

Configure Retrace for Single Sign-On

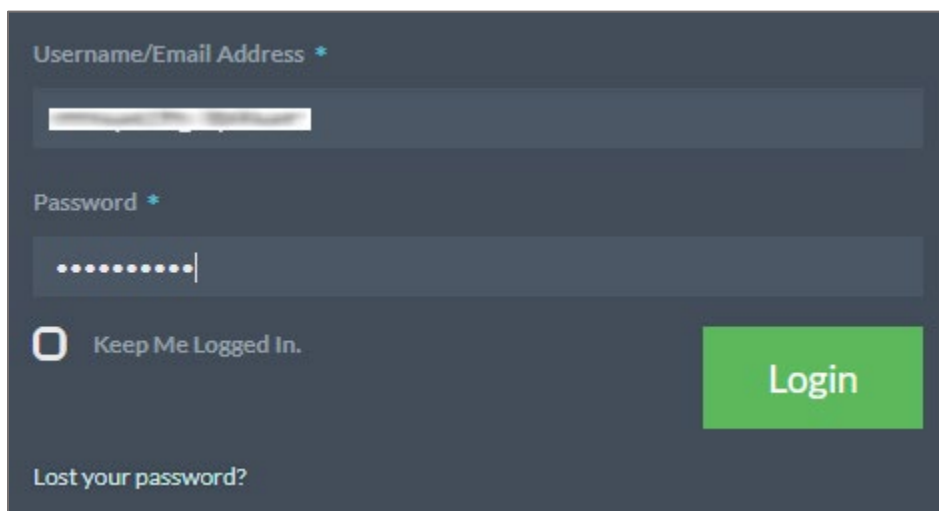
Configuring Retrace for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Retrace by using the enterprise credentials.

Prerequisite

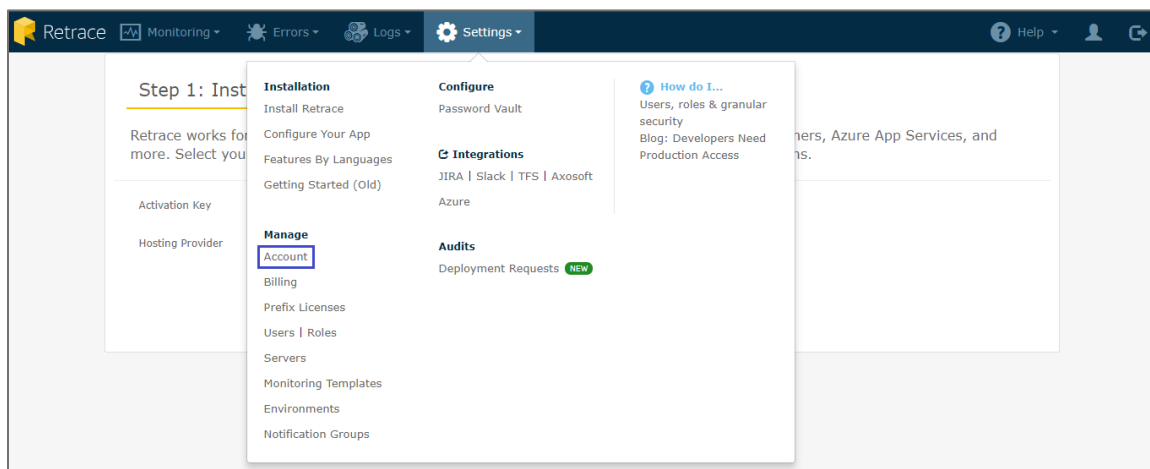
Browser Requirements: Internet Explorer 11 and above

To configure Retrace for SSO by using SAML:

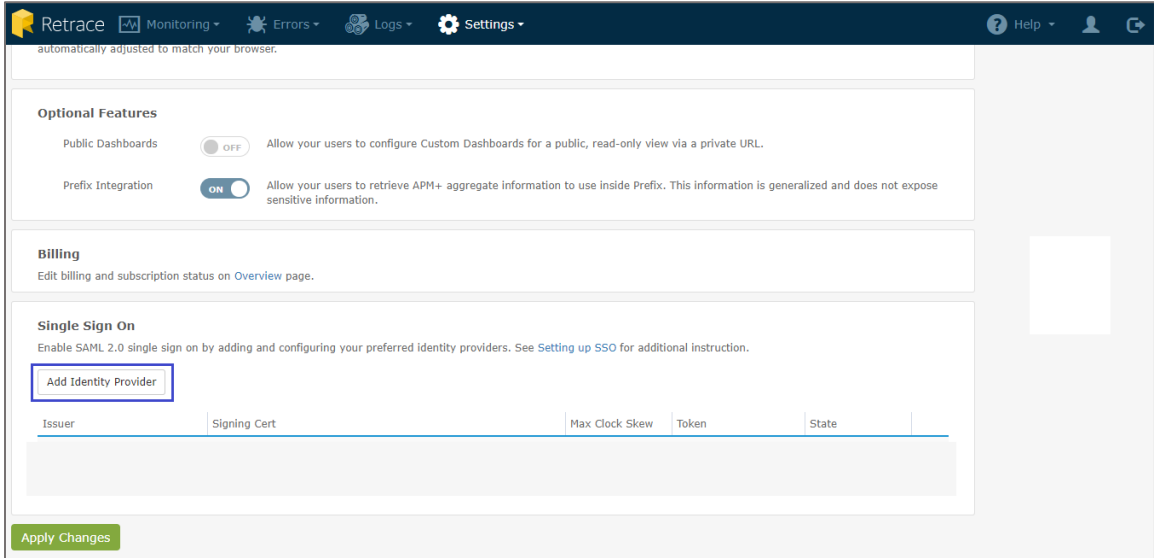
1. In a browser, type <https://stackify.com/retrace/> and press **Enter**.
2. Type your Retrace admin account credentials (**Username/Email Address** and **Password**) and click **Login**.



3. In the dashboard page, click **Settings** and select **Account** under **Manage**.



- In the **Manage Account** page, scroll down and click **Add Identity Provider** under **Single Sign On**.



- In the **SAML 2.0 Identity Provider Configuration** pop-up window, enter the values for the following fields:

Required Information	Description
Issuer	IdP Issuer URL
Enabled	Select the check box.
Upload Identity Provider Certificate	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate-----</p> <p>Note: The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app. <a href="https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml">https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml</p>

SAML 2.0 Identity Provider Configuration ✕

ACS Endpoint
https://s1.stackify.com/sso/saml2?clienttoken=:

Issuer
:

Max clock skew (seconds)
Enter max clock skew (seconds)

Enabled

Response / Assertion Signing Certificate

Subject	CN=DEV:IdP Assertion Signing Certificate.1, OU=Citrix Cloud, O="Citrix Systems, Inc", L=Fort Lauderdale, S=Florida, C=US
Thumbprint	:
Key Size	4096
Not Valid Before	4/24/2018
Not Valid After	9/9/2045

Upload Identity Provider Certificate

No file chosen

6. Finally, click **Save**.