Professional Services Data Sheet

SpinetiX ARYA - SSO Activation

When using SpinetiX ARYA, enterprise setups often require an authentication solution which integrates with the customer's user directory and where user authentication is controlled by the customer. The SpinetiX ARYA SSO (Single-Sign-On) Activation implements such a solution. Thanks to this service, users do not need to retype their password to sign-in to SpinetiX ARYA as authentication assertions are transparently passed between SpinetiX ARYA and the customer's user directory. The user only authenticates once to the customer's company.

Deliverables & Requirements

The SpinetiX Professional Services team can help you set up, configure, and activate SpinetiX ARYA SSO. Customers must be available to collaborate with SpinetiX according to the below process to setup the SpinetiX ARYA SSO Activation:

1. The customer agrees on an SSO setup offer from SpinetiX.
2. The customer chooses which protocol to use, either OpenID Connect (OIDC) or SAML 2.0. In general, OIDC should be preferred as it is a modern protocol, but some directories only support SAML 2.0.
3. The customer agrees with SpinetiX on its unique SSO identifier, which should be a short friendly string, generally the company name, composed of letters, numbers, hyphen and underscore.
4. SpinetiX sets up a SpinetiX ARYA enterprise account for the customer, if not already done, which assigns an account ID to the customer. This account will be the default account for new users signing in via SSO.
5. The customer does the OIDC or SAML 2.0 application setup on his own directory according to SpinetiX instructions.
6. The customer must restrict access to the OIDC or SAML 2.0 application to the users which are allowed to use SpinetiX ARYA.
7. The customer chooses its desired refresh token expiration (e.g., 12 hours); this is the time after which a user signed-in on the SpinetiX cloud needs to re-authenticate with the customer's directory and is thus the maximum time it takes for a user blocked in the customer's directory to be blocked on the SpinetiX cloud. The minimum is 1 hour.
8. The customer provides the OIDC or SAML 2.0 application information to SpinetiX (e.g., client ID, secret, discovery URL, metadata URL), refresh token expiration and any non-standard claims.
9. SpinetiX does the provisioning of SSO for the customer with the information provided by the customer.
10. The customer verifies that SSO is working as expected.
11. If the customer defines an OIDC client secrets he arranges with SpinetiX for secret rotation a few weeks before the secret expires.

Important information

- The protocol used, OIDC or SAML 2.0, cannot be changed once it is set up, so carefully consider the choice between the two.
- The number of users which are allowed to access SpinetiX cloud SSO via the customer's directory should be limited to a small number, normally no more than 10. It is indeed desirable to limit the number of users for security's sake, according to the least access principle.
- Authorization and management of user roles is not affected by SpinetiX cloud SSO, they are controlled on the SpinetiX cloud products, like SpinetiX ARYA, by users with admin privileges to the account.
- If the customer sets up a client secret for OIDC he is responsible for contacting SpinetiX to arrange for secret rotation before it expires with sufficient advance for SpinetiX to do provision a new secret. Once the secret expires SSO stops working and users can no longer access SpinetiX ARYA until a valid secret is re-provisioned.