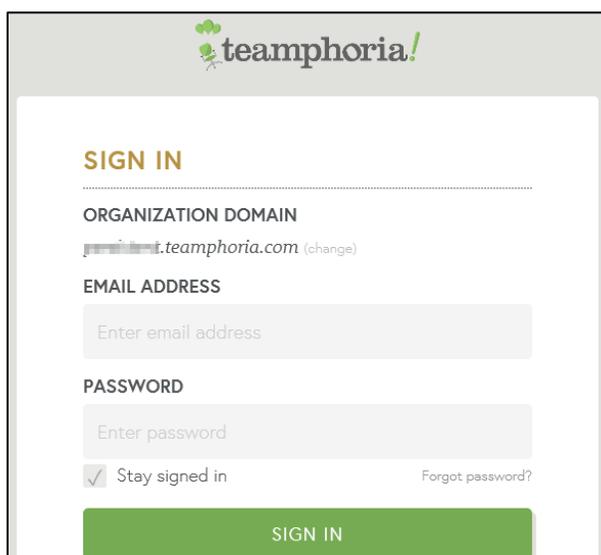


Configuring Teamphoria

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

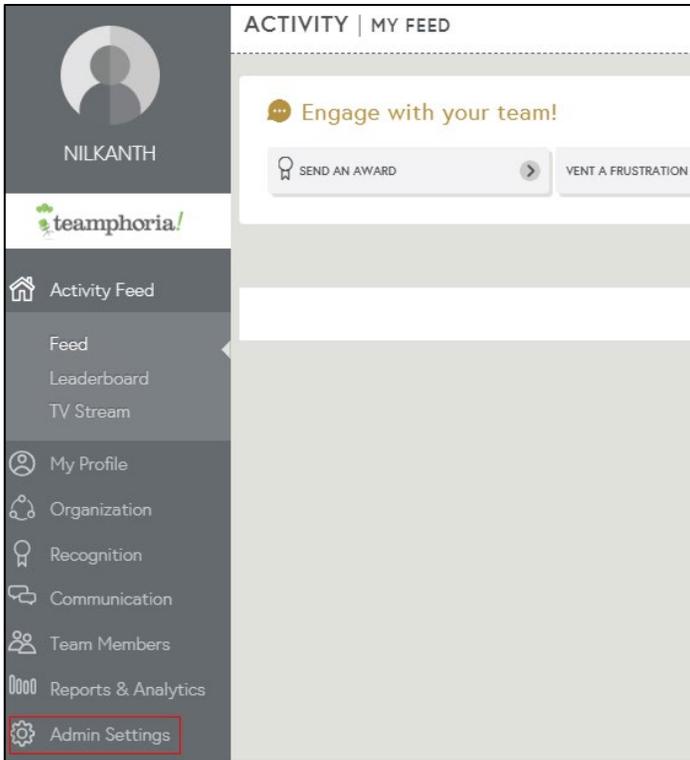
To configure Teamphoria for SSO through SAML, follow the steps below:

1. In a browser, type the URL, <https://<yourdomainname>.teamphoria.com/> and press **Enter**.
2. Type the credentials, and click **Sign In**.

