

AAI Resource Registry Guide

Version: 20111130 Authors: LH, TL

AAI web page: <http://www.switch.ch/> Contact: aai@switch.ch

This guide is aimed at users of the SWITCH Resource Registry and is intended to serve as a complimentary source of information to explanations and examples that are already integrated into the Resource Registry. It explains the most important aspects and processes to create, maintain and administrate Home Organization and Resource Descriptions.

Note: The screenshots in this guide may not reflect the actual interface because the Resource Registry is constantly extended and developed further.

Table of Contents

1. Description of the Resource Registry.....	2
2. Login.....	3
3. Administration Interface.....	4
4. Roles.....	6
4.1. Resource administrator.....	8
Basic Resource Information.....	9
Additional Language Descriptions.....	11
List of Contacts.....	11
Keywords.....	12
Service Locations.....	12
Used Certificates.....	13
Required Attributes.....	14
Intended Audience.....	14
Submit Resource Description for Approval.....	16
Duties as a Resource Administrator.....	17
4.2. Home Organization Administrator.....	18
Bootstrapping a Home Organization Registration.....	18
General Information.....	21
Additional Language Description.....	21
Technical Information.....	23
Used Certificates.....	24
List of Contacts.....	25
Supported Attributes.....	26
Default Attribute Release Policy.....	27
Specific Attribute Release Policy.....	28
Home Organization Setup & Environment.....	28
Duties as Home Organization administrator.....	29
4.3. Resource Registration Authority Administrator.....	30
Duties as a Resource Registration Authority administrator.....	30
5. Miscellaneous.....	32
5.1. Resource Registry data usage.....	32
5.2. Facts about the Resource Registry.....	32

1. Description of the Resource Registry

The Resource Registry is a web-based tool developed by SWITCH to manage information about Resources and Home Organizations participating in the SWITCHaai and AAI Test federations, which are operated by SWITCH. Since 2011 the Resource Registry is also capable of handling interfederated Resources and Home Organisations.

The intended users of the Resource Registry are Resource and Home Organization administrators.

The Resource Registry's main purpose and features are (see Figure 1):

- **Attribute requirements declaration**

Resource administrators specify the required attributes to provide for accessing the resource. In addition, desired attributes can be listed too. Desired attributes should provide additional benefit to justify their use. The data protection principle counts: Process only data which is really necessary!

- **Intended audience declaration**

Resource administrators can also specify from which Home Organizations it will accept users. For example, a Resource is only of interest to medical students. Then, there is no point in adding that Resource to the metadata of the universities not offering medical studies at all. However, it is still the duty of the Resource to configure its authorization rules properly!

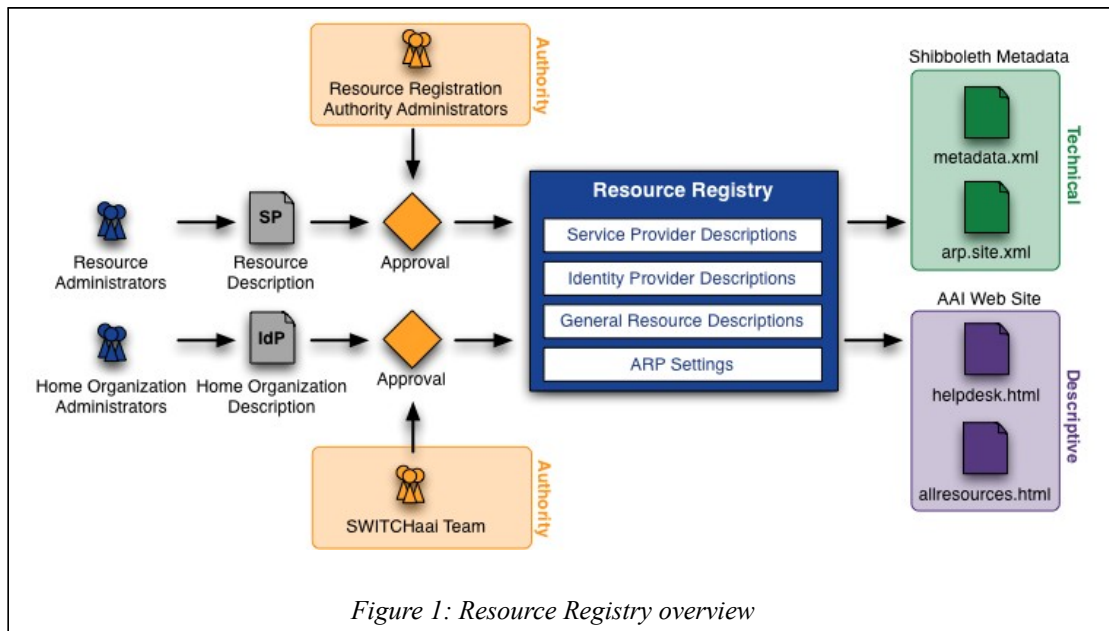


Figure 1: Resource Registry overview

- **Federation Members can control resources within their organization domain**

Each Resource needs to get approved before its entry gets activated in the Resource Registry. Each Federation Member approves Resources from its own domain and from the Federation Partners it sponsors. It delegates this control to one or more people who act as Resource Registration Authority administrators for the Federation Member. They are alerted by e-Mail, whenever approval is required for changes made to Resource Description in the Resource Registry.

- **Supported attributes declaration**

Not all of the attributes specified for SWITCHaai are mandatory to implement. The Identity Providers can document within their Resource Registry entry which ones are

implemented and potentially available to Resources.

- **Generate federation metadata**

Based on the information collected, the crucial federation metadata files for the Identity Providers as well as Service Providers can be generated. Each Identity Provider needs to know all potential Service Providers with whom it should communicate and vice versa.

- **Generate attribute release policy/filters**

Each Identity Provider has to maintain the Attribute Release Policy (ARP) configuration. The Resource Registry provides them tailored templates for the ARP and in some cases notifies the Identity Provider administrators in case of changes.

- **Generate configuration files**

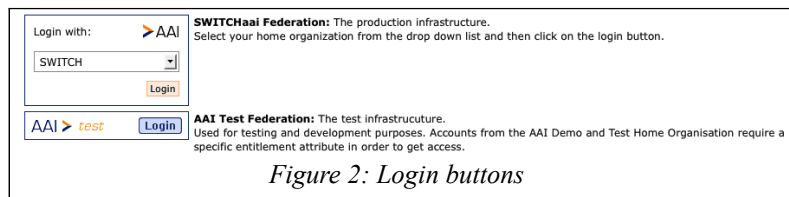
The Resource Registry can generate some configuration files for Service Providers and Identity Providers using information contained in its database.

- **Generate federation information and help pages**

Because the Resource Registry is also used to manage the attributes, attribute usage and requirement as well as contact information for all Resources and Home Organizations, it also can be used to generate various statistics and lists about to the federation.

2.Login

The Resource Registry is accessible via <https://rr.aai.switch.ch/> and requires an account in SWITCHaai or AAI Test. The start page contains a short description of the Resource Registry and two ways to log in. One can either log in using an account of a Home Organisation in the SWITCHaai Federation or the AAI Test Federation.



The Resource Registry also supports assurance levels, which can be used to ensure better authentication security.

After authentication at a Home Organization one is redirected back to the Resource Registry. Provided the Resource Registry receives all the required attributes from the Home Organization, login is successful. The Resource Registry needs the following attributes:

- Given Name (required)
- Surname (required)
- E-Mail Address (required)
- Unique ID (swissEduPersonUniqueID or eduPersonPrincipalName) (required)
- Targeted ID (optional)
- Business telephone number (optional)
- Mobile number (optional, for two-factor authentication)
- Home Organization Name (required)
- Home Organization Type (optional)

Note: When somebody is logged in via the AAI Test Federation he cannot modify Resource Descriptions or Home Organization Descriptions of the production SWITCHaai Federation. This is due to security considerations. The opposite way, editing AAI Test Resource

Descriptions with a SWITCHaai account is possible however.

When a user logs in the first time, a data storage consent screen (see Figure 3) has to be accepted first. In order to send notification e-Mails at least given name, surname and e-Mail address have to be stored in the Resource Registry database. The phone number is used in cases where an administrator needs to ask or confirm some data (e.g. fingerprint of a self-signed certificate) over the phone.

AAI Resource Registry

SWITCH
Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration | Lukas Hämmerle (switch.ch) | Logout | Help

↑ About Resource Registry
Resource Registry

Welcome to the Resource Registry

This is the first time you access the Resource Registry with the user current account. Therefore, we kindly ask you to give your consent to allow the Resource Registry to store your user data data shown below. The email address is needed by the Resource Registry to send you notification emails. The phone number may be required in order to contact you in case of emergencies or because of an out-of-band approval workflow required during resource registration.

ⓘ SWITCH won't give the personal data shown below to third parties, nor will it be published in metadata, nor will it be accessible by unauthenticated Internet users.

User Information that will be stored for Resource Registry	
Given Name	Lukas
Surname	Hämmerle
Phone number	+41 44 268 15 64
Home Organization Name	switch.ch
Home Organization Type	others
Affiliation	staff
E-Mail	lukas.haemmerle@switch.ch
Data protection	<input type="radio"/> I agree that an entry representing myself with the above data will be stored in the AAI Resource Registry database.

This field must be provided

Figure 3: Resource Registry data storage consent

Note: In case you just have set up a Home Organization but it is not yet registered in the Resource Registry, read the section 'Home Organization Administrator' on how to register a Home Organization for the first time.

3. Administration Interface



Figure 4: Main Menu

After successful authentication, one sees the main menu of the Resource Registry. Depending on the privileges and roles (see Chapter 4), there are between two and five different links in the navigation bar. They reflect the administration and access rights a user has.

Note: To log out of the Resource Registry (and all other AAI-enabled applications), the easiest and safest way is to just close the web browser. This will destroy all sessions that you may have for the Resource Registry, the WAYF and your Identity Provider. However, there also is a logout link at the bottom of the page that will destroy the Shibboleth session as well as the Resource Registry session of the currently logged in user. However, other sessions like the one at the Identity Provider where the user was authenticated won't be affected.

Figure 5 shows the 'General Information' section that provides various lists, search forms as well as matrixes that describe the federations managed by the Resource Registry. All users of the Resource Registry have access to this section.

Figure 5 shows the 'Resource Administration' options. If a user has no administration privileges for any Resource Descriptions he can only add new Resource Descriptions. Otherwise, a user will see links to manage all his approved Resource Descriptions.

