

# Configure JitBit for Single Sign-On

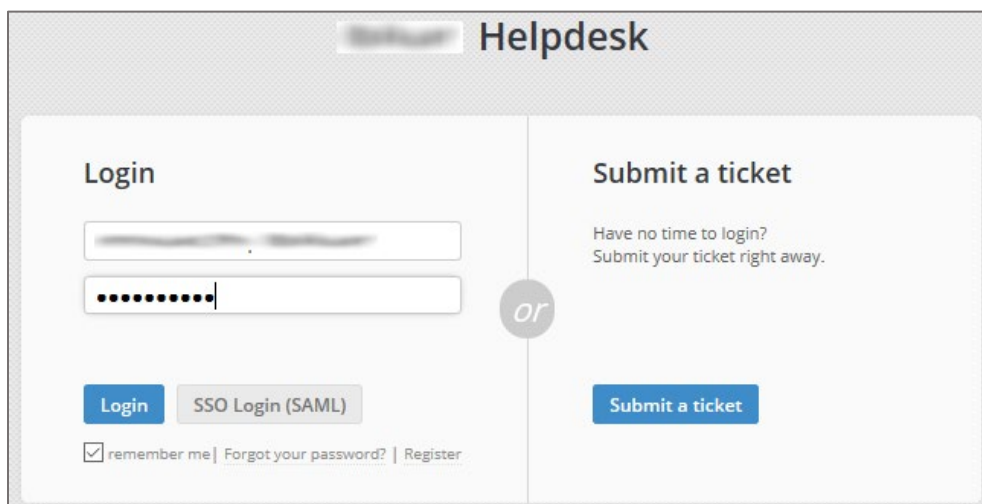
Configuring JitBit for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to JitBit by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

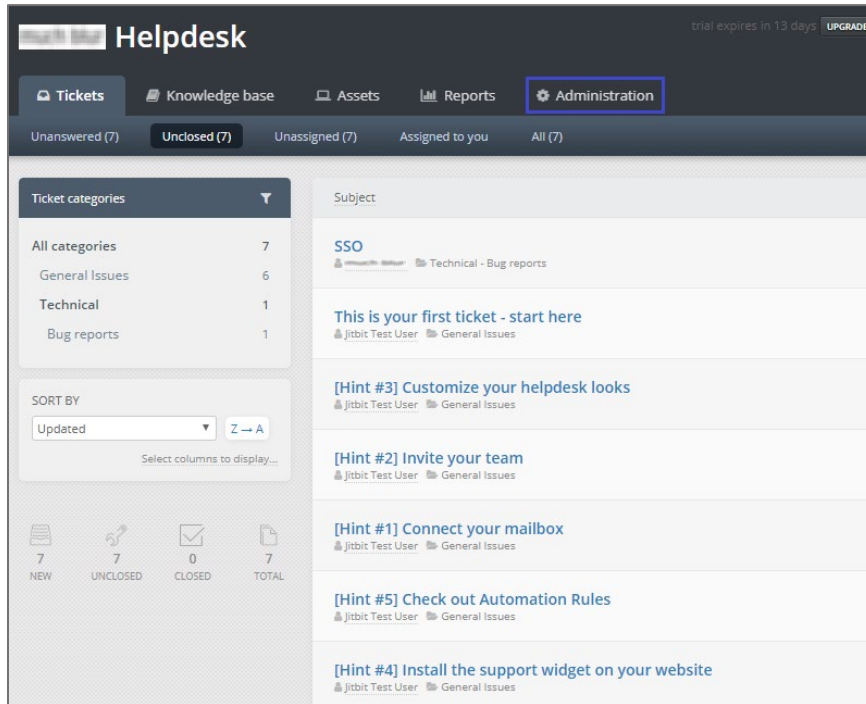
## To configure JitBit for SSO by using SAML:

1. In a browser, type <https://<customer domain>.jitbit.com> and press **Enter**.
2. Type your JitBit admin account credentials (**Username or Email** and **Password**) and click **Login**.

