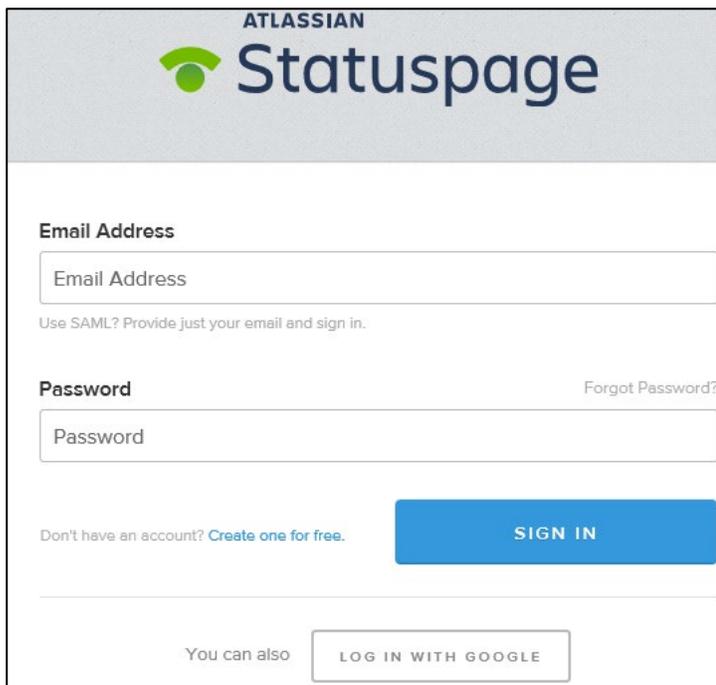


# Configuring Statuspage

Configuring Statuspage for SSO enables administrators to manage their users using Citrix Gateway. Users can securely log on to Statuspage using their enterprise credentials.

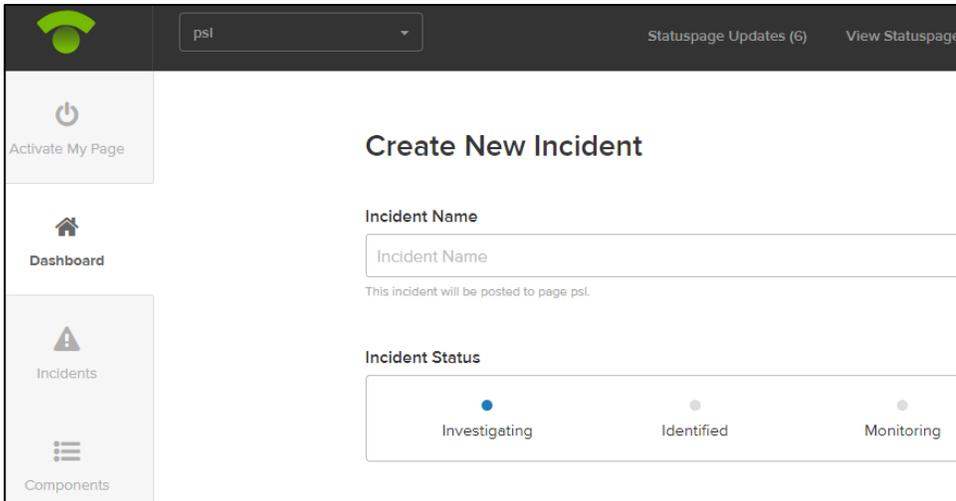
To configure Statuspage for SSO through SAML, follow the steps below:

1. In a browser, type the URL, <https://manage.statuspage.io/login> and press **Enter**.
2. Type the credentials, and click **Sign In**.

