PingOne

Important: These instructions apply **only** to Flow on-premises.

Overview

Below is a step-by-step guide for connecting your PingOne account to Flow with SSO.

Configuring Your PingOne Integration

Step 1: Sign into your PingOne Admin Account.

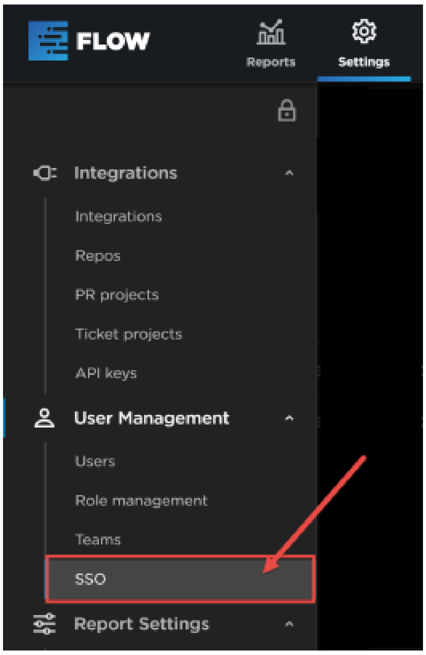
Step 2: In your Dashboard go to *Applications.*

Step 3: On the Applications page go to *Add Application* then select *New SAML Application.*

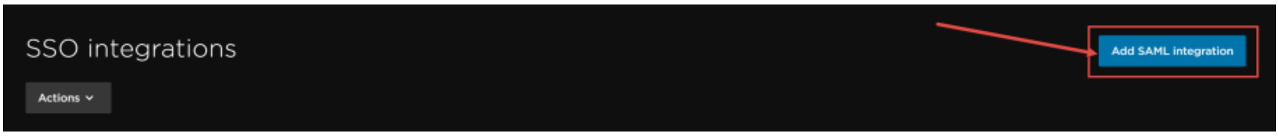
Step 4: On this page you fill out the following fields then click *Continue to Next Step.*

- Application Name: **Pluralsight Flow**
- Application Description: ***Flow***
- Category: **Engineering**

Step 5: After clicking *Continue to Next Step* leave this **Tab Open** and open Flow in a new tab. Navigate to *Settings* > *SSO.*



Step 6: Select *New SAML Integration*.

