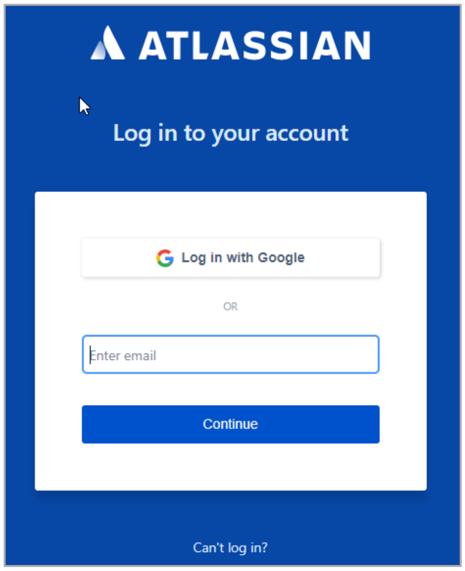
Configuring Jira

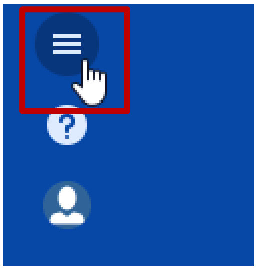
Configuring Jira for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Jira using their enterprise credentials.

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

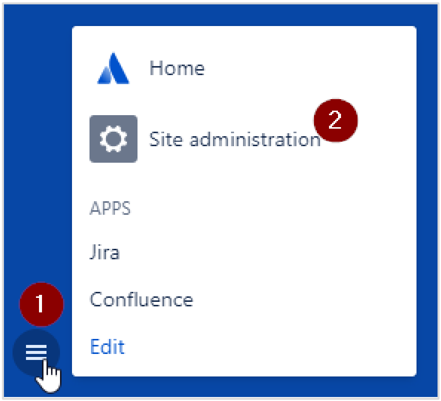
1. In a browser, type your organization's Atlassian cloud URL and press enter.
2. Log on to your Atlassian account.



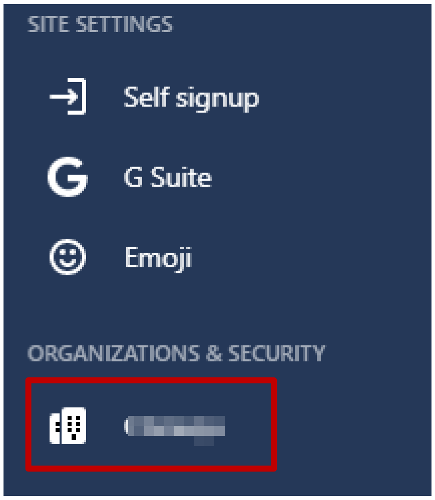
3. On the **Home** page, at the lower-left corner, click ≡.



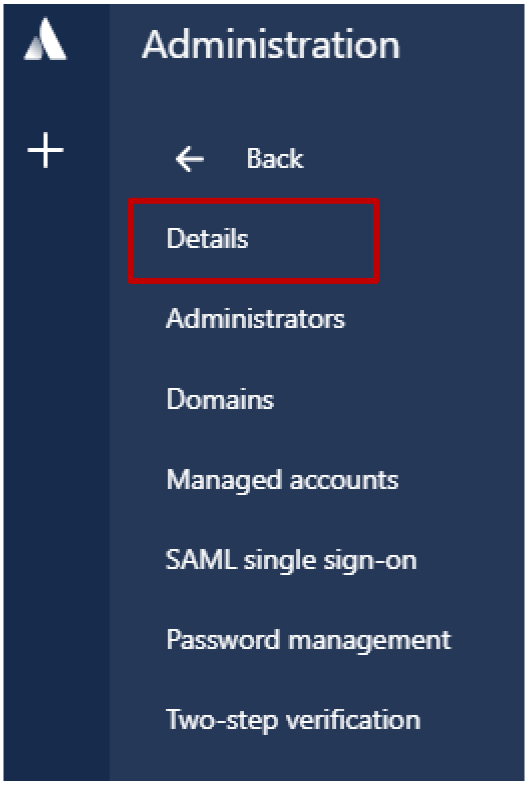
4. Click **Site administration**.



