Instructions & Technical Configuration to New SSO Users

Technical Configuration for SAML 2.0

This document describes how to configure your service/product to use Joint Web Login, a service within Uppsala University that enables simple login for staff and students.

Note: Before performing configuration, preparatory steps must be taken to start the work. See the checklist for more information.

Contents:

- Technical Configuration for SAML 2.0
- Formal Requirements, Rules and Recommendations
- Prerequisites
- Setup and Configuration
- Metadata
- Publication of Metadata

Expectations:

As a provider, you are expected to

- be oriented in the field of SAML 2.0. Read more about SAML 2.0 here.
- be familiar with how your service/product connects to an IdP with SAML 2.0.

NOTE: All authorization (authorization management) and role management must be performed in your service/product.
The Joint Web Login service does not perform any authorization management or role management for your service/product.

Read more under Authentication and authorisation principles (Authorisation section).

Formal Requirements, Rules and Recommendations

Requirement / Rule / Recommendation	Clarification	Examples
All SAML keys/certificates you create when setting up your SP should have - a **key length** of at least 4096 bits (RSA) - a **validity period** that is very long (e.g. 100 years)	To comply with current recommendations and requirements and to avoid having to regenerate SAML certificates on an ongoing basis.	

The **entityID** of the service should be in **URL format**.	The entityID of the service must be unique and is usually set to be a base URL to the part of the service that handles SAML 2.0. Having a metadata URL as the entityID is recommended by Assertions and Protocols for the OASISSecurity Assertion Markup Language (SAML) V2.0 (section 8.3.6 Entity Identifier).	• `https://myservice.uu.se/Shibboleth.sso/Metadata` If using the SP software Shibboleth SP, this is the URL to its metadata generator. • `https://myservice.uu.se/Shibboleth.sso` If using the SP software Shibboleth SP, this is usually its base URL. • `https://myservice.uu.se/shibboleth` This indicates that the URL has something to do with Shibboleth and the Shibboleth SP software. • `https://myservice.uu.se/saml` This indicates that the URL has something to do with SAML. • `https://myservice.uu.se/` This is a URL that is unique to the service.
There are application processes to the entity categories that must be followed in order for the service to be tied to ("tagged with") them.	It is those formally responsible for the service who should be able to produce the required information, ensure that the necessary information pages and the like are available, and ensure that all the requirements for an application are met.	See Entity Categories for Service Providers for details for the respective entity category.
Your SP and service metadata should meet all the requirements in SWAMID SAML WebSSO Technology Profile section 6 Operational Requirements for Relying Parties.		

Prerequisites

Step	Instruction	Recommendation
1	**Identify the appropriate entity category** The entity category should contain the information (attributes) needed.	See Entity Categories for Service Providers or the comparative overview Entity Category attribute release in SWAMID and select one of these. For services that need a personal identity number, REFEDS Data Protection Code of Conduct (CoCo v2) is required. For services used for collaboration between students and researchers, and that do not need a personal identity number, REFEDS Research & Scholarship will usually suffice. For services that do not depend on the username being sent via the attribute *eduPersonPrincipalName,* REFEDS Personalized Access Entity Category will usually suffice.
2	**Check that the purpose of the service matches the purpose of the entity category** If e.g. the service is not used in whole or in part to carry out studies or research, then REFEDS Research & Scholarship cannot be used.	More information on the purpose of some of the available entity categories can be found on the following pages: • REFEDS Research & Scholarship (collaborative tools for conducting studies and research; see Definition) • REFEDS Data Protection Code of Conduct (CoCo v2), eller tidigare GÉANT Data Protection Code of Conduct (CoCo v1) (good, accurate, controlled, secure and minimized handling of personal data). • REFEDS Personalized Access Entity Category, contains basically the same attributes as Research & Scholarship, but with the username in the attribute *samlSubjectID*.