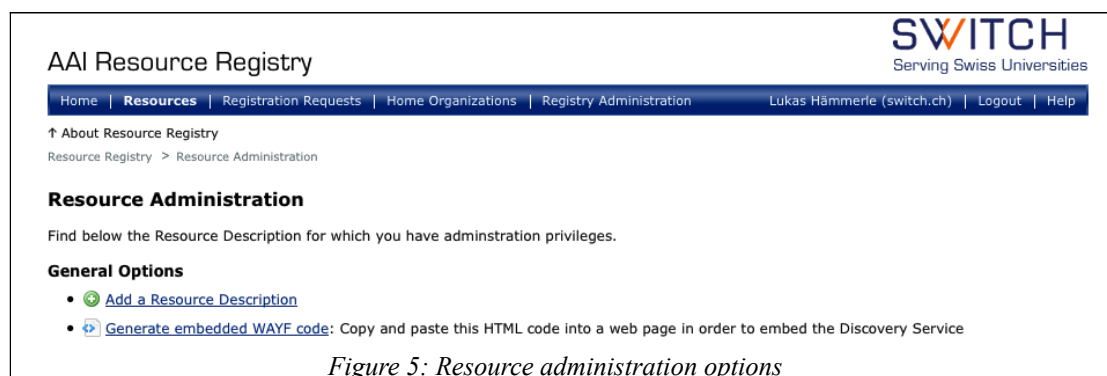


Figure 5: Resource administration options

When you have registered a resource and if it was approved by a Resource Registration Authority (RRA) administrator (see Chapter 4) of your Home Organization, the Resource Administration section looks like in Figure 6.

AAI Resource Registry

Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration | Lukas Hämmerle (switch.ch) | Logout | Help

↑ [About Resource Registry](#)

Resource Registry > Resource Administration

Resource Administration

Find below the Resource Description for which you have administration privileges.

General Options

- [Add a Resource Description](#)
- [Generate embedded WAYF code](#): Copy and paste this HTML code into a web page in order to embed the Discovery Service

Approved Resource Descriptions

- **AAI Attributes Viewer** (<https://aai-viewer.switch.ch/shibboleth, SWITCHaai>)
 - [View](#) | [Edit](#) | [Duplicate](#) | [Delete](#) | [Administrators](#) | [Deployment guide and configuration](#)
- **AAI Tools** (<https://tools.aai.switch.ch/shibboleth, SWITCHaai>)
 - [View](#) | [Edit](#) | [Duplicate](#) | [Delete](#) | [Administrators](#) | [Deployment guide and configuration](#)
- **AAI Viewer Interfederation Test** (<https://aai-viewer.switch.ch/interfederation-test/shibboleth, SWITCHaai>)
 - [View](#) | [Edit](#) | [Duplicate](#) | [Delete](#) | [Administrators](#) | [Deployment guide and configuration](#)

Figure 6: View with multiple approved Resource Descriptions

For Home Organization administrators, the corresponding administration options look like in Figure 7.

AAI Resource Registry

Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration | Lukas Hämmerle (switch.ch) | Logout | Help

↑ [About Resource Registry](#)

Resource Registry > Home Organisations Administration

Home Organisations Administration

Find below the Home Organisation descriptions for which you have administration privileges.

- **SWITCH** (SWITCHaai)
 - [View Home Organization Description](#): Textual representation of this Home Organization
 - [List Resource Descriptions registered for this Home Organisation](#)
 - [Edit Home Organization Description](#): Modify technical or descriptive attributes
 - [attribute-filter.xml](#): Custom-tailored attribute filter files
 - [Manage Home Organisation administrators](#): Transfer or revoke Home Organisation administration privileges
 - [View all administrators](#): See who has which administration privileges within your organization
- **VHO - Virtual Home Organization @SWITCHaai** (SWITCHaai)
 - [View Home Organization Description](#): Textual representation of this Home Organization
 - [List Resource Descriptions registered for this Home Organisation](#)
 - [Edit Home Organization Description](#): Modify technical or descriptive attributes
 - [attribute-filter.xml](#): Custom-tailored attribute filter files
 - [Manage Home Organisation administrators](#): Transfer or revoke Home Organisation administration privileges
 - [View all administrators](#): See who has which administration privileges within your organization

Figure 7: Home Organization administration options

The options for a Resource Registration Authority administrator look like in Figure 8.

AAI Resource Registry SWITCH
Serving Swiss Universities

Home | Resources | **Registration Requests** | Home Organizations | Registry Administration | Lukas Hämmerle (switch.ch) | Logout | Help

↑ About Resource Registry
Resource Registry > Registry Registration Authority Requests

Resource Registrations Authority Requests

Find below the Home Organisations for which you have Resource Registration Authority (RRA) privileges. The duty of an RRA administrator is to check and approve changes or Resource Descriptions.

- [Add a custom local attribute definition](#) for use within your organisation
- **SWITCH** (SWITCHaai)
 - [Approve Resources](#): Approve or reject new or modified Resource Descriptions
 - There are no resources to approve
 - [Approved Resource Descriptions](#): All resources registered in the name of this organization
 - [Manage administrators](#): Transfer or revoke administration privileges
 - [View all administrators](#): See who has which administration privileges within your organization
- **VHO - Virtual Home Organization @SWITCHaai** (SWITCHaai)
 - [Approve Resources](#): Approve or reject new or modified Resource Descriptions
 - There are no resources to approve
 - [Approved Resource Descriptions](#): All resources registered in the name of this organization
 - [Manage administrators](#): Transfer or revoke administration privileges
 - [View all administrators](#): See who has which administration privileges within your organization

Figure 8: Resource Registration Authority administration options

Note: You may not see all of the above administration options because you may not have the required roles to see them.

4. Roles

Every user in the Resource Registry can have one or more roles with additional administration privileges. These are:

- Resource administrator (of a Resource)
Registers and manages one or more Resource Descriptions. See Chapter 4.1.
- Home Organization administrator (of a Home Organisation)
At least one person per Home Organization. Manages Home Organization Description and attribute release settings. See Chapter 4.2.
- Resource Registration Authority administrator (of a Home Organisation)
At least one person per Home Organization. Approves or rejects new or modified Resource Descriptions. See Chapter 4.3.
- Resource Registry Operator (for everything)
Can view, edit and delete any entry. May require two-factor authentication. This role is reserved for operators of the Resource Registry.

When a user logs in for the first time he has none of the above roles assigned unless he was invited by another administrator. All administrator roles can be transferred to any other user with an AAI account. E.g. the administrator of Home Organization X could make any other user with an AAI account an administrator of X. Vice versa any Home Organization administrator can revoke rights for users of the same the Home Organization he has the rights for.

AAI Resource Registry SWITCH
Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration Lukas Hämmerle (switch.ch) | Logout | Help

↑ About Resource Registry
Resource Registry > Registry Registration Authority Requests > Administration Rights

Administration Rights

Manage Registration Authority Administrators for AAI Demo Home Organisation

Grant or revoke administration rights by choosing the available option for each user:

Users with Registration Authority rights	
Alessandra Scicchitano	Registration Authority administrator
Halm Reusser	Registration Authority administrator
Lukas Hämmerle	Registration Authority administrator
Valéry Tschopp	Registration Authority administrator
Users from AAI Demo Home Organisation without Registration Authority rights	
Dominic Stellwag	
Khaled Zaidan	

Delegate Registration Authority rights to any AAI user using an invitation email.
Add a comma- or space-separated list of e-mail addresses of people you want to grant Registration Authority rights too. Any email address can be used as long as the recipient has an AAI account.

Cancel Reset Apply Save and go back to menu

Figure 9: Manage administration rights

Figure 9 illustrates how to grant or revoke Resource Registration Authority rights to or from other users. Users can be invited by manually entering their e-Mail addresses in the text area at the bottom of the page. The invited users receive an e-Mail containing an invitation link that will grant them the administration rights that were bound to this invitation.

AAI Resource Registry SWITCH
Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration Lukas Hämmerle (switch.ch) | Logout | Help

↑ About Resource Registry
Resource Registry > Registry Registration Authority Requests > Administration Rights

Administration Rights

Manage Registration Authority Administrators for AAI Demo Home Organisation

Grant or revoke administration rights by choosing the available option for each user:

Users with Registration Authority rights	
Alessandra Scicchitano	Registration Authority administrator
Halm Reusser	Registration Authority administrator
Lukas Hämmerle	Registration Authority administrator
Valéry Tschopp	Registration Authority administrator
Pending Administration Invitations	
patrick.schnellmann@switch.ch	Pending
Users from AAI Demo Home Organisation without Registration Authority rights	
Dominic Stellwag	
Khaled Zaidan	

Delegate Registration Authority rights to any AAI user using an invitation email.
Add a comma- or space-separated list of e-mail addresses of people you want to grant Registration Authority rights too. Any email address can be used as long as the recipient has an AAI account.

Cancel Reset Apply Save and go back to menu

An invitation mail has been sent to the following users: patrick.schnellmann@switch.ch

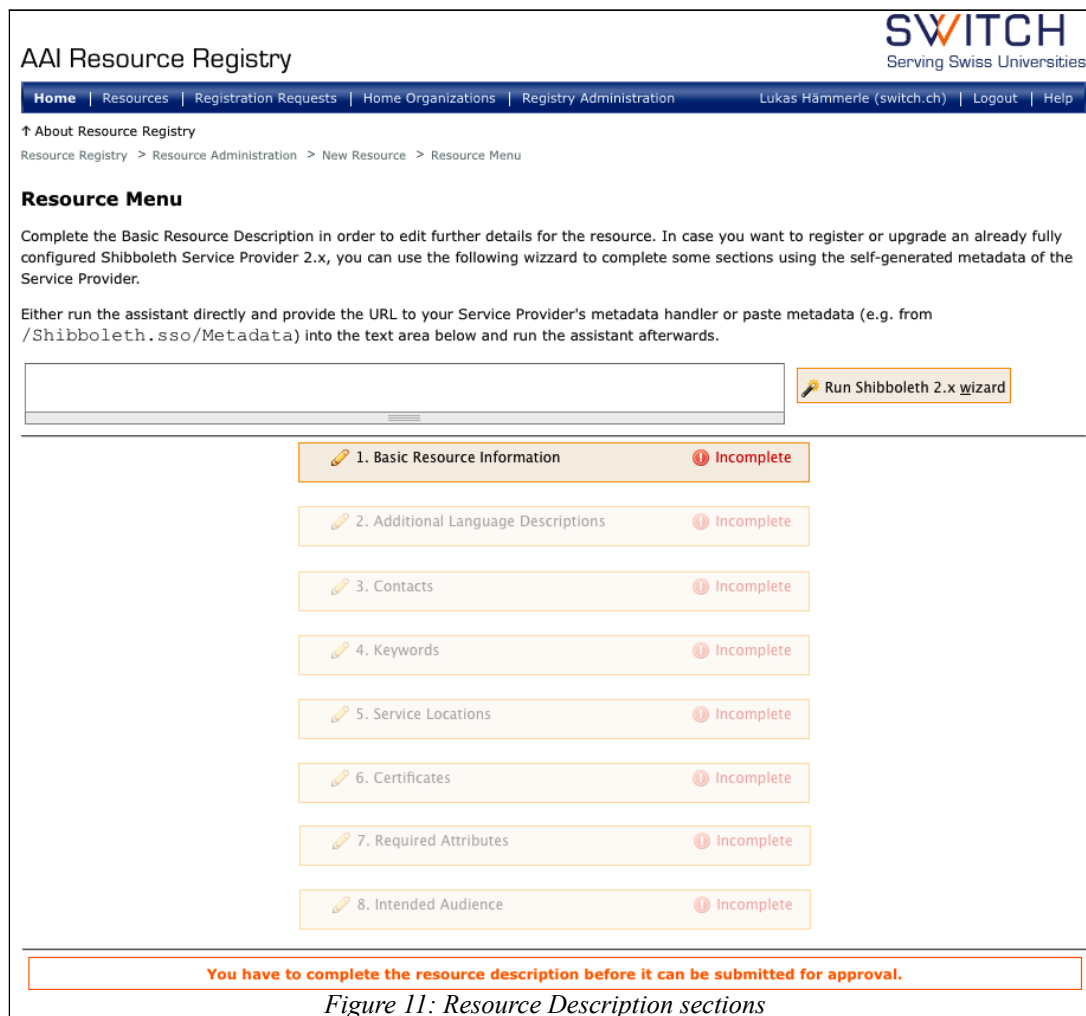
Figure 10 shows a situation where there is a pending invitation and where a user from a

