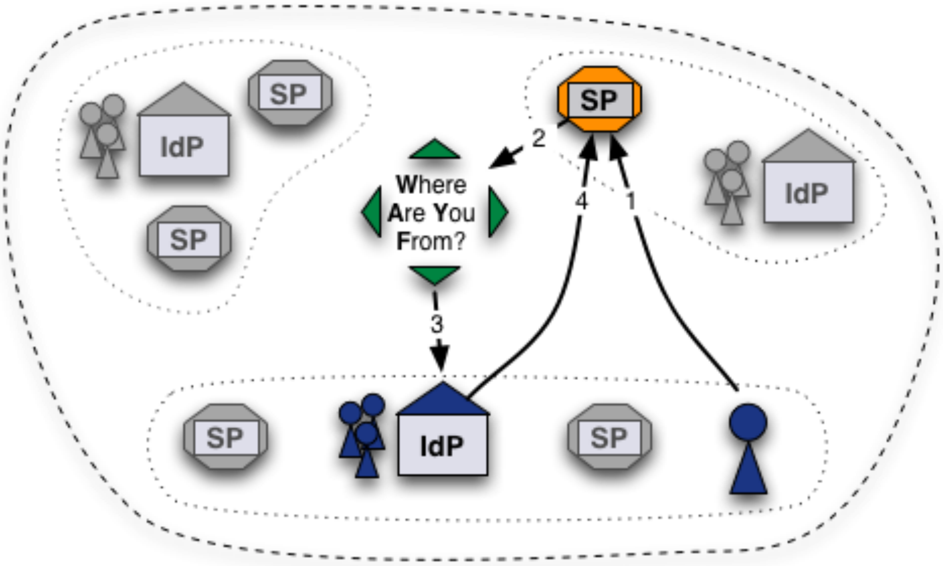
Discovery Service Options

SWITCHaai Team
aai@switch.ch

No Central WAYF for Interfederation

- The classic way: One WAYF per Federation



WAYF achieves high availability through redundancy and IP Anycast.

Alternatives to Central WAYF

- Direct Login URLs
- SWITCH Embedded WAYF

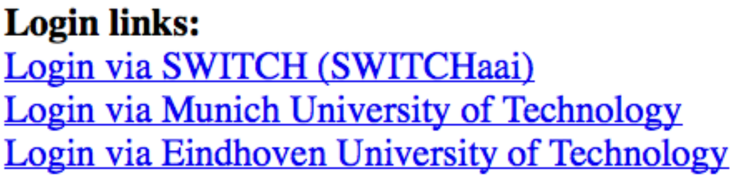
SWITCH
WAYF

- Shibboleth Embedded Discovery Service

Shibboleth.
EDS

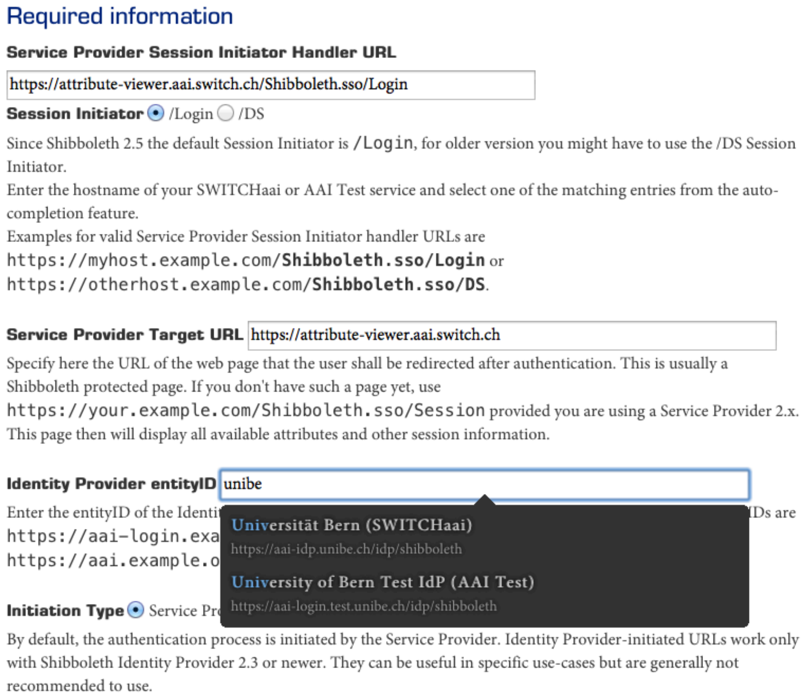
Solution 1: Direct Login URLs

- A separate login link for a specific IdP
- 1 click direct redirect to IdP without going via WAYF
- Useful when only users of few IdPs use resource



