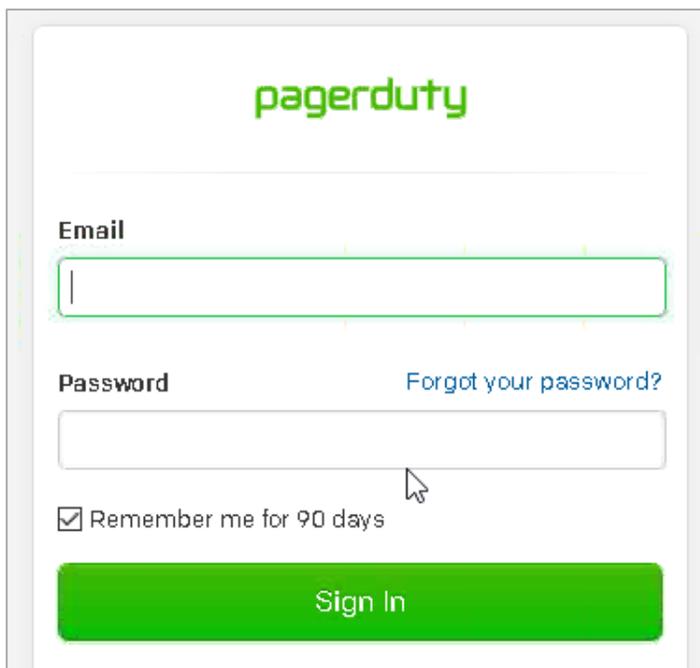


Configuring PagerDuty

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

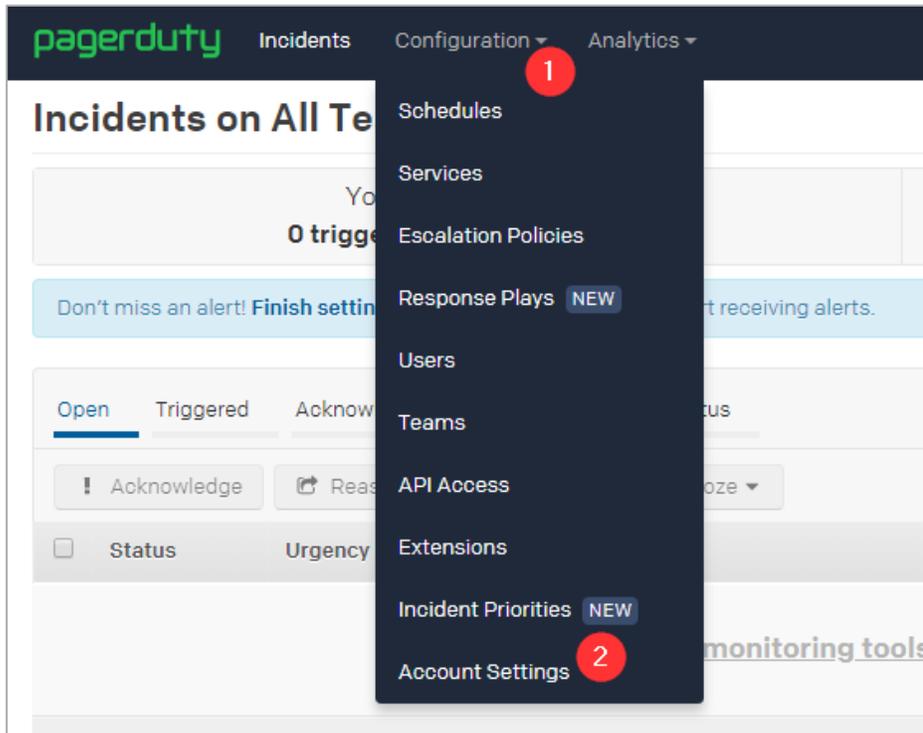
To configure PagerDuty for SSO through SAML, follow the steps below:

1. In a browser, type <https://<your-organization>.pagerduty.com/> and press enter.
Note: For example, if the URL you use to access pager duty is <https://myserver.pagerduty.com>, then you must replace <your-organization> with myserver.
2. Log on to your PagerDuty account as an administrator.

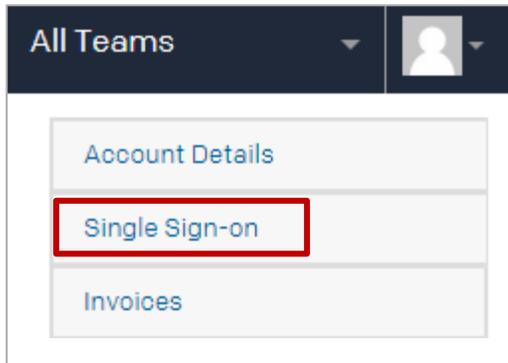


The image shows a screenshot of the PagerDuty login interface. At the top, the 'pagerduty' logo is displayed in green. Below the logo is a horizontal line. The form contains the following elements: an 'Email' label above a text input field; a 'Password' label above another text input field, with a 'Forgot your password?' link in blue text to its right; a checkbox labeled 'Remember me for 90 days' which is checked; and a large green button at the bottom labeled 'Sign In'.

