Below is a step-by-step guide for setting up Okta as the SSO provider for Flow Enterprise Server.

**Important:** These instructions apply only to Flow Enterprise Server.

1. In Okta, begin the process to create an app integration (external site, opens in new tab).
   - 1. Select SAML 2.0 as your sign-in method.
   - 2. Fill out the App name field.
   - 3. When you get prompted to enter the Single sign on URL, stop and move to the next step.

2. In another tab, open Flow.

3. From the top navigation, click **Settings**.

4. In the left navigation, click **SSO** under **User Management**.

5. Click **Add SAML integration**.

6. In the Configure SAML modal, fill in the **Entity ID/Sign in URL** field with the URL you will use to log in with after you configure your integration. You can use your organization name or something else, but it must be unique.

7. Copy the **Entity ID/Sign in URL** from Flow and go back to Okta.

8. Enter the following fields for SAML settings in Okta:
   - 1. Single Sign on URL: This is the URL you copied from Flow. Check the box next to **Use this for Recipient URL and Destination URL**.
   - 2. Audience URI (SP Identity ID): This is the URL you copied from Flow.
   - 3. Application username: Select **Email**.

9. In the Attribute Statements section, add three attributes:

   **Important:** These fields are case-sensitive.

   - FirstName
10. In the **Value** column, use the dropdown menu to map the values to the fields you just created. They should be:
   - user.firstName
   - user.lastName
   - user.email

11. In the Group Attribute Statements section, map your current roles in Okta to their respective roles in Flow.

   **Important**: These fields are case-sensitive. Make sure your roles are spelled exactly the same in Flow and Okta.

12. Finish creating your app integration.

13. Once your app integration is completed in Okta, copy the IdP metadata from Okta. Return to Flow.

14. In Flow, paste the metadata in the **Metadata** field.

15. Type all the fields that map to your SAML fields. These fields are case-sensitive and must match exactly what you used in Okta.

16. Enable optional settings if desired:
   - Manage Roles within Flow: If you want Flow to manage your roles, check this box.
   - Merge new users on Email: If you already have users in Flow with non-SSO logins, check this box. This option automatically deletes previous logins and forces all existing users to log in via your SSO platform.

17. Click **Save**. Your Okta integration is now complete in Flow.

18. Next, assign users to the Flow app integration. Learn more about [assigning app integrations](https://example.com) (external site, opens in new tab).

Once these steps are completed, users can use the sign in URL set up above to log in to Flow.

**Troubleshooting**

If users are unable to log in to Flow using your Sign in URL, review the following configuration steps:

- Make sure the Sign in URL matches the URL in Flow.
- Review your Attribute and Group Attribute statements to make sure they are identical to their respective Flow role and Okta group. These fields are case-sensitive.

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