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

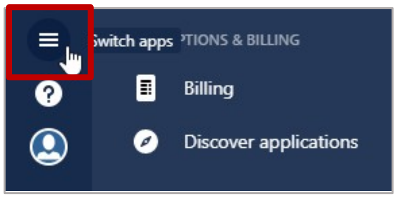


6. Click **Details** and verify the domain.

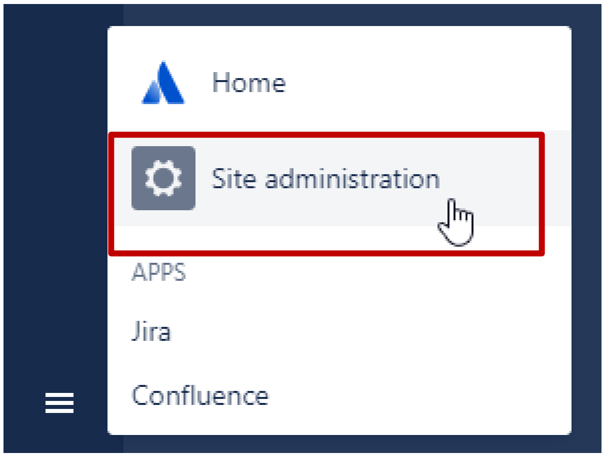


To verify the domain, follow the steps below:

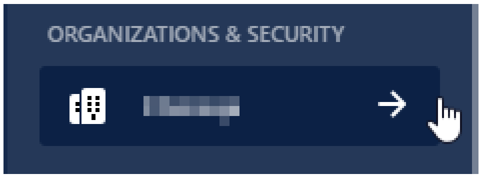
i. Click the **Switch apps** icon in the lower-left corner.



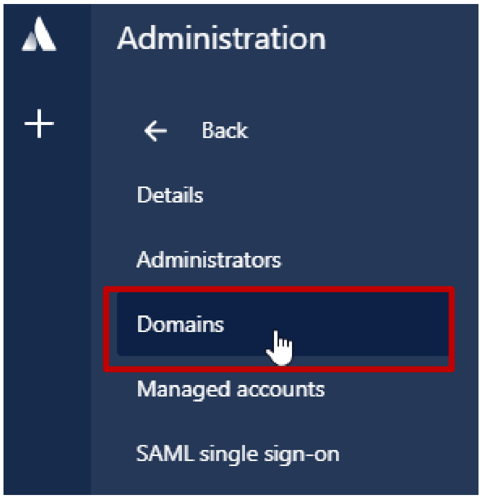
ii. Click **Site administration**.



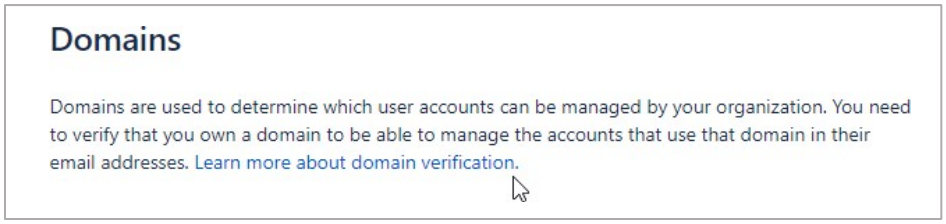
iii. Click the organization name.



iv. Click **Domains**.



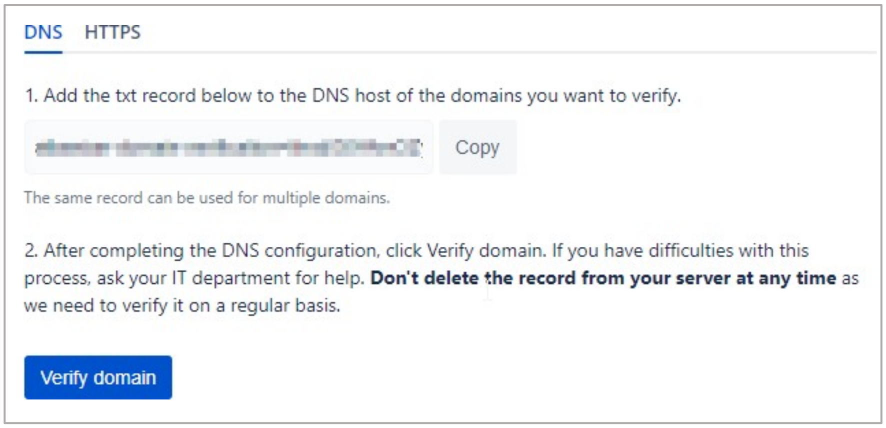
v. You can verify a domain using DNS or HTTPS. For more information about the steps to verify a domain, in the right pane under **Domains** section, click the **Learn more about domain verification** link.



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**.



