Configure Postman for Single Sign-On

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

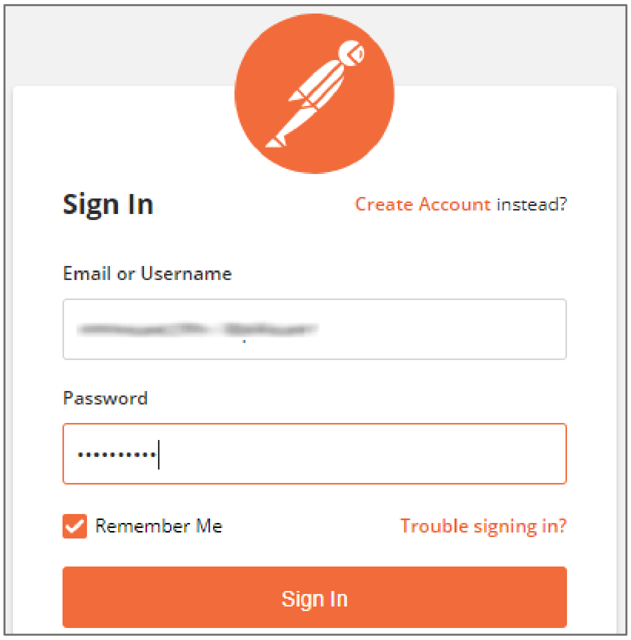
Prerequisite

Browser Requirements: Internet Explorer 11 and above

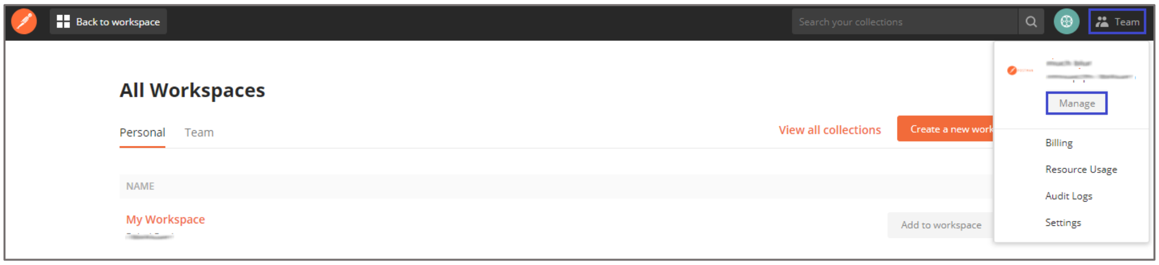
To configure Postman for SSO by using SAML:

1. In a browser, type https://identity.getpostman.com/login and press **Enter**.

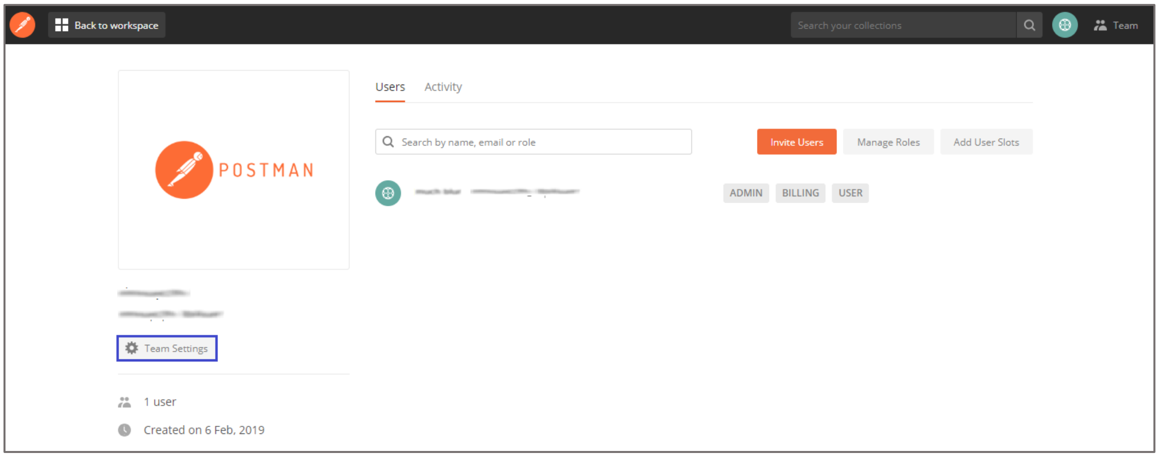
2. Type your Postman admin account credentials (**Email or Username** and **Password**) and click **Sign In**.