different Home Organization also has administration privileges. As can be seen, invitations can also be revoked from an invited user.

In the following chapters the three above-mentioned administrator roles are illustrated in greater detail.

4.1.Resource Administrator

Unless you were invited as a Resource administrator, you find the Resource administrator options empty as shown in Figure 5. So, the only option will be to add a Resource Description. Clicking the link 'Add a Resource Description' one sees a page like in Figure 11.



The screenshot displays the 'AAI Resource Registry' interface. At the top right is the SWITCH logo with the tagline 'Serving Swiss Universities'. Below the logo is a navigation bar with links for Home, Resources, Registration Requests, Home Organizations, Registry Administration, and user information (Lukas Hämmerle (switch.ch) | Logout | Help). The main content area is titled 'Resource Menu' and includes instructions on how to complete the resource description, mentioning the Shibboleth 2.x wizard and the option to paste metadata. A text input field is provided for the URL. Below this is a list of 8 sections, each with a pencil icon and a red 'Incomplete' status: 1. Basic Resource Information, 2. Additional Language Descriptions, 3. Contacts, 4. Keywords, 5. Service Locations, 6. Certificates, 7. Required Attributes, and 8. Intended Audience. A 'Run Shibboleth 2.x wizard' button is located to the right of the input field. At the bottom, a red-bordered box contains the warning: 'You have to complete the resource description before it can be submitted for approval.'

Figure 11: Resource Description sections

As can be seen in Figure 11, the Resource Description contains several sections, each of them should but not all of them have to be completed, and some of them won't require more input because of reasonable default values. When all sections are marked green, the Resource Description can be submitted for approval.

Note: In case you already have an installed and configured Shibboleth 2.0 Service Provider, you can use the Shibboleth 2.0 wizard that completes many of the required sections by using the Service Provider's self-generated Metadata. In order to use the wizard, you will have to provide the URL to the Service Provider's Metadata handler URL. Alternatively, you can

also provide metadata directly in case the Service Provider is not (yet) reachable via the network.

Basic Resource Information

The Basic Resource Information section is for providing the most essential details of the Resource Description. You must complete this section first before you can continue further, which is why they are grayed out beforehand.

In Figure 12 you see an example of this section:

AAI Resource Registry **SWITCH**
Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration Lukas Hämmerle (switch.ch) | Logout | Help

↑ About Resource Registry
Resource Registry > Resource Administration > AAI Wiki - Waaikiki > Basic Resource Information

Basic Resource Information

Basic Properties

Home Organization
You can register resources only

- for Home Organizations which you have an AAI account for
- for which you are Resource Registration Authority (RRA) administrator
- for Home Organizations in the AAI Test Federation

Federation Partner

Name
English name of the Resource or Service, e.g. "SWITCH e-Conferencing Portal", "ETHZ CompiCampus".

Description
Short English description of the resource.

Technical Information

Entity ID
Unique identifier in form of a URL.
This value should be configured in your Shibboleth configuration file (e.g. /etc/shibboleth2/shibboleth2.xml or /etc/shibboleth/shibboleth.xml). It should be 'stable' and not change, even if the hostname changes.
The convention is to set this to https://<HOSTNAME>/shibboleth, e.g. https://www.olat.uzh.ch/shibboleth.
Modifying this value will cause service interruptions. Please ask the [Resource Registry webmaster](#) before you change it.

Relying Party
Including the Service Provider in a non-default relying party allows controlling the behaviour of how the attributes are transmitted from the Identity Provider to the Service Provider. Only change this if you know the implications of the change.
SAML1 Attribute Push is faster, more reliable but less secure because attributes are sent unencrypted via the user's web browser. Therefore, this is mostly suited for resources that require no personal attributes.

Home and Helpdesk URLs

Home URL
The entry point URL or home page of the resource: e.g. https://sp.example.org/index.html
This page may or may not be AAI-protected.

Helpdesk URL
A web page that offers users help and guidance in case of AAI related problems with the resource

Validity

Valid from
Set this to a future date in order to make only active by then. As long as a resource is inactive, it is hidden in the metadata and in the [list of public resources](#).

Valid until
Set these fields to '-' in order to make the Resource Description valid indefinitely.

Visibility

Public
If checked, this Resource Description will show up in the [list of public resources](#).

• This field must be provided

Figure 12: Basic Resource Description

First you have to decide for which federation and for which Home Organization you register a Resource. You can only register Resources for Home Organizations that you have an

account for or for which you are Resource Registration Administrator of or for AAI Test Home Organizations.

If you are testing something related to AAI and if no real users are involved, choose a Home Organization from the AAI Test Federation if possible.

The entityID (formerly known as providerId) is of great importance because it is the identifier for a resource. Be sure to check that you insert the value that you configured or will configure in shibboleth2.xml file of your Shibboleth Service Provider if you haven't already.

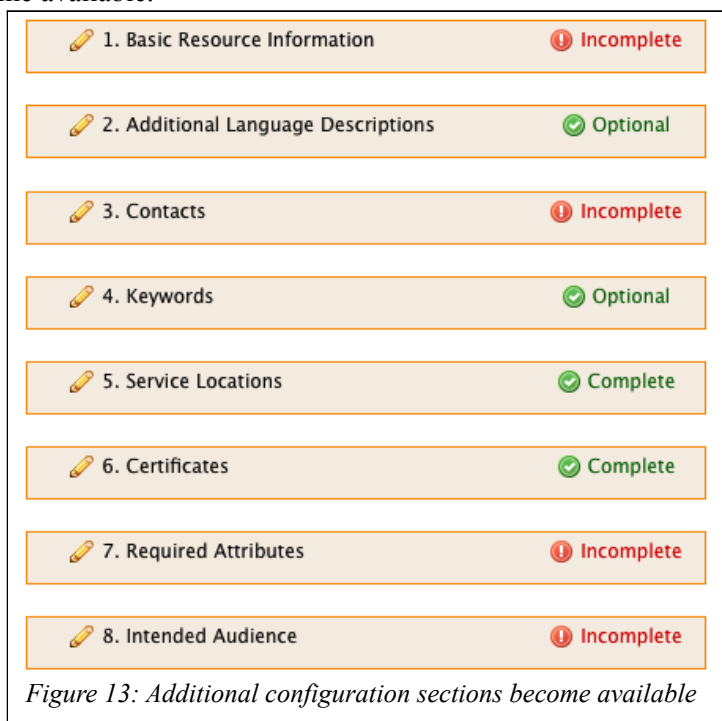
Warning: Don't change the entityID unless you know exactly what you are doing. A change of this value as well as some other values must propagate to all Identity Provider first before it becomes active. The propagation time can be up to one day where your service may not be accessible from Identity Providers, which haven't yet downloaded the latest metadata file.

Relying Party: Depending in which relying party a resource is, it has to fetch the attributes from an identity provider or it receives the attributes directly via an authenticated user's web browser. For most cases, it is recommended to leave this with the default setting.

Validity: If your resource is only temporarily available or shall only become active sometime in the future, you can specify this in the resource validity section. A Resource only is mentioned in the metadata and ARP files if it is valid at the moment the metadata is generated.

Visibility: Un-checking the public checkbox will hide the Resource Description within the Resource Registry from non-RRA users and in public resource lists on the SWITCH web page. It also will affect the metadata and ARP generation in the sense that name and description of the resource won't be included in these files.

After the form was successfully submitted, one returns to the resource menu that contains all the configuration sections of the Resource Description. As you can see, additional options have now become available.



Additional Language Descriptions

The multilingual language descriptions can be used to supply a name and a description for the Resource in multiple languages. These additional descriptions then will be shown on public resource listing web pages provided the visibility is marked public.

List of Contacts

Additional Language Descriptions

Main language English English
Language that this resource's name and description shall be displayed as default.

English

Name AAI Attributes Viewer

Description The AAI Attribute Viewer is a service that displays all available attributes of a user. This is useful for development and debugging. Attributes are stored 10 days in a log file.
You can modify the above entry on the [Resource Basic](#) page

German

Name Attributes Viewer

Description Der AAI Attribute Viewer ist ein Dienst, der alle verfügbaren Attribute eines Benutzers anzeigt. Attribute werden 10 Tage in einer Logdatei aufbewahrt.

French

Name

Description

Italian

Name

Description

This field must be provided

Figure 14: Resource contacts

At least three contacts must be provided for every Resource: an administrative, a technical and a support contact. These then will be shown on the Resource Registry itself as well as on SWITCH's public resource list as well as in the federation metadata. As can be seen in Figure 14, more than three contacts could be provided if needed.

Note: Support and technical contact names and addresses should be non-personal if possible. It should also be taken into account that these addresses will show up not only in the federation metadata but also on the list of all SWITCHaai Home Organizations.

Keywords

Adding keywords that describe the resource, allows searching for specific resources within the Resource Registry.

Service Locations

In this section, which is shown in Figure 15, you define the SAML endpoint URLs of the Service Provider. If you were using the wizard, this section probably already was completed for you. Otherwise, the easiest way to complete it is to use one of the assistants. If you plan to operate the resource using multiple host names, you should provide service locations for all host names protected by your Service Provider.

