

Configure Fastly for Single Sign-On

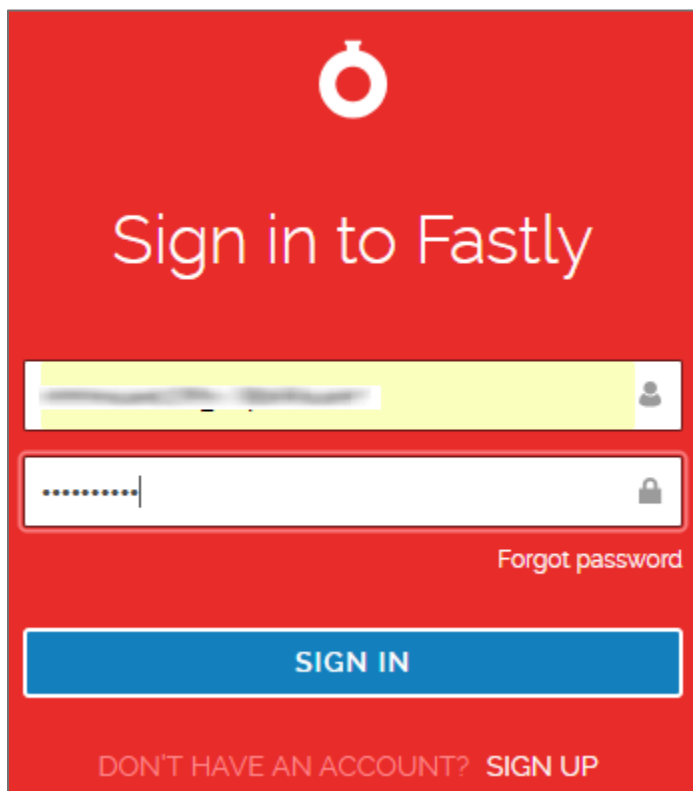
Configuring Fastly for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Fastly by using the enterprise credentials.

Prerequisite

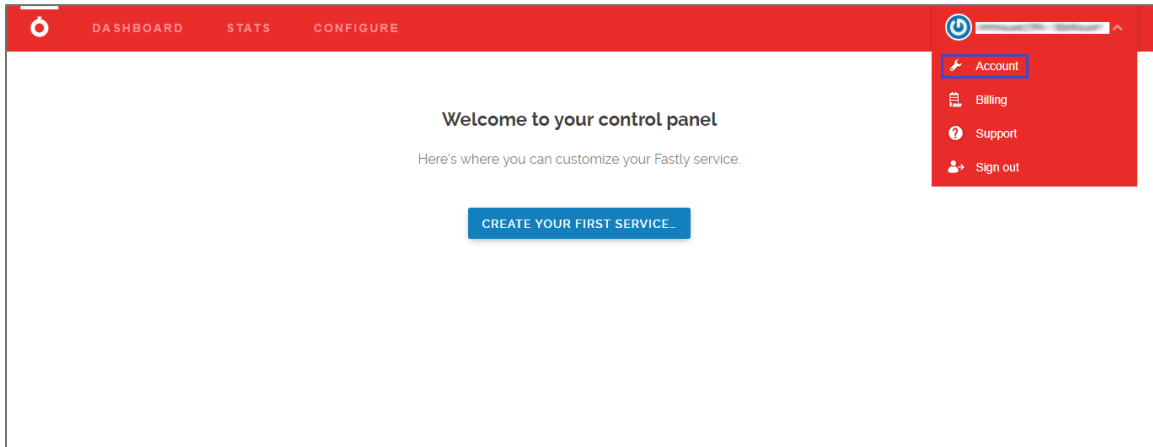
Browser Requirements: Internet Explorer 11 and above

To configure Fastly for SSO by using SAML:

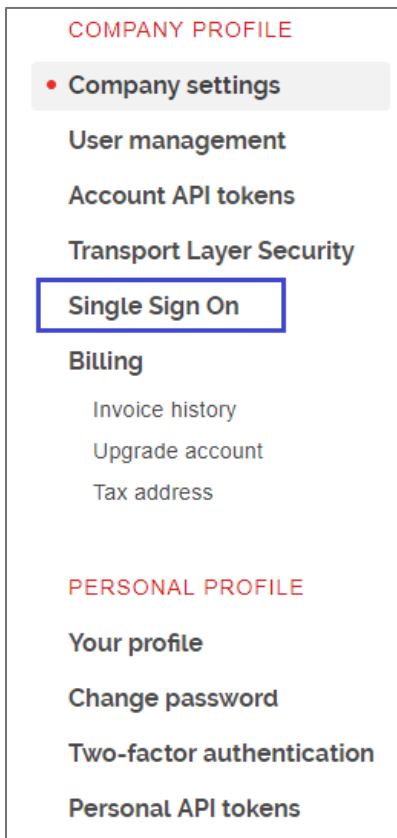
1. In a browser, type <https://www.fastly.com/> and press **Enter**.
2. Type your Fastly admin account credentials (**email** and **password**) and click **SIGN IN**.

The image shows the Fastly sign-in page. It has a red background. At the top center is the Fastly logo, a white circle with a smaller circle inside. Below the logo, the text "Sign in to Fastly" is written in white. There are two input fields: the first is for an email address, highlighted in yellow, and the second is for a password, with dots for characters and a lock icon on the right. Below the password field is a link that says "Forgot password". At the bottom, there is a blue button with the text "SIGN IN" in white. At the very bottom, there is a link that says "DON'T HAVE AN ACCOUNT? SIGN UP" in white.

