

# Configure Split for Single Sign-On

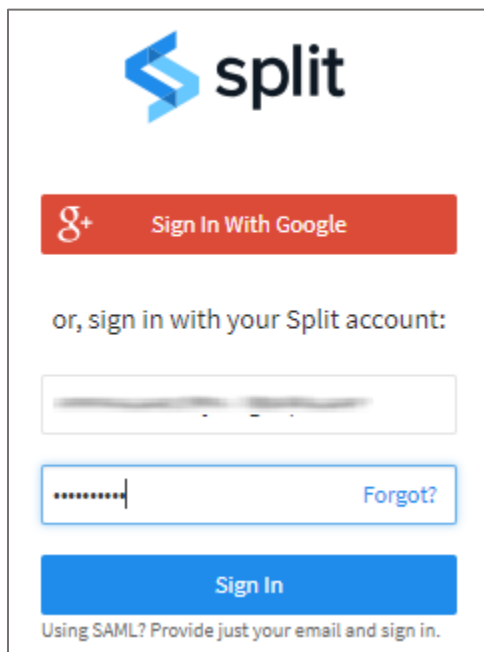
Configuring Split for single sign-on (SSO) enables administrators to manage users of Citrix Gateway service. Users can securely log on to Split by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

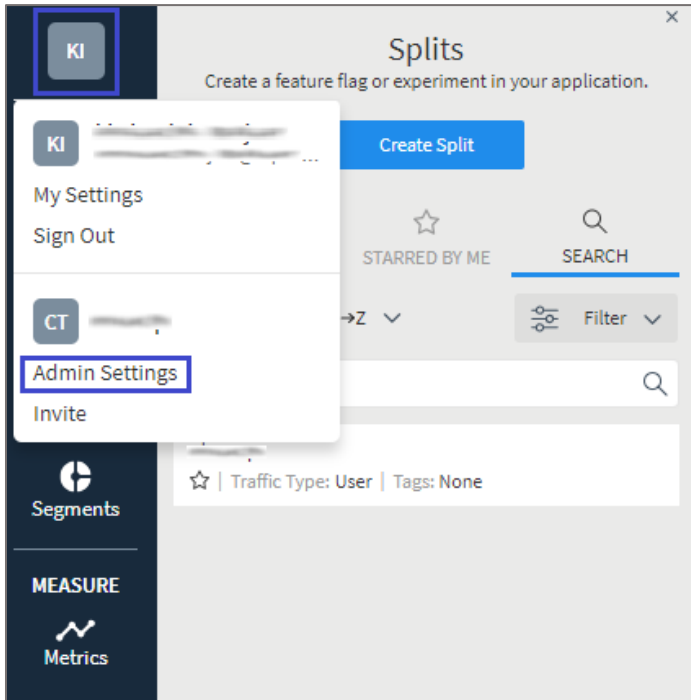
## To configure Split for SSO by using SAML:

1. In a browser, type <https://app.split.io/login> and press **Enter**.
2. Type your Split admin account credentials (**Email address** and **Password**) and click **Sign In**.

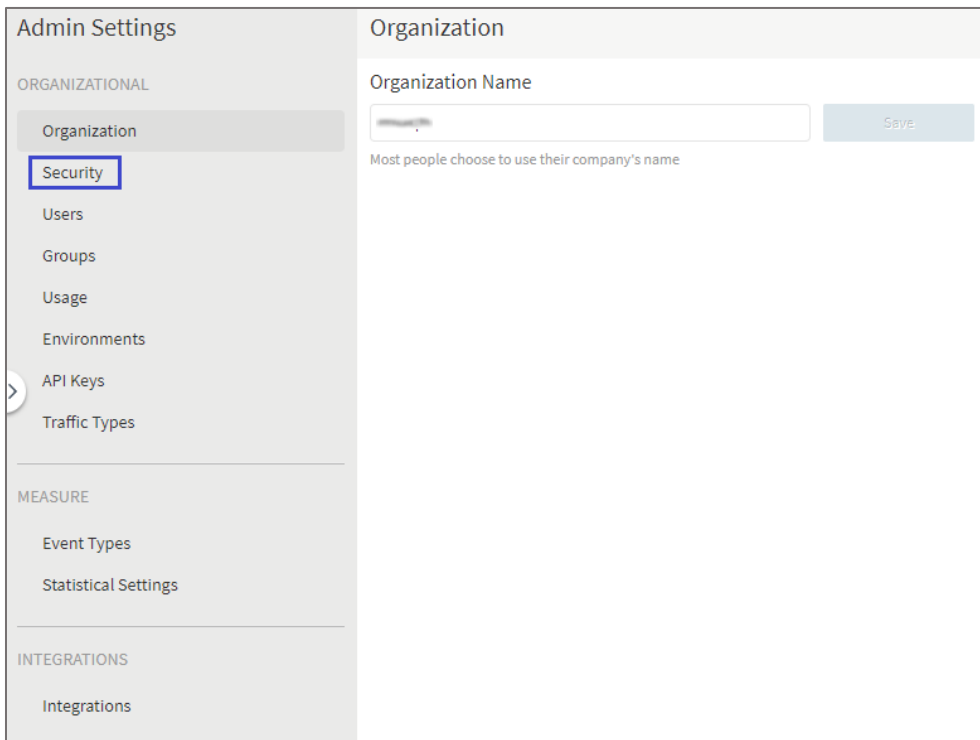


The screenshot shows the Split login interface. At the top is the Split logo. Below it is a red button with the Google logo and the text "Sign In With Google". Underneath, it says "or, sign in with your Split account:". There are two input fields: the first is for the email address, and the second is for the password, with a "Forgot?" link to its right. At the bottom is a blue "Sign In" button. A note at the very bottom reads "Using SAML? Provide just your email and sign in."

3. In the dashboard page, click the username in the top-left corner and select **Admin Settings**.



4. In the **Admin Settings** page, click **Security** under **ORGANIZATIONAL**.



- In the **Security** page, enter the values for the following fields:

Required Information	Description
Identity Provider (IdP) Metadata	The IdP metadata URL 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>

Security

SAML      Session Settings

**SAML is enabled**

**Single Sign-on URL:** <https://api.split.io/internal/api/v1/saml/login/> Copy

**IdP Entity id:** [REDACTED] Copy

**Service Provider Metadata:** [metadata.xml](#) download

**Assertion Consumer Service URL:** <https://api.split.io/internal/api/v1/saml/acs/> Copy

[Update below or disable](#)

Configuring SAML (Security Assertion Markup Language) for your Split account will let you and all your teammates log in to Split using the credentials stored in your organization's Active Directory, LDAP, or other identity store that has been configured with a SAML Identity Provider. [Learn more about configuring SAML in Split.](#)

**Identity Provider (IdP) Metadata**

[REDACTED]

**SAML Strict Mode**  
With SAML Strict Mode, all non-admin users must use SAML to log in to Split. Any existing Split username/passwords, or alternatives such as Google OAuth, will not be valid. Admins retain access to alternatives in case you need to fix issues with SAML.

**Just-in-Time Provisioning**  
With Just-in-Time provisioning, you can use a SAML assertion to create a Split user on the fly the first time they try to log in, eliminating the need to create users in advance.

[Save](#)

- Clear the **SAML Strict Mode** check box.
- Clear the **Just-in-Time Provisioning** check box.
- Finally, click **Save**.

**Note:** Note down the **Single Sign-on URL**, **IdP Entity id**, **Service Provider Metadata**, and **Assertion Consumer Service URL** for IdP configuration.