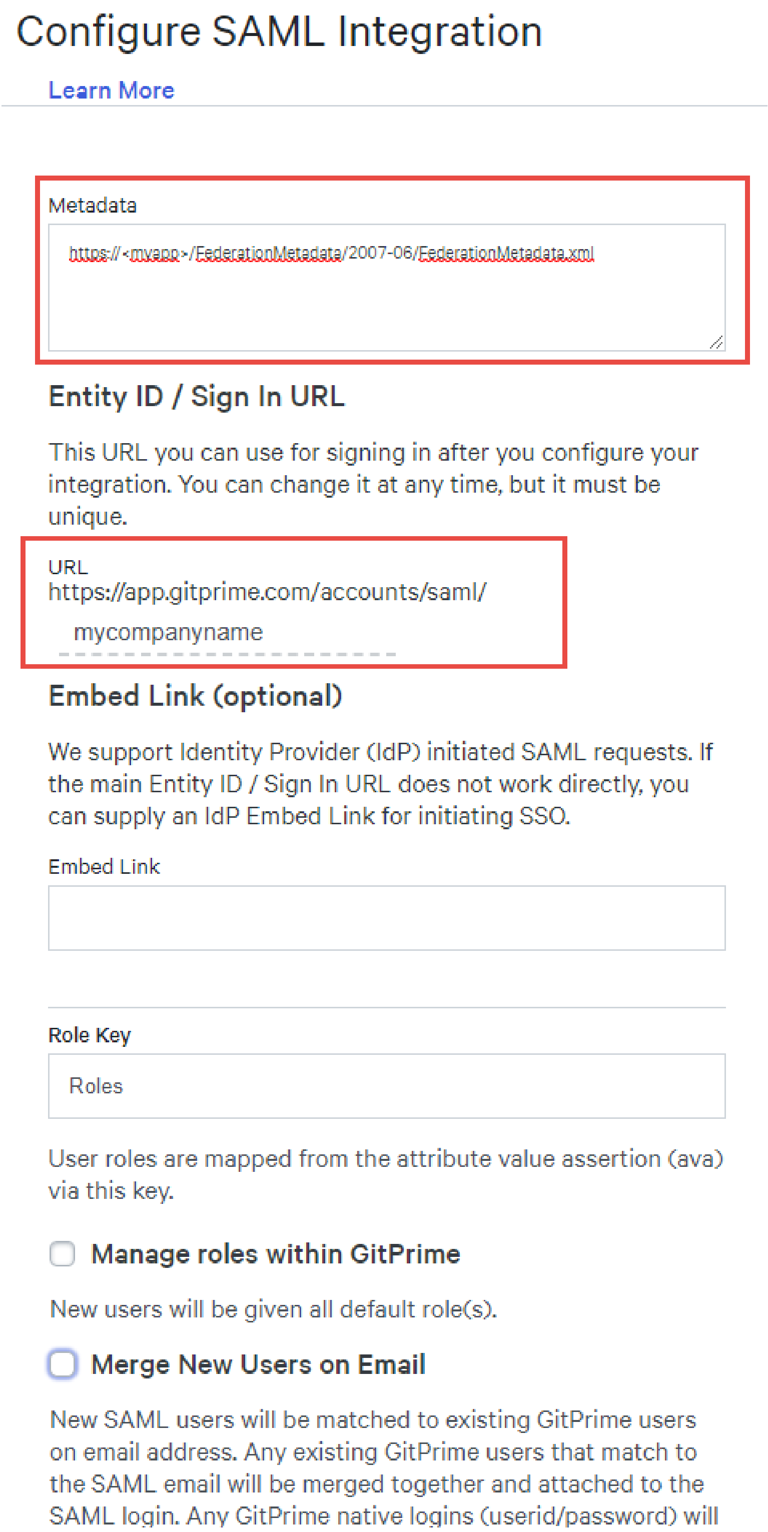


Step 7: In the *Configure SAML integration* modal, fill out these four field:

1. Metadata ADFS has a metadata URL (generally formatted as: https:///FederationMetadata/2007-06/FederationMetadata.xml). Copy/paste the URL or the raw XML into this field. **We will get the metadata in the following step.**

2. Login URL this is the entity ID which also doubles as your login URL, you can use your company name or division or team of the company in the field, whatever is most relevant. Make note of this URL as it will be re-used in PingOne.

3. Attributes we can map the various details of a user from PingOne into these field templates. They can be anything you'd like, but the capitalization/format must match perfectly.



Configure SAML Integration

Learn More

Metadata

https://<myapp>/FederationMetadata/2007-06/FederationMetadata.xml

Entity ID / Sign In URL

This URL you can use for signing in after you configure your integration. You can change it at any time, but it must be unique.

URL
https://app.gitprime.com/accounts/saml/
mycompanyname

Embed Link (optional)

We support Identity Provider (IdP) initiated SAML requests. If the main Entity ID / Sign In URL does not work directly, you can supply an IdP Embed Link for initiating SSO.

Embed Link

Role Key

Roles

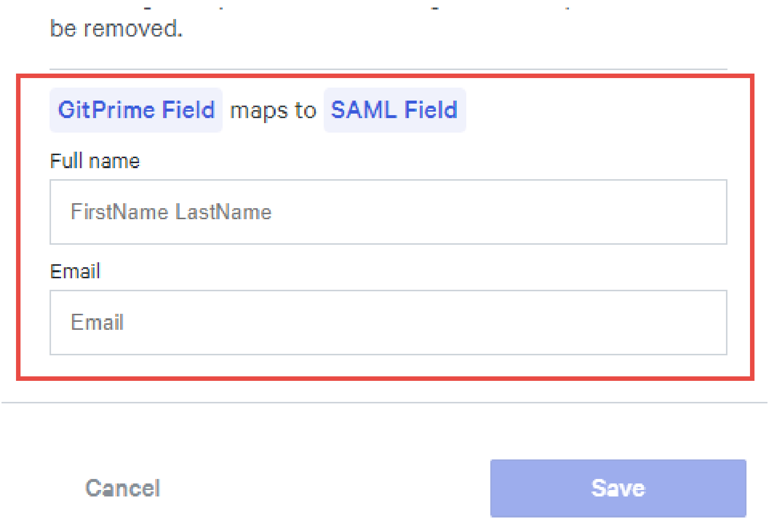
User roles are mapped from the attribute value assertion (ava) via this key.

□ Manage roles within GitPrime

New users will be given all default role(s).

□ Merge New Users on Email

New SAML users will be matched to existing GitPrime users on email address. Any existing GitPrime users that match to the SAML email will be merged together and attached to the SAML login. Any GitPrime native logins (userid/password) will



be removed.