Login links:
Login via SWITCH (SWITCHaai)
Login via Munich University of Technology
Login via Eindhoven University of Technology

Composing Login URLs



Required information

Service Provider Session Initiator Handler URL

https://attribute-viewer.aai.switch.ch/Shibboleth.sso/Login

Session Initiator ● /Login ○ /DS

Since Shibboleth 2.5 the default Session Initiator is `/Login`, for older version you might have to use the /DS Session Initiator.
Enter the hostname of your SWITCHaai or AAI Test service and select one of the matching entries from the auto-completion feature.
Examples for valid Service Provider Session Initiator handler URLs are
`https://myhost.example.com/Shibboleth.sso/Login` or
`https://otherhost.example.com/Shibboleth.sso/DS`.

Service Provider Target URL https://attribute-viewer.aai.switch.ch

Specify here the URL of the web page that the user shall be redirected after authentication. This is usually a Shibboleth protected page. If you don't have such a page yet, use
`https://your.example.com/Shibboleth.sso/Session` provided you are using a Service Provider 2.x.
This page then will display all available attributes and other session information.

Identity Provider entityID unibe

Enter the entityID of the Identi IDs are
`https://aai-login.exa`
`https://aai.example.o`

Universität Bern (SWITCHaai)
https://aai-idp.unibe.ch/idp/shibboleth

University of Bern Test IdP (AAI Test)
https://aai-login.test.unibe.ch/idp/shibboleth

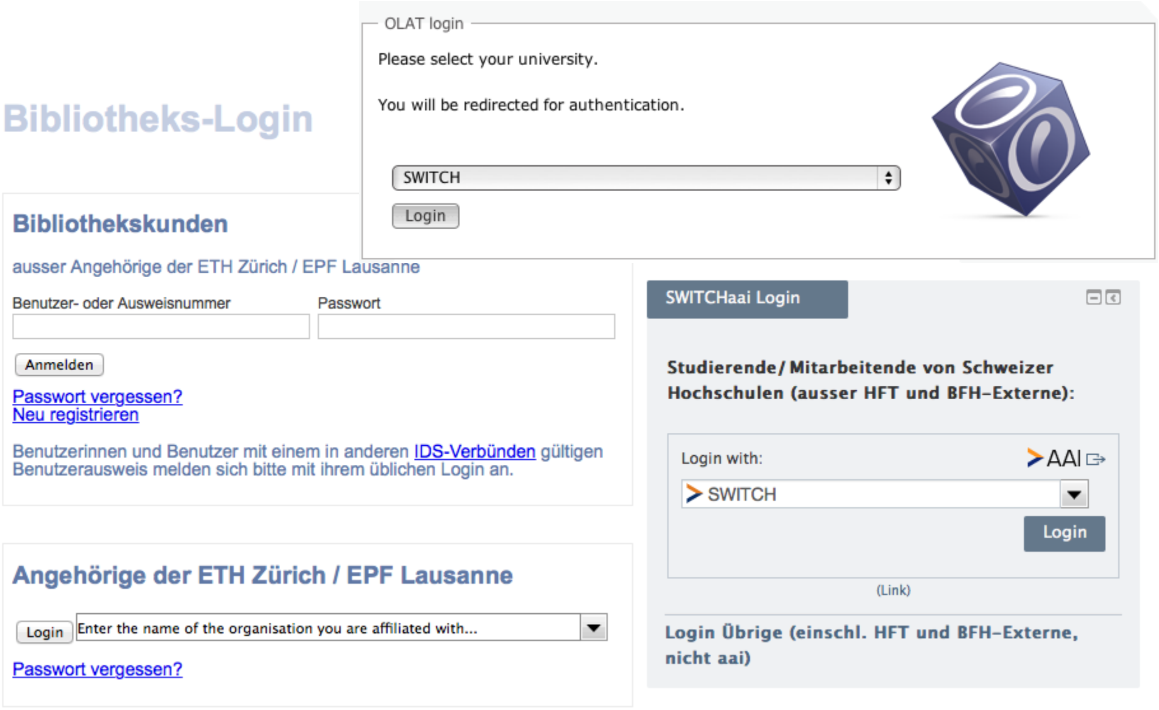
Initiation Type ● Service Pr

By default, the authentication process is initiated by the Service Provider. Identity Provider-initiated URLs work only with Shibboleth Identity Provider 2.3 or newer. They can be useful in specific use-cases but are generally not recommended to use.

https://www.switch.ch/aai/guides/discovery/login-link-composer/

Solution 2: Embedded WAYF

SWITCH WAYF



Bibliotheks-Login

OLAT login

Please select your university.

