Sysnet.air Single Sign On (SSO)

Requirements for our clients

Sysnet.air uses Security Assertion Markup Language (SAML) as authentication and authorisation language for SSO in Sysnet.air

In order to configure a client's instance of Sysnet.air to support SSO, we require the following:

- Client provides the identity provider. This is the server that authorises access to our services
- Sysnet.air is the service provider.
- Sysnet generates service provider metadata. This describes our application and our endpoints in XML. Sysnet also sign this document with a SSL cert. The client registers us as a service provider on their Identity Provider.
- The client will provide Sysnet with their Identity Provider metadata in XML. Again, this is signed by the client with their SSL cert. Sysnet registers their metadata inside Sysnet Air.
- Sysnet will map existing assertion attributes to attributes within the Sysnet.air application so that no changes to the SAML assertions clients current send are required.
- For clients that need to initiate the SSO flow from the SP side, the following URL needs to be used. This URL is static and will not change: *https://produs-strustusa.sgsonline.net/services/login/initiateSSO*
- Certificates need to be signed properly. For testing, Sysnet can use self-signed certs if required.
- On Authentication, if Sysnet cannot find the MID within the sub-client hierarchy our default action is to redirect to our login screen. Alternatively, there is a product config option to redirect back to the client's IDP server as an alternative. Please specify the desired option and if redirect back to the client's IDP is required, please specify the logout URL.
- On Authentication, if any other authentication error occurs (e.g. valid mid but account is closed; or any security error such as cert expired) Sysnet also redirect to our login screen. Alternatively, there is a product config option to redirect back to the client's IDP server as an alternative. Please specify the desired option and if redirect back to the client's IDP is required, please specify the logout URL.

FAQ

- What SAML signature requirements do you support?
  - Sign SAML assertion
  - Sign SAML response
  - Sign both SAML assertion and response
- What signature signing keys do you support?
  - 2048 bit keys are supported. We have generally not been required to support any others so please contact us to conduct testing if alternative is required (e.g. 4096 bit keys)
- What signing algorithms do you support?

    - RSA-SHA256 is supported. We have generally not been required to support any others so please contact us to conduct testing if alternative is required (e.g. RSA-SHA384 or RSA-SHA512)
- Do you have SAML encryption requirements (other than over HTTPS)? For example, SAML token encryption is required for SAML assertions that are sent to you?
    - No
- Which SAML bindings do you support?
    - POST, this is our preferred option in case the payload exceeds the query length on a redirect.
    - Redirect
- Who do we contact when our SAML signing certificate is up for renewal?
    - Please contact your project/alliance/business relationship manager to initiate discussions and plans for certificate updates.