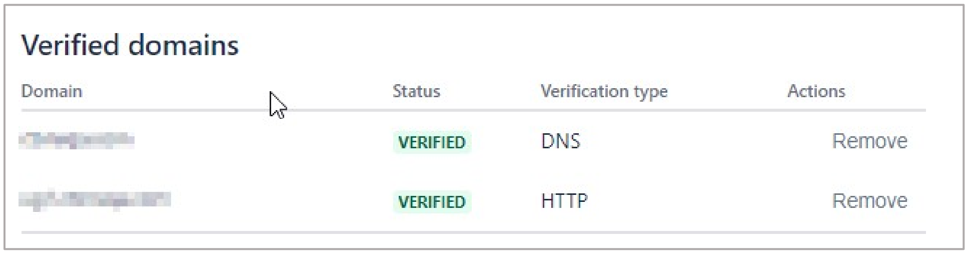
1. Add the txt record below to the DNS host of the domains you want to verify.

[redacted] Copy

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.

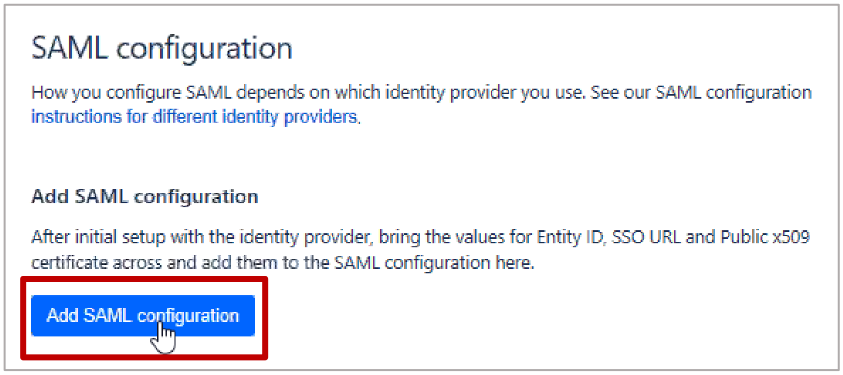
The **Status** column in the **Verified Domains** section displays **VERIFIED**.



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**.



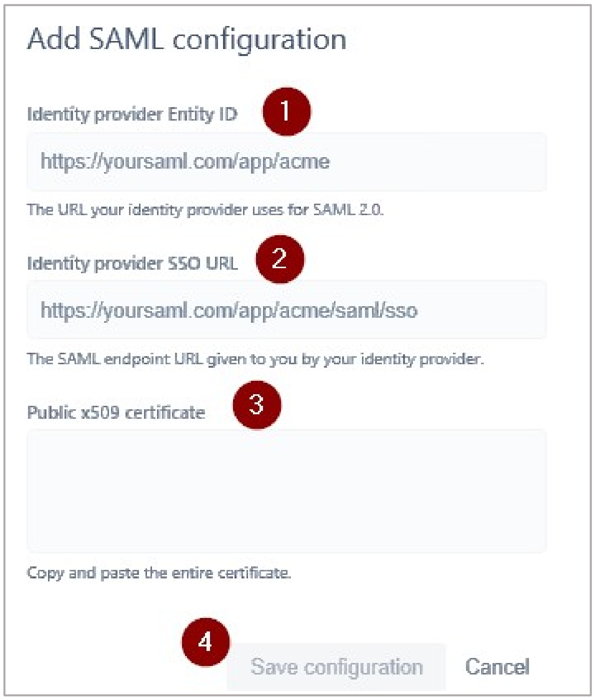
SAML configuration

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_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

https://yoursaml.com/app/acme

The URL your identity provider uses for SAML 2.0.

Identity provider SSO URL

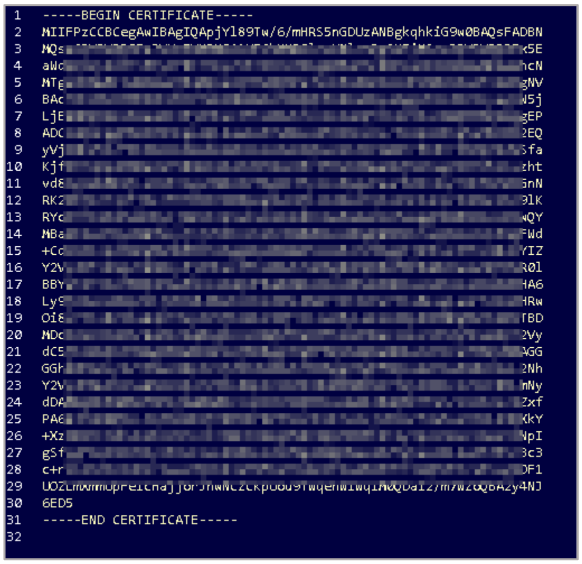
https://yoursaml.com/app/acme/saml/sso

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.