3	**Find out if the service needs to have the user ID sent to it via so-called SAML2 Persistent NameID instead of via "normal" attributes** Many services use this technique because it is a more standardised way of transmitting user IDs.	

Setup and Configuration

Step	Instruction	Guidance and Examples
1	**Create a Service Provider (SP) for the service** Install and configure software capable of handling SAML 2.0 for the service. If the service has built-in support for SAML 2.0, configuration in the service administration interface is what needs to be performed instead.	See SAML SP Best Current Practice for guidance.
2	**Use a specific login server (IdP) or choice of higher education institution (DS) in the SP of the service** IdP: entityID: `https://weblogin.uu.se/idp/shibboleth` DS: discoveryURL: `https://service.seamlessaccess.org/ds/`	See Discovery Service Integration for more information.
Option 3 a URL	**Load metadata for IdP via URL** In order for your SP to know how to communicate with (or interpret data from) the IdP – either the IdP you have chosen or the one chosen by the user in the choice of higher education institution (DS) – it needs to have access to the metadata of the IdP. Signing certificates are used to validate IdP metadata. Standard: IdP metadata: `http://mds.swamid.se/md/swamid-idp.xml` Signing certificate: `http://mds.swamid.se/md/md-signer2.crt` Here we assume that the IdP belongs to an organisation that is a member of the SWAMID identity federation, which is the case with the Joint Web Login service at Uppsala University. Exception: IdP metadata: `https://weblogin.uu.se/idp/shibboleth` Signing certificate: `https://weblogin.uu.se/md/uu-signer.crt` This option should only be used in case memory limitations or metadata parsing restrictions prevent the default option from being used.	
Option 3 b Static data	**Load IdP metadata via static data** If your SP does not support loading IdP metadata from a URL (see option 3 a), e.g. if you can only enter "static" data in an administration interface or similar. Note that the following static strings are specific to the Joint Web Login service. Signing certificate for SAML messages:	SSO = Single Sign On SLO = Single Log Out

```
MIIFCTCCAvGgAwIBAgIUJo9vlK2vIasBCUsWuyN3fATLizgwDQYJKoZIhvcNAQEL
BQAwGTEXMBUGA1UEAwwOd2VibG9naW4udXUuc2UwIBcNMjYwNDIwMDczODQxWhgP
MjEyNjA0MjAwNzM4NDFaMBkxFzAVBgNVBAMMDndlYmxvZ2luLnV1LnNlMIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2c+/nGvFofp4RP0IsPf7k/9UkZLB
A/eATCtol13Xp4CHnaZCtS+TNrhoAavIlYPtv33YYihiDmpL7MIYj4pvUJq5Sg/u
CLN7sd5GaDOyVKnq7/6YJjNChzVK3vurHewTW+/lCxy7PMeIYFTjwqrp+qzC2LOL
hrSM1iYC6tadycJYrh4qGfCgsENtmu9qhtUqNEuq35XqPVRU4JADRBcan8QtGike
jzHjzoxTQnkVdHT88feaqB3++eRCN5DDjjduIXx0+GesR3YXGaGEfaxPHpZIz2Mw
OXa3CCJZ+MTDdQnJAdymsigNz1Lnu8mGl1G9den5Lpjp1xb8/HcaCWPM21I24sJh
MvJgi+yOqVp/RRcjX2mO63e6UH4vC5rK7tG27AT6AraSOQ96lf6q2EaQFS0BuyU0
pSWgcD4Q7K83Gc/4zd1wZDS2sMdoeFLjzFHHz3erkPHJXzWlqHBLf8V3yPuk/yXW
1Uob5+ywVaPD3INAkfGz+Vf947P22tjrPMuDcWmiciwocYnvKITF1+9GnzbP+GL2
mFvn0QWtT0BypVM+l+0kWol6j4ywE+s1YAIvGYPqleD3TS2zvOyj2cM/nawzf0D2
z8LU8+uriIQo4yKzz1SNR/KxZpx24ztUZ9p+7nVlWnv6HWCnVHMJcNNItxscb7wY
ENve999fD5QbZNMCAwEAAaNHMEUwHQYDVR0OBBYEFL8mNGIAnl6/wzYW2iy2Wg9C
LnhCMBkGA1UdEQQSMBCCDndlYmxvZ2luLnV1LnNlMAkGA1UdEwQCMAAwDQYJKoZI
hvcNAQELBQADggIBABM+iN5+8BhCBFIzZBVIJmofeaEtaPbGsN1j0dct0r+Ns5Hy
WFr7IZ2PP9kM0eghOMUBWWZQn92CcJlftOmUtJzbKDHLwTQS9QmaK62EhLSZJa/
r9Y3nx2dl0uACSatSqIKAPY6gp3A9d+7JM0mRnTsH6P7FrmbJLWh6LieBVSIIbv1
cdoircoKFWLGJiI0eqBlWd9T229xX8GRfxdJGX8yesIaa2gM9OYVpEFcbCSv8QHv
lBgezb/St3WIsZgJFxT5ZCIva2S4LNfJRbVTjLnSaS4s/JvwpNZ9/09PlvyqZ25G
XeyUyr5BgbHZLbHrwhlVpalANvVeladKLjyQYr0MnhRehlZqv5QpaQfm3i4pfezA
iB8y9FxYg4tSYLQ8TtUu8DCbqzNediRnfHImyTd+9Q4bSuRLfCaE6q70iXZ4z0Er
Ksp/wEX5JZlyQehyC79ypsuBPaKn7yA1glHRCt+lM5mSTrjLfgDhltY6qTZFZbvY
BJ69dR63MMZdEB2t+UcSNp24cOTA6If8TziDtXgXMtiSlyg1JaJjGpYqsEXaTZ52
KGuQk4H+S10r+Hpu9uc+WJgTYpdv0oF8MlCeT+1bH23HijZv+LlKxsRQhtl47mcd
/89K58iXyDJYmEOH8FK2dTnsPXsJ4E2xUUCPmveyRauCm7ni6t10vvYBTewe
```


