

# AAI Resource Registry Guide

Version: 20080612

Authors: LH, TL

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

Contact: [aai@switch.ch](mailto: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 the already integrated explanations. It explains the most important aspects and processes that are needed to register and maintain Home Organization and Resource Descriptions.

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

## Table of Contents

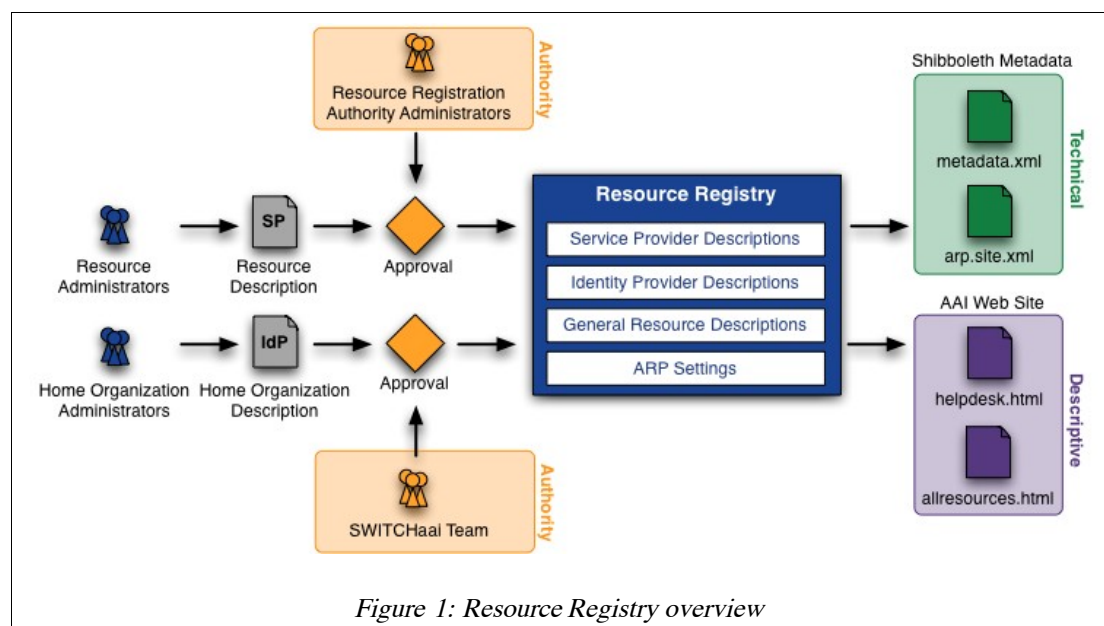
AAI Resource Registry Guide.....	1
1.Description of the Resource Registry .....	2
2.Login.....	3
3.Configuration Sections.....	4
4.Roles.....	6
5.Resource administrator.....	8
Basic Resource Information.....	9
Multiple Language Descriptions.....	11
List of Contacts.....	12
Keywords.....	12
Service Locations.....	12
Used Certificates.....	13
Required attributes.....	13
Resource Audience settings.....	14
Submit Resource Description for Approval.....	15
Duties as a Resource administrator.....	17
6.Home Organization Administrator.....	18
Bootstrapping a Home Organization Registration.....	18
General Information.....	20
Technical Information.....	20
Used Certificates.....	21
List of Contacts.....	22
Supported Attributes.....	22
General Attribute Release Policy.....	23
Specific Attribute Release Policy.....	24
Home Organization Setup & Environment.....	24
Duties as Home Organization administrator.....	25
7.Resource Registration Authority Administrator.....	26
Duties as Resource Registration Authority (RRA) administrator.....	26

## 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. 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!
- **Resource 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!



- **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.
- **Identity Providers 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 also is 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 relating to the federation.

The Resource Registry is written in PHP 5 using PEAR/QuickForm and MySQL.

## 2. Login

The Resource Registry is accessible via <https://aai-rr.switch.ch/> and requires an account in SWITCHaai or AAI Test. The start page contains a short description of the Resource Registry and two login buttons. These login buttons are the entrance to the Resource Registry for the production SWITCHaai Federation and the AAI Test Federation.

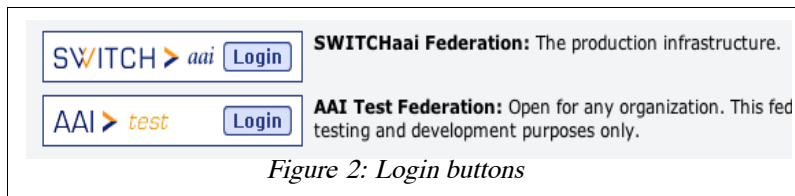


Figure 2: Login buttons

To log in one has to click on the login button that represents the federation of which ones Home Organization is part of. After the authentication at a Home Organization one gets redirected back to the Resource Registry. Provided the Resource Registry receives all the required attributes from the Home Organization, login is successful. The required attributes are:

- Given Name
- Surname
- E-Mail Address (optional)
- Unique Identifier
- Business telephone number (optional)
- Home Organization Name
- Home Organization Type

**Note:** Whether you log in via SWITCHaai or AAI-Test doesn't matter, the Resource Registry and its procedures work almost the same. However, when you are logged in via the AAI Test Federation you cannot modify Resource Descriptions or Home Organization Descriptions that are part 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 though.

When a user logs in the first time, a data protection agreement (see Figure 3) has to be first accepted. 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 some cases where an administrator needs to ask you something (e.g. fingerprint of your self-signed certificate) on the phone.

Therefore, you have to give your consent for the storage of personal information. SWITCH won't use personal data for anything else than for AAI related matters and no data will be used or processed by third parties.

User Information that will be stored for Resource Registry	
Given Name	Lukas
Surname	Hämmerle
Phone number	+41 44 268 1505
Home Organization Name	switch.ch
Home Organization Type	others
Affiliation	staff
E-Mail	lukas.haemmerle@switch.ch
Data protection	<input type="checkbox"/> I agree that an entry representing myself with the above data will be stored in the AAI Resource Registry database.
	<input type="button" value="Submit"/>

• 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.

**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 yourIdentity Provider.

### 3. Configuration Sections

**Main Menu**

DB Administration   RRA Administration   Home Organization Administration   Resource Administration   General Information

**Warning:** Although you have DB administration privileges, you don't meet the required assurance level. Therefore, certain DB administrator actions cannot be performed.

**General Information**

- Resource Registry Guide. Explains the basic principles and mechanisms of the Resource Registry.
- Federations operated by the Resource Registry
- Approved Home Organizations
- Federation Partners
- Approved Resource Descriptions
- Search for resources
- Metadata refresh times of Service Providers and Identity Providers
- All Resource Registry users from switch.ch
- Attribute definitions
- Home Organization attribute release matrix
- Resource attribute requirement matrix

**Metadata Files**

The following files are **directly generated by the Resource Registry**. This means that these files are as up-to date as possible. All files are unsigned and are not validated with a schema, so **do not download the metadata files directly from the Resource Registry**. You can get XML-validated and signed files from the official AAI Metadata page, which is updated every full hour if the metadata changed.

- For Shibboleth 1.3
  - Metadata file
    - metadata.switchaa1.xml for SWITCHaa1 Federation
    - metadata.aaitest.xml for AAI Test Federation
- For Shibboleth 1.2
  - Sites file
    - sites.switchaa1.xml for SWITCHaa1 Federation
    - sites.aaitest.xml for AAI Test Federation
  - Trust file
    - Can be downloaded from the Metadata page for all Federations.

Figure 4: General Information

After successful authentication, you see to the main menu of the Resource Registry. Depending on your privileges and roles (see Chapter 4), you will see between two and five different tabs reflecting the administration and access rights you have.

Figure 4 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.

At the bottom you also find links to the metadata that is directly generated by the Resource Registry. In the federation metadata files all Home Organizations and Resource Descriptions managed by the Resource Registry are reflected.

Figure 5 shows the 'Resource Administration' options. Unless you already have registered a resource you can only add a new Resource Description.

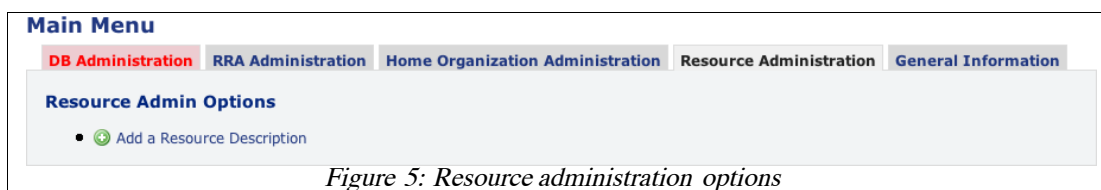


Figure 5: Resource administration options

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.



