How to use an ADFS server as SSO Identity Provider for SecuTix

This service allows our clients to connect to SecuTix back-office (parametrization + box-office) using their corporate credentials instead of having to remember a securitx-dedicated login and password. It then allows their regular system administrators to control who can access SecuTix and from which location (because a VPN to the institution or a "remote office" access will then be mandatory)

Basically, the secutix login page redirects the user to the cutomer's login page, the user enters the login/password on their login page (if needed), and then the user is redirected to secutix.

Prerequisit

- ws federation metadata of the ADFS server (xml file or URL)

Configuring the ADFS server (customer side)

Note: this is only a basic configuration guide which shows the minimal required configuration. The customer may want customize the configuration to strengthen the security.

Follow the steps of https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-relying-party-trust, using the following configuration values:

- At Step 6., use the CAS certificate (see Configuration items)
- At step 7., only enable support for the WS-Federation Passive protocol URL (disable SAML one)
- use SecuTix CAS login url as URL (like https://<institution>.pos.secutix.com/cas/login)
- At step 8., use the Relying Party Identifier (see Configuration items)
- After step 11, add the following claims in "Issuance Transform Rules":
    - Use "Send LDAP Attributes as Claim"
    - Claim rule name: "SecuTix"
    - LDAP attribute: User-Principal-Name (if the operator's login matches the SecuTix login, or a customer dependent attribute containing the name of the SecuTix operator), Outgoing claim: SecuTix/login

Internal documentation for SecuTix configuration is here