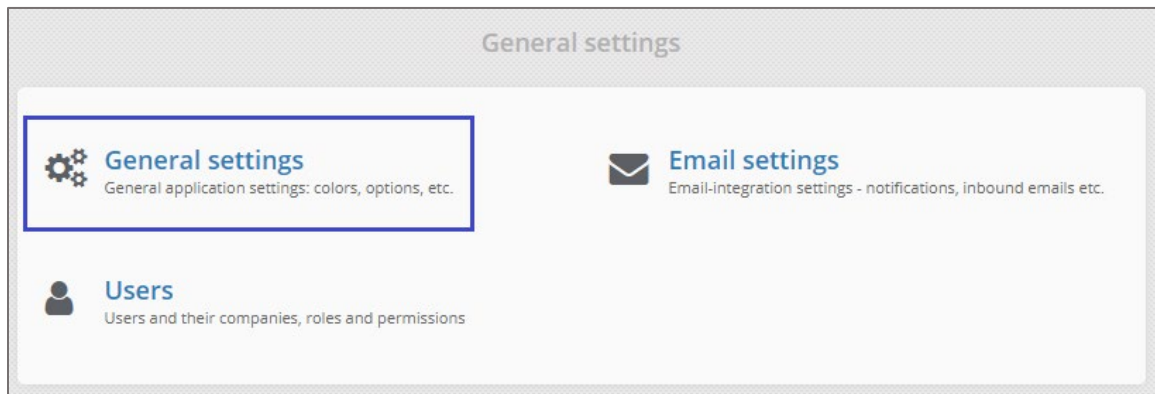


The screenshot shows the JitBit Helpdesk interface. At the top, there is a header with the JitBit logo and the word "Helpdesk". Below the header, the page is divided into two main sections: "Login" on the left and "Submit a ticket" on the right. In the "Login" section, there are two input fields: one for the username or email and one for the password. Below these fields are two buttons: "Login" and "SSO Login (SAML)". There is also a checkbox labeled "remember me" and links for "Forgot your password?" and "Register". In the "Submit a ticket" section, there is a blue button labeled "Submit a ticket". A vertical line with the word "or" in a circle separates the two sections. The text "Have no time to login? Submit your ticket right away." is located between the two sections.

3. In the dashboard page, click the **Administration** tab.



4. In the **Administration** page, click the **General settings**.



5. Scroll down and turn on the **Enable SAML 2.0 single sign on** setting in the **Authentication settings** tile.
6. Enter the values for the following fields:

Field Name	Description
EndPoint URL	IdP logon URL
x509 certificate	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with            -----Begin Certificate----- and -----End Certificate-----</p> <p><b>Note:</b> 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/&lt;citrixcloudcust_id&gt;/&lt;app_id&gt;/idp_metadata.xml">https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust_id&gt;/&lt;app_id&gt;/idp_metadata.xml</a></p>

**Authentication settings**

- Allow unregistered users submit tickets without logging in
- Allow new users to register themselves (uncheck if you want to create all new users MANUALLY)
- Allow users to edit their username and email
- Enable 'login with Google'

Shared secret for remote authentication:    
Used for automatic user sign-in. See the manual for more info about the remote authentication API.

Remote login URL:   
Optional. Redirect users to a custom login page of your site or app. Access "/User/Login?noredirect=1" in your browser to prevent redirecting for debugging purposes.

Enable SAML 2.0 single sign on

EndPoint URL:

x509 certificate:

Entity ID:   
"Entity ID" aka "Relying Party ID", you can leave the default value in most cases

Hide regular 'login' controls from the form when SAML enabled

Active Directory: If you want to remotely-authenticate users via your Active Directory - download the AD-authentication integration script here, you'll find the IIS-installation instructions inside.

7. Finally, click **Save changes**.