Figure 6: View with multiple approved Resource Descriptions

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



Figure 7: Home Organization administration options

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



Figure 8: Resource Registration Authority administration options

**Note:** You may not see all of the above administration options because only the options are shown that reflect one's roles. To get the role of a Home Organization administrator, you either have to register a Home Organization or you have to be given that role by another Home Organization administrator. The same applies for a Resource Registration Authority (RRA) administrator. To become a Resource administrator one can register a Resource and the administration rights are received after approval by an RRA administrator. Alternatively, the Resource administration rights also can be granted by another Resource administrator.

## 4. Roles

Every user in the Resource Registry can have one or more roles that grant certain administration rights. Currently, the following roles are defined:

- Resource administrator  
Registers and manages one or more Resource Descriptions. See Chapter 5.
- Home Organization administrator  
At least one person per Home Organization. Manages Home Organization Description and attribute release settings. See Chapter 6.
- Resource Registration Authority administrator  
At least one person per Home Organization. Approves or rejects new or modified Resource Descriptions. See Chapter 7.

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 also 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.

**Administration Rights**

RRA Administration Home Organization Administration Resource Administration General Information

Home Organization Description menu of "AAI Shibboleth 2.0 Test IdP" - Administration Rights

**Resource Registration Authority Administrator**

Transfer administrator rights to other users from your Home Organization or even to users from other Home Organizations:

Users with RRA rights	
Lukas Hämmerle (switch.ch)	Authorized
Thomas Lenggenhager (switch.ch)	Authorized
Valéry Tschopp (switch.ch)	Authorized
Halm Reusser (switch.ch)	Authorized
Users from lewotolo.switch.ch without RRA rights	
Demouser2 SWITCHhai	Not authorized

**Delegate RRA rights with an invitation mail to any AAI user**

Add comma- or space-separated e-mail addresses.  
 You can use any email address as long as the recipient has an AAI account.  
 Click on **Apply** to send an invitation key to the recipient(s) or delegate the rights directly in case the user is already in the Resource Registry Database.

patrick.schnellmann@switch.ch kaspar.brand@switch.ch

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. Two users are invited by manually entering their e-Mail addresses. Clicking on “Apply” results in one user (that already was in the Resource Registry database) being added directly as administrator. The other (unknown) user receives an e-Mail containing an invitation link that will grant him the administration rights.

After entering the two email addresses and submitting the form, one should see a page like in Figure 10. As can be seen, invitations can also be revoked from an invited user, thus invalidating an invitation link.

**Administration Rights**

RRA Administration Home Organization Administration Resource Administration General Information

Home Organization Description menu of "AAI Shibboleth 2.0 Test IdP" - Administration Rights

**Resource Registration Authority Administrator**

Transfer administrator rights to other users from your Home Organization or even to users from other Home Organizations:

Users with RRA rights	
Lukas Hämmerle (switch.ch)	Authorized
Thomas Lenggenhager (switch.ch)	Authorized
Valéry Tschopp (switch.ch)	Authorized
Halm Reusser (switch.ch)	Authorized
Kaspar Brand (switch.ch)	Authorized
Pending Admin Invitations	
patrick.schnellmann@switch.ch	Pending
Users from lewotolo.switch.ch without RRA rights	
Demouser2 SWITCHHaai	Not authorized

**Delegate RRA rights with an invitation mail to any AAI user**

Add comma- or space-separated e-mail addresses.  
 You can use any email address as long as the recipient has an AAI account.  
 Click on **Apply** to send an invitation key to the recipient(s) or delegate the rights directly in case the user is already in the Resource Registry Database.

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: Invitation pending

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

## 5. 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.



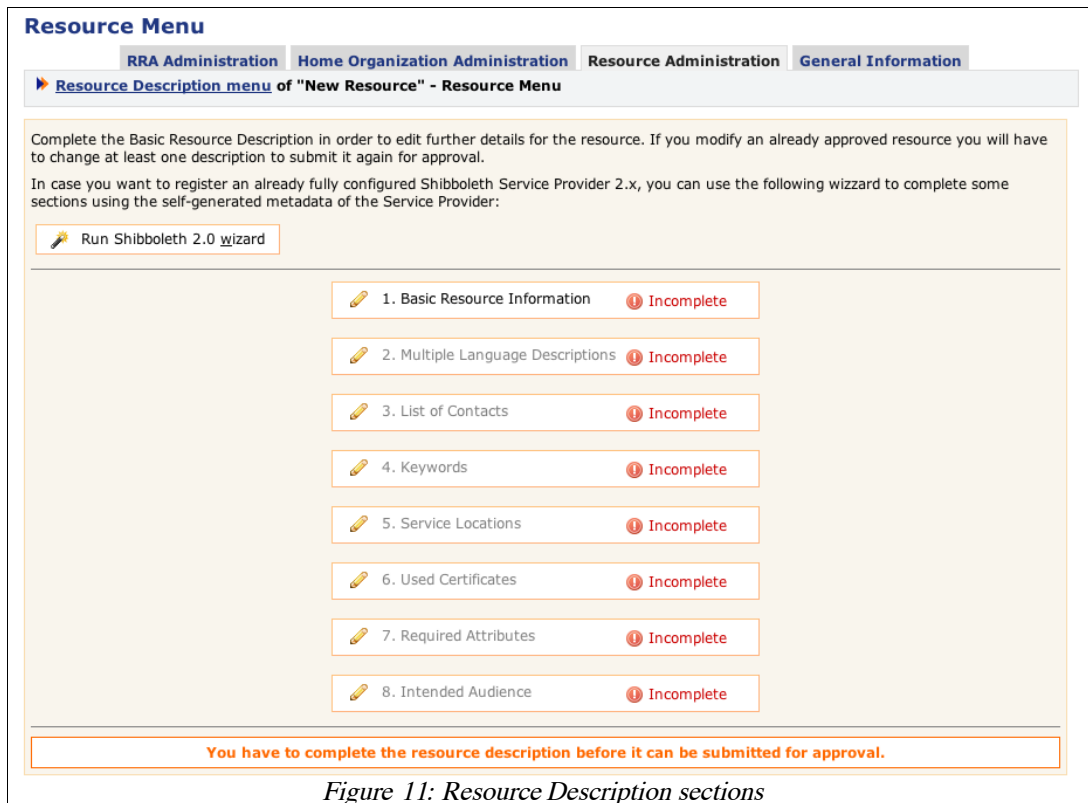


Figure 11: Resource Description sections

As can be seen, 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.

### 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:

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 your are Resource Registration Administrator of or for AAI Test Home Organizations.

Basic Information	
<b>Home Organization</b>	<ul style="list-style-type: none"> <li>switch.ch</li> </ul> <p>You can register resources only</p> <ul style="list-style-type: none"> <li>for Home Organizations which you have an AAI account for</li> <li>for which you are Resource Registration Authority (RRA) administrator</li> <li>for Home Organizations in the AAI Test Federation</li> </ul>
<b>Main language</b>	English
<b>Main Descriptive Name</b>	SWITCH AAI Wiki: waaikiki Name of the Resource or Service, e.g. "SWITCH e-Conferencing Portal", "ETHZ CompiCampus".
<b>Main Description</b>	This Wiki-based Wiki deals with AAI relevant topics. <small>Should describe the resource and its use in the language you selected as main language</small>
Unique Identifier of the Resource	
<b>Entity ID</b>	https://aai-wiki.switch.ch/shibboleth <small>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://&lt;HOSTNAME&gt;/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.</small>
<b>Relying Party</b>	Default <small>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. SAML2 Attribute Pull provides only a slightly increased security benefit, but is slower and more error-prone because the attributes are fetched like for SAML1 via a separate back-channel connection.</small>
Home and Helpdesk URLs	
<b>Home URL</b>	https://aai-wiki.switch.ch/ <small>The entry point URL or home page of the resource: e.g. https://sp.example.org/index.html. It doesn't have to be AAI-protected but can be.</small>
<b>Helpdesk URL</b>	 <small>A web page that offers users help and guidance in case of AAI related problems with the resource</small>
Validity	
<b>Valid from</b>	18 October 2005 <small>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.</small>
<b>Valid until</b>	- - - <small>Set these fields to '-' in order to make the Resource Description valid indefinitely.</small>
Visibility	
<b>Public</b>	<input checked="" type="checkbox"/> <small>If checked, this Resource Description will show up in the list of public resources.</small>
<input type="button" value="Back"/> <input type="button" value="Reset"/> <input type="button" value="Apply"/> <input type="button" value="Save and continue"/>	
<small>This field must be provided</small>	

Figure 12: Basic Resource Description

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 your *shibboleth.xml* or *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 Resource may not be accessible from some Identity Providers.

