

# Configure Bananatag for Single Sign-On

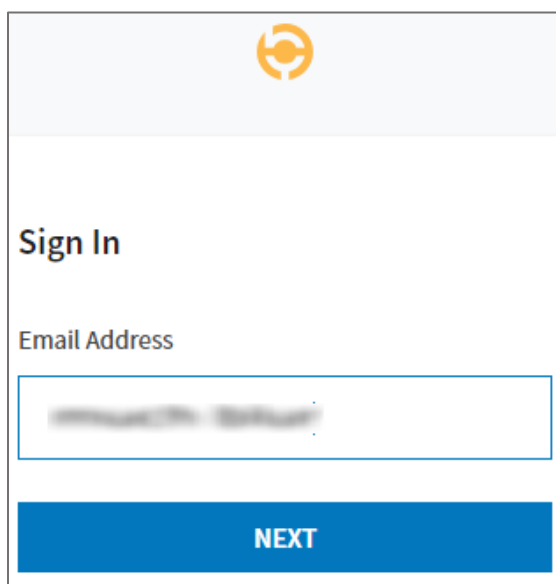
Configuring Bananatag for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Bananatag by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

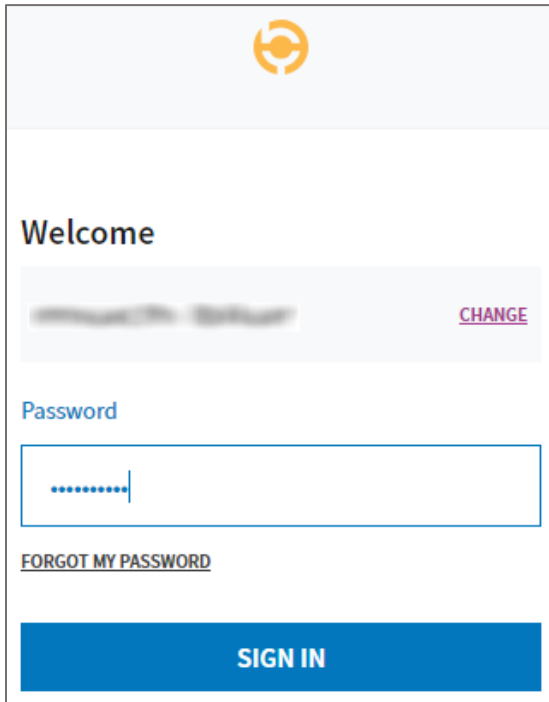
## To configure Bananatag for SSO by using SAML:

1. In a browser, type <https://login.bananatag.com/> and press **Enter**.
2. Type your Bananatag admin email address and click **NEXT**.



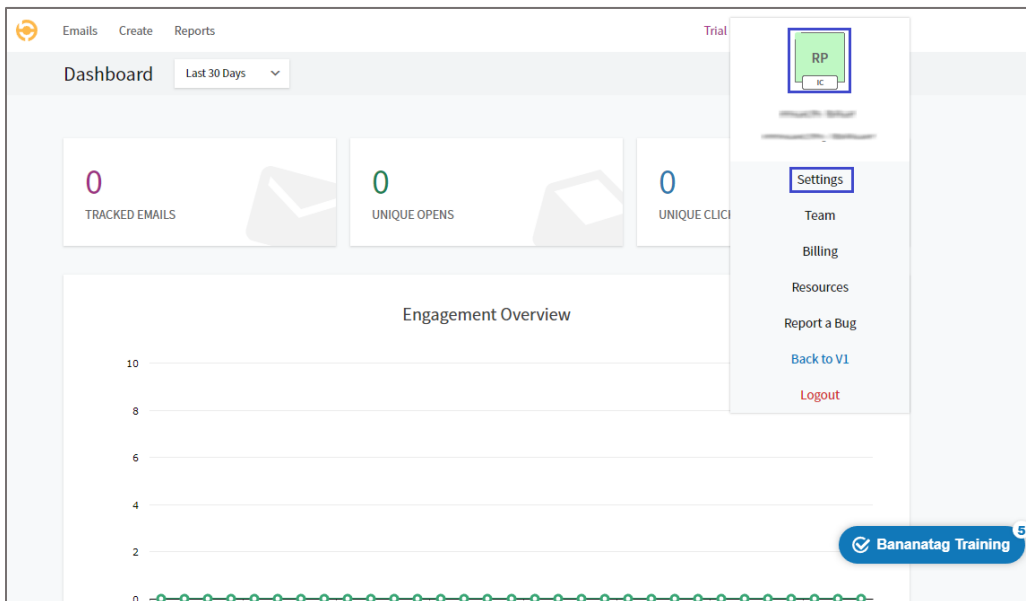
The screenshot shows the Bananatag login interface. At the top center is the Bananatag logo, a stylized orange 'C' with a circular arrow. Below the logo, the text 'Sign In' is displayed in a bold, black font. Underneath, the label 'Email Address' is positioned above a white text input field with a blue border. The input field contains a blurred email address. At the bottom of the form is a prominent blue button with the word 'NEXT' written in white, uppercase letters.

