HARRINGTON QUALITY MANAGEMENT SOFTWARE

HQMS

SINGLE SIGN ON (SSO) CAPABILITY

OpenID connect:

OpenID Connect, or OIDC, is an identity layer on top of the OAuth 2.0 protocol framework. Using JSON web tokens (JWT), the technology verifies the identity of the user and obtains basic user profile information. This is done for authentication through utilizing familiar and shared credentials, a single sign-on (SSO) methodology. These sync up with an OpenID Connect identity provider, a partial list of which include:

✓ **ADFS (Active Directory Federation Services),** ✓ **Azure AD (Active Directory),** ✓ **Google,**
✓ **IBMid (IBM identity provider),** ✓ **OKTA,** ✓ **Ping,** ✓ **SalesForce,** ✓ **SiteMinder**

Each time the user logs in using OIDC they are redirected to a login process tied to the identity provider. After completing that process, they are then being taken back to the service. In these cases, information is shared between the service and identity provider.

Auto Login with Windows Authentication:

In this mode the user is automatically logged in without needing to type in a username and password because it uses the credentials they are logged into the computer as to authenticate.

Auto login without Windows Authentication:

In this mode the user enters the same credentials they log into the computer with, but they must enter then by hand instead of being auto logged into the system.

Third Party SSO:

This option should work for SSO's that can be configured to send a token over the URL of requests. In this case you specify the token value being sent in the Admin utility and that value is used to authenticate the user

REQUEST A DEMO

(3175-JAN-23)

HGI | sales@hgint.com | www.hgint.com | 1-800-ISO-9000