3. In the dashboard page, click the username and select **Account**.



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



5. In the **Single Sign On** page, click **SSO Setup** and select **Generic SAML**.

Single Sign On

Setting up Single Sign On (SSO) for this account will let you and all your team log in to Fastly via an Identity Provider (IdP) that supports SAML 2.0.

If you have users in your Fastly account and want to import them to your SSO provider, you can [download a CSV of all current user email addresses](#).

▼ SSO Setup

1 Select your Identity Provider (IdP).

Generic SAML

Okta

OneLogin

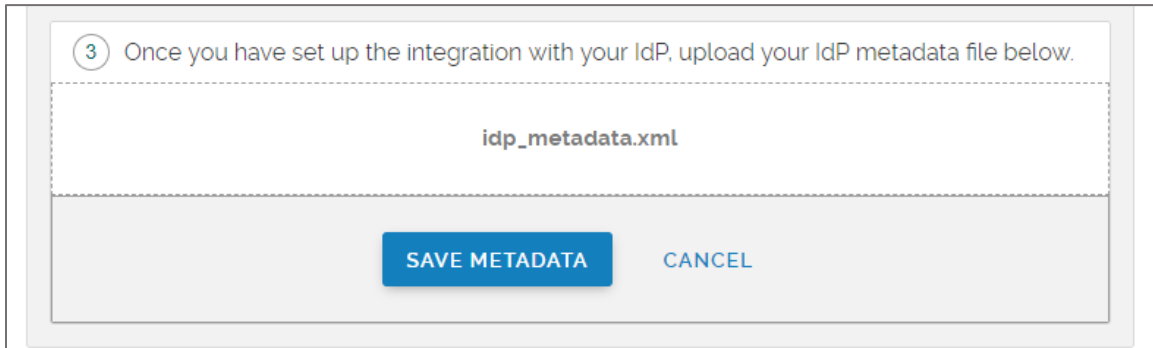
G Suite

6. Note down the values under **Use the following to configure your IdP to use SSO**. They would be needed for configuring your IdP.

2 Use the following to configure your IdP to use SSO.

```
Web SSO Profile - POST Bindings
Assertion Consumer Service URI:
https://manage.fastly.com/saml/consume
Audience URI (SP Entity ID):
https://api.fastly.com/saml/
Recipient:
https://manage.fastly.com/saml/consume
Name ID Format:
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Default RelayState:
Leave blank
```

7. Upload the IdP metadata file in XML format and click **SAVE METADATA**.

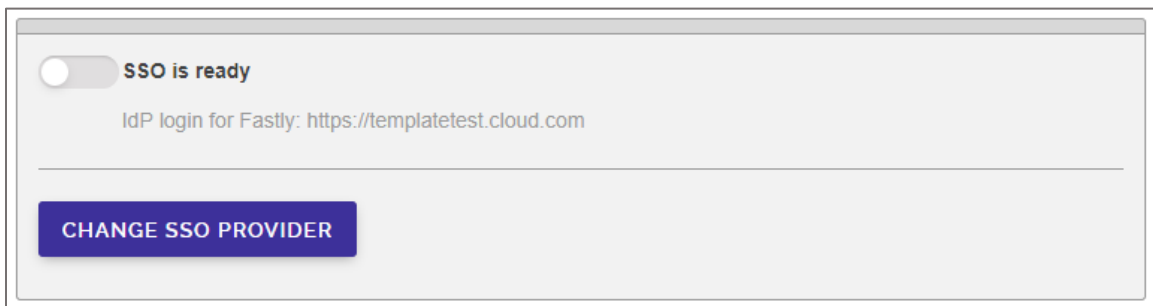


A screenshot of a configuration window. At the top, a step indicator '3' is followed by the text: 'Once you have set up the integration with your IdP, upload your IdP metadata file below.' Below this is a dashed-line box containing the filename 'idp_metadata.xml'. At the bottom of the window are two buttons: 'SAVE METADATA' (highlighted in blue) and 'CANCEL'.

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.

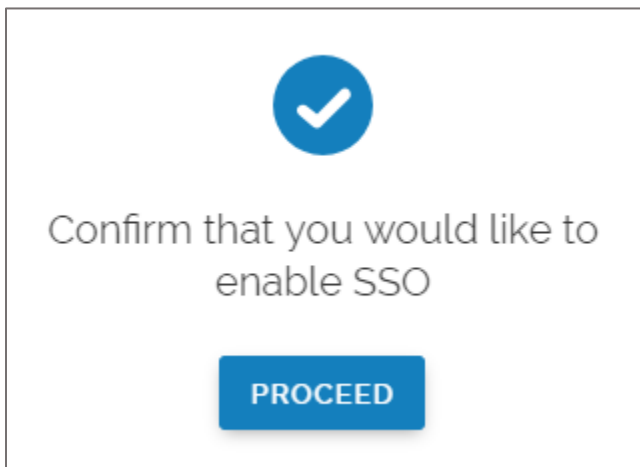
https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml

8. Enable the **SSO is ready** button.



A screenshot of a configuration panel. At the top, there is a toggle switch labeled 'SSO is ready' which is currently turned off. Below the toggle, the text reads 'IdP login for Fastly: https://templatetest.cloud.com'. At the bottom of the panel is a blue button labeled 'CHANGE SSO PROVIDER'.

9. In the pop-up window, click **PROCEED**.



A screenshot of a confirmation pop-up window. It features a blue circular icon with a white checkmark at the top. Below the icon, the text reads: 'Confirm that you would like to enable SSO'. At the bottom of the window is a blue button labeled 'PROCEED'.