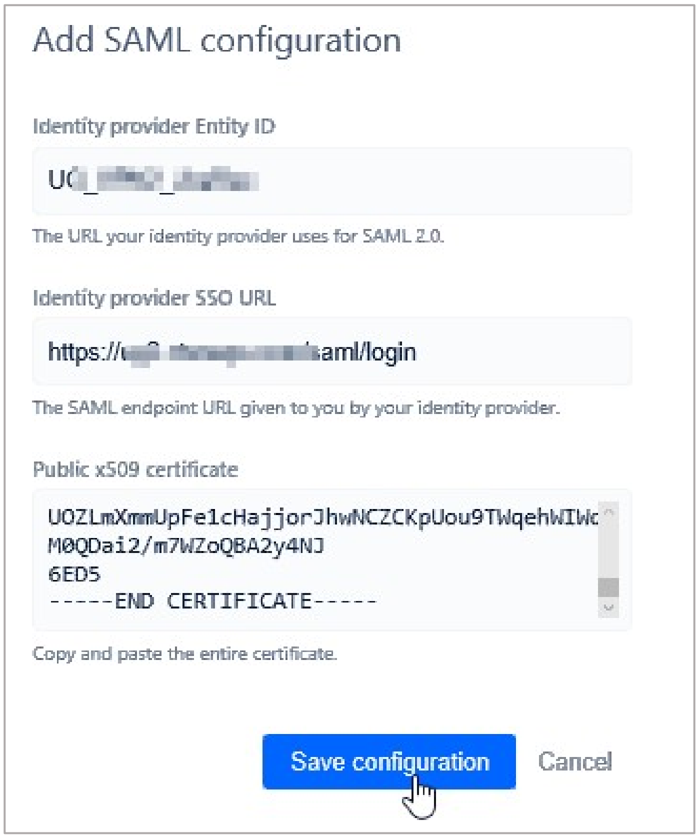


```
-----BEGIN CERTIFICATE-----
MIIFPzCCBCegAwIBAgIQApjYl89Tw/6/mHRS5nGDUzANBgkqhkiG9w0BAQsFADBN
[redacted]
6ED5
-----END CERTIFICATE-----

```

  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

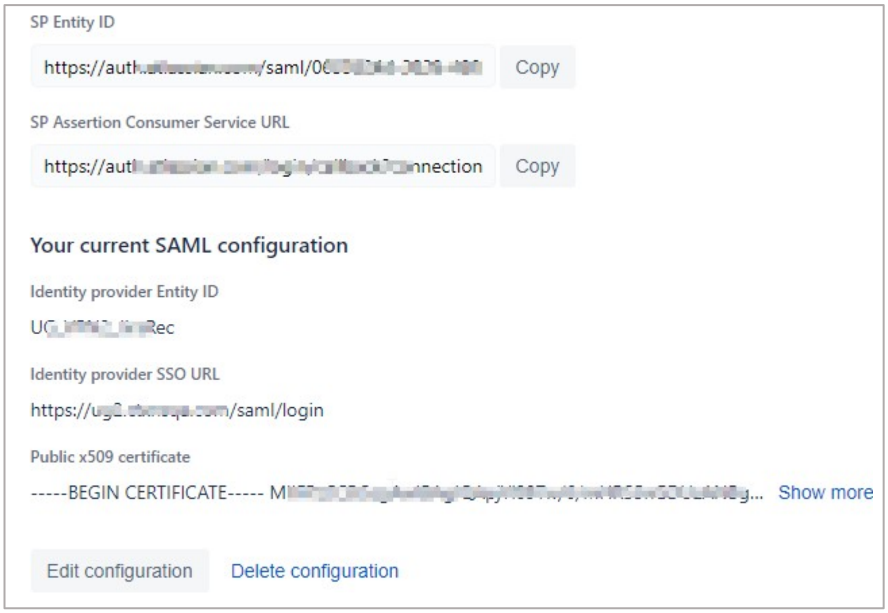
The SAML endpoint URL given to you by your identity provider.

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]nnection

Your current SAML configuration

Identity provider Entity ID

UC[redacted]Rec

Identity provider SSO URL

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

Public x509 certificate

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

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