3. Type your Bananatag admin password and click **SIGN IN**.



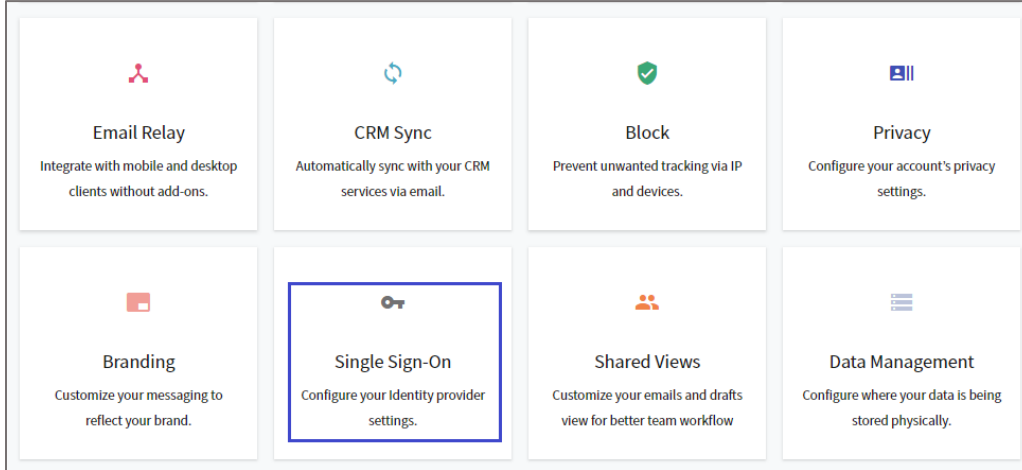
The image shows a login form for the Bananatag admin interface. At the top center is the Bananatag logo, a stylized orange 'B' with a circular arrow. Below the logo, the word "Welcome" is displayed in a large, bold, black font. Underneath "Welcome" is a blurred text field, likely for the username, with a purple "CHANGE" link to its right. Below this is a "Password" label in blue text, followed by a password input field containing several dots. Under the password field is a link that says "FORGOT MY PASSWORD". At the bottom of the form is a large blue button with the text "SIGN IN" in white, bold, uppercase letters.

4. In the dashboard page, click the username in the top-right corner and select **Settings**.



The image shows the Bananatag dashboard interface. At the top left, there are navigation links for "Emails", "Create", and "Reports". In the top right corner, the word "Trial" is visible. The main header area includes the word "Dashboard" and a dropdown menu set to "Last 30 Days". Below the header, there are three summary cards: "0 TRACKED EMAILS" with an envelope icon, "0 UNIQUE OPENS" with an envelope icon, and "0 UNIQUE CLICKS" with an envelope icon. Below these cards is a section titled "Engagement Overview" which contains a line graph with a y-axis ranging from 0 to 10 and a series of green data points. On the right side of the dashboard, there is a user profile menu. At the top of this menu is a small profile picture placeholder with the initials "RP" and "IC" below it. Below the profile picture, the menu items are: "Settings" (highlighted with a blue box), "Team", "Billing", "Resources", "Report a Bug", "Back to V1", and "Logout". At the bottom right of the dashboard, there is a blue button with a checkmark icon and the text "Bananatag Training" followed by a small "6" in a circle.

- In the **Settings** page, scroll down and click the **Single Sign-On** tile.



- In the **Single Sign-On** page, enter the values for the following fields:

Required Information	Description
IdP Metadata	<p>Upload the IdP certificate.</p> <p><b>Note:</b> The IdP metadata is provided by Citrix and can be accessed from the link below: <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.</p> <p><a href="https://gateway.cloud.idp/saml/&lt;citrixcloudcust_id&gt;/&lt;app_id&gt;/idp_metadata.xml">https://gateway.cloud.idp/saml/&lt;citrixcloudcust_id&gt;/&lt;app_id&gt;/idp_metadata.xml</a></p>

The image shows the 'Single Sign-On' configuration page. It includes a breadcrumb 'Settings > Single Sign-On' and a 'Configuration' section. The 'Email Domain' field is empty, and the 'SSO Integration Protocol' is set to 'SAML 2.0'. Below this, there is a note about email domain formatting. The 'IdP Metadata' field contains the file 'idp\_metadata-bananatag.xml' and a 'SELECT' button. At the bottom right, there is a 'SAVE AND UPDATE' button.

7. Finally, click **SAVE AND UPDATE**.
8. Note down the values in the **Relying Party SAML 2.0 SSO Service URL (Attribute Consume Service Endpoint)** and **Relying Party Trust Identifier (Entity Id)** fields for IdP configuration.

Settings > Single Sign-On

### IdP Setup

Email Domain	SSO Integration Type
<input type="text"/>	SAML 2.0

Relying Party SAML 2.0 SSO Service URL (Attribute Consume Service Endpoint)

Relying Party Trust Identifier (Entity Id)

Bananatag supports SSO integration with all major Identity providers (**ADFS, Azure, Ping Identity, OneLogin, Okta, Centrify, ...**).

To get more information on how to setup your IdP correctly, check out our technical SSO documents available in [Bananatag help center](#).