JUVARE

Juvare Project Description

External Authentication

1.0 Services Overview

Juvare will provide the services necessary to enable the client's users to log in to Juvare solutions using the credentials they set up in the client's authentication service.

2.0 Project Scope

Juvare will develop and implement an authentication interface for the client that includes the following functionality.

2.1 The client administrators can set up Juvare solution accounts to authenticate against the client's authentication service.

2.2 Account users can log in to the Web version of the Juvare solution using the credentials they set up in the client's authentication service.

2.3 Account users can log in to the Mobile version of the Juvare solution using the credentials they set up in the client's authentication service.

2.4 Account users can access any Juvare solution if their account has the appropriate access rights granted in those solutions.

3.0 Assumptions

3.1 The client will designate a project manager to serve as the primary contact ("Client POC") for ongoing communications and project planning.

3.2 The client will designate information technology staff to communicate with Juvare's information technology staff and make the required configuration changes on the client's authentication service.

3.3 The client's authentication service supports OpenID Connect.

3.4 Account users share the same instance of the client's OpenID Connect authentication service.

3.5 Juvare will use the following scopes: 'openid', 'profile', and 'email'.

3.5.1 Juvare authentication services expect following standard claims from above listed scopes:

3.5.1.1 email

3.5.1.2 given_name

3.5.1.3 family_name

If, for some reason, a client cannot provide these claims, agreement with Juvare on how to provide alternate information needs to be established.

3.6 Password management, including complexity and expiration, will be enforced by the client's authentication service.

The client will share their OpenID Connect configuration with Juvare, including the following information.

3.6.1 Authority URL: the URL to which Juvare should send authentication requests.

3.6.2 Client ID: the identification assigned to the Juvare solution in the client's OpenID Connect authentication service.

3.6.3 Client Secret: the secret assigned to the Juvare solution in the client's OpenID Connect authentication service.

3.6.4 At least one account, for testing purposes, for each authentication environment.

3.7 The following Juvare environments are whitelisted in the client's external authentication services as return URLs.

- https://login.juvare.com
- https://login.lab.juvare.com

3.8 The client administrator has user management rights in the Juvare solution for specific account users.

3.9 After external authentication has been established for a user, the Juvare Support Center is no longer able to assist the user with log in and credentialing issues without removal of the external authentication mapping.

3.10 After external authentication has been established for a user, the user is no longer able to use the Juvare password forgiveness functionality.

3.11 External authentication functionality will be configured in a testing environment to accommodate thorough testing prior to configuration in the production environment.

3.12 The client will participate in end-to-end testing in both the testing and production environments.

Juvare envisions a future where communities are resilient in the face of danger. Offering precise, vigilant, and connected solutions, Juvare fosters networks of mutual assistance to help organizations bounce forward. For more information about Juvare solutions, contact the Juvare Support Center, support@juvare.com or 877-771-0911.