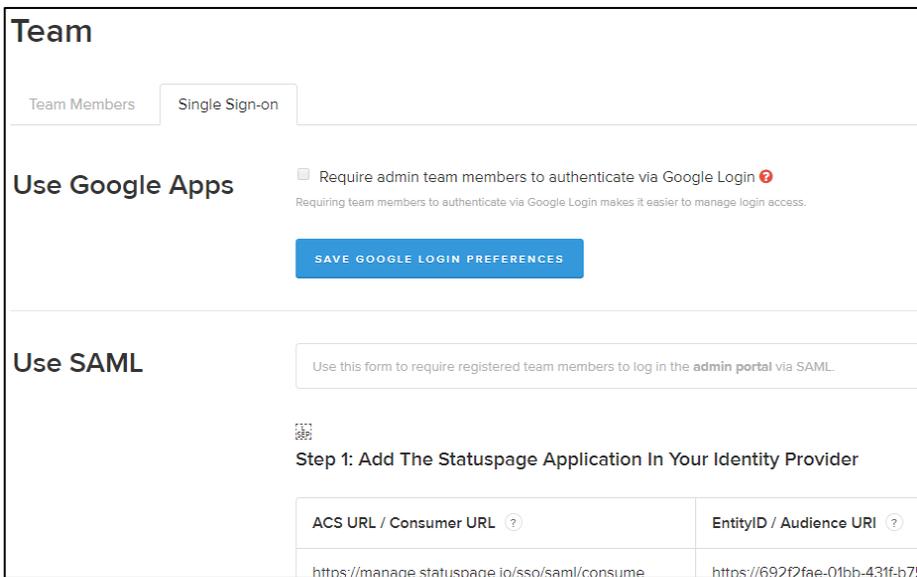


The screenshot shows the Atlassian Statuspage login interface. At the top, the Atlassian logo and the word "Statuspage" are displayed. Below this, there is a form with two input fields: "Email Address" and "Password". The "Email Address" field has a placeholder text "Email Address". Below the "Email Address" field, there is a link that says "Use SAML? Provide just your email and sign in." The "Password" field has a placeholder text "Password". To the right of the "Password" field, there is a link that says "Forgot Password?". Below the "Password" field, there is a link that says "Don't have an account? Create one for free." To the right of the "Password" field, there is a blue button that says "SIGN IN". At the bottom of the form, there is a link that says "You can also" followed by a button that says "LOG IN WITH GOOGLE".

The Dashboard page appears.



3. On the Dashboard page, click **Team Members** in the left pane. The Team page appears.
4. On the Team page, click **Single Sign-on** sub tab.



5. In the Use SAML section, under Step 1, **ACS URL / Consumer URL** and **EntityID/Audience URI** are displayed. These values are needed within your IdP. You can also *click service provider metadata XML file for this Organization URL* to see the raw SAML metadata.

**Using SAML**

Use this form if you want people to authenticate with SAML before being able to view the status page. If you want to require [team members](#) to log in the admin portal via SAML, use [this form](#) instead.

**Step 1: Add The Statuspage Application In Your Identity Provider**

ACS URL / Consumer URL ?	EntityID / Audience URI ?
<a href="https://manage.statuspage.io/sso/saml/consume">https://manage.statuspage.io/sso/saml/consume</a>	<a href="https://a8dc28de-b4dd-4965-bda4-9b3455dc8300.statuspage.io/">https://a8dc28de-b4dd-4965-bda4-9b3455dc8300.statuspage.io/</a>

You can also view the entire [service provider metadata XML file for this Page](#)

6. Under Step 2, type the following information:

**Step 2: Paste In The SSO Target URL And Certificate Returned By Your IDP**

**SSO Target URL**

SSO Target URL 1

ACS URL used to log in to your SSO provider.

**Certificate**

Paste in x.509 encoded certificate exactly as it's given by your Identity Provider, including the header and footer line. 2

**SAVE SSO CONFIGURATION**

- i. SSO Target URL- enter the IdP URL, SAML 2.0 endpoint, for example, <https://example.com/saml/login>
- ii. **Certificate** - click the certificate link and browse to the folder where you saved the Identity provider certificate in.pem format. Add the IdP certificate.

**Note:** To upload your IdP certificate, follow the steps below:

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

```
1 -----BEGIN CERTIFICATE-----
2 MIIFPzCCBCegAwIBAgIQApjY189Tw/6/mHRS5nGDuzAMBgkqhkiG9w0BAQsFADBN
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 gSt
28 c+r
29 UOZLmnmupre1cnaJjor3tiwLCzckpou9tqenWZwLAdQdAIz/m7wz0qBzy4ND
30 6EDS
31 -----END CERTIFICATE-----
32
```

d. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

7. Click **Save SSO Configuration**.