SAML 2

Introduction

The SAML 2.0 configuration varies from application to application.
This page provides information about the most commonly used settings on both the application and Trustelem.
In SAML terminology, there is a client application which is called Service Provider (SP) and an identity provider (IdP), here Trustelem.

If you are the application developer

Note: our recommendation is to use OpenID Connect rather than SAML 2.0. OpenID Connect is more modern and more simple than SAML 2.0. If you still want to use SAML, you have 3 options:

- Deploy a SAML module in the framework underlying the application (e.g. Wordpress, Drupal, Symphony). This option does not require any development in the application itself.
- Deploy a SAML module in the application's frontal web server (Apache, Nginx).
- Use a SAML 2.0 library that will authenticate the user.

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 08:42:58 by WALLIX Admin
Updated 24 November 2023 14:49:26 by WALLIX Admin