You will be redirected for authentication.

SWITCH

Login

Bibliothekskunden

ausser Angehörige der ETH Zürich / EPF Lausanne

Benutzer- oder Ausweisnummer | Passwort

Anmelden

Passwort vergessen?
Neu registrieren

Benutzerinnen und Benutzer mit einem in anderen IDS-Verbünden gültigen Benutzerausweis melden sich bitte mit ihrem üblichen Login an.

Angehörige der ETH Zürich / EPF Lausanne

Login | Enter the name of the organisation you are affiliated with...

Passwort vergessen?

SWITCHaai Login

Studierende/ Mitarbeitende von Schweizer Hochschulen (ausser HFT und BFH-Externe):

Login with: AAI

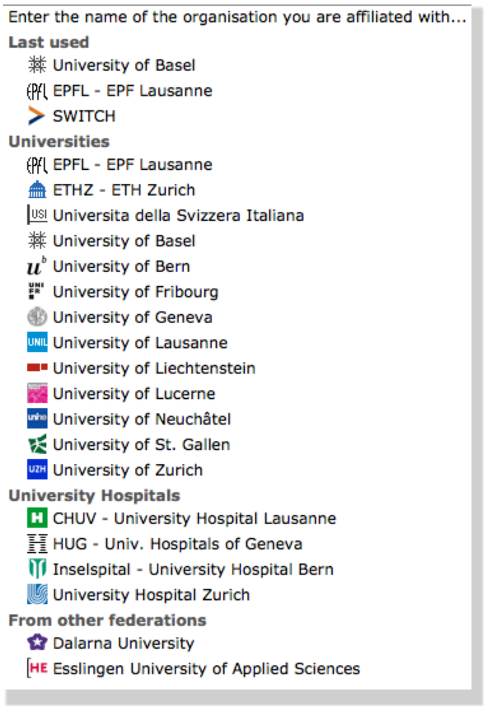
SWITCH

Login

(Link)

Login Übrige (einschl. HFT und BFH-Externe, nicht aai)

Embedded WAYF



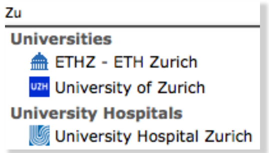
Enter the name of the organisation you are affiliated with...

Last used
- University of Basel
- EPFL - EPF Lausanne
- SWITCH

Universities
- EPFL - EPF Lausanne
- ETHZ - ETH Zurich
- Universita della Svizzera Italiana
- University of Basel
- University of Bern
- University of Fribourg
- University of Geneva
- University of Lausanne
- University of Liechtenstein
- University of Lucerne
- University of Neuchâtel
- University of St. Gallen
- University of Zurich

University Hospitals
- CHUV - University Hospital Lausanne
- HUG - Univ. Hospitals of Geneva
- Inselspital - University Hospital Bern
- University Hospital Zurich

From other federations
- Dalarna University
- Esslingen University of Applied Sciences



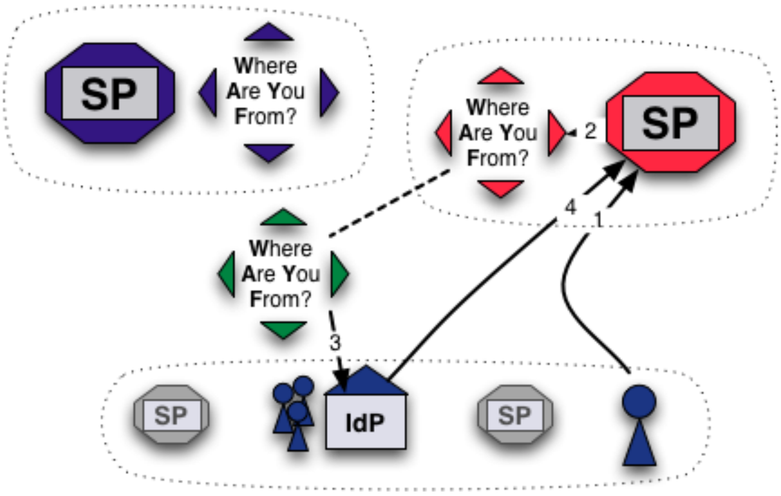
Zu

Universities
- ETHZ - ETH Zurich
- University of Zurich

University Hospitals
- University Hospital Zurich

Embedded WAYF

- Embed WAYF on Web Application
- customize look and feel
- still transparently uses central WAYF



