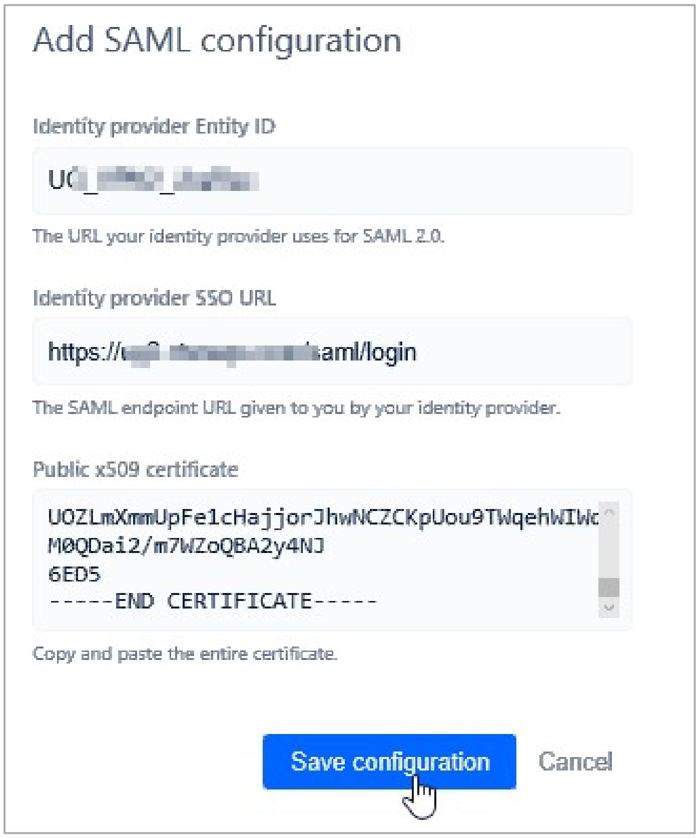
- **Public x509 Certificate** – copy and paste the SAML IdP signing certificate.
  To obtain the certificate, follow the steps below:
  To obtain your IdP certificate, follow the steps below:
  i. Remotely access your NetScaler instance using PuTTY.
  ii. Navigate to /nsconfig/ssl folder (using shell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



```
-----BEGIN CERTIFICATE-----
MIIFPzCCBCegAwIBAgIQApjYl89Tw/6/mHRS5nGDUzANBgkqhkiG9w0BAQsFADBN
[redacted]
6ED5
-----END CERTIFICATE-----
```

  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**.



Add SAML configuration

Identity provider Entity ID

UC_[redacted]

The URL your identity provider uses for SAML 2.0.

Identity provider SSO URL

https://[redacted]aml/login

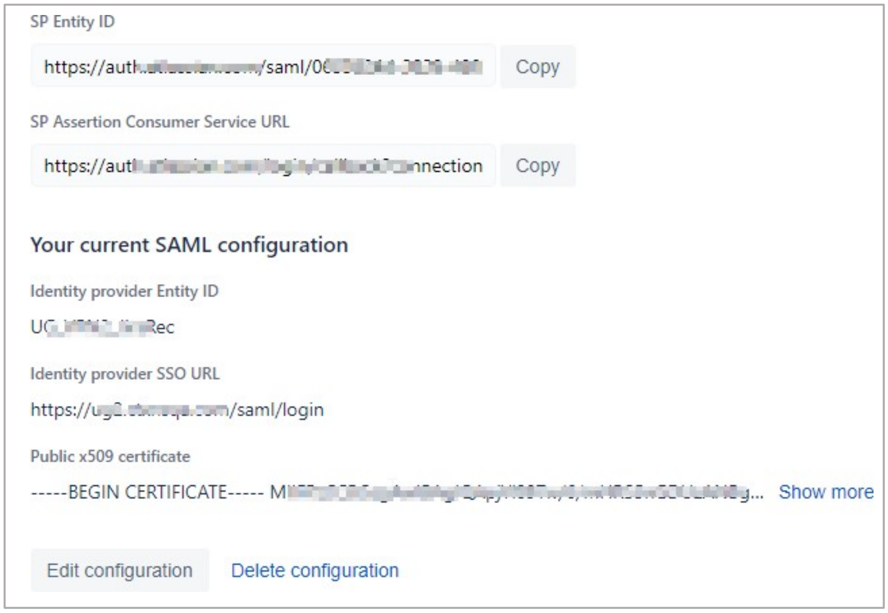
The SAML endpoint URL given to you by your identity provider.