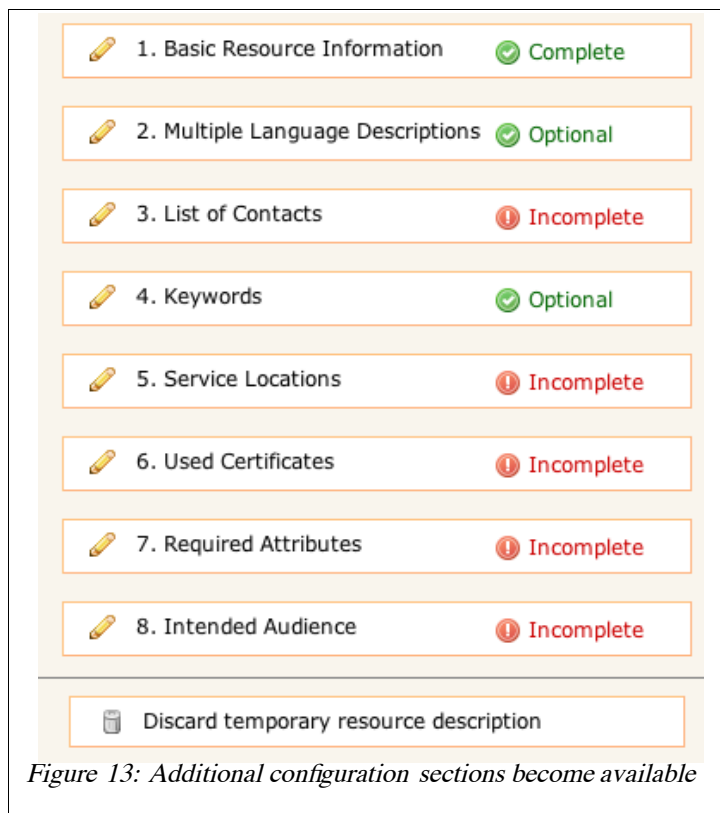
**Relying Party:** Depending in which relying party a resource is, it has to fetch the attributes from an identity provider or it receives the attributes directly via an authenticated user's web browser. For most cases, it is recommended to leave this with the default setting.

**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.



### Multiple 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

The screenshot shows a web form titled 'List of Contacts' with four distinct contact entries. Each entry has a 'Contact Type' dropdown menu, a 'Contact Name' text input, and an 'E-Mail' text input. The entries are as follows:

- Entry 1:** Contact Type: Technical; Contact Name: Lukas Hämmerle; E-Mail: lukas.haemmerle@switch.ch
- Entry 2:** Contact Type: Support; Contact Name: SWITCHaai Team; E-Mail: aai@switch.ch
- Entry 3:** Contact Type: Administrative; Contact Name: SWITCHaai Team; E-Mail: aai@switch.ch
- Entry 4:** Contact Type: Billing; Contact Name: (empty); E-Mail: (empty)

At the bottom right of the form, there are four buttons: 'Back', 'Reset', 'Apply', and 'Save and continue'.

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. 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.

## Keywords

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

## Service Locations

The screenshot shows a web form titled 'Service Locations'. At the top, there are three buttons: 'Run Shibboleth 1.x assistant...', 'Run Shibboleth 2.x assistant...', and 'Clear all fields...'. Below these buttons, there is a note: 'In case your Service Provider is accessible with multiple hostnames, provide the URLs separated with comas, e.g. https://host1.ch/Shibboleth.sso, https://other.host.ch/secure/Shibboleth.sso, http://insecure.host.ch/unprotected/Shibboleth.sso'. The main part of the form is a table with the following rows:

AssertionConsumerService	
<b>SAML1 default browser-post binding</b>	https://tools.switch.ch/Shibboleth.sso/SAML/POST Default AssertionConsumerService with SAML1 browser-post binding
<b>SAML1 browser-post binding</b>	(empty input field)
<b>SAML1 artifact-01 binding</b>	https://tools.switch.ch/Shibboleth.sso/SAML/Artifact
<b>SAML2 HTTP-POST binding</b>	https://tools.switch.ch/Shibboleth.sso/SAML2/POST
<b>SAML2 HTTP-POST-SimpleSign binding</b>	https://tools.switch.ch/Shibboleth.sso/SAML2/POST-SimpleSign
<b>SAML2 HTTP-Artifact binding</b>	https://tools.switch.ch/Shibboleth.sso/SAML2/Artifact
<b>SAML2 PAOS binding</b>	https://tools.switch.ch/Shibboleth.sso/SAML2/ECP

Figure 15: Service location endpoint URLs

In this section, which is shown in Figure 15, you define the SAML endpoint URLs of the

Service Provider. 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.

**Warning:** As applies to the entityID, changes of the endpoint URLs 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 not very easy to solve, which is why it won't be implemented earlier than Shibboleth 2.2.

## Used Certificates

**Certificate Information**

You have to provide A. the common name (CN) of the certificate in section **and/or** B. the certificate itself that Shibboleth is using. **It is recommended to provide A. and B.**  
 Try using the the assistant if you don't want to complete the form manually and if you use the same certificate for the web server as well as for Shibboleth.

[Run assistant...](#)

**A. Certificate Subject Common Name**

**CN of the certificate subject**   
 If the certificate has several common names, you should provide the first one.  
**Example:** If the certificate's subject is 'C=CH/O=Test Organization/OU=Test Departement/CN=server.example.ch' you should provide 'server.example.ch' as the common name.

**B. Embedded certificates**

**PEM formatted X.509 certificate**

```
-----BEGIN CERTIFICATE-----
MIIE4zCCA8ugAwIBAgILAQAAAAABGZ/kGG0wDQYJKoZIhvcNAQEFBQAwXzELMAkG
A1UEBhMCQkUxEzARBgNVBAoTCkN5YmVydHJlc3QxZjZAVBgNVBAsTDkVkdWNhdGlv
bmFsIENBMSIwIAYDVQQDExlDeWJlcnRydXN0IEVkdWNhdGlvbmFsIENBMSIwIA
MDQzMDE1MTIwNVVoXDEwMDQzMDE1MTIwNVVowATELMAkGA1UEBhMCQ0gxQDA+BgNV
BAoTN1N3aXRjaCAtIFRlbGVpbmZvcmlhdGlrZG1lbnN0ZSBmdWVyeIE1aHJlIHVu
ZCBGb3JzY2Y2h1bmcxGDAwBgNVBAMTD3Rvb2xzLnN3aXRjaC5jaDCCASIwDQYJKoZI
```

**Second PEM formatted X.509 certificate**

Use the second certificate for certificate roll over if you want to replace the first certificate. If you use a second certificate, make sure it is configured in your Service Provider, otherwise encrypted attributes cannot be decrypted in certain circumstances.

Click in a textarea containing a certificate in order to see some additional details about it.

**Subject:** / C=CH / O=Switch - Teleinformatikdienste fuer Lehre und Forschung / CN=tools.switch.ch  
**Type:** Issued  
**Issuer:** / C=BE/O=Cybertrust/OU=Educational CA/CN=Cybertrust Educational CA  
**Expiration date:** Apr 30 15:12:05 2010 GMT  
**Fingerprint:** 70:84:18:11:3F:DA:D8:27:97:BD:17:54:26:93:51:E9:3F:0A:96:96

[Back](#) [Reset](#) [Apply](#) [Save and Continue](#)

Figure 16: Used certificates

Provide the certificate subject common name and/or the certificate itself, that later on will be used by your Service Provider. Depending on the certificate that you provide, a different way of approving the Resource Description later on is used. As is shown in Figure 16, a second certificate could be added as a backup certificate for roll-over procedures. The order of the two certificates doesn't matter.

**Warning:** As with the entityID changes of these values need to propagate first to all identity providers before they become active.

## Required attributes

The Required attributes section is very important because it affects the Attribute Release Policies (ARP) and attribute filters of all Identity Providers. As shown in Figure 17, you have to declare which attributes your Resource really requires in order to work and which attributes are desired or nice to have.

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

**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 your Resource.

The screenshot displays a configuration interface for SWITCHaai Scope, divided into two main sections: SWITCHaai Scope and Local Scope.

**SWITCHaai Scope:**

- Unique ID:** Remove checkbox is unchecked. Usage is 'required'. Comment: 'To map users to WikiName'.
- Given name:** Remove checkbox is unchecked. Usage is 'required'. Comment: 'To generate the WikiName'.
- E-mail:** Remove checkbox is unchecked. Usage is 'desired'. Comment: 'Nice to communicate with users'.
- Surname:** Remove checkbox is unchecked. Usage is 'required'. Comment: 'To generate the WikiName'.
- Below these are four more attribute entries, each with 'Attribute' (dropdown), 'Usage' (dropdown), and 'Comment' (text area) fields.