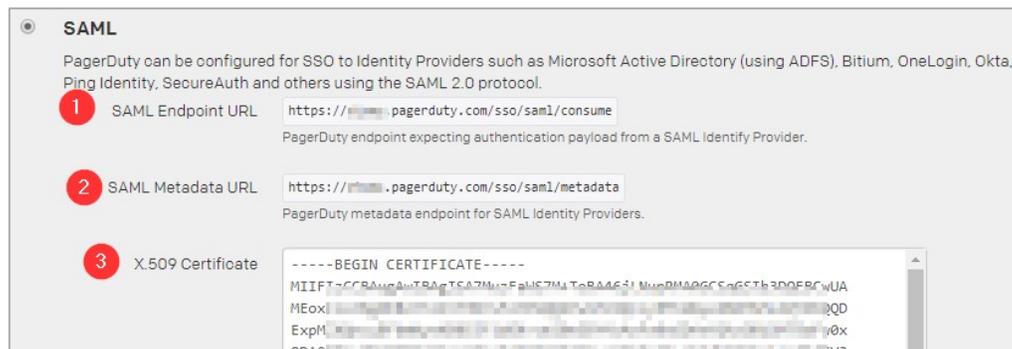
3. On the home page, click **Configuration > Account Settings**.



4. In the upper right corner, click **Single Sign-on**.



5. On the **Enable Single Sign-on (SSO)** page, in the **SAML** area, review and specify required details.



Note: By default, SAML option is selected. If not, ensure that you click **SAML**.

- i. **SAML Endpoint URL** – displays assertion consumer service URL.
Note: Copy this value to use it while configuring NetScaler for SSO for the Assertion Consumer Service URL field.
- ii. **SAML Metadata URL** – displays metadata URL. This is an XML file that contains data such as endpoints, supported bindings, identifier, and public keys required for interaction with SAML-enabled identity or service provider.
Note: Copy this value to use it while configuring NetScaler for SSO.
- iii. **X.509 Certificate** – paste the Identity provider certificate.
Browse to the folder where you saved the IdP provided certificate and upload it.
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.
 - iv. Copy the text from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----`
 - v. Paste the text in a text editor and save the file in an appropriate format such as `<your organization name>.pem`

```
root@pers:~# cd /nsconfig/ssl
root@pers:~# cd /nsconfig/ssl
-----BEGIN CERTIFICATE-----
MIIClzCCAkcCgAwIBAgIIGAWHYpN18MA0GCSqGSIb3DQEBBQUAMIGuMQswCQYDVQQGEwJVUzETMBEG
A1IqNDkl
f2MDEx
N1MRYw
FAaWR1
cjlBgkq
7aff
5OyZ
FF3k
H99Z
hr8i
PrC4ydcwMxqGdFFSQ/LHWUPGvGlpHzj47MzcN0EbdVmkF61e4/fTkVz3ST3U=
-----END CERTIFICATE-----
root@pers:~#
```

- iv. **Login URL** - type the IdP URL followed by /saml/login. For example:
`https://<customerFQDN>/saml/login`

Login URL
The URL used for logging into the SAML Identity Provider.

- v. **Logout URL (optional)** - type a redirect URL for logging out.
- vi. **Allow username/password login**-. select the check box. Clear the check box after completing testing of logging on via Identity Provider if you do not want users to log on using user name and password.

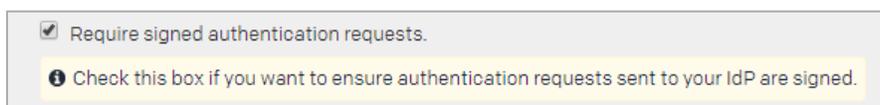
Allow username/password login
▲ Turn this off when you have completed testing login via your Identity Provider.

- vii. **Require EXACT authentication context comparison** – select the check box if you want to mandate exact authentication. For this configuration, leave the check box unchecked.



Require EXACT authentication context comparison.
ⓘ Check this box if you want to require an EXACT match (rather than MINIMUM) to PasswordProtectedTransport.

- viii. **Require signed authentication requests** - select the check box if you want to ensure authentication requests are signed. For this configuration, leave the check box unchecked.



Require signed authentication requests.
ⓘ Check this box if you want to ensure authentication requests sent to your IdP are signed.

- ix. **Auto-provision users on first login** – select the checkbox in the **User provisioning** section to auto-provision users. After you enable auto-provisioning, if a user for whom a user account is not created uses SSO to log on to PagerDuty, the associated user account is created automatically.



User Provisioning

Auto-provision users on first login
⚠ Be aware that adding new users will impact your bill.

Redirect non-provisioned users
When enabled, login attempts from people without accounts will be redirected to the destination link.

Destination Link

- x. **Redirect non-provisioned users** – select the check box to redirect people without an account to a specific link and type the link in the **Destination Link** box.

6. Click **Save Changes**.

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