Public x509 certificate

```
UOZLmXmmUpFe1cHajjorJhwNCZCKpUou9TWqehWIWc
M0QDai2/m7WZoQBA2y4NJ
6ED5
-----END CERTIFICATE-----
```

Copy and paste the entire certificate.

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



SP Entity ID

https://auth[redacted]/saml/0[redacted]

SP Assertion Consumer Service URL

https://aut[redacted]nection

Your current SAML configuration

Identity provider Entity ID

UC[redacted]Rec

Identity provider SSO URL

https://u[redacted]/saml/login

Public x509 certificate

-----BEGIN CERTIFICATE----- M[redacted]...

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

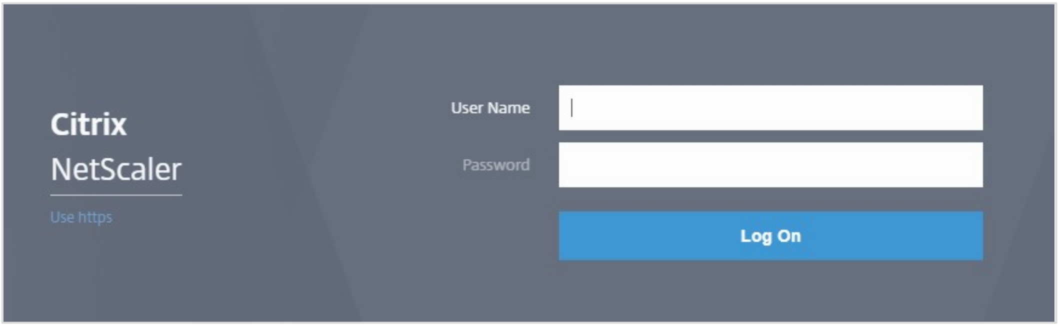
Configuring NetScaler for Single Sign-On

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

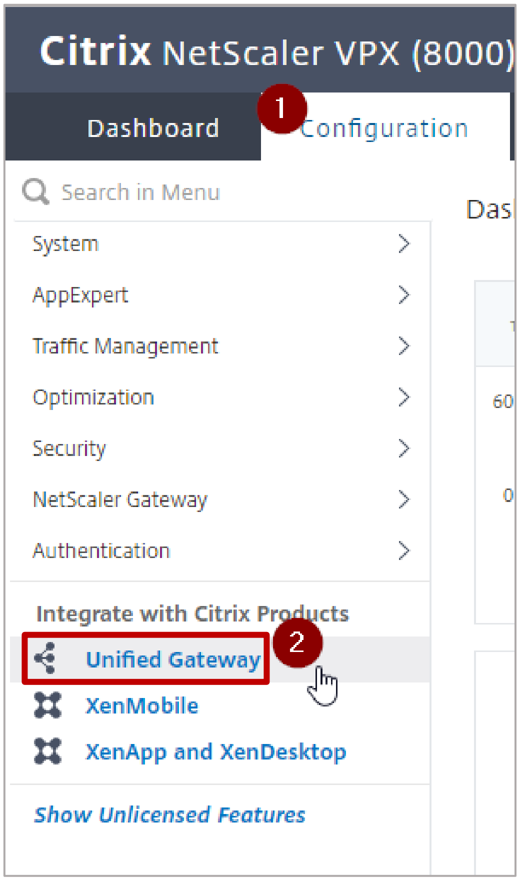
To configure NetScaler for single sign on through SAML, complete the following steps:

1. Connect to VPN using NetScaler with Unified Gateway.

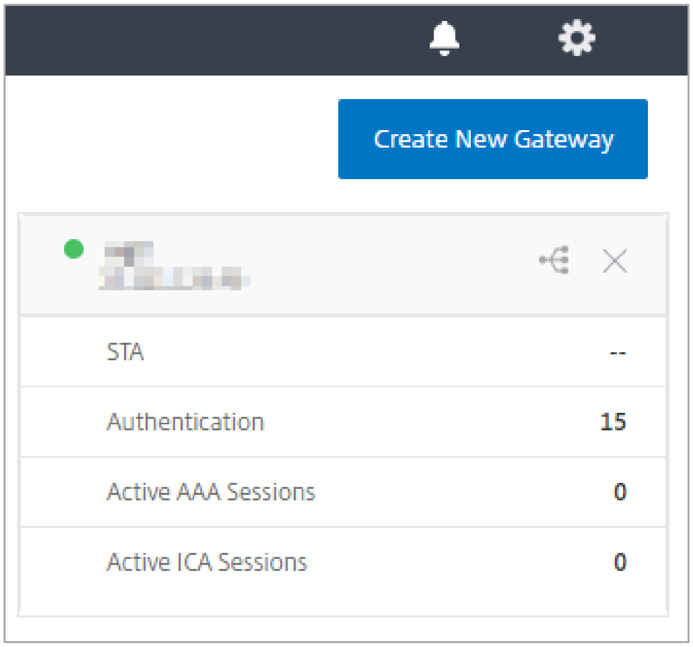
2. Log on to NetScaler using your user name and password.



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



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

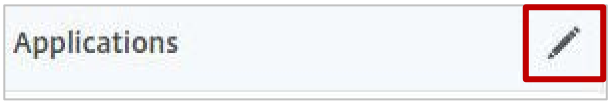


Create New Gateway

[redacted]

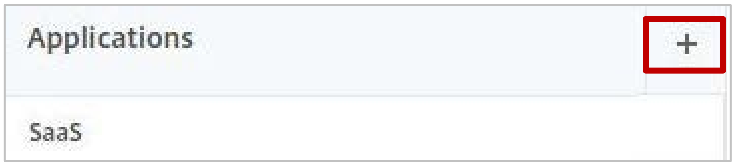
STA	--
Authentication	15
Active AAA Sessions	0
Active ICA Sessions	0

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



Applications

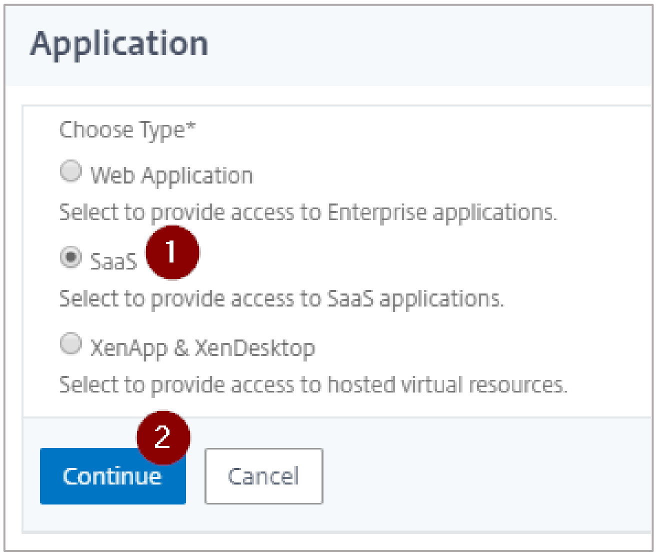
6. For adding a SaaS application, click the plus icon ⊞ that appears in the edit mode.



Applications +

SaaS

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



Application

Choose Type*

○ Web Application

Select to provide access to Enterprise applications.

● SaaS

Select to provide access to SaaS applications.