**Local Scope:**

- Header: 'Local Scope' with subtext: 'Local/bilateral attributes can be defined by each Home Organization.'
- Three attribute entries, each with 'Attribute' (dropdown), 'Usage' (dropdown), and 'Comment' (text area) fields.

At the bottom of the SWITCHaai Scope section, there are four buttons: 'Back', 'Reset', 'Apply', and 'Save and continue'.

Figure 17: Required attributes

## Resource Audience settings

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, you probably would protect your Resource in the web server's configuration with something like:

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

Since only you know the configuration of your authorization and access rules, it is impossible for Home Organization administrators to know to which Resources their users have access to. Therefore, you should declare the intended audience in the Resource Registry. Please refer to Figure 18 to see how this looks like.

**Note:** Be accurate but not too restrictive when declaring filling out this form because it also will affect the ARP files and attribute filters of the Identity Providers.

Default Audience	
Universities	Include ▾
Universities of Applied Sciences	- ▾
Hospitals	Include ▾
Libraries	- ▾
Virtual Home Organizations	- ▾
Other	- ▾

Specific Intended Audience Rules	
<small>Exceptions to the above default rules. These settings have precedence over default audience settings.            To define more than 5 exceptions, fill out all entries and click on "Apply" to display additional entries.</small>	
1.	SWITCH - Serving Swiss Universities ▾ Include ▾
2.	Choose a HomeOrg ... ▾ Choose action ... ▾
3.	Choose a HomeOrg ... ▾ Choose action ... ▾
4.	Choose a HomeOrg ... ▾ Choose action ... ▾
5.	Choose a HomeOrg ... ▾ Choose action ... ▾

Figure 18: Intended audience

This 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 ARP/attribute filter files of a Home Organization only Resources appear that may include users of a Home Organization.

### Submit Resource Description for Approval

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 having the rights to approve Resource Descriptions for your Home Organization has to examine and approve it, provided it is complies with the AAI Policies and the Swiss data protection law.

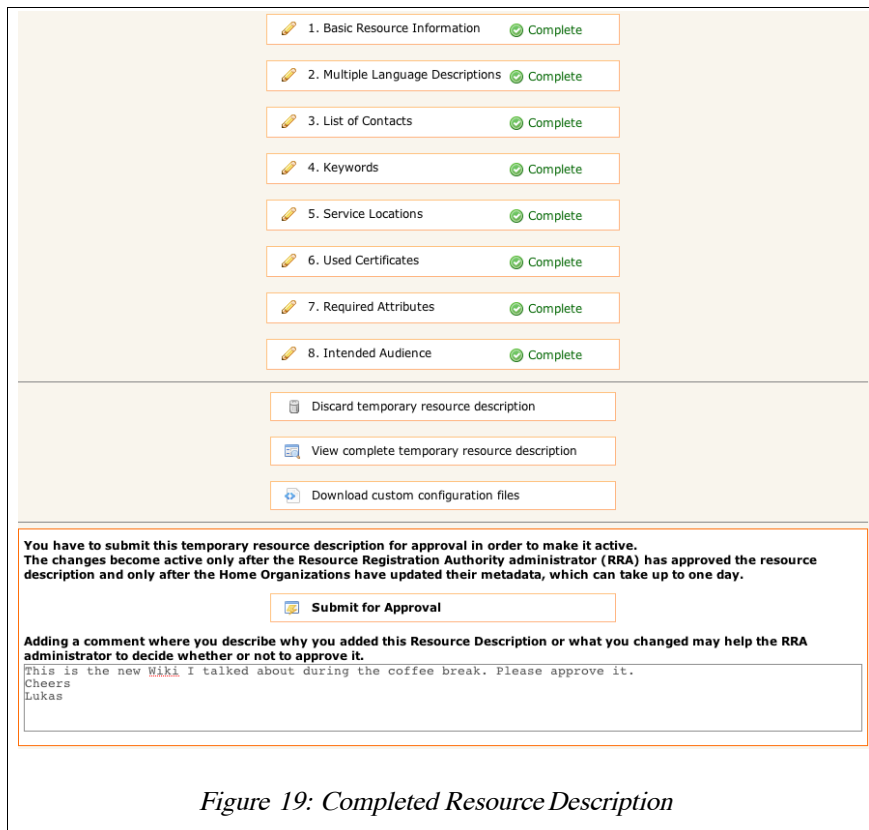


Figure 19: Completed Resource Description

As you can see, there is also a button to discard the temporary Resource Description. This will delete all changes you made but will leave the most recently approved Resource Description intact.

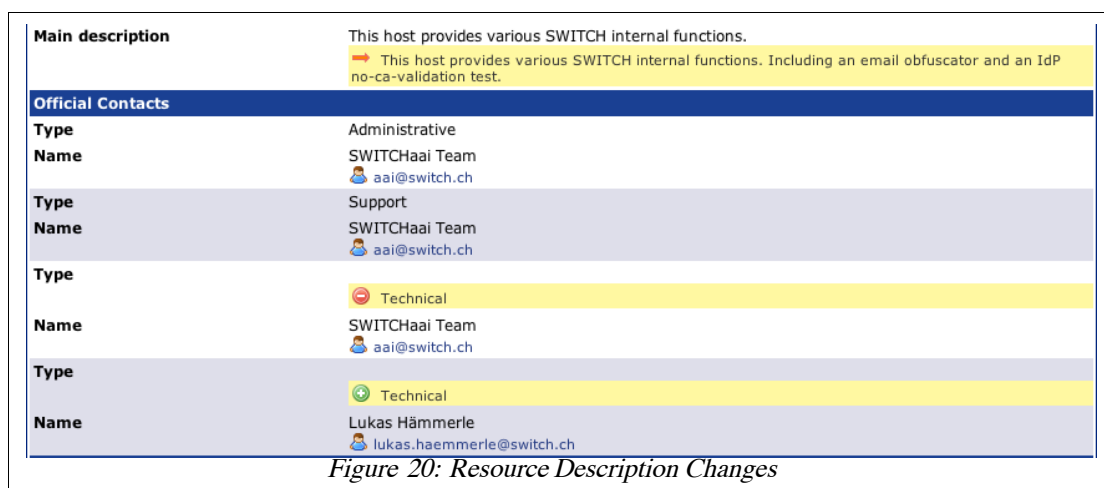


Figure 20: Resource Description Changes

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 a set of custom-tailored configuration files that can be used to configure the Service Provider. 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 can download either the Service Provider main configuration file (*shibboleth.xml* or *shibboleth2.xml*) or a whole set of configuration files, which are specifically adapted for the SWITCHaai or AAI Test federation.



**Configuration parameters**

**Installation setup**    
 Choose your installation setup to set some default values for this form

**Path to Shibboleth library**

**Path to 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 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.

**Download options**

Download configuration files as ZIP archive

Download configuration files as TAR archive

Only download shibboleth.xml/shibboleth2.xml

The complete set of configurations files includes shibboleth2.xml, attribute-map.xml, attribute-policy.xml, shibd.logger, shibboleth.logger, native.logger, the current metadata.xml and all Shibboleth HTML error pages. It is assumed that during the installation all default options were chosen (e.g. under Windows the standard port 1600).

**After downloading:**

1. Save and unpack the file in your Shibboleth configuration directory (e.g. /etc/shibboleth2/ or C:\opt\shibboleth2\etc\shibboleth\)
2. Restart your web server and the Shibboleth daemon
3. Define the web pages that shall be protected by AAI

This field must be provided

Figure 21: Download custom Service Provider configuration files

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

After a Resource has been approved, it is included in the official federation metadata. 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 the Basic Resource description setup. You can transfer this role also to other users later on. All Resource administrators have equal rights, there is no master Resource administrator.

### Duties as a Resource administrator

It is essential that all Home Organizations have an up to-date description of all Resources. 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:** There will be 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 each full hour if something changed. The Identity Provider should at least update metadata once a day. SWITCH even recommends to update hourly.

**Warning:** Replacing/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](mailto:aai@switch.ch) for assistance.

For policy reasons every Home Organization needs at least one RRA administrator, whose task is to approve Resource Descriptions. This includes the approval or rejection of

Resource Descriptions. An RRA administrator basically has to check that all Resources that are operated within his Home Organization are operated in compliance with the SWITCHaai Service Agreement (see <http://www.switch.ch/aai/agreement/>).

## 6. 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 are completed, the new Home Organization has to be registered with the Resource Registry. In order to do so, the 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, you have to go to <https://aai-rr.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](mailto:aai@switch.ch).

