

Configure NexTravel for Single Sign-On

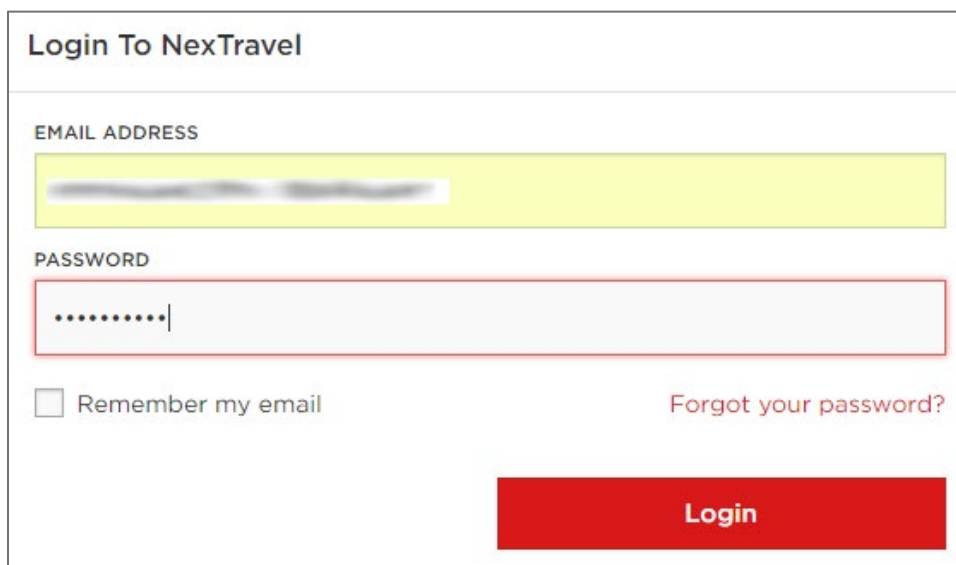
Configuring NexTravel for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to NexTravel by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure NexTravel for SSO by using SAML:

1. In a browser, type <https://www.nextravel.com/login> and press **Enter**.
2. Type your NexTravel admin account credentials (**EMAIL ADDRESS** and **PASSWORD**) and click **Login**.



Login To NexTravel

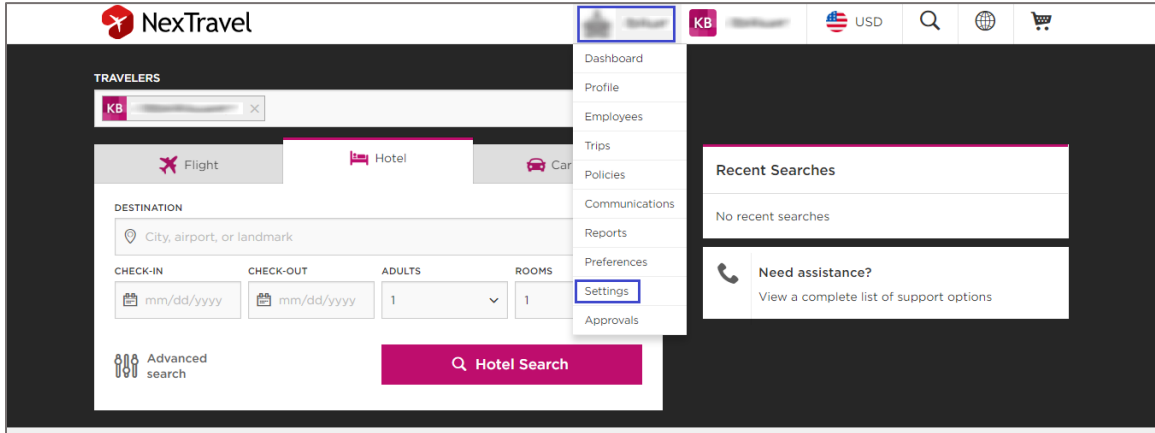
EMAIL ADDRESS

PASSWORD

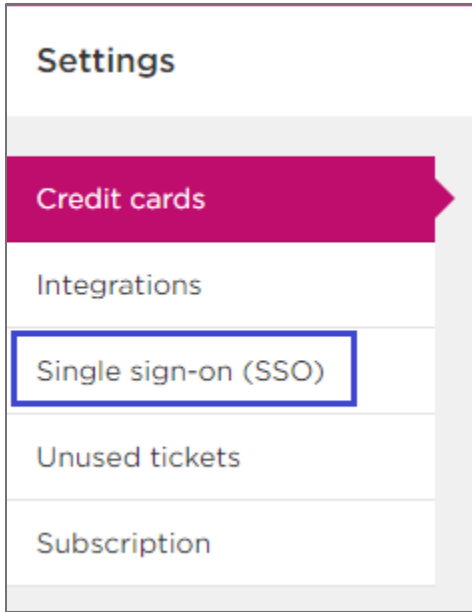
Remember my email [Forgot your password?](#)

Login

3. In the dashboard page, click the organization name and select **Settings**.



4. In the **Settings** page, click **Single sign-on (SSO)** from the left panel.



5. In the **Single Sign-On (SSO)** section, click **+ Add**.



- Note down the **SP - ENTITY**, **SP - ASSERTION CONSUMER SERVICE (ACS)**, **SP - SINGLE LOGOUT (SLO) URL** for IdP configuration.

Add Single Sign-On (SSO)

Service Provider (SP) Enter this data in your IDP (Okta, Onelogin, etc.)

SP - ENTITY / AUDIENCE URL

SP - ASSERTION CONSUMER SERVICE (ACS) / SINGLE-SIGN ON (SSO) URL

SP - SINGLE LOGOUT (SLO) URL

- Scroll down and enter the values for the following fields:

Field Name	Description
IDP - ENTITY	IdP entity ID
IDP - SSO URL	IdP logon URL
IDP - CERTIFICATE	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- Note: The IdP Certificate is provided by Citrix and can be accessed from the link below: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml

Identity Provider (IDP)

IDP - ENTITY / ISSUER / METADATA URL *

IDP - SSO URL / SIGN-IN URL *

IDP - SLO URL / LOG-OUT URL

IDP - CERTIFICATE *

- Finally, click **Save**.