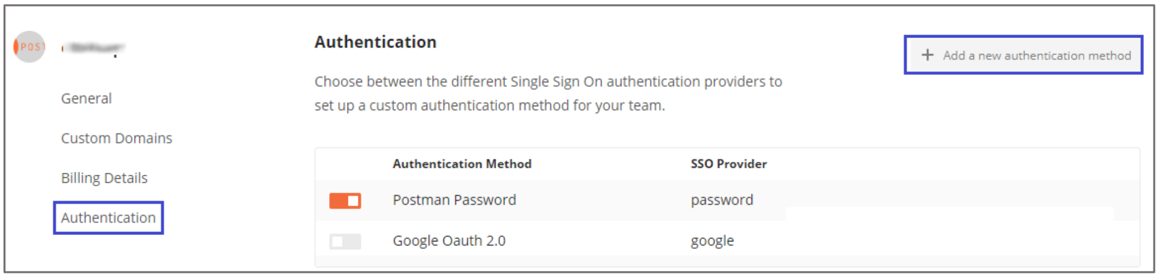
3. In the dashboard page, click **Team** > **Manage**.



4. Click **Team Settings** in the left pane.



5. Click **Authentication** > **Add a new authentication method**.



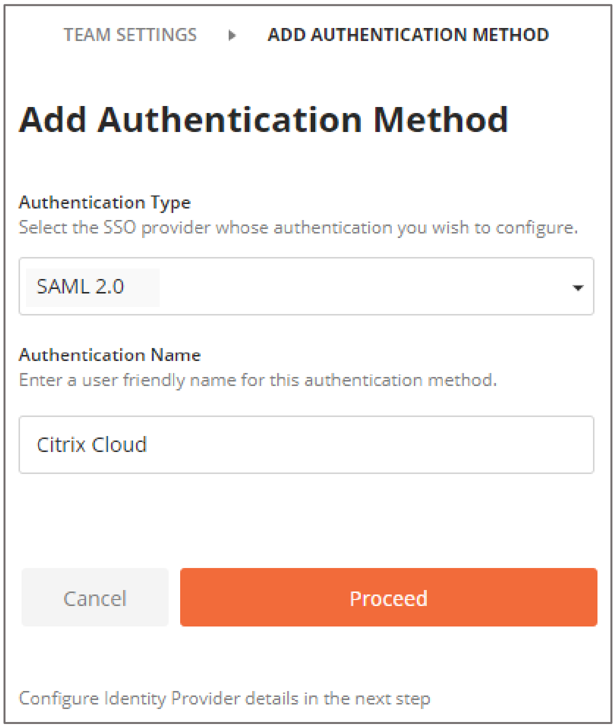
Authentication

Choose between the different Single Sign On authentication providers to set up a custom authentication method for your team.

	Authentication Method	SSO Provider
●	Postman Password	password
○	Google Oauth 2.0	google

6. Enter the values for the following fields:

Required Information	Description
Authentication Type	Select **SAML 2.0** from the drop-down list.
Authentication Name	Citrix Cloud



TEAM SETTINGS ▸ ADD AUTHENTICATION METHOD

Add Authentication Method

Authentication Type
Select the SSO provider whose authentication you wish to configure.

SAML 2.0

Authentication Name
Enter a user friendly name for this authentication method.