Figure 22: Bootstrapping procedure

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

General Information	
<b>Home Organization Name</b>	<input type="text" value="Example Home Org Name"/> <small>Usually the domain name of your organization, e.g. 'switch.ch', 'uzh.ch', 'zhwin.ch'</small>
<b>Federation</b>	<input type="text" value="AAI Test Federation"/>
Technical Information	
<b>entity ID</b>	<input type="text" value="https://idp.example.org/idp/shibboleth"/> <small>Use a URL https://&lt;HOSTNAME&gt;/idp/shibboleth. This URL should not resolve yet to a web page, but it should be possible to later on place an XML file at this location.</small>
<b>URL of Single Sign-on Handler</b>	<input type="text" value="https://idp.example.org/idp/profile/Shibboleth/SSO"/> <small>In Shibboleth 1.3 and 2.0 this is the location of the Shibboleth SSO-Handler e.g. https://aai-logon.example.ch/shibboleth-idp/SSO</small>
<b>SSO Certificate Subject</b>	<input type="text" value="idp.example.org"/> <small>The CN of the certificate subject, e.g. aai-logon.example.ch</small>
<b>URL of Attribute Query Handler</b>	<input type="text" value="https://idp.example.org:8443/idp/profile/SAML1/SOAP/AttributeQuery"/> <small>In Shibboleth 1.3 this is the location of the SAML 1.1 Attribute Authority, e.g. https://aai-logon.example.ch:8443/shibboleth-idp/AA For Shibboleth 2, you should use something of the form https://idp-aa.example.org/idp/profile/SAML1/SOAP/AttributeQuery or https://idp.example.org:8443/idp/profile/SAML1/SOAP/AttributeQuery</small>
<b>AA Certificate Subject</b>	<input type="text" value="idp.example.org"/> <small>The CN of the certificate subject, e.g. aai-aa.example.ch</small>
Contact address	
<b>Name</b>	<input type="text"/>
<b>E-Mail</b>	<input type="text"/>
<input type="button" value="Reset"/> <input type="button" value="Submit and wait for Approval"/>	
<small><span style="color: red;">•</span> This field must be provided</small>	

Figure 23: Bootstrapping registration form

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

**Note:** For now, one can only register SAML 1 Identity Providers using this bootstrapping process. After the Home Organization was approved by SWITCH, the Home Organization administrator can upgrade the description to be SAML 2 compliant.



Figure 24: Adding a new Home Organization Description

After submission of the bootstrapping form SWITCH will then approve or reject the new Home Organization within some days. In either case, you will receive a notification email with further instructions. After the Home Organization has been approved, you should be able to access the Resource Registry with an account of the newly set up Identity Provider.

The first time you log in as user from a newly approved Home Organization you will not only receive Home Organization rights as shown in Figure 24 but also Resource Registration Authority administration rights, described in the following Chapter .

You will have multiple options as Home Organization administrator. It is recommended that you edit the Home Organization description again because the first time you access the Resource Registry, only a very basic SAML 1.1 representation is created using data you entered during the Home Organization registration process. Edit the Home Organization Description by clicking the link "Edit Home Organization Description" on top of the page. This will bring you to the Home Organization Description menu shown in Figure 25. There, you will have to edit several sections in order to define various aspects of your Home Organization.

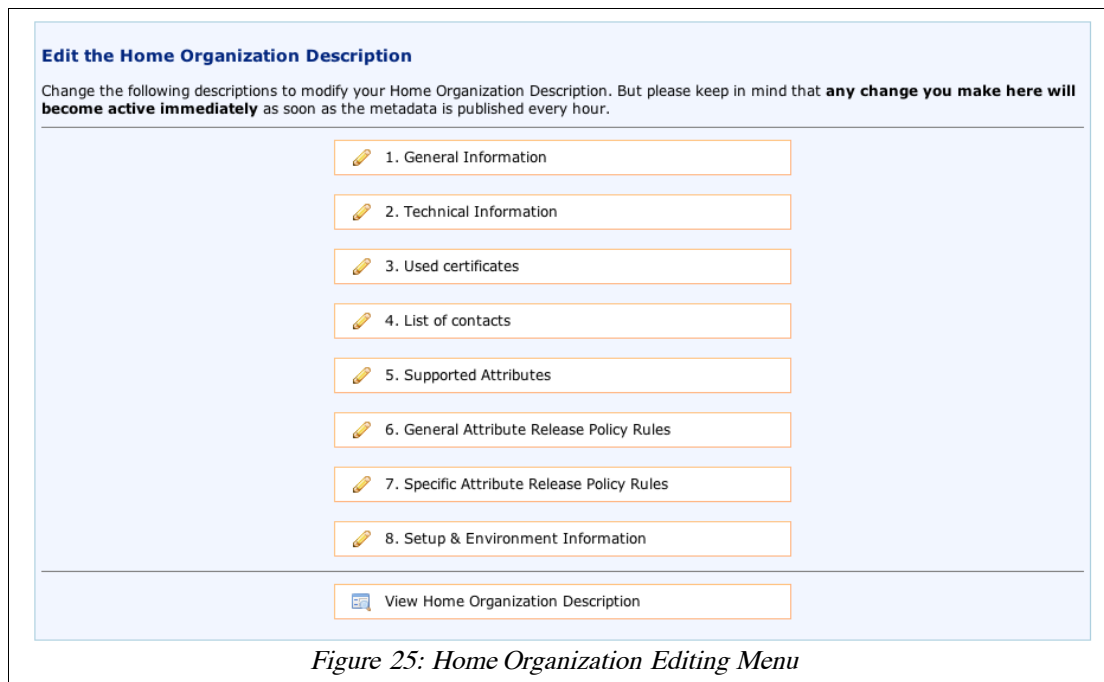


Figure 25: Home Organization Editing Menu

## General Information

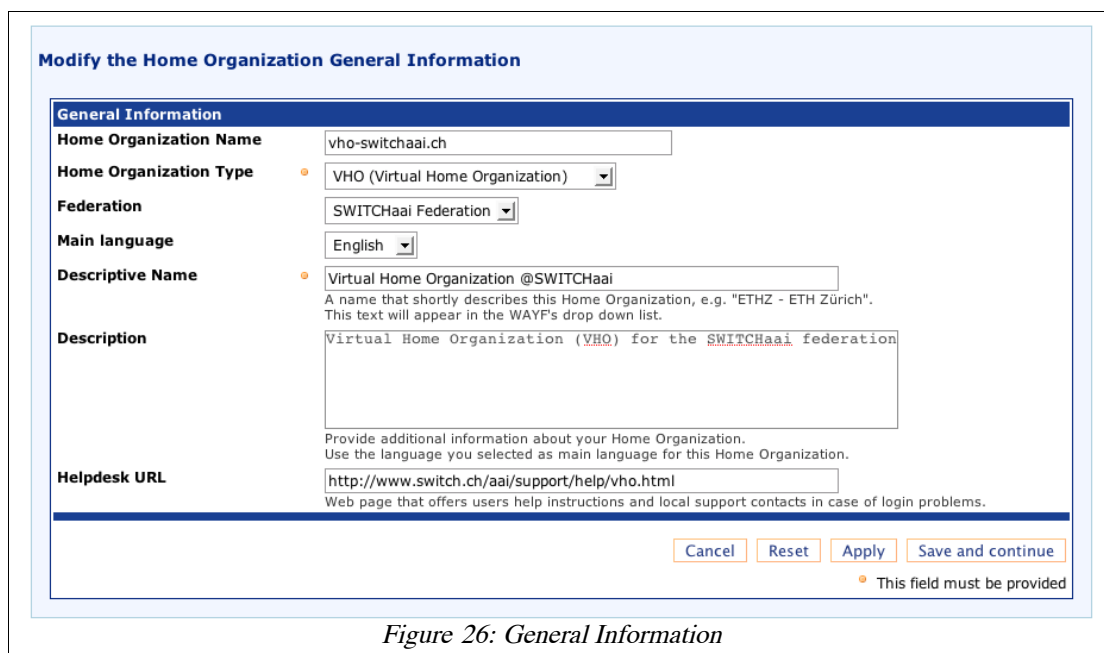


Figure 26: General Information

In the General Information section you first define the very basic settings of a Home Organization like its name, its Federation, a description and a help desk web page like shown in Figure 26. All of these settings 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.

## 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. While the *entityID* used to be a URN of the form 'urn:mace:switch.ch:SWITCHAai:some-organization.ch', we now recommend to use an entityID of the form of a URL (e.g. '<https://some-organization.ch/idp/shibboleth>'), similar to the ID of Service Providers. It is highly recommended that the used host name

Bear in mind that changing any of the following values can cause service disruptions because users won't be able to log in or because the Service Providers cannot request attributes anymore until they have updated their metadata.