If you run one of the above assistants and your Service Provider serves multiple hostnames, provide the Shibboleth handler URLs separated with commas, e.g. <https://host1.ch/Shibboleth.sso>, <https://other.host.ch/secure/Shibboleth.sso>, <http://insecure.host.ch/unprotected/Shibboleth.sso>

Assertion Consumer Service	
SAML1 browser-post binding	<input type="text" value="https://aai-viewer.switch.ch/Shibboleth.sso/SAML/POST"/>
	Binding URN: urn:oasis:names:tc:SAML:1.0:profiles:browser-post
SAML1 artifact-01 binding	<input type="text" value="https://aai-viewer.switch.ch/Shibboleth.sso/SAML/Artifact"/>
	Binding URN: urn:oasis:names:tc:SAML:1.0:profiles:artifact-01
SAML2 HTTP-POST binding	<input type="text" value="https://aai-viewer.switch.ch/Shibboleth.sso/SAML2/POST"/>
	Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

Figure 15: Service location endpoint URLs

Warning: Changes in this section need to propagate first to all identity providers before they become active.

Note: Although you will see endpoint URLs for multiple SAML 2 Single Logout Services, this feature so far has only been implemented on the Service Provider side. However, in order for it to work as expected the Identity Provider first has to support this feature as well. Unfortunately, Single Logout is a problem that is very difficult to solve¹ for various reasons, which it hasn't been implemented yet as of Shibboleth 2.2.

Used Certificates

Certificate Information	
<input type="button" value="Run assistant..."/> Use the assistant to complete the form automatically.	
Embedded certificates	
PEM certificate	<pre>-----BEGIN CERTIFICATE----- MIIFRzCCBC+gAwIBAgICMcUwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCk0x GTAXBgNVBAoTEFF1b1ZhbG1zIEExpbW10ZWQxHzAdBgNVBAsTFnd3dy5xdW92YWRp c2dsb2JhbC51 DTEwMTIwNjA1 AxMCQ0gxFTA1 dXNlIDUoYik -----END CERTIFICATE-----</pre> <p> Subject: / CN=aai-viewer.switch.ch Type: Self-signed Key Length: 2048 Expiration date: Jul 24 11:49:27 2014 GMT Fingerprint: 23:AC:5B:F2:48:4A:7B:D0:4E:B7:53:2C:24:B6:B5:28:96:16:82:1C </p>
Additional PEM certificate	<pre>-----BEGIN CERTIFICATE----- MIIDLCCAhS BAMTFGFhaS1 NDExNDkyN1o CSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQDTAMxt4JA8xURwcdSfv8orb41uix+4 bSsn2Vap1V2UZz/5JLm6OuCqvRHu94zdW03jsFDCfeWD1JGFm0W+vQ4f0PHe3XE hnOWY2+kpkXt5N699Bt1JC5U5b2512txWmKwyqNL66MwTh5qpAd+Helph+WwzMCS -----END CERTIFICATE-----</pre> <p> Note: ✔ This certificate was previously approved by an RRA administrator. Therefore, it won't need the fingerprint approval procedure again. </p>
Use the additional certificate for certificate roll over if an older certificate is used, make sure it is already configured for the Service Provider, otherwise encrypted assertions cannot be decrypted yet.	
Click in a textarea containing a certificate to see additional certificate details.	
Certificate Subject Common Name (deprecated)	
CN of the certificate subject	<input type="text"/> <p>Providing a certificate subject name is deprecated.</p>
<input type="button" value="Back"/> <input type="button" value="To Resource Menu"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Save and Continue"/>	

Figure 16: Used certificates

In this section one has to provide the X.509 PEM certificate, which is used by the Shibboleth Service Provider. Please have a look at the certificate requirements page which are linked on this page. As is shown in Figure 16, a second certificate can be added as a backup certificate for roll-over procedures. If have to renew a certificate, please also have a

¹ Also see <https://spaces.internet2.edu/display/SHIB2/SLOIssues> for more detailed explanations

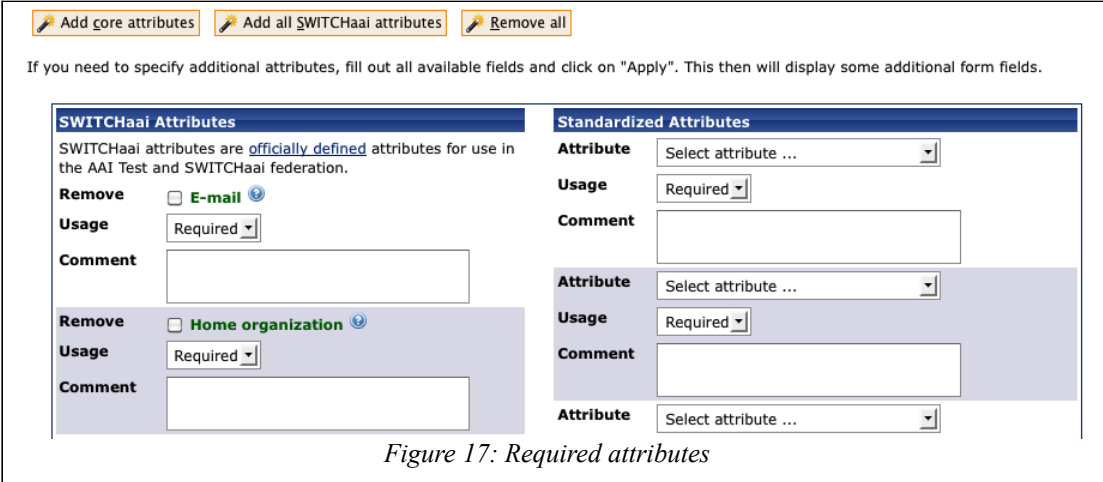
look at the certificate migration guide which is also linked. The order of the two certificates doesn't matter.

Warning: Changes in this section need to propagate first to all Identity Providers before they become active.

Required Attributes

The Required attributes section is very important because it directly affects the Attribute Release Policies of all Identity Providers. As shown in Figure 17, one has to declare which attributes a Resource requires in order to work and which attributes are desired/nice to have. It is recommended to provide a short comment for all attributes why they are required or desired.

The attributes on the right-hand side of the page are local attribute, that are not officially supported but can be used by some Home Organizations for internal or bilateral use.



Add core attributes Add all SWITCHAai attributes Remove all

If you need to specify additional attributes, fill out all available fields and click on "Apply". This then will display some additional form fields.

SWITCHAai Attributes	Standardized Attributes
SWITCHAai attributes are <u>officially defined</u> attributes for use in the AAI Test and SWITCHAai federation.	Attribute Select attribute ...
Remove <input type="checkbox"/> E-mail	Usage Required
Usage Required	Comment
Comment	Attribute Select attribute ...
Remove <input type="checkbox"/> Home organization	Usage Required
Usage Required	Comment
Comment	Attribute Select attribute ...

Figure 17: Required attributes

Note: Please keep in mind that the Swiss data protection law states that only absolutely necessary user information shall be requested and processed. This implies that you should declare only attributes as 'required' that are essential for the proper functioning of a Resource.

Intended Audience

The last section of a Resource Description configures the intended audience settings of the Resource. Assume your Resource is an e-learning tool for medical students. In that case it makes no sense to allow users from a university not offering medical studies to access it. On the other hand, you may want that SWITCH staff members can access the Resource for debugging or development purposes. So, one probably would protect a Resource in the web server's configuration with access control rules like:

```
AuthType shibboleth
ShibRequireSession On
ShibExportAssertion On
require homeOrganizationType university hospital
require homeOrganization switch.ch
```

Therefore, one should declare the intended audience in the Resource Registry for this example as shown in Figure 18.

Interfederation

Interfederation **Enable interfederation for this resource**
Activate this checkbox if the resource shall be accessed by users from non-SWITCHaai organizations.

Enabling interfederation means that metadata about this resource is published in non-SWITCHaai organization and can be used by other Identity Providers which are not part of SWITCHaai. The metadata will also include contact information about this resource. Before enabling interfederation support for this resource, make sure that:

- That the `attribute-map.xml` and `attribute-policy.xml` contain configurations that support all the attributes that may be received from interfederation Home Organisations.
- That the [access control rules](#) are set properly.

Default Intended Audience

University users are generally ...	included ▾
University of Applied Sciences users are generally ...	included ▾
Hospital users are generally ...	included ▾
Library users are generally ...	included ▾
Virtual Home Organization users are generally ...	included ▾
Others users are generally ...	included ▾

Specific Intended Audience

This section allows defining exceptions to the above default intended audience. The settings below have always precedence over the default audience settings.

1.	<input type="text" value="Lookup"/>	<input type="text" value="Choose a Home Organization..."/>	<input type="text" value="... and a policy"/>	
	<input type="text" value="Lookup"/>	<input type="text" value="Choose a Home Organization..."/>	<input type="text" value="... and a policy"/>	
	<input type="text" value="Lookup"/>	<input type="text" value="Choose a Home Organization..."/>	<input type="text" value="... and a policy"/>	

To define more than 3 exceptions, fill out all entries and click on "Apply" to display additional entries.
To delete an entry, set it to the top option of the drop-down list and click on "Apply".

Figure 18: Intended audience

At the top of the page there might be a special section called “Interfederation”. The interfederation checkbox is only visible if the organization as a whole was enabled for interfederation. Please contact aai@switch.ch for further information about interfederation support and how to enable it.

This section as well as the “Required Attributes” sections have a direct influence on the ARP and attribute filter files that are generated for each Home Organization. In the attribute filter files of a Home Organization only those Resources will appear which included this Home Organization to the intended audience.

Note: Be accurate but not too restrictive when declaring filling out this form because the settings on this page also will affect the Attribute Release Policy of the Identity Providers.

Submit Resource Description for Approval

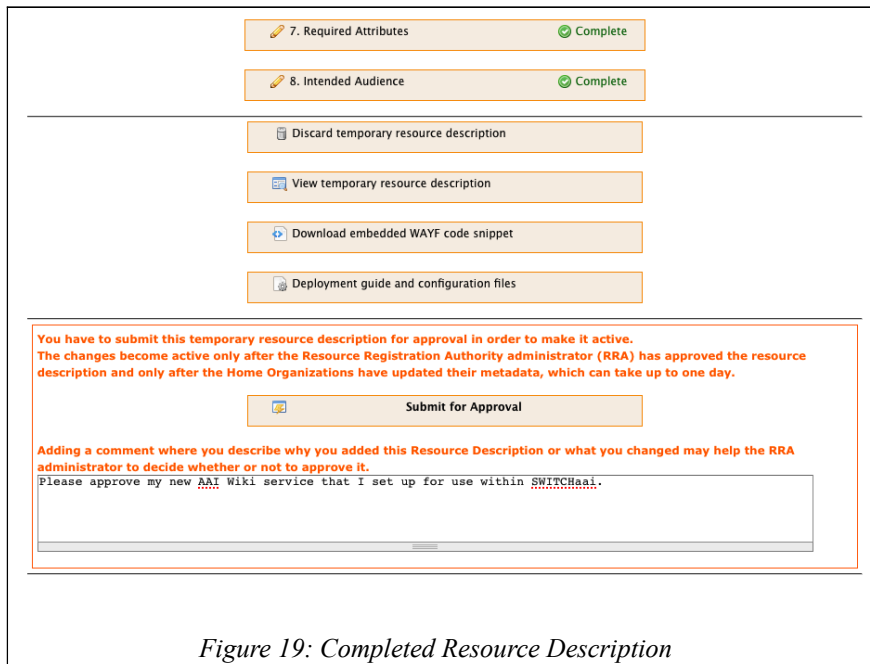


Figure 19: Completed Resource Description

Finally, if all sections were completed, the Resource Description has to be submitted and approved before it becomes active. One of the Resource Registration Authority (RRA) administrators for your Home Organization has to examine and approve it. He will check whether you are eligible to register a Resource Description in the name of your organization, whether the service URLs you provided are within your organisation's domain, whether the attribute requirements comply with the AAI Policies and the Swiss data protection law, etc.