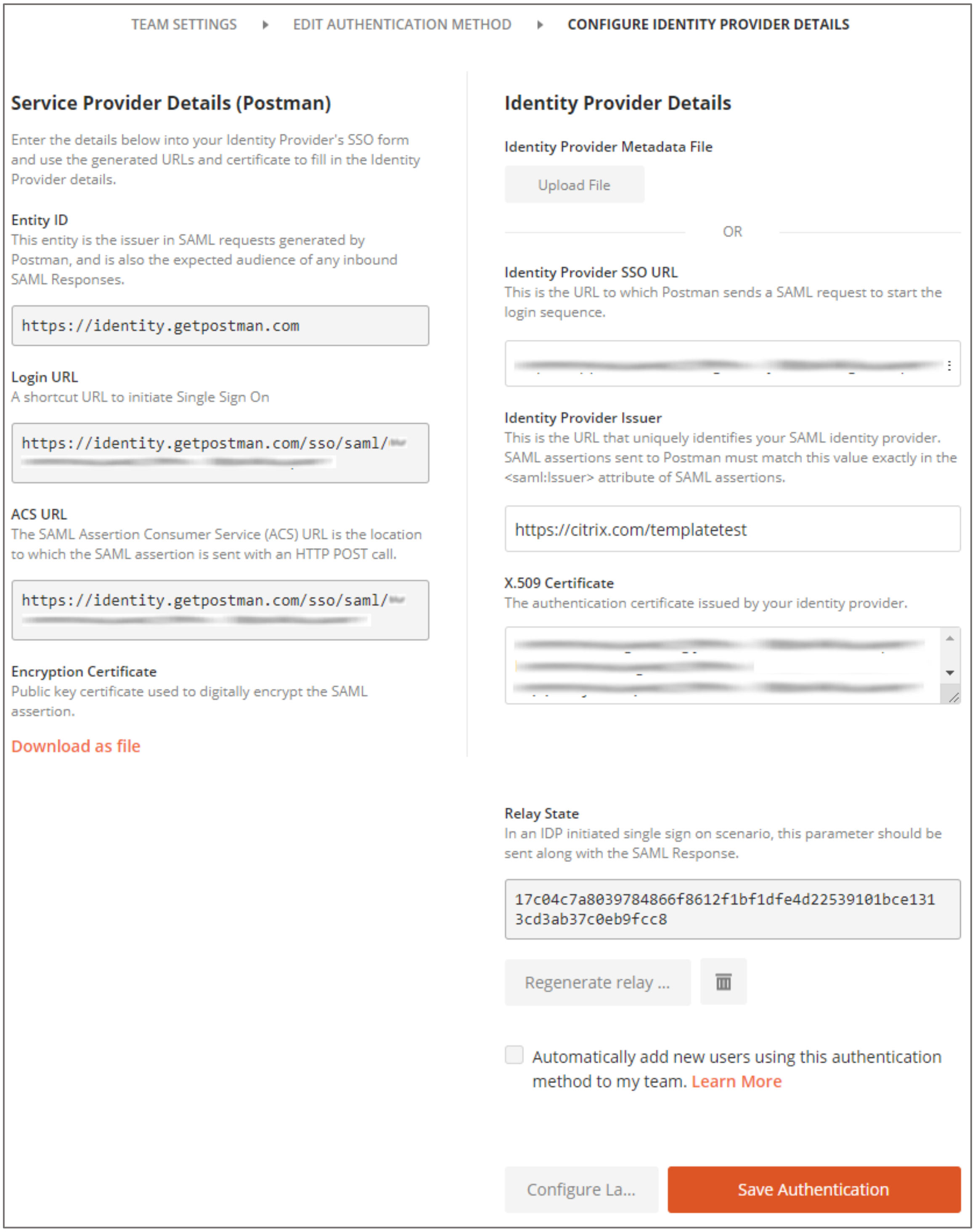
Citrix Cloud

Configure Identity Provider details in the next step

7. Click **Proceed**.

8. Enter the values for the following fields under **Identity Provider Details**:

Required Information	Description
Identity Provider SSO URL	IdP logon URL
Identity Provider Issuer	Issuer URL
X.509 Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with - - - - -Begin Certificate- - - - - and - - - - -End Certificate- - - - - **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



TEAM SETTINGS ▸ EDIT AUTHENTICATION METHOD ▸ CONFIGURE IDENTITY PROVIDER DETAILS

Service Provider Details (Postman)

Enter the details below into your Identity Provider's SSO form and use the generated URLs and certificate to fill in the Identity Provider details.

Entity ID

This entity is the issuer in SAML requests generated by Postman, and is also the expected audience of any inbound SAML Responses.

`https://identity.getpostman.com`

Login URL

A shortcut URL to initiate Single Sign On

`https://identity.getpostman.com/sso/saml/`[redacted]

ACS URL

The SAML Assertion Consumer Service (ACS) URL is the location to which the SAML assertion is sent with an HTTP POST call.

`https://identity.getpostman.com/sso/saml/`[redacted]

Encryption Certificate

Public key certificate used to digitally encrypt the SAML assertion.

Download as file

Identity Provider Details

Identity Provider Metadata File

OR

Identity Provider SSO URL

This is the URL to which Postman sends a SAML request to start the login sequence.

[redacted]

Identity Provider Issuer

This is the URL that uniquely identifies your SAML identity provider. SAML assertions sent to Postman must match this value exactly in the <saml:Issuer> attribute of SAML assertions.

https://citrix.com/templatetest

X.509 Certificate

The authentication certificate issued by your identity provider.

[redacted]

Relay State

In an IDP initiated single sign on scenario, this parameter should be sent along with the SAML Response.

`17c04c7a8039784866f8612f1bf1dfe4d22539101bce1313cd3ab37c0eb9fcc8`

□ Automatically add new users using this authentication method to my team. Learn More

9. Finally, click **Save Authenticaton**.