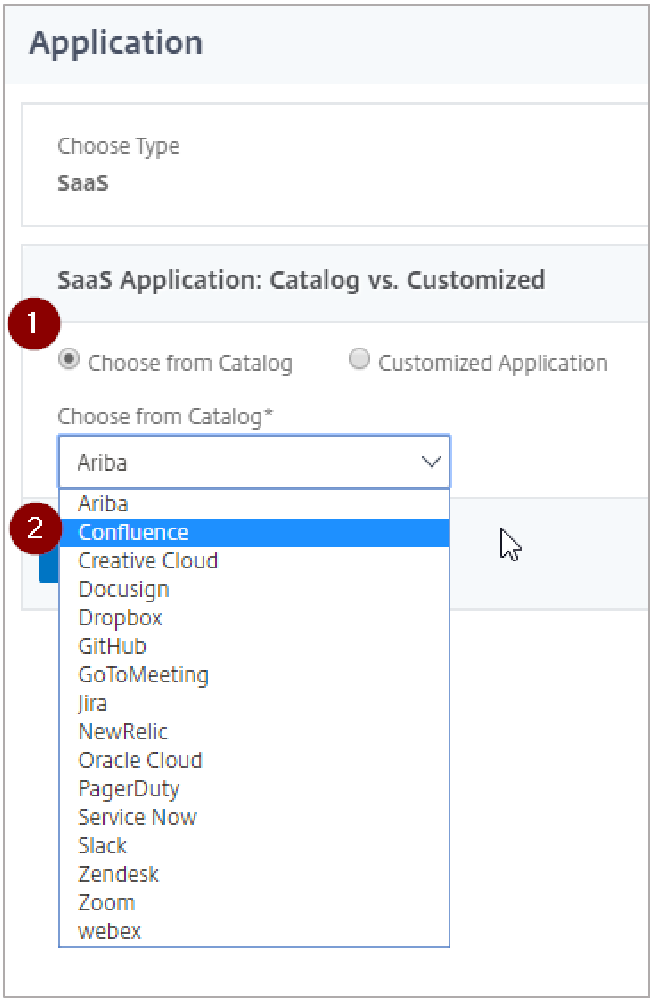
○ XenApp & XenDesktop

Select to provide access to hosted virtual resources.

Continue Cancel

8. Click **Choose from Catalog**.

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

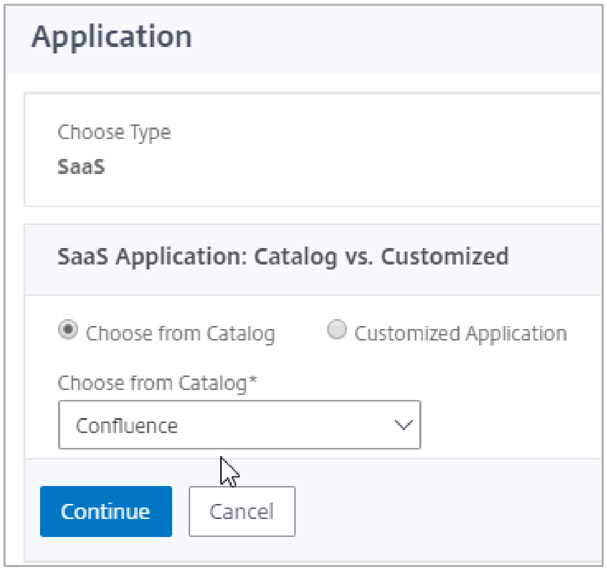


Choose Type
SaaS

● Choose from Catalog ○ Customized Application

Choose from Catalog*: Ariba

10. Click **Continue**.

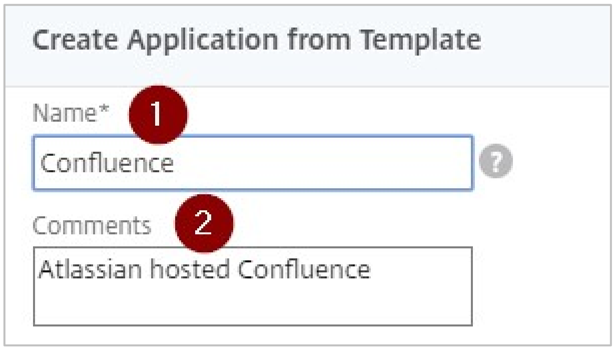


Choose Type
SaaS

● Choose from Catalog ○ Customized Application

Choose from Catalog*: Confluence

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*

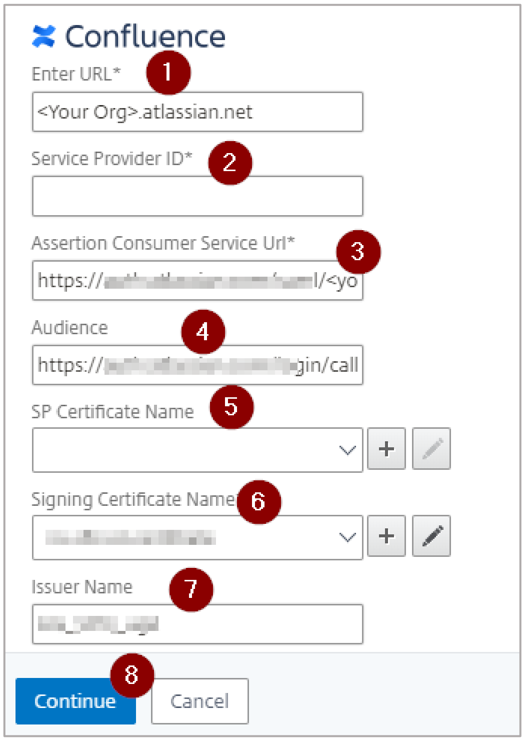
Confluence

Comments

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 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.



