SPIGIT

SSO User Attributes

Implementing a single sign-on solution for your Spigit platform allows your audience to participate in your platform with as little effort as possible. Spigit supports two popular protocols to enable single sign-on: SAML and LDAP. By passing user attributes via this authentication method, site access can be controlled and reports can be at a more granular level. The first step is to discover what attributes are available from your IT team. Using that information, a decision can be made about what should be passed to Spigit.

PRIMARY ACTIVITIES

- Customer determines final list of attributes with corresponding field names
- Customer informs the Account Director of the project, working together on the payment method
- Once payment is determined, the customer submits a support ticket to schedule a meeting with the SSO Integration Engineer.
- Spigit adds fields to Spigit database and code in Staging
- Customer verifies attributes are populated in Staging
- Spigit adds fields and code in Production
- Customer verifies attributes are populated in Production

REQUIREMENTS AND ASSUMPTIONS

- Customer's technical team or consultants will configure their attributes to be passed.
- Spigit will configure Spigit database to accept the agreed attributes.
- Customer's team will be available for testing and validation.

DELIVERABLES

- Values of attributes are stored correctly in the Spigit database
- Customer determines whether or not User attributes are displayed on the User Profile page or hidden and only used as authorization mechanism to control access to a specific campaigns

SSO User Attributes

SSO

Required: Standard Claims or Attributes

While Spigit can receive any number of attributes that may be useful for the support of an innovation program, it requires four attributes and requires that they have the following names and properties:

1. **username**
   a unique and immutable identifier
   - typically the user's network ID
2. **email**
   the user's email address
3. **firstname**
   the user's given name
4. **lastname**
   the user's surname

If some of the users in your network do not have email addresses (e.g. factory workers, retail workers, etc.), some means for populating email addresses in the network must be achieved. The email addresses also must be unique.

Regardless of whether you are using SAML or LDAP to authenticate, the high level process is the same. The detailed implementation method will vary. If LDAP is in place, the VPN tunnel will already be established and the attributes must be available in the directory for Spigit to retrieve. In order to retrieve user's attributes in the LDAP implementation, the root of the user's DN must be available to perform an LDAP search

Timelines

The process from beginning to end typically takes a week, but can be affected by the resources being available on both sides. When the project teams are able to focus on the project as a priority, the addition of attributes goes much faster than when it is one of many projects they are working on. In addition to the elapsed project time, there is sometimes a lead time on one side or the other as projects can get backed up in the respective team queues.

If the specific details of integration timing are a concern, work with your Account Director and internal project team during the statement of work negotiation process to understand the current workloads and expected implementation timelines.