GitPrime Field maps to SAML Field

Full name

FirstName LastName

Email

Email

Step 8: Navigate back to your PingOne tab, you should still be on Configure SAML Connection page. You will be using the **Login URL** you just created in Flow in three different fields:

1. Assertion Consumer Service (ACS URLs)

2. Entity ID

3. Target Application URL

Depending on the version you are using of PingOne there may be some additional settings:

- If the option to select **SAML v 2.0** is available make this is enabled.
- You may be required to input the Assertion Validity Duration (in seconds)

Everything else on this page can remain as is. Go to bottom of page and hit *Save and continue.*

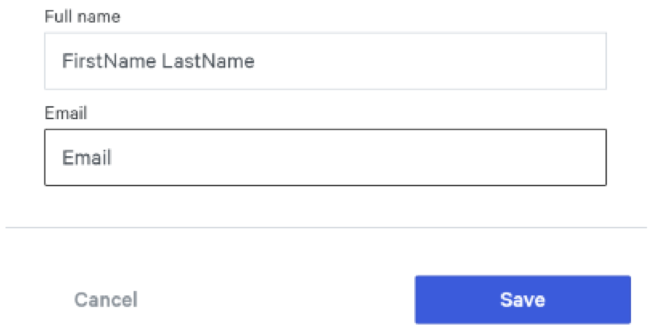
Step 9: On this page you will need to add Attributes. FirstName, LastName, Email and Roles (if you are planning on handling Roles in PingOne).

Step 10: Roles: Hit Advanced and select *GetLocalPartFromEmail* then Save (this may not be available in every version of PingOne)

Step 11: Make sure you select the "Required" checkboxes for all the attributes except for Roles. Click *Save and Continue*.

Step 12: On the next page you will find the SAML Metadata. Download and Copy.

Step 13: Return to your Flow SSO tab you have open and paste that Metadata in the top box.



Full name

FirstName LastName

Email

Email

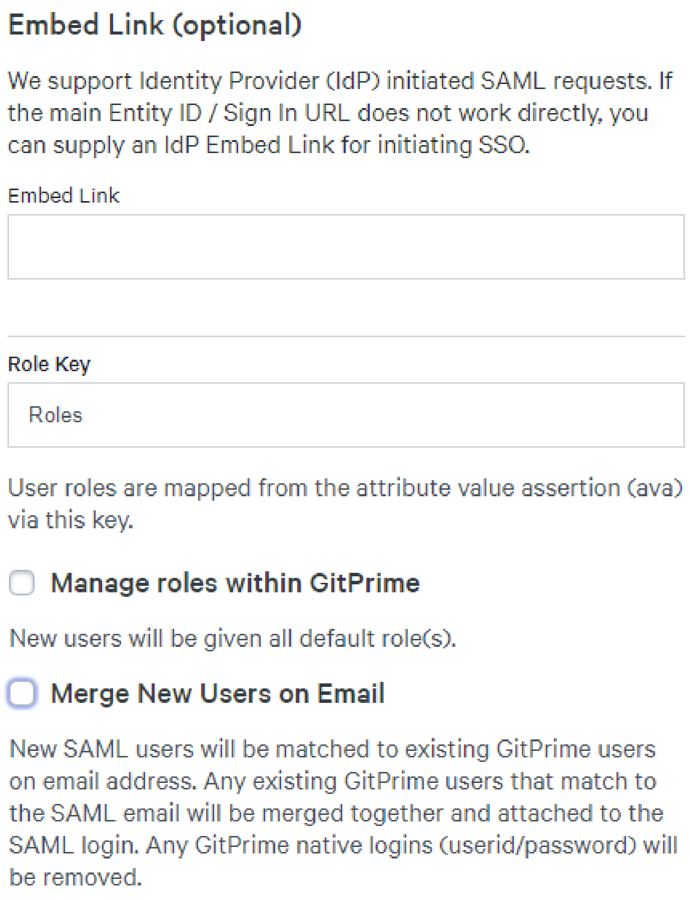
Optional Settings

1. Embed Link: This setting should only be used if the main Entity ID does not work directly.

2. Role Key: User roles will be mapped from the attribute value assertion via this key.

3. Manage Roles within Flow: Check this box if you want Flow to manage your user's role. New users will be give a default role upon logging in.

4. Merge New Users on Email: Check this box if you already have Users invited into your Flow account using non-SSO logins. This will automatically delete the previous logins and force all existing Users to login via your SSO platform.



Embed Link (optional)

We support Identity Provider (IdP) initiated SAML requests. If the main Entity ID / Sign In URL does not work directly, you can supply an IdP Embed Link for initiating SSO.

Embed Link

Role Key

Roles

User roles are mapped from the attribute value assertion (ava) via this key.

□ Manage roles within GitPrime

New users will be given all default role(s).

□ Merge New Users on Email

New SAML users will be matched to existing GitPrime users on email address. Any existing GitPrime users that match to the SAML email will be merged together and attached to the SAML login. Any GitPrime native logins (userid/password) will be removed.

Step 14: Users should now be able to successfully login. If users see nothing upon initial login, then it is likely none of the users roles mapped properly to a role in Flow.

back to top

If you need help, please email support@pluralsight.com () for 24/7 assistance.