SAML WebSSO Service Provider Best Current Practice

> ⓘ A company or organization that wants to provide services that rely on identities provided by SWAMID members does not usually need to become a member of SWAMID. For the SAML WebSSO technology profile the service provider only has to accept the SWAMID Metadata Terms of Use (ToU). This acceptance does not have to be communicated to SWAMID.

> ⓘ **NOTE WELL**
> Requesting registration of a service provider in SWAMID implies acceptance of the SWAMID Metadata Terms of Use (ToU).

SWAMID WebSSO Service Provider

How to provide services to users associated with SWAMID members

Is your service provider already published to the interfederation eduGAIN by another federation?

We have an opt-out policy regarding eduGAIN for SWAMID Identity Providers, so you should already been able to communicate with most SWAMID member institutions. You may need to talk to the federation that publishes your metadata to eduGAIN about which eduGAIN enabled entity categories to use to get the appropriate attributes released by our IdPs.

If you still want to register your service with SWAMID:

1. Review and decide to accept the SWAMID Metadata Terms of Use (ToU). If you accept the ToU you do *not* need to communicate this to SWAMID Operations.
2. We tag Service Providers with entity categories and encourage our IdPs to use them for attribute release. Please read through our 4.1 Entity Categories for Service Providers and decide which apply best for you. Please provide a motivation for your choice as described in the defined request processes for each entity category! SWAMID has a defined Attribute Profile that describes the normal use of attributes within the federation.
3. Email SWAMID Operations to register and publish metadata for the service provider. This step *implies* acceptance of the ToU and constitutes a legally binding agreement to abide by the ToU. Please look into step 4 in the Shibboleth Service Provider installation instructions below to make your service provider work better with users within the federation and inter-federations.
4. Integrate SWAMID Metadata into the service provider and optionally configure use of the SWAMID Discovery Service.

How to install a Shibboleth Service Provider

Step 1 - Installing a Web Server

- 1.1 Installing Apache Web Server 2.0 or higher for Shibboleth Service Provider
- 1.2 Configuring Apache Web Server to use Shibboleth
- 1.3 Configuring IIS for MS windows

Step 2 - Installing Shibboleth Service Provider

- 2.1 Installing Shibboleth SP 3.x on Linux with yum
- 2.2 Installing Shibboleth SP on Windows with IIS Web Server
- 2.3 Docker Image with apache and shibboleth
- 2.4 Shibboleth for Java Applications

Step 3 - Configuring Shibboleth Service Provider for use in the SWAMID federation

- 3.1 Configure Shibboleth SP - shibboleth2.xml
- 3.2 Configure Shibboleth SP - attribute-map.xml
- 3.3 Configure Shibboleth SP - Check for Identity Assurance or REFEDS SIRTFI
- 3.4 Configure Shibboleth SP - Automatically validate metadata with ws-* extensions for ADFS IdPs

Step 4 - Get the correct attributes from Identity Providers

To make the login work smoother for your users you need to get the right attributes from the Identity Providers. To make it more easy to get the right attributes you need to follow the instructions below.

- 4.1 Entity Categories for Service Providers is used to enable support for automatic attribute release from Identity Providers.

-
- enhance user experience in Identity Providers and Discovery Services.
- 4.4 If your service shall be available within the international academic identity federations inform SWAMID Operations that your Service Provider shall be exported to eduGAIN.
- 4.5 If nothing else helps or you need special attributes that is not part of entity categories contact the Identity Providers that you've users from and that doesn't release needed attributes.

Step 5 - Register your Service Provider metadata in SWAMID

- When you your Service Provider is ready for production you must register your metadata with SWAMID. Please send the metadata file to SWAMID Operation togther with extra metadata information from step 4.