ADFS

Linnéa Nyberg - 2022-11-22 - Login (IdP)

To configure ADFS as a login to Skolon, you as a customer need to upload Skolon's metadata, and then send the metadata back to Skolon. It is also important that the claim you set up in the SAML response is created without a NameID.

Skolon parameters and metadata:

Sign on URL: https://ext-idp.skolon.com/a/

App identifier
URL: https://ext-idp.skolon.com/simplesaml/module.php/saml/sp/metadata.php/skolon

Reply URL:
https://ext-idp.skolon.com/simplesaml/module.php/saml/sp/metadata.php/skolon

Skolon metadata:
https://ext-idp.skolon.com/simplesaml/module.php/saml/sp/metadata.php/skolon

Email must be an extra attribute/claim in the SAML response. Suggestion is to name it "mail", regardless of the name of the attribute.

Keep in mind that the attribute/claim must be sent in transient format.

Example of claim attribute after it is set in transient format:
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Links to guides

Exactly how the configuration is done varies from AD version to AD version, but below are links to documentation from Microsoft that is most often used and examples of how to configure a claim to Transient nameID.

Guide to setting up a Relying Party in ADFS:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-relying-party-trust

Set up rules to be sent about LDAP attributes such as claims:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-rule-to-s

end-ldap-attributes-as-claims

Guide to setting up rules for transform claims:

https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-rule-to-transform-an-incoming-claim

Rules for making a claim to Transient:

NameID-opaque

c1:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

&& c2:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant"]

=> add(store = "_OpaqueIdStore", types = ("http://adfs.adfs.net/internal/sessionid"), query = "{0};{1};{2};{3};{4}", param = "useEntropy", param = c1.Value, param = c1.OriginalIssuer, param = "", param = c2.Value);

Create transient name identifier

c:[Type == "http://adfs.adfs.net/internal/sessionid"]

=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient")