

# Configuring Buildkite

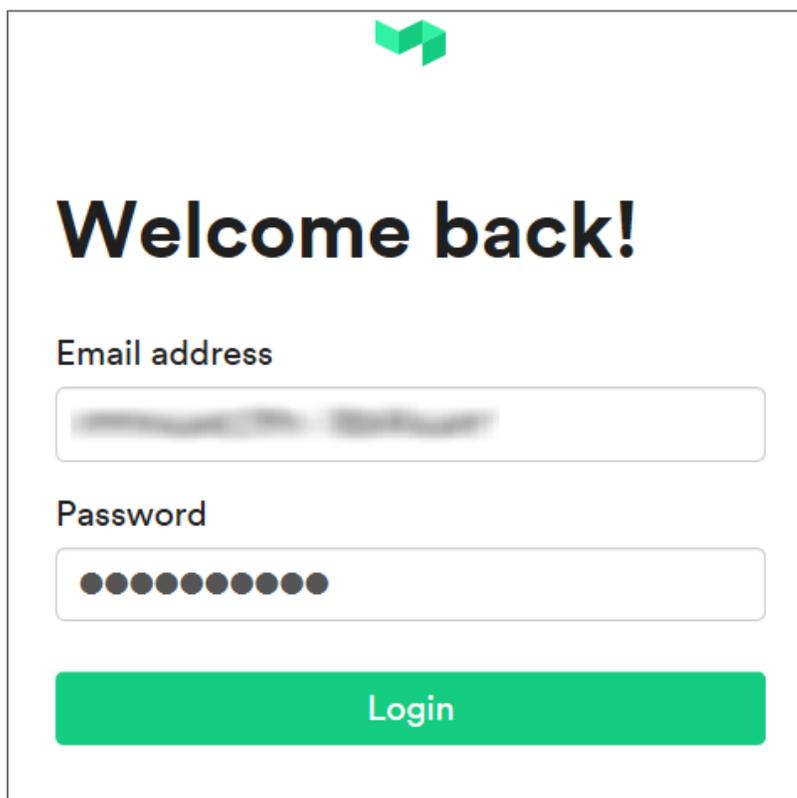
Configuring Buildkite for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Buildkite by using the enterprise credentials.

## Prerequisite

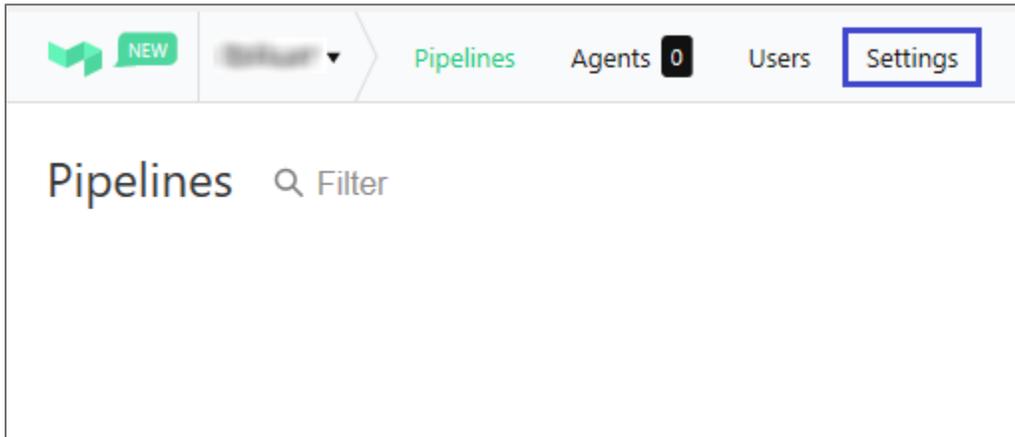
Browser Requirements: Internet Explorer 11 and above

## To configure Buildkite for SSO by using SAML:

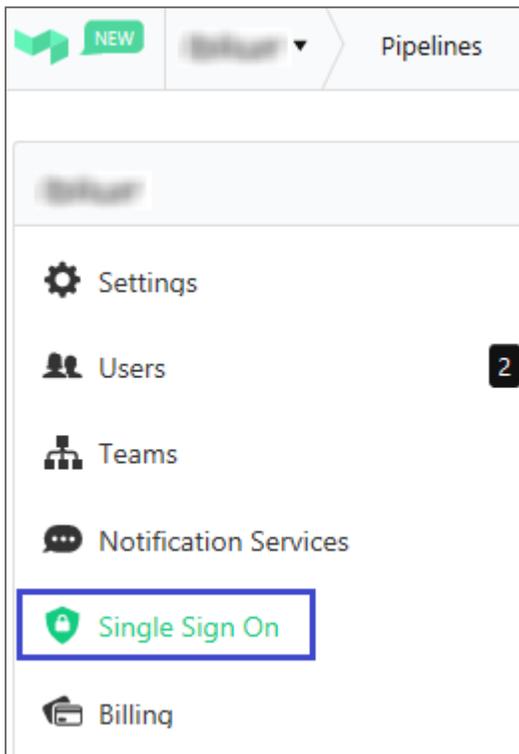
1. In a browser, type <https://buildkite.com/> and press **Enter**.
2. Type your Buildkite admin account credentials (**Email address** and **Password**) and click **Login**.

A screenshot of the Buildkite login page. At the top center is the Buildkite logo, a green chevron shape. Below the logo is the text "Welcome back!" in a large, bold, black font. Underneath this is the "Email address" label followed by a white input field with a light gray border. Below the email field is the "Password" label followed by a white input field with a light gray border and a series of ten black dots representing a password mask. At the bottom of the form is a large, solid green button with the word "Login" in white text.

3. In the login page, click **Settings**.



4. In the left panel, click **Single Sign On**.



- In the **Single Sign On** page, click **Contact Support**.



## Single Sign On

Manage your organization's Single Sign On settings

Single Sign On (SSO) allows you to use your own authentication server for signing into Buildkite.

During the sign in process, new users will be automatically added to your organization.

Supported SSO systems:

- Bitium ([Instructions](#))
- Okta ([Instructions](#))
- Google Apps (G Suite)
- SAML
- ADFS (SAML)

To enable SSO for this organization, contact support with your authentication server details.

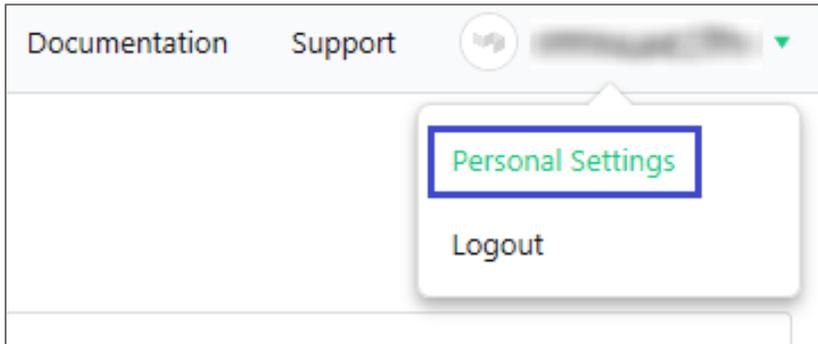
Contact Support

- To enable SSO, the user must contact Buildkite support team and provide them with the SSO URL and X.509 certificate.

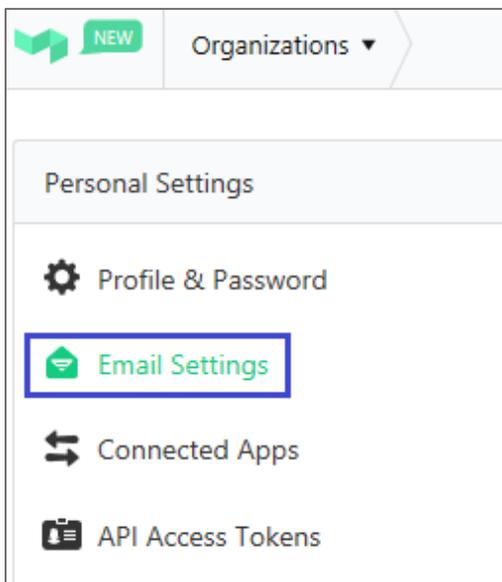
Field Name	Description
Single Sign-On URL	IdP logon URL
X.509 Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- <b>Note:</b> The IdP Certificate is provided by Citrix and can be accessed from the link below: <a href="https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml">https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml</a>

**Note:** The support team will configure the SP from the backend and the user will be provided with the ACS URL after authentication.

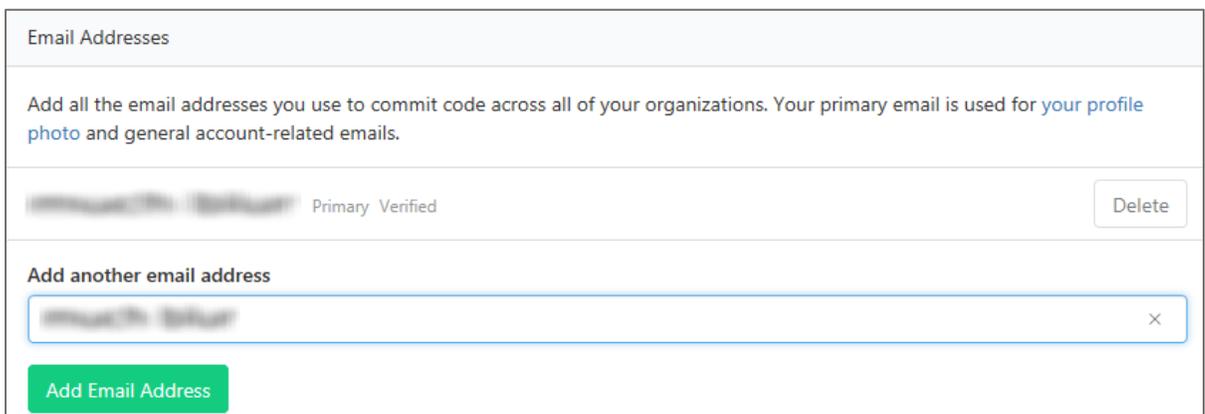
7. In the top-right corner, click **Personal Settings** from the user account drop-down menu.



8. In the left panel, click **Email Settings**.



9. To add and verify user, enter the user's email address and click **Add Email Address**.



**Note:** Verify by clicking the confirmation link sent to the user address.