Securely Navigate Niagara Stations with Single Sign On

September 3, 2020

Q&A

1. When using OKTA for SSO as the IdP We are having issue switching servers and having SAML pass the token. Do you support 3rd party IdP?

   We do support third party IdPs and have tested a significant number of them, such as ADFS, Salesforce, OpenAM, G-Suite and others. Additionally, we do have customers successfully using OKTA. As a point of clarification for this feature, we do not currently support an IdP-initiated SAML login workflow (This is when the IdP sends a POST request directly to our stations to log in), as we must start the process at the station for authentication to work.

2. Any existing integrations with OpenID Connect?

   We do not currently have core support for OpenID Connect. However, if needed, we do have an extensible authentication framework which allows third parties to create their own authentication schemes.

3. Do the stations have to be version 4.9 to allow this or does only the supervisor need to be 4.9?

   Only the supervisor needs to be at 4.9, as the other stations in the system just need to be at 4.4+ and have the saml and samlEncryption modules installed therein. As a best practice, ensure that the stations are running the latest version of Niagara 4.4 (U3), as it supports SAML encryption, which streamlines its setup.

4. Will this work with older JACE's JACE-6's, JACE-7's etc. as long as they are running 4.4?

   Yes, only the supervisor needs to be at 4.9. The only requirement for the JACEs is that they're at 4.4, which could be JACE-6s or JACE-3s (for example). It is recommended to use the latest version of Niagara 4.4 (U3), because it supports SAML encryption and will make the set up easier since Niagara provisioning features a job step which enables encryption automatically. Please note, installing the samlEncryption module on older JACEs that are already running at capacity may be a challenge due to the size of the jar file.

5. If you are not part of a domain do you need to create one? Give all of the stations URL?

   No, it's not necessary, as you can use IP addresses for your stations. Nevertheless, having a domain will allow you to use an additional SSO feature named the "Remember My Choice Domain" (found in Authentication Service > SSO Configuration), which will allow you to automatically utilize SSO without clicking on the login button for the whole domain.

6. Will this work with bajaui - Button - value binding - hyperlink?

   As long as it is placed in a PX graphic and viewed from a browser, you are able to use SAML SSO to access other connected stations.

7. When linking to a subordinate station, it would be nice NOT to have the buttons on the login page. A user can click on the "wrong" button.

   In Authentication Service > SSO Configuration, you can set “Auto Attempt Single Sign On” to ‘true’ to bypass the login page and buttons. Although this only works if you have only one single sign on scheme, the Circle of Trust model is very flexible and can easily allow you to have only one single sign on scheme on your stations. If this is not possible, the “Remember my choice” button will at least allow you to only have to press the button once.

8. Any support for RSA dongles? Or other factors than just passwords? Multifactor?

   SAML with the Niagara IdP will use whatever authentication scheme the user is configured to use in the supervisor, which enables the user to utilize our Google Authentication Scheme, which is two-factor, or Client Cert Authentication, Kerberos, LDAP, or any of our other authentication schemes.

   RSA dongles were supported in Niagara AX 3.7 but are not currently supported in Niagara 4.

9. Will the certificate expire? What happens at that point? Will we have to go in and renew it?

   Even if the certificate is expired, as long as it is expected by the station, then it will be accepted. If the IdP changes which certificate it is using, then you would need to update your stations to use the new certificate. SAML uses a certificate pinning model rather than PKI, which means it is not interested in certificate data such as issuers, key purposes and expiration dates.

10. Can you use this with a customer’s LDAP server managing the users?

    Yes. The supervisor will need to have an LDAPAuthenticationScheme as well as a SAMLIdPService. Other stations will need a SAMLAuthenticationScheme (which can be automatically configured via provisioning). When logging in to a connected station, you will be redirected to the supervisor, which will log you in using LDAP, then redirect you back to the original station, successfully logged in. After you have logged in with your username/password the first time, all those redirects will happen seamlessly under the hood.

11. Is it in the roadmap to set this up via fox/foxs as well?

    Not at the moment, as this feature is currently under design.