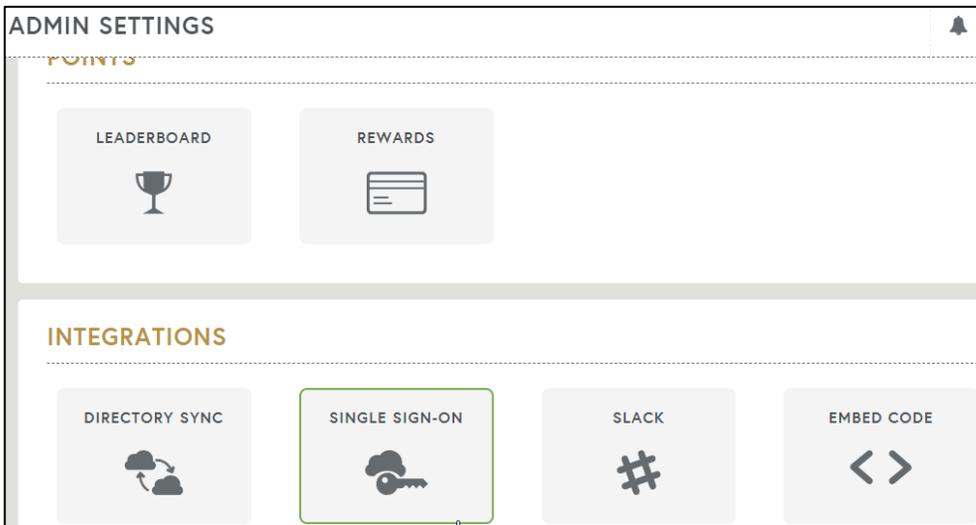


The screenshot shows the Teamphoria sign-in interface. At the top, there is a header with the Teamphoria logo and the text "teamphoria!". Below the header, the page is titled "SIGN IN". Underneath, there are three main sections: "ORGANIZATION DOMAIN" with a text input field containing "i.teamphoria.com" and a "(change)" link; "EMAIL ADDRESS" with a text input field containing the placeholder "Enter email address"; and "PASSWORD" with a text input field containing the placeholder "Enter password". Below the password field, there is a checkbox labeled "Stay signed in" which is checked, and a link labeled "Forgot password?". At the bottom of the form is a large green button labeled "SIGN IN".

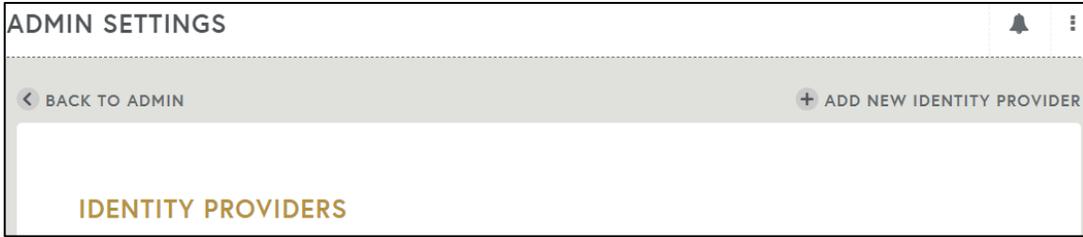
3. On the Activity page, click **Admin Settings** in the left pane.



4. On the Admin Settings page, click **Single Sign-On** under the Integrations Section.



5. Click **Add New Identity Provider**.



6. On the Identity Provider page, type the following information:

The screenshot shows the 'IDENTITY PROVIDER' configuration form. It includes an 'IMPORTANT' note about SSO integration. The form has several fields: 'CALLBACK URL' (with a placeholder message), 'DISPLAY NAME' (with callout 1), 'BUTTON NAME' (with callout 2), 'CERTIFICATE' (with callout 3), 'ENTRY POINT' (with callout 4), and 'Status' (with callout 5). At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

- i. **Display Name:** Type the display name for identity provider.
- ii. **Button Name:** Type the button name, for example, Login with @company name.
- iii. **Certificate:** To upload the certificate:
 - 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/mHRS5nGDuzAMBgqhkiG9w0BAQsFADBN
3 NQs=
4 allc
5 HTe
6 BAe
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 dCE
22 GGF
23 Y2V
24 dDA
25 PA6
26 +Xz
27 gSf
28 c+r
29 UOZLmnmupre1cnaJjor3tiwIL2ckpobu9TqenWZwLAdQdaIz/m7az0qBzy4ND
30 6EDS
31 -----END CERTIFICATE-----
32
```

d. Copy the certificate from BEGIN CERTIFICATE----- to -----END CERTIFICATE-----

- iv. **Entry Point:** Enter the IdP URL, SAML 2.0 endpoint, for example, <https://example.com/saml/login>.
- v. **Status:** Switch the toggle button to **ON**.

7. Click **Save**.

The configuration is complete.