There is also a button to discard the temporary Resource Description, which will delete all changes that were made to an already approved Resource Description or will completely delete a not yet approved Resource Description.

Official Contacts	
Type	Administrative
Name	SWITCHaai Team aai@switch.ch , Phone: +41 44 268 15 05
Type	Support
Name	SWITCHaai Team aai@switch.ch , Phone: +41 44 268 15 05
Type	>Technical
Name	SWITCHaai Team aai@switch.ch , Phone: +41 44 268 15 05
Type	<Technical
Name	>Lukas Hämmerle lukas.haemmerle@switch.ch , Phone: +41 44 268 15 64

Figure 20: Resource Description Changes

Clicking on the 'View complete temporary resource description' button will show all changes (highlighted in yellow) that were applied to the last approved version, as shown in Figure 20.

Using information available in the Resource Description, one also can download custom-tailored configuration files to configure Shibboleth 2.x Service Providers. This is depicted in Figure 21. Selecting the setup that was used to install the Service Provider and providing the paths to certificate/key pair, one is redirected to the corresponding deployment guide where all needed configuration files can be directly downloaded.

AAI Resource Registry SWITCH
Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration | Lukas Hämmerle (switch.ch) | Logout | Help

↑ About Resource Registry
Resource Registry > Resource Administration > AAI Attributes Viewer > Service Provider Configuration

Service Provider Configuration

**Custom-tailored Service Provider 2.x Deployment Guide for:
AAI Attributes Viewer**

If you complete the form below and click on "Go to guides and configuration files", you will be redirected to a specific deployment guide that is custom-tailored for this Service Provider. You then also can create a book-mark of that link for later use.

Deployment settings

Installation setup
Choosing the installation setup will set some default values

Path to installation directory
This should be the parent directory of the shibboleth directory

Path to configuration directory
This usually is /etc/shibboleth for most Unix based operating systems.

Path to logging directory
This usually is /var/log/shibboleth for most Unix based operating systems.

Path to X.509 certificate
Provide an absolute or relative path (seen from the shibboleth/etc directory) to the certificate file that shall be used by Shibboleth.

Path to X.509 private key
Provide an absolute or relative path (seen from the etc/shibboleth directory) path to the private key file that shall be used by Shibboleth.

• This field must be provided

Figure 21: Download custom Service Provider configuration files

If one clicks on the 'Submit for Approval' button, an e-Mail is sent to all RRA administrators with the request to approve the Resource Description. It is recommended to add a comment in the text field for the RRA administrator, e.g. to describe what this Resource is used for or what and why something was changed. This is very useful for the RRA administrator in order to decide whether the changes are justified or not.

After a Resource has been approved, it is included in the official federation metadata at the full hour or earlier. It also will be included in the attribute release policy/filter files of the Identity Providers. Furthermore, you also become the initial administrator of the Resource Description together with any additional users you invited via email during completion of the Basic Resource Information section. The role of a Resource Administrator can be transferred also to other users later on.

Duties as a Resource Administrator

It is essential for the stability of a service that Resource Descriptions are as up-to-date as possible. Therefore, a Resource administrator should update the Resource Description as soon as a technical property has changed. E.g. this could for instance be adding an additional service location/host name or adding an additional rollover certificate or adding/removing requested attributes.

Note: Keep in mind that there is a propagation delay for changes applied to a Resource Description. First due to the required approval of the RRA administrator and second due to the delay for metadata refresh at the Home Organizations. The official metadata published by SWITCH is updated at least every full hour if something changed. The Identity Provider should update metadata at least once a day, most will update hourly.

Warning: Replacing or modifying certain Resource Description properties like certificates or service locations has to be done very carefully because these changes will take some time

to propagate to all Identity Providers. The propagation via the metadata may take up to one day during which your Resource may not be available because some Identity Providers may still use metadata with old properties while other Identity Providers are already using the new properties. If in doubt about a property you want to change, please send an email to aai@switch.ch for assistance.

4.2.Home Organization Administrator

When an organization decides to join the SWITCHaai or the AAI Test Federation, it has to set up an Identity Provider on the technical side and it has – in the case of SWITCHaai - to sign the SWITCHaai Service Agreement. When these two steps have been completed, the new Home Organization has to be registered with the Resource Registry. In order to do so, a Home Organization administrator has to provide the necessary (technical) information that resources require to communicate with that Home Organization.

Bootstrapping a Home Organization Registration.

After setting up of the new Identity Provider, has to go to <https://rr.aai.switch.ch/>. On the first page, you will find a link that guides you to the Home Organization Bootstrapping form.

If your newly set up Identity Provider is not yet registered for any of the above federations, you won't be able to log in yet. In this case, please complete the [Home Organization Bootstrap form](#). You then will be granted access to the Resource Registry after we reconfigured it.
Should you have problems accessing the Resource Registry or have any question, please contact the AAI team by phone on +41 (0)44 268 15 05 or email aai@switch.ch.

Figure 22: Bootstrapping procedure

On the following page some basic technical details about the Home Organization have to be provided.

General Information	
Home Organization Name	<input type="text" value="example.org"/> Usually the second of your organization, e.g. 'switch.ch', 'uzh.ch', 'zhwin.ch' or the fully qualified domain name of the host serving as Identity Provider, e.g. 'test-idp.switch.ch', 'caesar.ethz.ch'.
Federation	<input type="text" value="AAI Test Federation"/>
Technical Information	
entityID	<input type="text" value="https://idp.example.org/idp/shibboleth"/> Use a URL like https://<SERVICE-HOSTNAME>/idp/shibboleth. This URL does not have yet to resolve to a web page but it should later be possible to place an XML file at this location.
Although SAML 2 is becoming the standard for many federated identity management systems around the world, there still are many services that can only interoperate with SAML 1. Therefore, it still is mandatory for SWITCHaai to support SAML 1. This is the reason why this initial setup still requires SAML 1 endpoints to be provided. After the Identity Provider is bootstrapped, SAML 2 endpoints can be defined too.	
URL of SAML 1 Single Sign-on Handler	<input type="text" value="https://idp.example.org/idp/profile/Shibboleth/SSO"/> Location of the Shibboleth SSO-Handler. For Shibboleth 2.x this URL typically is of the form https://idp.example.ch/idp/profile/Shibboleth/SSO
Identity Provider Certificate	<input type="text"/> The PEM encoded X.509 certificate that is used by the Identity Provider to sign assertions. The certificate must meet the SWITCHaai certificate requirements
URL of SAML 1 Attribute Authority	<input type="text" value="https://idp.example.org:8443/idp/profile/SAML1/SOAP/AttributeQuery"/> In Shibboleth 2.x the location of the SAML 1.1 Attribute Authority typically is of the form https://idp-aa.example.org/idp/profile/SAML1/SOAP/AttributeQuery or https://idp.example.org:8443/idp/profile/SAML1/SOAP/AttributeQuery
Attribute Authority certificate	<input type="text"/> The PEM encoded X.509 certificate that is used by the web server of the Attribute Authority host.
Contact	
Given name	<input type="text"/>
Surname	<input type="text"/>
E-Mail	<input type="text"/>
In case we have questions regarding information you provided.	
<input type="button" value="Reset"/> <input type="button" value="Submit and wait for approval"/>	
<input type="radio"/> This field must be provided	

Figure 23: Bootstrapping registration form

Fill in the required information and click on the submit button afterwards.

Note: For now, one can register an Identity Providers only with SAML 1 endpoints for this bootstrapping process. After the Home Organization was approved by SWITCH, the Home Organization administrator can then also complete the description with SAML 2 endpoints.

AAI Resource Registry



Serving Swiss Universities

Home
Resources
Registration Requests
Home Organizations
Registry Administration
Lukas Hämmerle (switch.ch)
Logout
Help

↑ About Resource Registry

Resource Registry > Home Organisations Administration

Home Organisations Administration

Find below the Home Organisation descriptions for which you have administration privileges.

-  SWITCH (SWITCHaai)
 - [View Home Organization Description](#): Textual representation of this Home Organization
 - [List Resource Descriptions registered for this Home Organisation](#)
 - [Edit Home Organization Description](#): Modify technical or descriptive attributes
 - [attribute-filter.xml](#): Custom-tailored attribute filter files
 - [Manage Home Organisation administrators](#): Transfer or revoke Home Organisation administration privileges
 - [View all administrators](#): See who has which administration privileges within your organization

Figure 24: Adding a new Home Organization Description

After submission of the bootstrapping form, SWITCH will then examine the data and approve or reject the new Home Organization within a few business days. In either case, you will receive a notification email with further instructions. After the Home Organization has been approved, one is able to access the Resource Registry with an account of the approved Identity Provider.

The first time a user logs in as user from an newly approved Home Organization he receives not only Home Organization rights as shown in Figure 24 but also Resource Registration Authority administration rights, described in the following Chapter.

It is recommended to edit the Home Organization description after the first login because the data provided during the bootstrapping procedure is far from complete. Edit the Home Organization Description by clicking the link “*Edit Home Organization Description*” on top of the page. The resulting page will look like in Figure 25. There, one will have to edit several sections in order to define various aspects of a Home Organization.

