Logga in med SWAMID (SAML)

Nedan beskrivs hur processen att konfigurera SUNET Play för login med SAML (*Security Assertion Markup Language*) via Shibboleth kan gå till. I exemplet nedan används Swamid som identitetsfederation.

I exemplet används autentisering som initieras av tjänsten (SUNET Play). Man ombeds att autentisera sig när man använder en sida som kräver autentisering. Läs mer under stycket Service Provider Initiated Authentication på Kalturas sida Kaltura Mediaspace SAML integration guide.

Är du det minsta osäker på begreppen API, KMC, KMS och KAF så läs i vår FAQ.

Är du det minsta osäker på application och contextual roles i Kaltura så läs i vår FAQ.

Den här guiden förutsätter att du redan har ett SSL-certifikat för KMS på plats för play.**lärosäte**.se Lär mer i vår guide om hur du skaffar ett SSL-certifikat för KMS.

Steg-för-steg guide

1. Logga in som admin i KMS på https://play.**lärosäte**.se/admin
2. Konfigurera de globala inställningarna för AUTH såhär:

Option	Value
authNAdapter	SAML: SP Initiated
authZAdapter	SAML: SP Initiated

3. Konfigurera modulen för SAML såhär:

Option	Value
enabled	Ja
metadataMode	Automatic
enableMultiIdp	Nej

spMetadata (SAML metadata för tjänsten)

Option	Value
name	https://play.**lärosäte**.se
host	play.**lärosäte**.se
relayState	/
nameIdFormat	Transient
certificate	tryck *generate certificate and key* (om er Idp behöver en chain of trust för att fungera behöver ni ett certifikat från er certifikatleverantör. Sen fyller ni i public och private key manuellt)
privateKey	--

automaticIdpMetadata (konfiguration för automatic discovery av Idp)

Option	Value
metadataUrl	http://mds.swamid.se/md/swamid-idp.xml
refreshInterval	86400
discoveryServiceUrl	https://service.seamlessaccess.org/ds/
expiry	345600

supportedIdpList	**https://weblogin.lärosäte.se/idp/shibboleth** (Leta efter de Idp du vill godkänna login från på denna sida https://mds.swamid.se/md/swamid-idp.xml Sök efter "md:EntityDescriptor entityID". Om fältet lämnas tomt godkänns login från alla SWAMID-anslutna Idp. Du kan lägga till flera Idp i en kommaseparerad lista)

attributes (SAML mapping för användarnamn, förnamn, efternamn och email)

Option	Value
userIdAttribute	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
firstNameAttribute	urn:oid:2.5.4.42
lastNameAttribute	urn:oid:2.5.4.4
emailAttribute	urn:oid:0.9.2342.19200300.100.1.3

defaultRole (standard application role sätts till viewerRole)

Option	Value
allowDefaultRole	Ja
role	viewerRole

roleAttributes (här gör vi en konfiguration så att medarbetare får application role privateOnly och studenter får viewerOnly)

Option	Value
attribute	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
value	employee@**lärosäte**.se
role	privateOnly
attribute	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
value	student@**lärosäte**.se
role	viewerOnly

4. Skicka en beställning av tjänstemetadata för er playtjänst till operations@swamid.se
   Bifoga länken: https://play.**lärosäte**.se/saml/index/sp-metadata

Fördjupande läsning

Här finns en bra sida från NORDUnet som fördjupar din förståelse kring SAML och användarhantering.