Please ask [aai@switch.ch](mailto:aai@switch.ch) for assistance before you change any of these values

Technical Information	
Entity ID *	<input type="text" value="https://vho-switchaai.ch/idp/shibboleth"/> <p>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://&lt;HOSTNAME&gt;/idp/shibboleth</code>. This URL should not resolve yet to a web page, but it should be possible later on to place an XML file at this location. For SAML 1 based Identity Providers, please use only URN values e.g. under the urn:mace hierarchy. Refer to the examples or to SWITCH MACE for further information.</p>
SingleSignOnService	
SAML1 AuthnRequest binding *	<input type="text" value="https://aai.vho-switchaai.ch/idp/profile/Shibboleth/SSO"/>
SAML2 HTTP-POST binding	<input type="text" value="https://aai.vho-switchaai.ch/idp/profile/SAML2/POST/SSO"/>
SAML2 HTTP-POST-SimpleSign binding	<input type="text" value="https://aai.vho-switchaai.ch/idp/profile/SAML2/POST-SimpleSign/SSO"/>
SAML2 HTTP-Redirect binding	<input type="text" value="https://aai.vho-switchaai.ch/idp/profile/SAML2/Redirect/SSO"/>
AttributeService	
SAML1 SOAP binding *	<input type="text" value="https://aai.vho-switchaai.ch:8443/shibboleth-idp/profile/SAML1/SOAP/AttributeQue"/>
SAML2 SOAP binding	<input type="text" value="https://aai.vho-switchaai.ch:8443/shibboleth-idp/profile/SAML2/SOAP/AttributeQue"/>
ArtifactResolutionService	
SAML1 SOAP binding	<input type="text" value="https://aai.vho-switchaai.ch/idp/profile/SAML1/SOAP/ArtifactResolution"/>
SAML2 SOAP binding	<input type="text" value="https://aai.vho-switchaai.ch/idp/profile/SAML2/SOAP/ArtifactResolution"/>

\* This field must be provided

Figure 27: Technical Information

exists because in the future the *entityID* URL may be used to retrieve an entity's metadata. However, before you do this, please consult our migration guide on the AAI web page that will be available shortly after the Identity Provider deployment guide.

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

As for the Identity Provider service endpoints, you may use one of the available assistants in order to complete the form depending on which Identity Provider version you are using. The assistant then will use the root URL you provide to generate the default service locations for the given bindings as shown in Figure 27.

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

**Warning:** Modifying any properties in the Technical Information section has to be done very carefully because these changes will take some time to propagate to all Service Providers. The propagation via the metadata may take up several days during which your users may not be able to access Resources whose metadata has not yet been updated. If in doubt about a property you want to change, please send an email to [aai@switch.ch](mailto:aai@switch.ch) for assistance.

## Used Certificates

In the Used Certificates sections you have to provide the subject common names or the certificates themselves that are used by Shibboleth and the web server running the Identity Provider.

It is recommended that you provide subject common name as well as the certificates themselves although one of them would be sufficient to provide. Use the assistant in order to complete the form for you. As the name implies, the backup certificates could be used in case of emergency fall back certificates. This could be useful if your server was compromised and you have to replace the main certificates quickly. In such a case you

would just replace the certificates used by your web server and by Shibboleth with the backup certificates.

The Resource Registry will expire certificates if they have been used for more than 3 years even though the certificates validity may be longer. Before this is going to happen, you will however receive several notification emails announcing this procedure.

Certificate rollover must be done carefully. You have to make sure that the new certificate has been contained in the metadata for at least two days before the Service Provider actually can use this new certificate. Please refer to the Service Provider deployment guides at <http://www.switch.ch/aai/support/serviceproviders/> on how to carry out the certificate rollover.

**Note:** If you want to make use of the backup certificates, 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.

**Certificate Information**

- You have to provide A., the common names (CN) of the certificates in section A. Optionally you can provide B., the certificates themselves that Shibboleth and the web server are using.  
**It is recommended to provide A. and B.**

**A. Certificate Subject Common Name**

Certificate used by Shibboleth (SSO)	Certificate used by web server (AA)
This is the certificate configured in the <code>idp.xml</code> (Shibboleth 1.3) or <code>relying-party.xml</code> (Shibboleth 2.0)	This is the certificate configured in your Apache/IIS/Tomcat web server for the AA host. Try using the assistant to get the web server's certificate
<input type="text" value="aai.vho-switchaai.ch"/>	<input type="text" value="aai.vho-switchaai.ch"/>

**CN of the certificate subject**

If the certificate has several common names, you should provide only the first one.  
**Example:** If the certificate's subject is 'C=CH/O=Test Organization/OU=Test Department/CN=server.example.ch' you should provide 'server.example.ch' as the common name.

**B. Embedded certificates**

PEM formatted X.509 certificate	Backup PEM formatted X.509 certificate
<pre> A1UEBhMCQkUxEzARBqNVBAoTCkN5YmVydHJlc3QxPzZAbmFsIENBMSIwIAYDVQ0EEx1DeWJlcnRydXN0IEVkdWNMDUxOTE0MzIyNFoXDTEyMDUxOTE0MzIyNFowbWZELMkBAoTN1N3aXRjaCAatIFRlbGVpbmZvcmlhdGlrZGllbnNlZCBGbzJzY2h1bmcxHTAbBgNVBAMTFGFhaS52aG8tc3dAbGkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvbmB06D </pre>	<pre> -----BEGIN CERTIFICATE----- MIIExzCCA6+gAwIBAgILAQAAAAABGgY14UwDQYJKoZIhvcNAQEBBQADSwAwSAQBAQkUxEzARBqNVBAoTCkN5YmVydHJlc3QxPzZAbmFsIENBMSIwIAYDVQ0EEx1DeWJlcnRydXN0IEVkdWNMDUxOTE0MzIyNFoXDTEyMDUxOTE0MzIyNFowbWZELMkBAoTN1N3aXRjaCAatIFRlbGVpbmZvcmlhdGlrZGllbnNlZCBGbzJzY2h1bmcxHTAbBgNVBAMTFGFhaS52aG8tc3dAbGkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvbmB06D </pre>
<input type="text"/>	<input type="text"/>

Use the backup certificate for certificate roll over if you want to replace the first certificate. Which of the certificates is the backup certificate is not important because both will be included equally in the metadata.

Click in a textarea containing a certificate in order to see some additional details about it.

**Subject:** / C=CH / O=Switch - Teleinformatikdienste fuer Lehre und Forschung / CN=aai.vho-switchaai.ch  
**Type:** Issued  
**Issuer:** / C=BE / O=Cybertrust / OU=Educational CA / CN=Cybertrust Educational CA  
**Expiration date:** May 19 14:32:24 2011 GMT  
**Fingerprint:** 48:83:3E:43:64:B3:17:95:40:7B:0A:1F:FE:F6:9A:6B:9C:C5:76:77

Cancel Reset Apply Save and Continue

Figure 28: Used Certificates

## List of Contacts

As for every Service Provider, one should add contact persons for a Home Organization that can be contacted in case of support or technical inquiries. Although it is not mandatory to provide contact persons, it is strongly recommended to do so. Support and technical contact names and addresses 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.

## Supported Attributes

As the name suggests, the Supported Attributes section's purpose is to declare the attributes an Identity Provider can release. As depicted in Figure 29, 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 only within the same organization or within a small subset of organizations on the basis of a bilateral agreement.