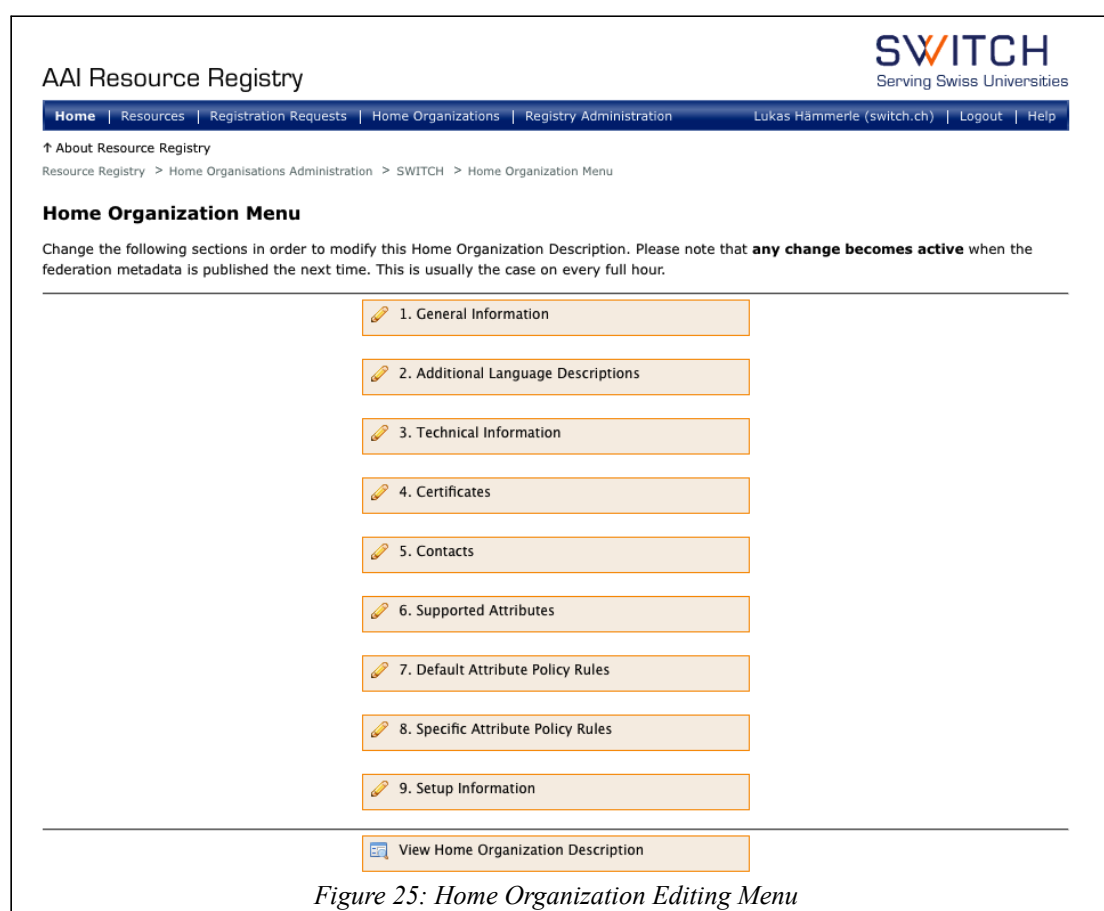


Figure 25: Home Organization Editing Menu

General Information

In the General Information section one first defines the very basic settings of a Home Organization like its name, its Federation, an description and a help desk web page like shown in Figure 26. The name and descriptions must be provided in English. Alternative version in other languages can be provided in the next section.

General Information

On this page you can edit the Home Organization's basic and general settings.

General Information	
Home Organization Name	<input type="text" value="switch.ch"/>
Home Organization Type	<input type="radio"/> Others <input type="text" value=""/>
Federation	<input type="text" value="SWITCHaai Federation"/>
English name and description	
Name	<input type="radio"/> SWITCH A name that shortly describes this Home Organization, e.g. "ETHZ - ETH Zürich".
Description	<input type="radio"/> The SWITCH Identity Provider is used by SWITCH staff members. <input type="text" value=""/>
Helpdesk URL	<input type="text" value="http://www.switch.ch/aai/contact"/> Provide additional information about your Home Organization. URL to a web page that offers assistance and support to users who experience authentication problems.
Interfederation	
Interfederation	<input checked="" type="checkbox"/> Enable interfederation for this Home Organisation Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources. Enabling interfederation means that metadata about this resource is published in non-SWITCHaai organization and can be used by other Identity Providers which are not part of SWITCHaai. The metadata will also include contact information about this resource. Before enabling a service for interfederation, make sure that:
	<ul style="list-style-type: none"> • All internationally standardized core attributes are declared as supported • The default attribute release policy is adapted such that internationally used attributes are released to interfederation resources • The specific attribute release rules are accurate and up-to-date
	<input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Save and continue"/>
	<input type="radio"/> This field must be provided

Figure 26: General Information

All settings in the section “General Information” are either of organizational or descriptive nature and are not technical in any way. Therefore, they could be changed without affecting the operation of an Identity Provider.

The interfederation checkbox is only visible if the organization as a whole was enabled for interfederation. Please contact aai@switch.ch for further information about interfederation support and how to enable it.

Additional Language Description

On this page one can add name and description of a Home Organisation in other languages than English. The main language for a Home Organization is the default language that will generally be used to display the name and description of a Home Organisation.

Additional Language Descriptions	
Main language	<input checked="" type="radio"/> English <input type="radio"/> German <input type="radio"/> French <input type="radio"/> Italian Language that this resource's name and description shall be displayed as default.
English	
Name	SWITCH
Description	The SWITCH Identity Provider is used by SWITCH staff members. You can modify the above entry on the Home General Information page
German	
Name	<input type="text"/>
Description	<input type="text"/>
French	
Name	<input type="text"/>
Description	<input type="text"/>
Italian	
Name	<input type="text"/>
Description	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Save and continue"/>	
<input checked="" type="radio"/> This field must be provided	

Figure 27: Additional Language Description

Technical Information

Technical Information	
<input type="button" value="Run Shibboleth 1.x assistant"/> <input type="button" value="Run Shibboleth 2.x assistant"/> <input type="button" value="Clear all fields"/>	
Entity ID	<input type="text" value="https://aai-logon.switch.ch/idp/shibboleth"/> URI value used as an ID for this Identity Provider. For SAML 2 Identity Providers like Shibboleth 2.x, please use a URL of the form <code>https://<HOSTNAME>/idp/shibboleth</code> . This URL doesn't have to resolve yet to a web page, but it is recommended that it is. Later on it should be possible to place the metadata file of this Identity Provider at this location.
Single Sign On Service	
SAML1 AuthnRequest binding	<input type="text" value="https://aai-logon.switch.ch/idp/profile/Shibboleth/SSO"/> Binding URN: urn:mace:shibboleth:1.0:profiles:AuthnRequest
SAML2 HTTP POST binding	<input type="text" value="https://aai-logon.switch.ch/idp/profile/SAML2/POST/SSO"/> Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
SAML2 HTTP POST SimpleSign binding	<input type="text" value="https://aai-logon.switch.ch/idp/profile/SAML2/POST-SimpleSign/SSO"/> Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign

Figure 28: Technical Information

In the Technical Information section, one has to define the Identity Provider's *entityID*, which is an ID following a special naming convention. The convention for the format of the *entityID* is to use a URL. More precisely, the URL should consist of 'https://' followed by the host name and the suffix '/idp/shibboleth', similar to the ID of Service Providers. This then looks for example like <https://some-organization.ch/idp/shibboleth>.

Note: It is highly recommended that the host name used in the entityID matches the hostname of the Identity Provider.

In order to set the the Identity Provider's endpoints, you may use one of the available

assistants in order to complete the URLs. The assistant then will use the root URL of the web application you provide to generate the default service locations for the given bindings as shown in Figure 28.

Note: Be sure that you are using either another port number (port 8443 is recommended) or a separate host name with its own IP address for the endpoints for the Attribute Service. This is essential because on the Attribute Service endpoints, X.509 client authentication has to be enabled while it shouldn't be enabled for the other endpoints. X.509 client authentication can only be reliably and securely enabled on a separate IP or port.

Warning: Modifications of any properties in the Technical Information section have to be performed very carefully because these changes will take some time to propagate to all Service Providers. The propagation delay normally is between one and two hours for Resources that are configured according to the SWITCHaai deployment guides. If in doubt about a property you want to change, please send an email to aai@switch.ch for assistance.

Used Certificates

In the Used Certificates sections the certificates used by Shibboleth and the web server have to be provided in PEM format. One can use the assistant in order to complete the form. The additional certificates can be used for certificate roll-over or for emergency fallback certificate.

In order to replace a certificate without any service disruptions, one has to make sure that the new certificate has been included in the federation metadata for at least one day before it can be used. Please refer to the Service Provider deployment guides at <http://www.switch.ch/aai/support/identityproviders/> on how to carry out the certificate rollover.

Using an additional certificate as emergency fallback certificate could be useful if a server was compromised and if the compromised main certificate has to be replaced quickly. In such a case one would just replace the certificates used by the web server and by Shibboleth with the fallback certificate.

Note: If you want to use the additional certificate as an emergency fallback certificate, make sure to add them in the Resource Registry for your Home Organization Description but don't actually store the private keys on the Identity Provider's host. Keep them in a safe location so that you can be sure they cannot be compromised as well in case your Identity Provider server should be compromised.

The Resource Registry will not expire certificates automatically if they have expired. Before the expiration date, several notification emails are being sent to the technical contact address of a concerned Home Organization.

Certificate Information

The certificates itself must be provided in PEM format (base64 encoded) and must meet the [SWITCHaai certificates requirements](#). The order of the certificates is not important. We recommend to use self-signed certificates as described on the above certificate requirements page. Moving the cursor over a PEM certificate in the text areas will show certificate details including subject, fingerprint and expiration date.

Identity Provider (SSO) Signing Certificate

This is the certificate configured in the Identity Provider configuration (e.g. `relying-party.xml` for Shibboleth 2.x). It is used to sign SAML assertions.

