Below is a step-by-step guide for setting up an SSO connection to Flow Enterprise Server using ADFS.

1. From the top navigation of Flow, click **Settings**.

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

3. Click **Add SAML integration**.

4. In the Configure SAML modal, fill out the Metadata field. ADFS has a metadata URL, generally formatted as: https://<base_url>/FederationMetadata/2007-06/FederationMetadata.xml. Copy/paste the URL or the raw XML into this field.

5. 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.

6. 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.
   - **We only support IdP-Initiated SAML requests but can accommodate SP-Initiated flows by filling out the Embed link field.**
   - **Check Merge New Users on Email** if you already have users in Flow using non-SSO logins. This automatically deletes previous logins and forces existing users to sign in via SSO.
   - In the **Full name** field, input **FirstName LastName**. These inputs are case sensitive and must match this exactly.
   - In the **Email** field, input **E-Mail**.

7. Copy the Entity ID/Sign in URL from Flow and open ADFS. Follow the steps to manually create a relying party trust in ADFS (external site, opens in new tab).
   1. Set the display name to Flow.
   2. Only click the check box for **Enable support for the SAML 2.0 WebSSO protocol**. Do not check **Enable support for the WS-Federation Passive protocol**.
3. Add the Entity ID/Sign in URL as the Relying party SAML 2.0 SSO service URL.

4. Add the Entity ID/Sign in URL as the Relying party trust identifier on the Configure identifiers page.

5. When finished, close the wizard.

8. The Edit Claim rules wizard should automatically open.

9. Next, create a rule to send LDAP attributes as claims (external site, opens in new tab). Create the following mappings of LDAP attributes to Outgoing claim types:
   - Given-Name to FirstName
   - Surname to LastName
   - E-Mail Addresses to E-Mail
   - Token-groups - Unqualified Names to Roles
   - E-Mail Addresses to Name ID
     - Name ID is a required attribute to validate the SAML assertions from ADFS.

If you need help, please contact Pluralsight Support.