

Configuring Absorb

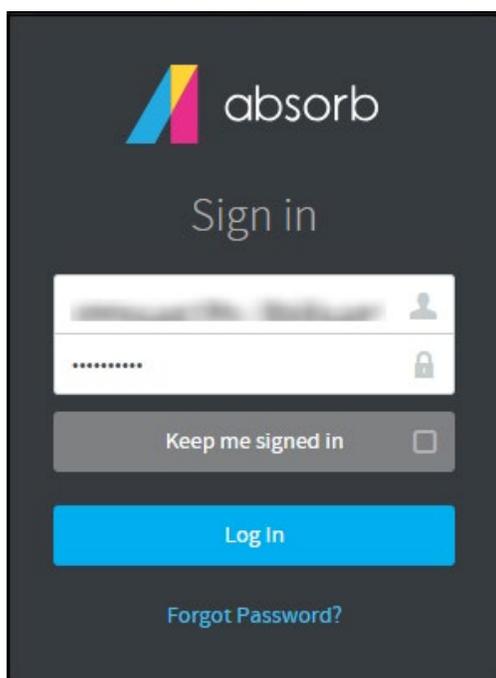
Configuring Absorb for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Absorb by using the enterprise credentials.

Prerequisite

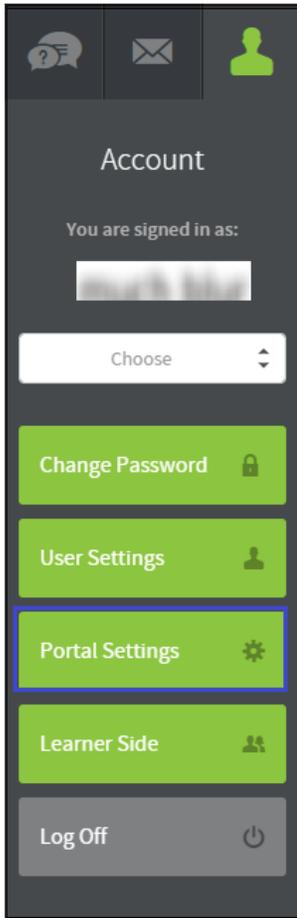
Browser Requirements: Internet Explorer 11 and above

To configure Absorb for SSO by using SAML:

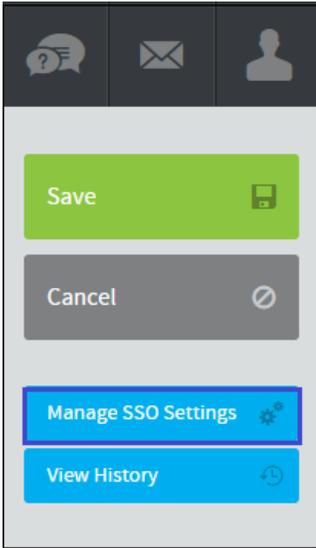
1. In a browser, type <https://<customer domain>.myabsorb.com.au/> and press **Enter**.
2. On the home page, click **Login**.
3. Type your Absorb admin account credentials (**Email** and **Password**) and click **Log In**.



4. In the user profile menu, select **ADMIN**.
5. In the user profile menu that is present at the top-right corner of the screen, click **Portal Settings** from the drop-down menu.



- Under **Portal Settings**, click **Manage SSO Settings**.



- Enter the values in the following fields:

Field	Description
Method	Select SAML from the drop-down list.
Key	Copy and paste the IdP 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
Mode	Select Identity Provider Initiated from the drop-down list.
Id Property	Email Address
Signature Type	Select sha256 from the drop-down list.
Login URL	IdP login URL
Logout URL	Landing URL
Assigned Routes	Add your route so that it will redirect to that URL after logging in.

Mode: Identity Provider Initiated

Name

Method

Key *

Mode *

Id Property *

Signature Type *

Login URL *

Logout URL

If left blank, will default to users absorb login page

Automatically Redirect

 Redirects the user to the Login URL if the user lands on Absorb and is unauthenticated.

Assigned Routes

Save 

Cancel 

8. Finally, click **Save**.