SAML parameters

To integrate the Authentication Server with any SAML Identity Provider, you need to add the Authentication Server configuration into the SAML Identity Provider (it should be registered as SAML v2 remote service provider). Next, you need to configure the following additional parameters in the **authserver.properties** file.

Parameter	Description	Default value
authentication.saml.enabled	Sets the value to **true**.	false
authentication.saml.entity.id	Sets an authentication server as a service provider ID if it is different than the default server.	com.nomagic.authentication.server
authentication.saml.name.id.format	Specifies the format of a username identifier.	urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
authentication.saml.idp.metadata.url	Specifies an Identity Provider metadata URL address if SAML Identity Provider supports metadata retrieval from the URL (e.g., ForgeRock OpenAM).	-
authentication.saml.idp.metadata.file	Specifies the name of a metadata file, which should be added into the same config directory where the **authserver.properties** file exists. This metadata file is required by some Identity Providers instead of metadata URL (e.g., WSO2 Identity Service).	-
authentication.saml.link	The title of the button for SAML user login displayed on the login page.	SAML User
authentication.saml.disable.force.authentication	Sets ForceAuthn to true or false in the AuthnRequest in SAML based authentication. Change it carefully as you won't be able to login with another user after user logout in the value is false	true
authentication.saml.signature.algorithm	SAML integration requests signature algorithm. Available values - SHA1, SHA256. and SHA512.	SHA1

Related pages

- **SAML integration**