Configuring PurelyHR

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

To configure PurelyHR for SSO through SAML, follow the steps below:
1. In a browser, type the URL, https://citrix.purelyhr.com/?ct=1 and press **Enter.**
2. Type your credentials, and click **Sign in**.
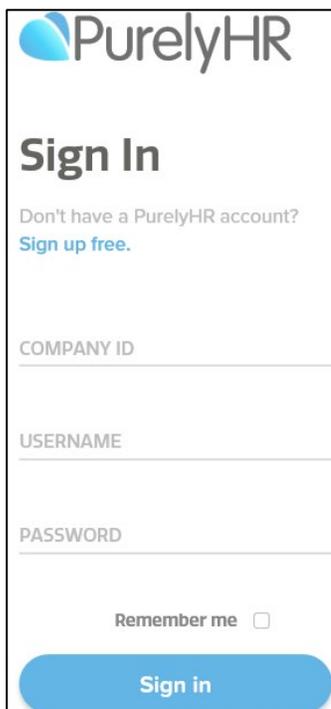
3. From the landing page, click icon, to navigate to your account Dashboard page.

4. On the **Dashboard** page, click **SSO Settings**.
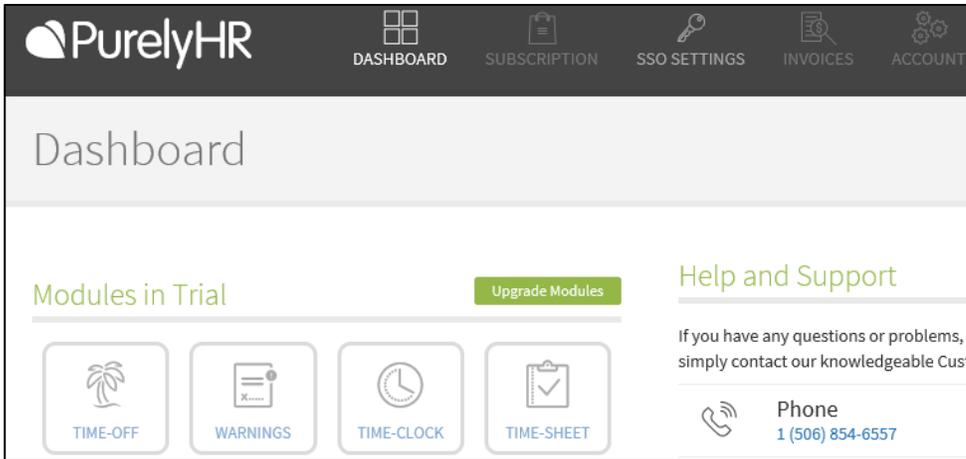
The SSO Settings page appears.
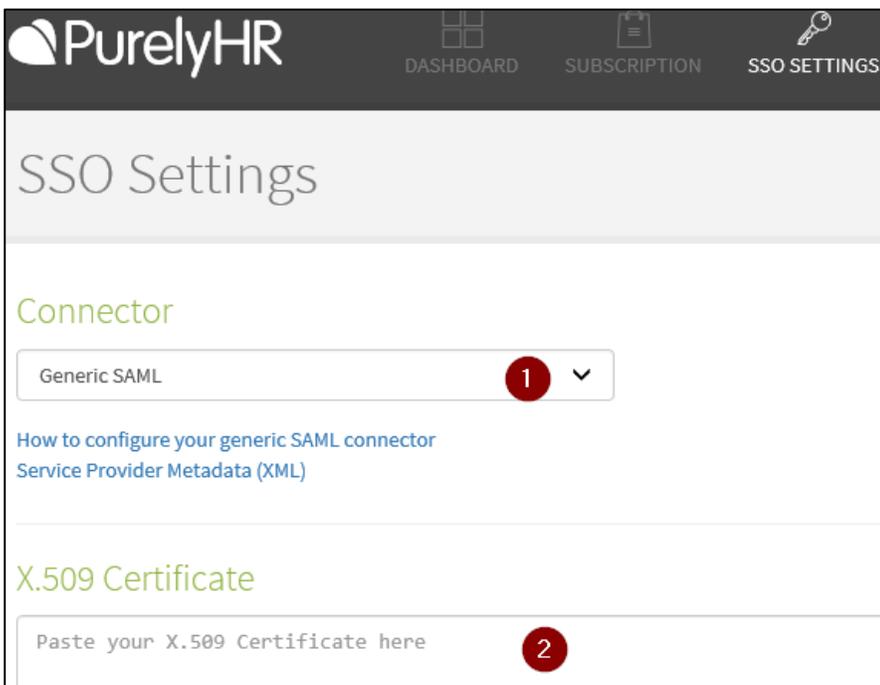
5. Type the following information on the SSO Settings page:

   i.   **Connector**- From the drop-down list, select the **Generic SAML** option.

   ii. **X.509 Certificate**- 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/mHRS5nGDUzANBgkqhkiG9w0BAQsFADBN
3   MQs                                                           X5E
4   aWd                                                           hcN
5   MTg                                                           gNV
6   BAc                                                           N5j
7   LjE                                                           gEP
8   ADC                                                           2EQ
9   yVj                                                           3fa
10  Kjf                                                           zht
11  vd8                                                           GnN
12  RKZ                                                           9lK
13  RYc                                                           wQY
14  MBa                                                           FWd
15  +Cc                                                           YIZ
16  Y2v                                                           R0l
17  BBY                                                           HA6
18  LyS                                                           HRw
19  Oi8                                                           fBD
20  MDc                                                           2Vy
21  dC5                                                           AGG
22  GGh                                                           2Nh
23  Y2v                                                           nNy
24  dDA                                                           Zxf
25  PA6                                                           kkY
26  +Xz                                                           NpI
27  gSf                                                           3c3
28  c+r                                                           DF1
29  UOZLmXmmupreIchajjor5fwNcZckpo6u9fwqenWiwq1AkQDaIz/m7wZ6Q6A2y4NJ
30  6ED5
31  -----END CERTIFICATE-----
32
```

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

iii. **IdP issuer Url**- type a unique issuer ID. For example:

https:// example.com/saml/metadata/546600

iv. **IdP Endpoint Url**- type the endpoint URL. For example,

https:// example.com/trust/saml2/http-post/sso/12345

v. **Force SSO**- Select the checkbox to force users to login through SAML connector.

vi. **Auto-Create users**- select the checkbox to auto create users.

vii. **Sign-in page URL**- enter the IdP URL, SAML 2.0 endpoint, for example, https://example.com/saml/login.

6. Click **Save Changes**.