Lockself

Introduction

- Lockself use SAML 2.0 to federate identities.
- In SAML terminology, there is a client application which is called Service Provider (SP) and an identity provider (IdP), here Trustelem.

Application configuration elements, on the SP side

- Definition of the pages where SSO authentication is enabled (LoginPath)
- Definition of the SAML URL for the SP side: Assertion Consumer Service (ACS)
- Definition of the identifier attribute (NameID) and its format
- Definition of the IdP (Trustelem) connection URLs
- Definition of the certificate(s) used for encryption and/or the signature of SAML content.
  Note: these configuration data can be requested in metadata.xml format.

Application configuration elements, on the IdP side

- **EntityID:** application identifier → must be identical to what was indicated on the SP side
- **Assertion Consumer Service (ACS):** URL on the SP side for receiving SAML assertions generated by the IdP → must be identical to what was indicated on the SP side
- **NameID Attribute:** name of the attribute containing the user's identity in the SAML response provided by the IdP Trustelem to the SP application → must be identical to what was indicated on the SP side
- **NameID Format:** format of the NameID attribute. Except in special cases, use the default value → must be identical to what was indicated on the SP side
- **Attributes List:** additional attributes that can be embedded by the IdP into the SAML responses, and used by the application on the SP side
- **RelayState:** URL of the page to which the user should be redirected after authentication
- **Custom login URL:** URL used to initialize login via SAML 2.0 in the Trustelem user's dashboard
- **Custom scripting:** script to add/modify attributes in the SAML responses (example: attribute from the Active Directory)

Revision #1
Created 1 July 2022 09:01:22 by WALLIX Admin
Updated 1 July 2022 09:18:03 by WALLIX Admin