Encryption certificate for SAML messages:


```
MIIFCjCCAvKgAwIBAgIVAP8M0xJKILTgOKDQb2iTBeSco64wMA0GCSqGSIb3DQEB
CwUAMBkxFzAVBgNVBAMMDndlYmxvZ2luLnV1LnNlMCAXDTI2MDQyMDA3MzgzOVoY
DzIxMjYwNDIwMDczODM5WjAZMRcwFQYDVQQDDA53ZWJsb2dpbi51dS5zZTCCAiIw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMS2rKgjFi7kQaKmSG212gq77urv
DHjmPqSkO5UFAPYhTMFOkInRPd3Q6yJXEer+aUTFcLZR9AcFnXZnMdeHE8A9m+os
A4uV3gA9Atm7Of//McdeSpnSU1AAgYUnN476wLtFDUdQU8h3W3PaTWoqF+nww6qT
nl/RcXO87EkoxCyO1Rr0H3aKM3KWazRlxwxF1S1d3k+zlLuPlR7XeT04Hs2vdwQJ
s50FByLcjZijMD60NOfTnjmFrMRirVk9vJhMxu3rROiDvoH+HWsIMbaDQvSKihid
LSg2AkCm2h56DE6UXVoasst2bUSp5OdctL1FxtlwuQOVXP140mz/RnzfELE+mSth
YckxlRukCJWccKAu/7ZRLp82jchxIFdDkqoNPPlzbq8JPw7aYnKCF2qiKQF+oCaR
RHgusswJltk+YHyulhnRzvWF1WQkNkunVtAw/f2oy9vrcuAnV+zTngo97IbecQNL
f+uXcStk4F70RG2bwpdMsnEOC9H7L30Z1/H27JeTi29l88C9Gziiz+dLUaLfZYlm
9+6Q87LL1qVBnM1ZbqgAwPlqWLoAzyNuGas1zsp9dUOgeWx5HR8MwRlP3KkM9JuS
eSEOCaM/x98XFp6itMaCfpnU5bTvX6Uz4zC3+MP5mpkgHScG55jXF/qUSnk33INA
Kc38NZP3rl0ZUX6xAgMBAAGjRzBFMB0GA1UdDgQWBBSFXbB1K9O5PIJVNkE6JBXL
7l7sXzAZBgNVHREEEjAQgg53ZWJsb2dpbi51dS5zZTAJBgNVHRMEAjAAMA0GCSqG
SIb3DQEBCwUAA4ICAQBcb9nBEOnpz6MK8ElG0j2jUBWHFQAH5NPWHuTEvI2RdQGU
PMa8+IJ4X/TO9Ch4b8YpHggfyLmloVQZCZ+chi4FNrZVyn3GP8f4oBr15mg3Vn8i
511KZbPBV4RyaPAucsFejUBKVi2IEchRbDXazp4h63Y99/rhWJD/fP1ep2pPD3I8
oPsV9dVrh66tSGRBpqRt63LclcNiLZbtQwkuo4mOQSKsMAofmbVuvBDiPlDMp1F5
RlOvNl4/ah0VvOsSkP+bDXje06Y5j8A23LGde34Q8vUDWMpOJpGmR5b7ayafLW98
h3AH/6DPyJljU3VILa0+2ZOak6ko1ZIHEq8inag1O83Q1O+Z84uuGhTPcqoi1etk
6kfMl5zunUJ/4DfFweFVkUPpACzp7WkjX2nPd3Y1knLiii3FUcfwSVoLjZsA28nW
1MfiC5gvd5nuRV1Rm8A2zcYnFsrelMBqbxBgrxanaFwC3TmOWKs/v/IttT2Yr5oZ
96eE5WTq5a6luFCD0tKRGrwtJv7vX9rzJQh34hVEiRvm995UCJasz5H5z+LKDzid
aFZMEVSLDu5BPoBw3rgdmYEPyvfFyb7FaqZK5ecbAR8eyM3e7wJkQ87AaBGEm+/Q
inC7KsChSz3K7mp3KWln4DRoiPFJ9ZXGI5FIIuX5LfXCoVTfvQQlkMTwTHc6ig==
```