Attributes supported			
SWITCHaai Attributes	Local/Bilateral Attributes		
Affiliation (mandatory) ⓘ	<input checked="" type="checkbox"/>	AAA Usage Limit ⓘ	<input type="checkbox"/>
E-mail (mandatory) ⓘ	<input checked="" type="checkbox"/>	Assurance Level ⓘ	<input type="checkbox"/>
Given name (mandatory) ⓘ	<input checked="" type="checkbox"/>	Authorization attribute ⓘ	<input type="checkbox"/>
Home organization (mandatory) ⓘ	<input checked="" type="checkbox"/>	Lausanne Group membership ⓘ	<input type="checkbox"/>
Home organization type (mandatory) ⓘ	<input checked="" type="checkbox"/>	Organization Unit Code ⓘ	<input type="checkbox"/>
Surname (mandatory) ⓘ	<input checked="" type="checkbox"/>	Organizational Unit ⓘ	<input type="checkbox"/>
Unique ID (mandatory) ⓘ	<input checked="" type="checkbox"/>	Principal Name ⓘ	<input type="checkbox"/>
Business phone number (recommended) ⓘ	<input checked="" type="checkbox"/>	UZH SAP User ID ⓘ	<input type="checkbox"/>
Business postal address (recommended) ⓘ	<input checked="" type="checkbox"/>		
Matriculation number (recommended) ⓘ	<input type="checkbox"/>		
Staff category (recommended) ⓘ	<input type="checkbox"/>		
Study branch 3 (recommended) ⓘ	<input type="checkbox"/>		
Study level (recommended) ⓘ	<input type="checkbox"/>		
Date of birth (optional) ⓘ	<input type="checkbox"/>		
Employee number (optional) ⓘ	<input type="checkbox"/>		
Entitlement (optional) ⓘ	<input checked="" type="checkbox"/>		
Gender (optional) ⓘ	<input type="checkbox"/>		
Home postal address (optional) ⓘ	<input type="checkbox"/>		
Mobile phone number (optional) ⓘ	<input type="checkbox"/>		
Organization path (optional) ⓘ	<input type="checkbox"/>		
Organizational unit path (optional) ⓘ	<input type="checkbox"/>		
Persistent ID (optional) ⓘ	<input type="checkbox"/>		
Preferred Language (optional) ⓘ	<input checked="" type="checkbox"/>		
Private phone number (optional) ⓘ	<input type="checkbox"/>		
Study branch 1 (optional) ⓘ	<input type="checkbox"/>		
Study branch 2 (optional) ⓘ	<input type="checkbox"/>		
User ID (optional) ⓘ	<input type="checkbox"/>		

**Don't forget to update the Attribute Release Policy preferences after you changed the supported attributes above.**

Figure 29: Supported Attributes

**List of Contacts**

At least one **support and one technical** contact should be provided:

- **Administrative contact:** The person that is generally responsible for AAI.
- **Technical contact:** The person that is responsible for the host and the Shibboleth Identity Provider.
- **Support contact:** The person that is responsible for the user directory, e.g. when users lost their password.

**Be aware that all data you provide will be included in the federation metadata and some user helpdesk web pages. Therefore, it will be published online and accessible for all Internet users.**

List of contacts	
<b>Contact Type</b>	Technical
<b>Contact Name</b>	SWITCHaai Team
<b>E-Mail</b>	aai@switch.ch
<b>Contact Type</b>	Support
<b>Contact Name</b>	SWITCHaai Team
<b>E-Mail</b>	aai@switch.ch
<b>Contact Type</b>	Administrative
<b>Contact Name</b>	Thomas Lenggenhager
<b>E-Mail</b>	lenggenhager@switch.ch
<b>Contact Type</b>	Billing
<b>Contact Name</b>	
<b>E-Mail</b>	
<b>Contact Type</b>	Administrative
<b>Contact Name</b>	
<b>E-Mail</b>	

Cancel   Reset   Apply   Save and continue

Figure 30: List of Contacts

According to the AAI Attribute Specification (see <http://www.switch.ch/aai/attributes>) your Identity Provider must be able to release at least the red (mandatory) attributes. However, the attributes will only be released if needed and generally only a small subset of attributes will be released to a resource.

### General Attribute Release Policy

In the General Attribute Release Policy a Home Organization administrator defines the general behavior regarding the release of attributes that will be reflected in the generated arp.site.xml (Shibboleth 1.3) or attribute-filter.xml (Shibboleth 2.0) files. Basically, one defines whether an attribute shall be released in case a Resource administrator defines it as 'required' or as 'desired' as shown in Figure 30.

**Note:** Only these attributes are shown which can be released by an 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.



Each resource has to self-declare the attributes that it needs by marking them as **required** (e.g. for user authentication) or **desired** (e.g. for user specific personalization). Decide if by default the Identity Provider should release attributes marked as **required** (highly recommended) and those marked as **desired** (recommended).

Attributes that are set to **Release** will in general be released for unless there is a user ARP file that denies the release. If you set the attribute to **Don't Release**, the attribute won't be released in the default configuration but it also won't be denied completely. In this case, the attribute only is released if there is a user ARP file that explicitly states that the attribute shall be released. The value **forbid** has the effect for Shibboleth 1.3 that an attribute under no circumstances will be released, even not if there is a user ARP file that would release it.

Shibboleth 2.x Identity providers will only release an attribute if it is set to **Release**. The other two options won't release the attribute.

Only attributes that are supported by your Home Organization are shown on this page. You must [modify the supported attributes](#) of your Home Organization first before you can define rules for them on this page.

Attribute Name	Required Policy	Desired Policy
Affiliation (mandatory) ⓘ	Release ▼	Release ▼
E-mail (mandatory) ⓘ	Release ▼	Release ▼
Given name (mandatory) ⓘ	Release ▼	Release ▼
Home organization (mandatory) ⓘ	Release ▼	Release ▼
Home organization type (mandatory) ⓘ	Release ▼	Release ▼
Surname (mandatory) ⓘ	Release ▼	Release ▼
Unique ID (mandatory) ⓘ	Release ▼	Release ▼
Business phone number (recommended) ⓘ	Release ▼	Release ▼
Business postal address (recommended) ⓘ	Release ▼	Release ▼
Entitlement (optional) ⓘ	Release ▼	Don't release ▼
Preferred Language (optional) ⓘ	Release ▼	Release ▼

**Note on Attribute Implementation:**  
**Mandatory** attributes are the SWITCHaai core attributes and **must** be available for all users.  
**Recommended** attributes **should** be implemented by all Home Organizations.  
**Optional** attributes **may be** implemented by all Home Organizations.

Figure 31: General Attribute Release Policy

### Specific Attribute Release Policy

While you could define a very general attribute release policy in the previous section, you can define very fine-grained rules in the Specific Attribute Release Policy section. As is shown in Figure 32, one can create custom-tailored rules for each Resource. Either a Resource can be totally excluded from the attribute-filter or one can specify attributes that shall not be released even though they are required or desired by the Resource administrator. For every Resource only the required and desired attributes are shown. If no specific rule is created for an attribute, the general attribute release policy will be applied.

Excluding a Resource from the attribute-filter.xml file is useful if an Identity Provider administrator wants 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](#). These rules can base the release decision on almost any criteria that one can possibly think of.

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

**Note:** The Specific Attribute Policy can only be used in conjunction with a Shibboleth 2.0 Identity Provider because it only will affect the attribute-filter.xml files generated by the Resource Registry. In case of Shibboleth 1.3, one can define specific rules for the arp.site.xml file using the [updateARP tool](#).

### Home Organization Setup & Environment

The last Home Organization section is the '*Setup & Environment*' section, which is shown in Figure 33. It is purely informational and solely serves the SWITCHaai team members as well as other Home Organization administrators to examine how different Identity Providers are set up. This allows to compare similar setups in case of problems or planning setup changes.

For **Shibboleth Identity Providers 2.x only**, define custom rules for certain Resources by specifying the attributes that shall be released. All further attributes, won't be released. You may also remove a Resource completely. That is useful if you want to create your own special rule for this resource using [advanced attribute filters](#).

In order to use your own rules, you create a separate `custom-attribute-filter.xml` file and [configure it](#) in the IdP's `service.xml`. Either choose to remove the Resource or select the attributes that you want to release or not release. In case you don't care about an attribute's rule and set the value to '-' the general ARP rule applies.

### Existing Specific ARP Rules

Resources	Actions
1. SWITCH, eConf Admin Portal, <a href="https://econfadmin.switch.ch/shibboleth">https://econfadmin.switch.ch/shibboleth</a> (switch.ch)	Edit
2. Microsoft Academic Software Distribution Pilot, <a href="https://shibboleth02.e-academy.com/shibboleth">https://shibboleth02.e-academy.com/shibboleth</a> (unibe.ch)	Edit

### Specific ARP Rule

**Attribute Release Policy Rule**

**Resource** <https://shibboleth02.e-academy.com/shibboleth>  
 Rule for Resource: **Microsoft Academic Software Distribution Pilot**  
 Create rule for another Resource...

**Exclude**  This will exclude the resource from the generated attribute filter file  
 Allows you to create your own custom attribute filter rule for this resource

**Required Attributes**

**Home organization** -

**Home organization type** -

**Unique ID** Don't Release

**Desired Attributes**

**Affiliation** Don't Release

#### Note on Attribute Implementation:

**Mandatory** attributes are the SWITCHHaai core attributes and **must** be available for all users.  
**Recommended** attributes **should** be implemented by all Home Organizations.  
**Optional** attributes **may be** implemented by all Home Organizations.

Figure 32: Specific Attribute Release Policy

### Home Organization Setup and Environment Information

Please specify on this page what is your Identity Provider setup. This may help us and others on one side to see which setups are preferred and on the other side it may be useful when it comes to pinpoint problems. In case, you don't find an option in the drop-down list, please choose "Other" and provide a comment in the textfield on the right.