PEM Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDLDCCAhSgAwIBAgIJALH1hdjM5J6tMA0GCSqGSI
b3DQEBBQUAMBA4xHDAaBgNV
BAMTE2FhaS1sb2dvbi5zd210Y2guY2gwHhcNMTEwOD
E4MDkxMDElWhcNMTEwODE4
MDkxMDElWjAeMRwwGgYDVQQDEXNhYWktbG9nb24uc3
dpdGNoLmNoMIIBIjANBgkq
```

Additional PEM certificate:
Guide for [certificate roll over](#)

Attribute Authority (AA) Host Certificate

This is the certificate configured on the web server of the Attribute Authority host (usually VirtualHost on port 8443). The Attribute Authority processes incoming TLS backchannel requests, e.g. when Service Providers make an attribute query to the Identity Provider. **In most cases, this certificate should be the same as the SSO certificate on the left.**

Use the assistant in order to get the web server certificate.

🔧 Assistant to get the web server AA certificate...

PEM certificate:

```
-----BEGIN CERTIFICATE-----
MIIDLDCCAhSgAwIBAgIJALH1hdjM5J6tMA0GCSqGSI
b3DQEBBQUAMBA4xHDAaBgNV
BAMTE2FhaS1sb2dvbi5zd210Y2guY2gwHhcNMTEwOD
E4MDkxMDElWhcNMTEwODE4
MDkxMDElWjAeMRwwGgYDVQQDEXNhYWktbG9nb24uc3
dpdGNoLmNoMIIBIjANBgkq
```

Additional PEM certificate:

```
-----BEGIN CERTIFICATE-----
MIIFXzCCBEegAwIBAgICHv8wDQYJKoZIhvcNAQEFBQ
AwazELMAkGA1UEBhMCk0x
GTAXBgNVBAoTEFF1b1ZhbG1zIEExpbW10ZWQxH2AdBg
NVBAsTFnd3dy5xdW92YWRp
c2dsb2JhbC5jb20xIDAeBgNVBAMTF1F1b1ZhbG1zIE
dsb2JhbCBTU0wgSUNBMB4X
```

Cancel Reset Apply Save and Continue

• This field must be provided

Figure 29: Used Certificates

List of Contacts

There should be at least one technical contact for each Home Organization. Although it is not mandatory to provide also support and administrative contacts, it is recommended to do so. All contacts should be non-personal if possible. One also should be aware that these addresses will show up not only in the federation metadata but also on the list of all SWITCHaai Home Organizations.

Administrative Contacts			
Given name	SWITCHaai	Surname	Team Empty
Email	aai@switch.ch	Phone	+41 44 268 1505
Given name		Surname	Empty
Email		Phone	Fill down
Technical Contacts			
Given name	SWITCHaai	Surname	Team Empty
Email	aai@switch.ch	Phone	+41 44 268 1505 Fill down
Given name		Surname	Empty
Email		Phone	Fill down
Support Contacts			
Given name	SWITCHaai	Surname	Team Empty
Email	aai@switch.ch	Phone	+41 44 268 1505 Fill down
Given name		Surname	Empty
Email		Phone	Fill down

Figure 30: List of Contacts

Supported Attributes

The Supported Attributes section's purpose is to declare the attributes an Identity Provider can release. As depicted in Figure 31, on the left-hand side, one has to check the official SWITCHaai attributes that can be released by the Identity Provider. On the right-hand side, there are the local/bilateral attributes that are either used solely within the same organization or within a small subset of organizations on the basis of a bilateral agreement.

SWITCHaai Attributes	
Internationally Standardized Attributes	SwissEduPerson Attributes
Affiliation (core) <input checked="" type="checkbox"/>	Home organization (core) <input checked="" type="checkbox"/>
E-mail (core) <input checked="" type="checkbox"/>	Home organization type (core) <input checked="" type="checkbox"/>
Given name (core) <input checked="" type="checkbox"/>	Unique ID (core) <input checked="" type="checkbox"/>
Surname (core) <input checked="" type="checkbox"/>	Card UID (other) <input type="checkbox"/>
Targeted ID/Persistent ID (core) <input checked="" type="checkbox"/>	Date of birth (other) <input checked="" type="checkbox"/>
Business phone number (other) <input checked="" type="checkbox"/>	Gender (other) <input type="checkbox"/>
Business postal address (other) <input checked="" type="checkbox"/>	Matriculation number (other) <input type="checkbox"/>
Employee number (other) <input type="checkbox"/>	Staff category (other) <input type="checkbox"/>
Entitlement (other) <input checked="" type="checkbox"/>	Study branch 1 (other) <input type="checkbox"/>
Home postal address (other) <input type="checkbox"/>	Study branch 2 (other) <input type="checkbox"/>
Mobile phone number (other) <input checked="" type="checkbox"/>	Study branch 3 (other) <input type="checkbox"/>
Nick name (other) <input type="checkbox"/>	Study level (other) <input type="checkbox"/>
Organization path (other) <input type="checkbox"/>	
Organizational unit path (other) <input type="checkbox"/>	
Preferred language (other) <input type="checkbox"/>	
Primary organizational unit (other) <input type="checkbox"/>	
Private phone number (other) <input type="checkbox"/>	
Scoped affiliation (other) <input checked="" type="checkbox"/>	
User ID (other) <input checked="" type="checkbox"/>	

Figure 31: Supported Attributes

According to the AAI Attribute Specification (see <http://www.switch.ch/aai/attributes>) your Identity Provider must be able to release at least the green core attributes in the SWITCHaai

section. Checked attributes will only be released if needed and generally only a subset of these attributes will be released to a resource depending of the resource's requirements.

If the interfederation option is enabled for a Home Organisation, additional attributes should be supported in order to be interoperable with entities from other federations, in particular the core attributes in the section “Internationally Standardized Attributes”.

Default Attribute Release Policy

In the Default Attribute Release Policy a Home Organization administrator defines the general behavior regarding the release of attributes that will be reflected in the generated attribute-filter.xml files. A Home Organisation administrator defines the release scope of an 'required' and 'desired' attributes as shown in Figure 30.

The release scopes are:

Nobody:

Attribute will not be released in general. This option is useful in case the release of an attribute is controlled only via specific attribute release rules mentioned below.

Resources of my organization:

Releases the attribute only to Resources which were registered by the same Home Organisation. This excludes all Federation Partner Resources.

Local Federation Resources:

Releases the attribute by default to the Resources of all the same federation as this Home Organisation Description.

Interfederated Resources:

Releases the attribute to all Resources in general, even such from other federations. This option is only available if interfederation support is enabled for this Home Organisation.

Note: Only those attributes are shown which can be released by the Identity Provider. If you add an additional attribute in the Supported Attributes section, you should also define a general attribute release policy rule for this attribute. Otherwise, the default rule (release required attributes, don't release desired attributes) will be used.

Release required attributes to	... desired attributes to
Have a look at the graphic in order to understand the effects of the different policy choices below.		
SWITCHHai attributes		
Affiliation (core) ⓘ	interfederation resources ▼	SWITCHHai resources ▼
E-mail (core) ⓘ	interfederation resources ▼	SWITCHHai resources ▼
Given name (core) ⓘ	interfederation resources ▼	SWITCHHai resources ▼
Home organization (core) ⓘ	SWITCHHai resources ▼	SWITCHHai resources ▼
Home organization type (core) ⓘ	SWITCHHai resources ▼	SWITCHHai resources ▼
Surname (core) ⓘ	interfederation resources ▼	SWITCHHai resources ▼
Targeted ID/Persistent ID (core) ⓘ	interfederation resources ▼	interfederation resources ▼
Unique ID (core) ⓘ	SWITCHHai resources ▼	SWITCHHai resources ▼
Business phone number (other) ⓘ	SWITCHHai resources ▼	SWITCHHai resources ▼
Business postal address (other) ⓘ	SWITCHHai resources ▼	SWITCHHai resources ▼
Date of birth (other) ⓘ	my organization's resources ▼	nobody ▼
Entitlement (other) ⓘ	interfederation resources ▼	my organization's resources ▼
Mobile phone number (other) ⓘ	my organization's resources ▼	my organization's resources ▼
Scoped affiliation (other) ⓘ	interfederation resources ▼	interfederation resources ▼
User ID (other) ⓘ	my organization's resources ▼	my organization's resources ▼

Figure 32: Default Attribute Release Policy

Specific Attribute Release Policy

While one could define a very general attribute release policy in the previous section, the Specific Attribute Release Policy section allows defining very fine-grained rules for the attribute release. As is shown in Figure 33, one can create custom-tailored rules for each Resource. Either a whole Resource can be excluded completely from the attribute filter or one can set individual exceptions to the default rule for specific attributes.

Excluding a Resource from the attribute-filter.xml file is useful if an Identity Provider administrator wants also to create a very custom-tailored rule for this Resource and therefore doesn't want it to include in the filter generated by the Resource Registry. Such rules can include advanced [PolicyRequirementRules](#), which can base the release decision on a huge variety of criteria.

Warning: Be careful not to break services for your users because you exclude them from the attribute filter or because you exclude certain attributes that are required by the resource.

Note: The specific attribute policy rules can only be used with Shibboleth 2.x Identity Providers and only if these Identity Providers load their attribute-filter.xml file directly from the Resource Registry.

Home Organization Setup & Environment

The last Home Organization section is the '*Setup & Environment Information*' section, which is shown in Figure 34. It is purely informational and solely serves the SWITCHHai team as well as other Home Organization administrators to examine how different Identity Providers are set up. This allows comparing similar setups in case of problems or intended setup changes.

The Resource Registry polls all Service and Identity Providers every day in order to update some of the setup and environment information. This is however only possible if they were deployed according to the SWITCHHai/AAI Test deployment guides, which include configuration files that allow the Resource Registry to access the status handlers.

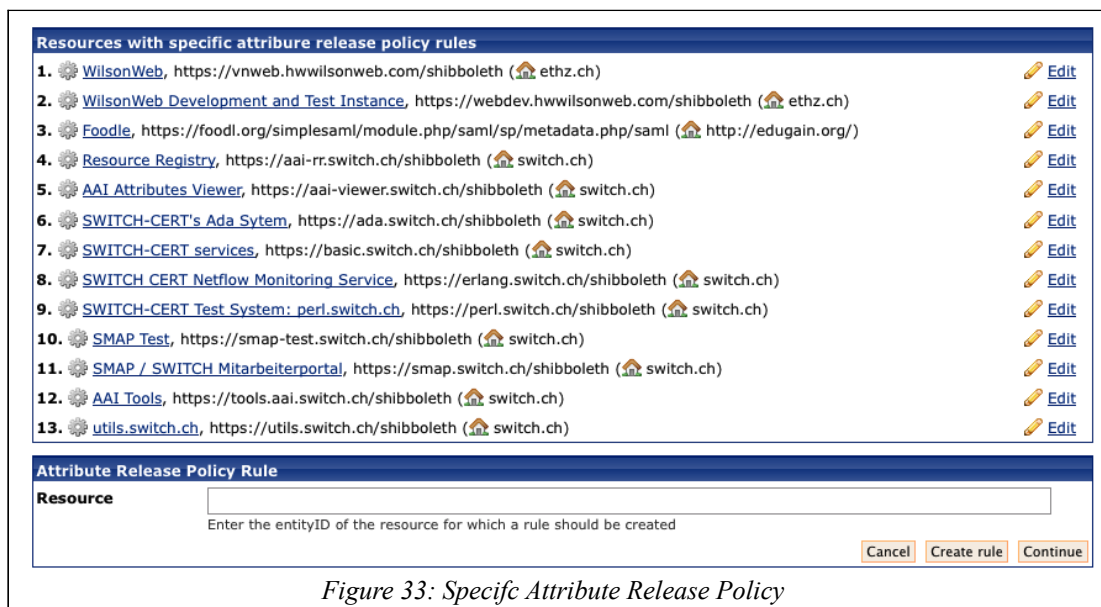


Figure 33: Specific Attribute Release Policy

Duties as Home Organization Administrator

Since the metadata generated by the Resource Registry heavily relies on the descriptions of Resources and Home Organizations, it is strongly recommended to keep them as up to-date as possible. Otherwise, problems may occur because third parties interacting with your Identity Provider may have outdated information. This means:

- If you change your Identity Provider DNS host names, modify its certificates, provide additional attributes for your users, please update the Home Organization Description.

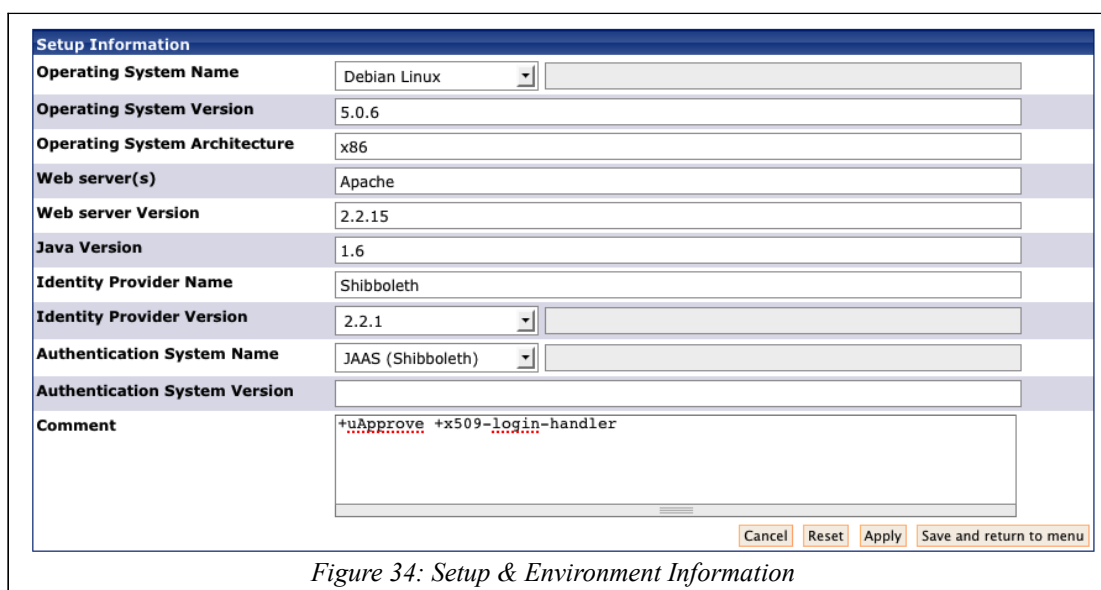


Figure 34: Setup & Environment Information

However, if you do so, please consult aai@switch.ch beforehand because certain changes could cause service disruptions if not planned and carried out carefully.

- Regularly update the metadata of your Identity Provider. It is recommended to update metadata more frequently because the file only will be downloaded if it changed.

Note: There will be a propagation delay of at least one hour for certain changes applied to the Home Organisation. In order to become active, a change in metadata first has to be

downloaded by a Service Provider.

- Regularly inspect the attribute release policy mails that are sent to the technical contact address of a Home Organisation. In case you see a Resource that requests too many attributes, create an exception in the specific attribute release policy for this Resource.

4.3.Resource Registration Authority Administrator

For policy reasons every Home Organization needs at least one Resource Registration Authority (RRA) administrator, whose task is to approve Resource Descriptions. This includes the approval or rejection of Resource Descriptions. An RRA administrator basically should ensure that all Resources operated within his Home Organization are in compliance with the SWITCHaai Service Agreement (see <http://www.switch.ch/aa/agreement/>).

Home Organizations can decide to enforce stricter approval procedures requiring the requesting user and approving user to use different accounts. This feature is called 'four-eyes approval' and can be activated on request for a Home Organisation.

In addition the Resource Registry supports a mode where certain actions for specific Home Organisations require two-factor authentication. Whereas the first factor is the standard AAI authentication, the second factor is implemented directly on the Resource Registry by a SMS one-time password, which is sent to a user's mobile phone. Thus, in order for this optional feature to work a Home Organisation must be able to provide a user's mobile phone number as attribute or manually via email. This then looks like in Figure 35.

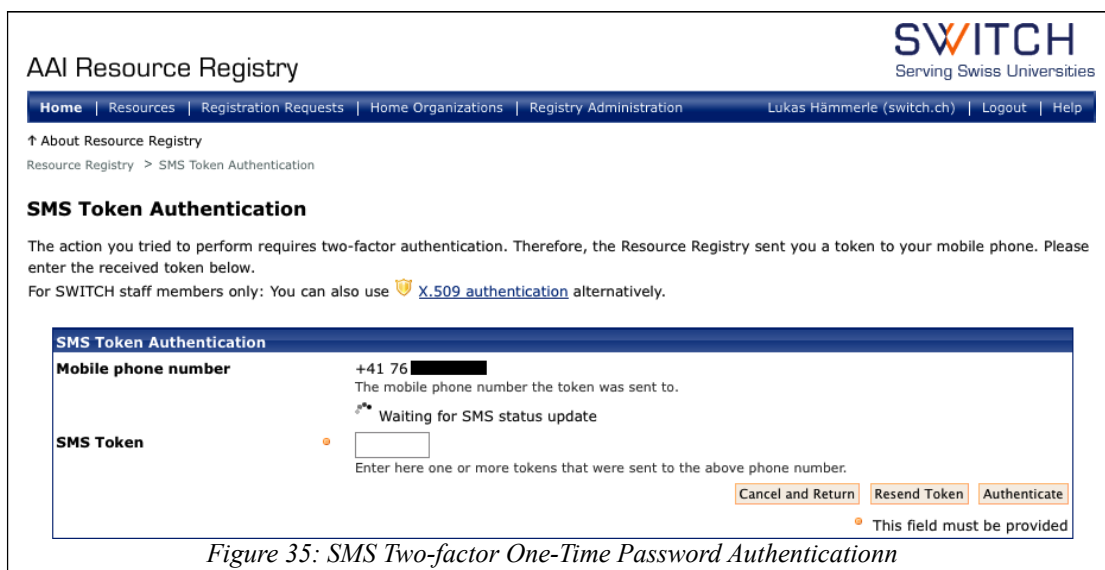


Figure 35: SMS Two-factor One-Time Password Authentication

Duties as a Resource Registration Authority Administrator

In particular the following requirements have to be checked carefully:

- The person that created or modified a Resource Description is allowed to operate an AAI Resource in the name of your Home Organization.
- Every Resource has at least one valid contact person for administrative, technical and support inquiries.
- The Resource declares only as many attribute as required as are needed for its proper functioning and complies with the Swiss data privacy law.
- The Resource's end point URLs (service locations) point to eligible host names that are affiliated with the Home Organization.
- If any self-signed certificates are used, the RRA has to proof that the person that presumably registered the Resource Description is in possession of the certificate's private key.

In order to examine these details, an RRA administrator should inspect a Resource Description before approving it. The Resource Registry will in some situations display warning messages when some of the above points should be checked in particular.

Every time a Resource Description is submitted for approval, all RRA administrators of the Home Organization the Resource was submitted for will receive a notification e-Mail. An RRA administrator will see the Resource Descriptions that still need approval on the Resource Registration Authority page as shown in Figure 36.

AAI Resource Registry

SWITCH
Serving Swiss Universities

Home | Resources | **Registration Requests** | Home Organizations | Registry Administration | Lukas Hämmerle (switch.ch) | Logout | Help

↑ About Resource Registry
Resource Registry > Registry Registration Authority Requests

Resource Registrations Authority Requests

Find below the Home Organisations for which you have Resource Registration Authority (RRA) privileges. The duty of an RRA administrator is to check and approve changes or Resource Descriptions.

- ➕ Add a custom local attribute definition for use within your organisation
- 🏠 SWITCH (SWITCHaai)
 - 🔍 Approve Resources: Approve or reject new or modified Resource Descriptions
 - Modification request for 🌐 AAI Attributes Viewer (<https://aai-viewer.switch.ch/shibboleth, SWITCHaai>)
 - 📄 Approved Resource Descriptions: All resources registered in the name of this organization
 - 👤 Manage administrators: Transfer or revoke administration privileges
 - 👥 View all administrators: See who has which administration privileges within your organization

Figure 36: Resource Description waiting for approval

Clicking the “Approve Resources” link then leads to a page like in Figure 37.

Resources waiting for approval

AAI Attributes Viewer (<https://aai-viewer.switch.ch/shibboleth, SWITCHaai>)

[View changes](#) | [Edit Resource Description](#) |

- Requester: [Lukas Hämmerle](#) (switch.ch), phone: +41 44 268 15 64
- Service Location URLs:
 - https://aai-viewer.switch.ch/Shibboleth.sso/NIM/Artifact
 - https://aai-viewer.switch.ch/Shibboleth.sso/NIM/POST
 - https://aai-viewer.switch.ch/Shibboleth.sso/NIM/Redirect
 - https://aai-viewer.switch.ch/Shibboleth.sso/NIM/SOAP
 - https://aai-viewer.switch.ch/Shibboleth.sso/SAML/Artifact
 - https://aai-viewer.switch.ch/Shibboleth.sso/SAML/POST
 - https://aai-viewer.switch.ch/Shibboleth.sso/SAML2/Artifact
 - https://aai-viewer.switch.ch/Shibboleth.sso/SAML2/ECP

Figure 37: Approve a Resource Description

Figure 37 shows a single Resource Description to approve or reject. Clicking on 'View changes' an RRA administrator can inspect the difference between the currently active and the new Resource Description.

Together with the approval or rejection notification email a comment can be sent to the user who requested the modification of the Resource Description.

5. Miscellaneous

This chapter contains various topics that weren't mentioned above but that nevertheless deserve some attention.

5.1. Data Usage

Data stored in the Resource Registry is not only used for the management of the SWITCH federations but it is also used to serve as information source to end users. In particular, the

following web pages directly access the SWITCH Resource Registry database:

- <http://www.switch.ch/aai/help>
- <http://www.switch.ch/aai/participants/allresources.html>
- <http://www.switch.ch/aai/participants/allhomeorgs.html>
- <http://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html>

If a Resource Description is changed, this is reflected on the above web pages as soon as the change gets approved. Changes of Home Organisation Descriptions become effective immediately.

5.2.Facts about the Resource Registry

The Resource Registry is programmed in PHP5. It requires the PEAR QuickForm libraries as well as a MySQL database. For X.509 related functions openssl has to be installed.

All development work has been done by SWITCH. The code is developed under a BSD-like license and can be requested by sending an email to aai@switch.ch. However, the code was custom-tailored to the needs of SWITCH and it never was meant to be a generic federation registry tool.