URLs for SAML messages:

SSO:
HTTP POST: `https://weblogin.uu.se/idp/profile/SAML2/POST/SSO`

HTTP Redirect: `https://weblogin.uu.se/idp/profile/SAML2/Redirect/SSO`

SLO:
HTTP POST: `https://weblogin.uu.se/idp/profile/SAML2/POST/SLO`

HTTP Redirect: `https://weblogin.uu.se/idp/profile/SAML2/Redirect/SLO`

Which variant of URL should be used depends on what your SP supports, but HTTP POST is most common.

4 If MFA is required	**Add multifactor authentication (MFA)** The Joint Web Login service currently supports TOTP multifactor authentication through the REFEDS MFA profile. Users activate TOTP for their user accounts on the user account website. Normally, the SP of the service should indicate that multifactor authentication is required and with which technology. Important: • that the SP of the service only indicates **one** preferred technology (REFEDS MFA) for multifactor authentication in login requests! The Joint Web Login service currently has no way of knowing which technology/technologies are supported for a given user. • that the SP of the service **verifies** that multifactor authentication was performed and with the correct technology! See `require authnContextClassRef` in the examples. • that the SP of the service **prevents manipulation** of login requests so that the multifactor authentication requirement cannot be circumvented! Turn on signing of login requests in the SP of the service and add `<SPSSODescriptor AuthnRequestsSigned="true" ...>` to the service metadata. The Joint Web Login service will then require all login requests to be signed by the SP of the service.	See e.g. Requiring Multi-Factor Authentication and Multi-Factor Access for further information and SP configuration examples. For REFEDS MFA, the authentication class (`AuthnContextClassRef`) should be: `https://refeds.org/profile/mfa`

