Statement of Work (SOW) - Single Sign On (Back Office) One-Time Services

Project Summary

The Provider will deliver services to support the implementation of Single Sign-On (SSO) using the SAML protocol for the back-office component of the Enterprise Solution. The back office refers to the internal area used exclusively by the Customer's staff to manage operations, administration, and other essential business functions. This SSO implementation will enable staff users to authenticate securely using a centralized identity provider.

Assumptions

Single Sign On (Back Office)

The Customer has been onboarded and a test environment is available for use.
The Customer is utilizing a supported Identity Provider (IdP), which must support the SAML protocol. Supported IdPs include, but are not limited to, Azure AD, Okta, OneLogin, Jump Cloud, ForgeRock, Shibboleth, and F5. The Provider shall not be responsible for enabling Single Sign-On (SSO) where the Customer's selected Identity Provider (IdP) does not support SAML.
The Customer is responsible for preparing two Identity Provider (IdP) configurations: one for the production environment and one for the test environment.

Limitations

Single Sign On (Back Office)

The Provider is not accountable for user adoption, user login behavior, or business process outcomes resulting from the implementation of Single Sign-On (SSO).
The Provider will perform one (1) round of configuration in each environment (test and production). Any additional configuration efforts resulting from changes on the Customer's side will require a separate change request.
Configuration of the production environment will be based on the validated setup from the test environment. Any deviations introduced by the Customer in the production environment may affect expected outcomes and fall outside the Provider's responsibility.
The Provider's ability to meet agreed timelines depends on the timely delivery of required information, completed documentation, and configuration inputs from the Customer.
The Provider's role is limited to the configuration and enablement of Single Sign-On (SSO) within the agreed scope and environment(s). Configuration or troubleshooting of the Customer's Identity Provider (IdP) is not included.
This scope is limited to applications accessed by users assigned a Professional or Express user license. Scope does not include implementation for any public-facing portals (e.g., ESC, Exhibitor Portal) or custom-built solutions.

Scope of Services

Kick Off

Provider responsibility

- Internal handover and preparation.
- Deliver the Single Sign-On (SSO) Questionnaire to the Customer for completion.

Customer responsibility

- Ensure project scope is accurate and fully aligns to all business requirements.
- Raise any risks, blackout periods for software release, resourcing plan.
- Return the fully completed Single Sign-On (SSO) Questionnaire prior to the commencement of the project.

Build

Provider responsibility

- Installing the necessary certificates on the Provider's web servers and configuring the test environment to support Single Sign-On (SSO) functionality. Excluding user configuration.
- Supply the Customer with all necessary information required to configure user accounts for Single Sign-On (SSO) integration and to enable Single Sign-On (SSO) functionality within the system.

Customer responsibility

- Configurations within the Identity Provider (IdP) and shall ensure the availability of a technical resource with appropriate knowledge and understanding of the SAML protocol and the IdP configuration.
- Setting up all users in the test system in accordance with the requirements of the Single Sign-On (SSO) configuration.

Testing

Provider responsibility

- Conduct one (1) 30-minute remote meeting to review and address any identified issues, followed by appropriate follow-up as necessary.
- Maintain an issue log to monitor, document, and track the status and resolution progress of all issues raised during the project.

Customer responsibility

- Customer is responsible for preparing for and executing user testing, including creation of test plans, test cases, and test scripts.
- Ensure that all relevant key resources are available and attend all scheduled testing meetings.
- Promptly raise any issues found (that are within scope).
- The testing phase will be no more than one (1) week in duration.

Launch & Post Launch

Provider responsibility

- Configuring the production environment in alignment with the setup of the test environment, excluding user configuration and the final cutover to Single Sign-On (SSO).
- Project closure.
- Post-launch activities shall be completed within one (1) week.

Customer responsibility

- Setting up all users in the production system in accordance with the requirements of the Single Sign-On (SSO) configuration.
- Conducting user training and executing the cutover to Single Sign-On (SSO).
- Complete customer satisfaction survey.
- Post-launch activities shall be completed within one (1) week.

Project Management

Provider responsibility

- Coordination of resources, activities, meetings in alignment with timelines and milestones.

Customer responsibility

- Nominate a technical project lead who will serve as the primary point of contact and be responsible for coordinating all technical activities.
- Coordination of activity and resources on customer side to align to project plan and schedule.

Exclusions

- Direct communication or coordination with third-party vendors (e.g., Identity Provider [IdP] vendors, software vendors).
- Implementation of Single Sign-On (SSO) for other software solutions offered by the Provider, including any SSO integration for public-facing portals such as the ESC, Exhibitor Portal, or similar platforms.
- Implementation or support for Single Sign-On (SSO) in any custom-built or bespoke software solutions developed by or for the Provider.
- Setup and configuration of the Customer's Identity Provider (IdP).
- Development of training materials or delivery of customized training sessions beyond standard guidance.
- Configuration or support of the Customer's internal network, firewalls, or IT infrastructure required to enable Single Sign-On (SSO).
- Configuration of the system for user enablement or user provisioning workflows.
- Migration, transformation, or cleanup of existing user data to meet Single Sign-On (SSO) requirements.
- Bulk user data migration or transformation activities.

Project Schedule

The estimated timeline for this project is 4 weeks. However, Provider and Customer will create and agree to a joint project plan. The plan is an estimate and may change.