Confluence

Enter URL*

<Your Org>.atlassian.net

Service Provider ID*

Assertion Consumer Service Url*

https://[redacted]l/<yo

Audience

https://[redacted]gin/call

SP Certificate Name

Signing Certificate Name

[redacted]

Issuer Name

[redacted]

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

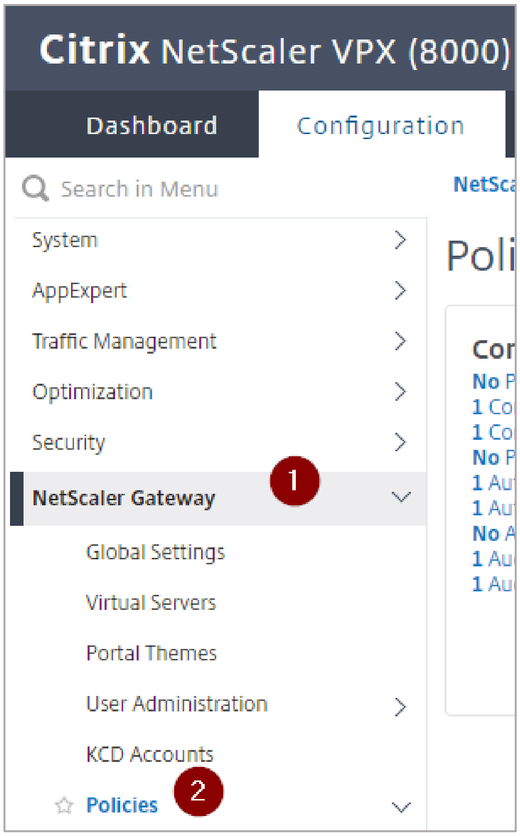
- **Signing Certificate Name -** click an appropriate certificate that will be used for signing SAML requests and responses.
- **Issuer Name -** type a unique issuer ID that you entered in the **Identity Provider Entity ID** box, while configuring SAML for Confluence.

12. Click **Continue.**

13. Click **Done**.

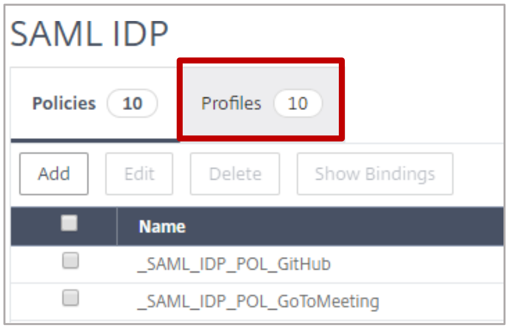
14. As Confluence does not provide SP certificate, you must clear the **Reject Unsigned Requests** check box. To do so, follow the steps below:

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



    ii. Click **Authentication** > **SAML IDP**.

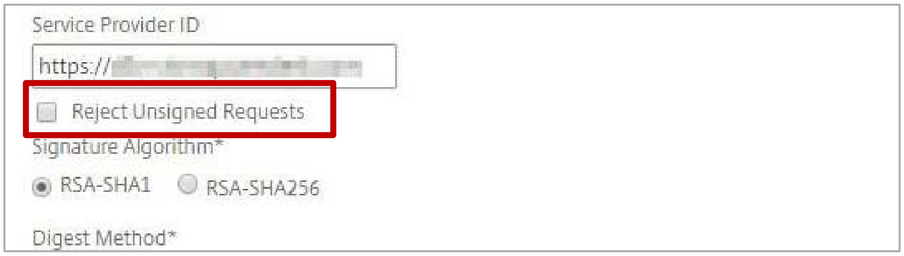
    iii. In the **SAML IDP** area, click the **Profiles** tab.



☐	Name
☐	_SAML_IDP_POL_GitHub
☐	_SAML_IDP_POL_GoToMeeting

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.



Service Provider ID

https://[redacted]

☐ Reject Unsigned Requests

Signature Algorithm*

● RSA-SHA1 ○ RSA-SHA256

Digest Method*

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.