Metadata

Step	Instruction	Guidance and Examples
1	**Create metadata in XML format** The most fundamental part of this is purely technical details such as the unique ID of the service (entityID), keys (for signing and possibly encrypting SAML messages) and URLs (SAML endpoints). In most cases, SP software can be used to generate this metadata. See the SP software documentation for details.	Examples of metadata for *other* services can be found at https://metadata.swamid.se/. Select any service and then `Show XML` or `Download XML` and look at the file with any suitable text viewer. This may also be helpful to see if you seem to have "missed" anything in the metadata for your service compared to others.
2	**Supplement with user information** Supplement with information displayed to the user at login, known as MDUI information. This may include formal requirements, use of the service and handling of personal data.	See SWAMID SAML WebSSO Technology Profile (section 6.1.12–6.1.13 Metadata Extensions for Login and Discovery User Interface (MDUI)) for formal requirements. See Service Provider Metadata Extensions for Login and Discovery User Interface (MDUI) for examples See Service Provider Privacy Policy Template for the appropriate template to use for the service usage and personal data handling page.
3	**Supplement with contact information** Contact information is needed so that responsible persons can be reached.	See SWAMID SAML WebSSO Technology Profile (section 6.1.21 Organization samt 6.1.22–6.1.27 ContactPerson) for formal requirements. See Contact and Organization information for Service providers for examples.
4 If DS	**Supplement with special tag for DS** When selecting the higher education institution (DS), you must supplement the service metadata with a tag `<DiscoveryResponse>` inside the tag `<SPSSODescriptor>` and `<Extensions>`. This is a security feature to prevent arbitrary web pages from misusing institution selection and tricking the user after login. In principle, this controls which URL the user is allowed to be redirected to after login, and thus where the login information is allowed to be sent.	See Identity Provider Discovery Service Protocol and Profile (section Use of Metadata), for information on this security feature. See Enabling OpenAthens Wayfinder: Shibboleth for illustrative examples of how this configuration can be done. See Redirect to SSO Service at the IdP for general information on how the web flow works when selecting the institution (DS).

5 If SAML2 Persistent NameID is used	**Specify NameID format** If the service uses SAML2 Persistent NameID for user ID transmission, the NameID format `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` must be specified in the service metadata or in the login request. **NOTE!** It is **very important** that the NameID format `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` is **not** listed as an available option in the service metadata. Otherwise, **all** NameID formats in the metadata will be ignored and the NameID may not be sent at all. **You need to let us know** if the service needs the user's actual user ID (e.g. abcd1234@user.uu.se) or the value of any other SAML attribute sent as SAML2 Persistent NameID. Otherwise, an anonymised version of the user ID will be sent by default.	

Publication of Metadata

Step	Instruction	Further Information
1	**Verify metadata before publishing** Check that your SP and service metadata meet all the requirements in SWAMID SAML WebSSO Technology Profile (section 6 Operational Requirements for Relying Parties).	
2	**Submit the service metadata to SWAMID for publication** Metadata should be published either in the `SWAMID` (IdP) metadata stream or in `SWAMID and eduGAIN` (DS). From January 2022 onwards, this is something you normally do yourself (see blog post) via the SWAMID metadata tool. Metadata tool login is done here with an account from any organisation connected to SeamlessAccess via eduGAIN. **NOTE!** When requesting publication of metadata from within the metadata tool, an email will be sent which must be manually forwarded to SWAMID Operations in order for the publication to be performed.	For further information on the metadata tool and its use, please contact SWAMID.
3	**Done! Your service is now ready to use the Joint Web Login service** **NOTE!** It is not until the metadata is published (plus a certain time delay, up to 8 hours) that Joint Web Login is aware of your service and can be used to log in to it.	

If you have any questions, please contact IT Support and ask to be put in touch with the operators of the Joint Web Login service.