VERSION LOG OUT

User: amAdmin Server: sp.example.com

FORGEROCK

## update rest sts instance

Save Back

General Configuration Issued SAML2 Token Configuration

Deployment Configuration

### General Configuration

**The issuer name:** sp.example.com

**Supported Token Transforms:**

UNT->SAML2;invalidate interim OpenAM session
UNT->SAML2;don't invalidate interim OpenAM session
OPENIDCONNECT->SAML2;invalidate interim OpenAM session
OPENIDCONNECT->SAML2;don't invalidate interim OpenAM session

Supported token transformations

Back to top

### Deployment Configuration

**Deployment Url Element:** test-sts

STS endpoint Url will be composed of rest-sts/realm/uriElement

**Authentication Target Mappings:**

**Current Values**

X509|module|cert_module|x509_token_token_auth_target_header_key=client_cert
USERNAME|service|ldapService
OPENIDCONNECT|module|oidc|oidc_id_token_auth_target_header_key=oidc_id_token

Remove

**New Value** Add

Authentication target mappings

**Client Certificate Header Key:**

TLS-offload host certificate header key

**Trusted Remote Hosts:**

**Current Values** Remove

**New Value** Add

IP addresses of TLS-offload hoasts

Back to top

## Issued SAML2 Token Configuration

**Service Provider Entity Id:**

sp

Values will be used to populate the Audiences of the AudienceRestriction element of the Conditions element. This value is required when issuing Bearer assertions. See section 4.1.4.2 of http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf for details.

**Service Provider Assertion Consumer Service Url:**

When issuing bearer assertions, the recipient attribute of the SubjectConfirmation element must be set to the Service Provider Assertion Consumer Service Url. See section 4.1.4.2 of http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf for details. Value required when issuing Bearer assertions.

**NameIdFormat:**

urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified

**Token Lifetime (Seconds):**

60000

**Custom Conditions Provider Class Name (optional):**

If the Conditions of the issued SAML2 assertion need to be customized, implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.ConditionsProvider interface, and specify the class name of the implementation here.

**Customs Subject Provider Class Name (optional):**

If the Subject of the issued SAML2 assertion needs to be customized, implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.SubjectProvider interface, and specify the class name of the implementation here.

**Custom AuthenticationStatements Class Name (optional):**

If the AuthenticationStatements of the issued SAML2 assertion need to be customized, implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthenticationStatementsProvider interface, and specify the class name of the implementation here.

**Custom AttributeStatements Class Name (optional):**

If the AttributeStatements of the issued SAML2 assertion need to be customized, implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeStatementsProvider interface, and specify the class name of the implementation here.

**Custom Authorization Decision Statements Class Name (optional):**

If the AuthorizationDecisionStatements of the issued SAML2 assertion need to be customized, implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthzDecisionStatementsProvider interface, and specify the class name of the implementation here.

**Custom Attribute Mapper Class Name (optional):**

If the class implementing attribute mapping for attributes contained in the issued SAML2 assertion needs to be customized, implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeMapper interface, and specify the class name of the implementation here.

**Custom Authentication Context Class Name (optional):**

If the AuthnContext mapping implemented by the org.forgerock.openam.sts.token.provider.AuthnContextMapperImpl class, implement the org.forgerock.openam.sts.token.provider.AuthnContextMapper interface, and specify the name of the implementation here.

**Attribute Mappings:**

**Current Values**

Remove

**New Value**

Add

Contains the mapping of saml attribute names (Map keys) to local OpenAM attributes (Map values) in configured data stores.

**Sign Assertion:**

**Encrypt Assertion:**

Check this box if the entire assertion should be encrypted. If this box is checked, the Encrypt NameID and Encrypt Attributes boxes cannot be checked.

**Encrypt Attributes:**

Check this box if the assertion Attributes should be encrypted. If this box is checked, the Encrypt Assertion box cannot be checked.

**Encrypt NameID:**

Check this box if the assertion NameID should be encrypted. If this box is checked, the Encrypt Assertion box cannot be checked.

**Encryption Algorithm:** http://www.w3.org/2001/04/xmlenc#aes128-cbc

Algorithm used to encrypt generated assertions.

**KeystorePath:**

Path to keystore

**Keystore Password:**

**Confirm Keystore Password:**

**Encryption Key Alias:**

This alias corresponds to the SP's x509 Certificate identified by the SP Entity ID for this rest-sts instance. Not necessary unless assertions are to be encrypted.

**Signature Key Alias:**

Corresponds to the private key of the IdP. Will be used to sign assertions. Value can remain unspecified unless assertions are signed.

**Signature Key Password:**

**Confirm Signature Key Password:**

Back to top

Save Back