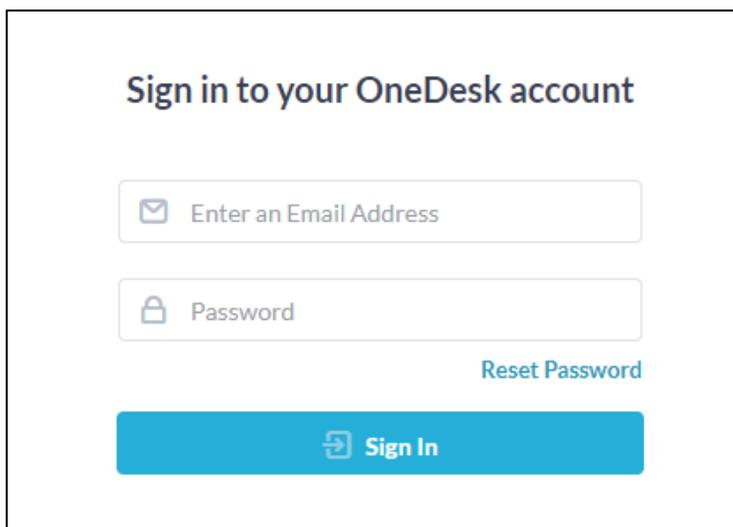


Configuring OneDesk

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

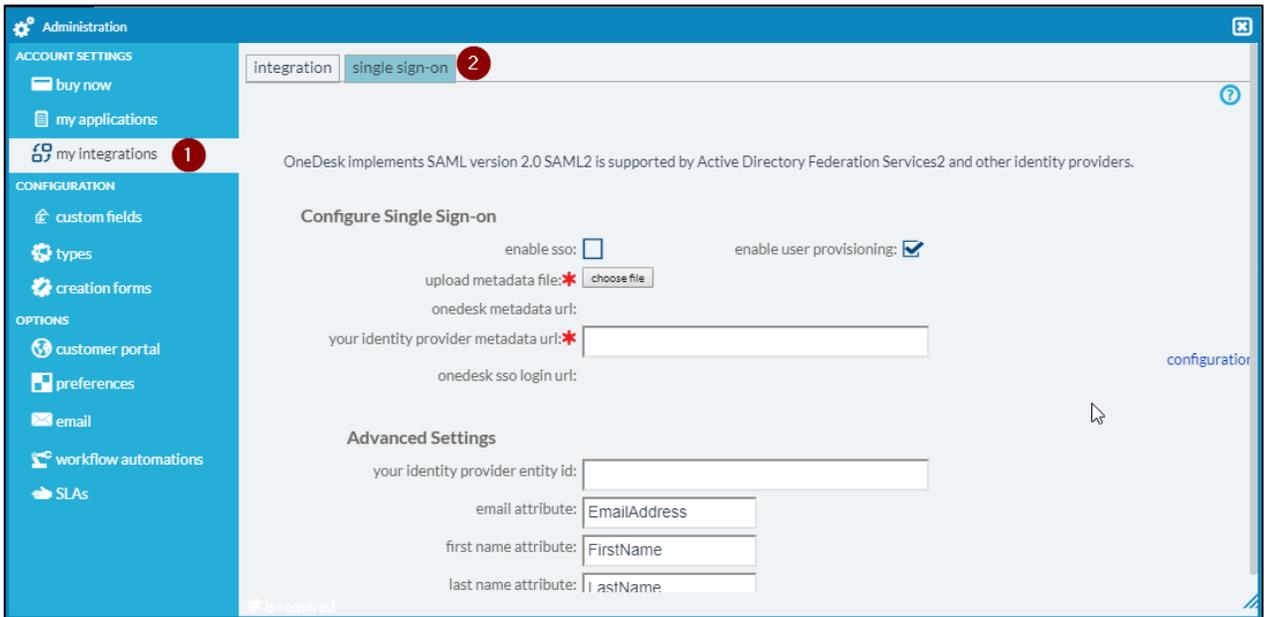
To configure OneDesk for SSO through SAML, follow the steps below:

1. In a browser, type <https://app.onedesk.com/> and press **Enter**.
2. Log on to your OneDesk account as an administrator.
3. Type your credentials, and click **Sign In**.

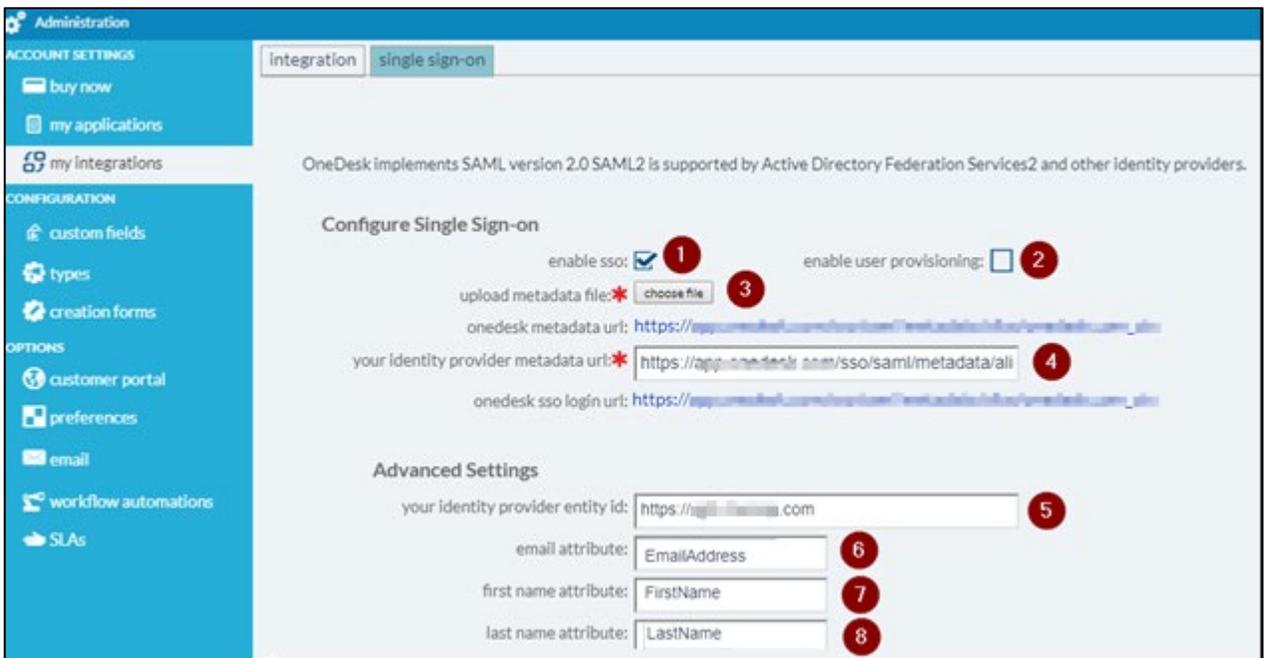


The screenshot shows the OneDesk sign-in interface. At the top, the text reads "Sign in to your OneDesk account". Below this, there are two input fields: the first is labeled "Enter an Email Address" with an envelope icon, and the second is labeled "Password" with a lock icon. To the right of the password field is a link that says "Reset Password". At the bottom of the form is a large blue button with a white arrow icon and the text "Sign In".

4. On the Home page, click Administration  icon. The Administration page appears. Click **my integrations > single sign-on**.



5. On the **single sign-on** page, specify the following information:



- i. **Enable sso** – select the check box
- ii. **Enable user provisioning**- select the check box if you want IdP authenticated users to automatically get created and granted access when they attempt to access the OneDesk application.
- iii. **Upload metadata file**- Click **Choose File** to select the IDP (Netscaler) metadata file.

- iv. **your identity provider metadata url**- Specify the IDP (Netscaler) metadata URL.
For example,
https://app.onedesk.com/sso/saml/metadata/alias/onedesk.com_<your-Org-domain>
- v. **your identity provider entity id**- Specify the unique name or URL of IDP as entity id.
- vi. **Email attribute**- specify the email attribute.
- vii. **First name attribute**- type the first name of the attribute.
- viii. **Last name attribute**- type the last name of the attribute.

The configuration gets saved.