**Setup & Environment Information**

**Operating system** Debian Linux

**Webserver** Tomcat + Apache

**Authentication System** CAS 3

**IdP version** 1.3.3

**Comments**  
 Uses custom CAS authentication module in order to access MySQL database.

Figure 33: Setup & Environment

## 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.

However, if you do so, please consult [aai@switch.ch](mailto: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. For Shibboleth 1.3 there is a [metadatarrefresh script](#) that can be used to automate it. We recommend to run this tool at least once a day. For Shibboleth 2.x please use the built-in metadata provider that reads the metadata from a URL and stores a backup copy locally. For Shibboleth 2.0 it is recommended to update metadata more frequently because the file only will be downloaded if it changed.

**Note:** There will be a delay for changes to be applied, due to the delay for metadata refresh at the Service Providers.

- Regularly update your 1.3 Identity Provider's arp.site.xml file. SWITCH has developed a tool called [updateARP](#) that downloads your custom-tailored ARP file and can even more customize it according to rules you can set in a configuration. For a 2.x Identity Provider, please use the built-in attribute-filter provider that reads the file from a URL.

**Note:** You don't have to restart your Identity Provider after updating the metadata or the ARP file. However, it takes about a minute until the Identity Provider notices that these files changed.

## 7. Resource Registration Authority Administrator

### Duties as Resource Registration Authority (RRA) administrator

For policy reasons every Home Organization requires at least one RRA administrator, whose task it is to decide whether to approve or reject a submitted Resource Descriptions. Therefore, an RRA administrator has to examine and make sure that all Resources registered for his Home Organization are operated in compliance with the SWITCHaai Service Agreement (see <http://www.switch.ch/aai/agreement/>). 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 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 prior to approve it. The Resource Registry will in some situations show 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 receive a notification e-Mail. After login, an RRA administrator will notice the Resource Descriptions that need to be approved in the Resource Registration tab as shown in Figure 34.

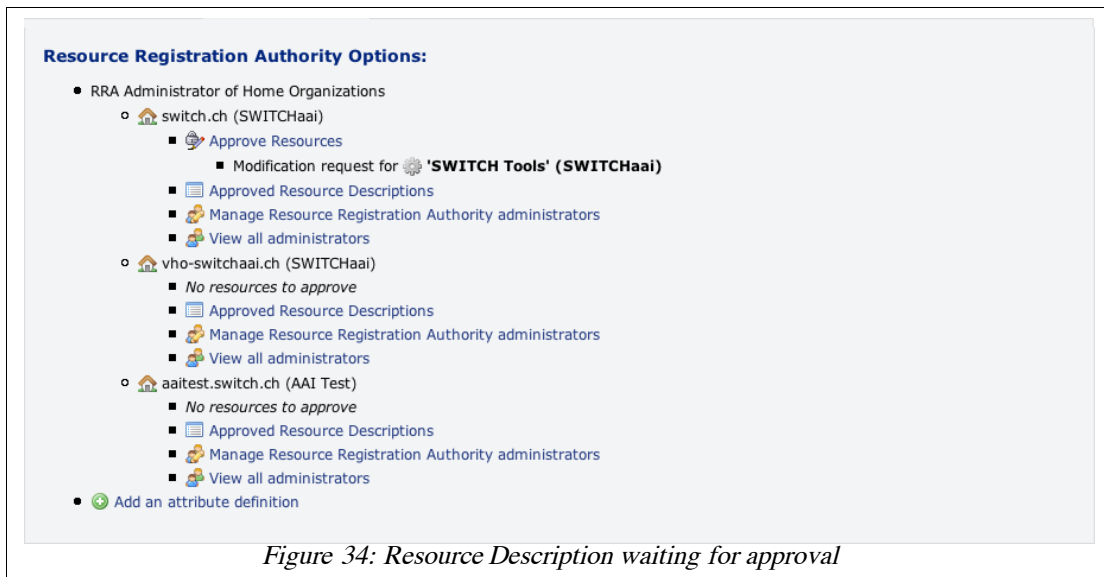


Figure 34: Resource Description waiting for approval

Clicking the “Approve Resources” link then leads to a page like in Figure 35.

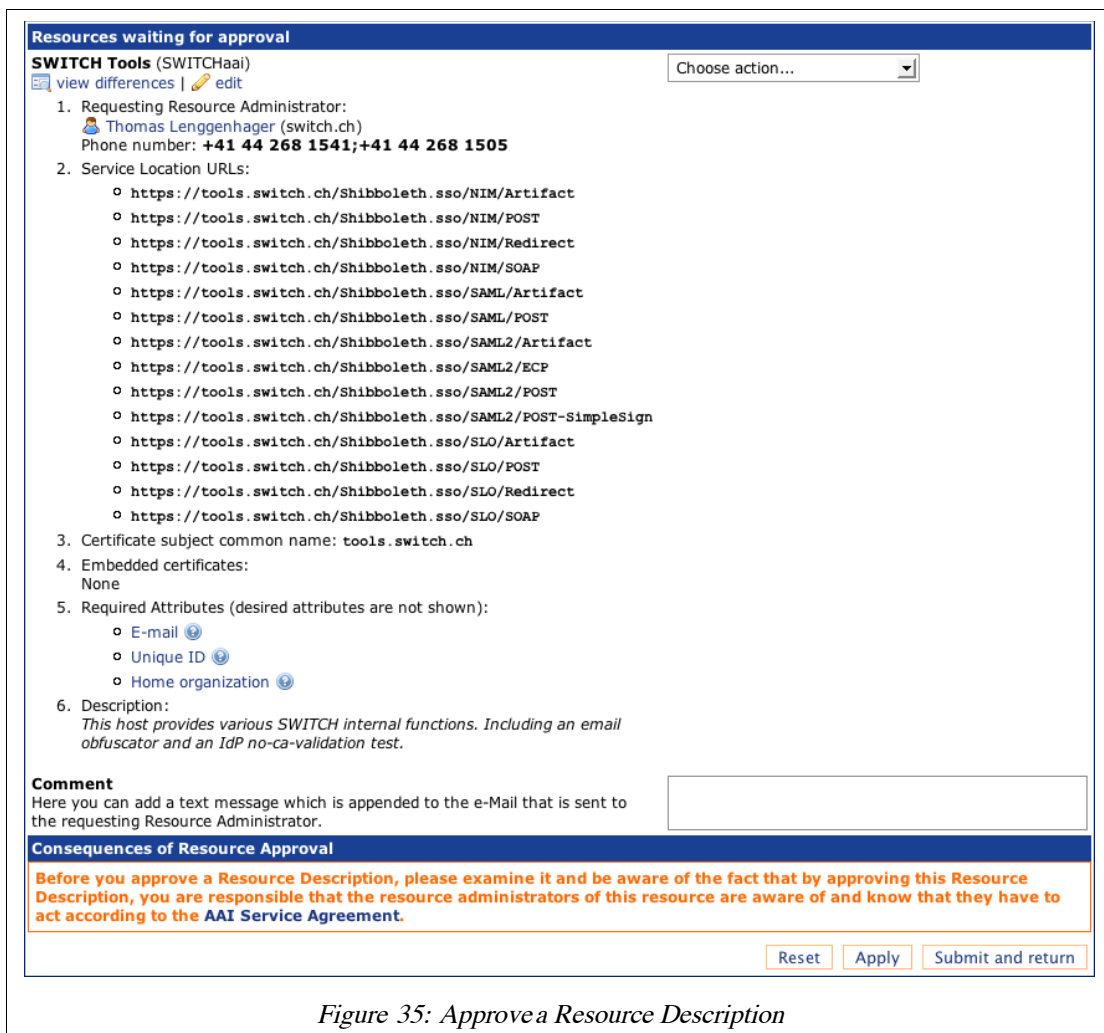


Figure 35: Approve a Resource Description

Figure 35 shows a single Resource Description to approve or reject. Clicking on '*View changes*' an RRA administrator can inspect the changes before approving it, as is shown in Figure 20.

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

## Miscellaneous

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

## Resource Registry data usage

As was pointed out, data stored in the Resource Registry doesn't only serve the management of the SWITCH federations but data also is used for informational purposes. In particular, the following web pages directly access data from the Resource Registry:

- <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/metadata/monitoring.php>

If a Resource Description is changed, this is immediately reflected on the above web pages as soon as the change gets approved.

## Facts about the Resource Registry

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

All development work has been done by SWITCH. The code is protected by a BSD-like license and can be requested by sending an email to [aai@switch.ch](mailto:aai@switch.ch).