Imaginatik plc
745 Atlantic Ave, 8th Floor
Boston, MA 02111

Phone: +1 (866) 917 2975
www.imaginatik.com

Innovation Central – Standard Single Sign-On

To facilitate and improve participation, Imaginatik offers Single Sign-On (SSO) for Innovation Central.

The technology used to implement SSO is the industry standard SAML 2.0 protocol.

The communication with the Imaginatik Innovation Central and Single Sign-On Service Provider (SP) server will always be over HTTPS. Service Provider initiated SSO is used in all cases. The SP server uses the RelayState to track the ultimate destination URL and it needs to be preserved throughout the authentication process.

In ordinary SSO, the SAML Assertion only needs to contain the userid. We can use any single-byte alphanumeric string, up to 32 characters long, as the userid. This can be an employee ID, NT or network ID, or an MD5 hash of these, so long as it is unique to each user.

Implementing SSO delegates authentication to the Identity Provider. As a consequence, all Innovation Central users have to be able to connect to the existing identity management and authentication systems.

SSO on mobile devices

Single Sign-On integration for Innovation Central works on mobile devices in the same way that it does on desktops and laptops. When a user that hasn't already been logged in attempts to access the site in their mobile internet browser, they will be redirected to their Identity Provider. There they will log in, before being redirected back to Innovation Central.

User account provisioning

To perform authorization Innovation Central requires an extract of the corporate directory, containing at least the given name, middle initial, surname, userid (as included in the SAML Assertion) and email address of each Innovation Central user. This should be sent as a CSV to our Secure FTP (SFTP) server on a regular (up to daily) basis. The CSV may contain additional information, such as company, location, department, etc. This will facilitate audience selection and reporting in Innovation Central. The format of this CSV file is documented separately.

Alternatively, these user details can be transmitted through the SAML Assertion. This enables Just-In-Time (JIT) user account provisioning: accounts will be created and updated as and when users authenticate and access the Innovation Central application. JIT provisioning has the limitation that accounts cannot be removed through the same process, however accounts can be disabled or deleted manually. Another thing to consider is that the Campaign Management and Special Roles functions in Innovation Central can only operate on profiles that exist in the system. When JIT provisioning is used for account creation, anyone that hasn't accessed the system at least once can not receive any emails, or be assigned any special roles or access by name, from within Innovation Central..

With JIT provisioning, the assertion needs to contain at least the given name, middle initial, surname, userid and email address of each Innovation Central user. It may contain additional information, such as company, location, department, etc.