Information and Configuration

More information about the Embedded WAYF:

https://www.switch.ch/aai/guides/discovery/embedded-wayf/

Generate the Embedded WAYF code for your SP:

https://rr.aai.switch.ch/gen_embedding_code.php

Configuration

Configuration Example of Embedded WAYF

```
// Example of how to add Identity Provider from other federations
var wayf_additional_idps = [
        {name:"Esslingen University of Applied Sciences",
        entityID:"https://idp.hs-esslingen.de/idp/shibboleth",
        logoURL:"https://www2.hs-esslingen.de/favicon.ico"
        },
        {name:"Dalarna University",
        entityID:"https://login.du.se/idp/shibboleth",
        logoURL:"https://login.du.se/duse-logo-16x16.png"
        }
];
```

Configuration (2)

Configuration Example of Embedded WAYF

```
// EntityIDs of Identity Provider that should not be shown at all
// [Optional, commented out by default]

var wayf_hide_idps = new Array ("https://idemfero.units.it/idp/shibboleth",
"https://idp.it.su.se/idp/shibboleth");

// Categories of Identity Provider that should not be shown
// Possible values
   are:"university","uas","hospital","library","vho","others","all"

var wayf_hide_categories =  new Array("library","vho","others","hospital");
```

Enable JSON Discovery feed to use local metadata of SP

In shibboleth2.xml:

```
  <Sessions lifetime="28800"
                   timeout="3600"
                   relayState="ss:mem"
                   checkAddress="false"
                   consistentAddress="true"
                   handlerSSL="true"
                   cookieProps="https">
...
 <!-- JSON feed of discovery information. -->
      <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>
  </Sessions>
```

JSON Discovery feed example

SP

JSON result of an example discovery feed:
https://sp.example.org/Shibboleth.sso/DiscoFeed

```
[
{ "entityID": "https://shibboleth-idp.uni-goettingen.de/uni/shibboleth",
 "DisplayNames": [
  { "value": "Georg-August Universität Göttingen", "lang":  "de" },
  { "value": "Georg-August University Göttingen", "lang":  "en" }
  ]
},
{ "entityID": "https://login.ntua.gr/idp/shibboleth",
"DisplayNames": [
  { "value": "National Technical University of Athens", "lang": "en" },
  { "value": "Εθνικό Μετσόβιο Πολυτεχνείο", "lang": "el" }
  ]
},
]
```

Configuration (3)

WAYF

Configuration Example of Embedded WAYF

```
// Whether to load Identity Providers from the Discovery Feed provided by
// the Service Provider.
// IdPs that are not listed in the Discovery Feed and that the SP therefore is
// not able to accept assertions from, are hidden by the Embedded WAYF
// IdPs that are in the Discovery Feed but are unknown to the SWITCHwayf
// are added to the wayf_additional_idps.
// The list wayf_additional_idps will be sorted alphabetically
// The SP must have configured the discovery feed handler that generates a
// JSON object. Otherwise it won't generate the JSON data containing the IdPs.
// [Optional, default:false]

var wayf_use_disco_feed = true;
```

MetadataFilter Example

SP

In shibboleth2.xml:

```
<MetadataProvider type="XML" .....>

    <MetadataFilter type="Whitelist">
       <Include>https://idp.nordu.net/idp/shibboleth</Include>
       <Include>https://idp.ids-mannheim.de/idp/shibboleth</Include>
       <Include>https://shibboleth.fhwn.ac.at/idp/shibboleth</Include>
       <Include>https://idp.it.su.se/idp/shibboleth</Include>
       <Include>https://tumidp.lrz.de/idp/shibboleth</Include>
    </MetadataFilter>

</MetadataProvider>
```

Solution 3:
Embedded Discovery Service

EDS

- Requires the Discovery Feed provided by the SP
- Embed the DS directly into the service
- Search-as-you-type or select from list
- JavaScript, CSS and HTML only
- developed and maintained by the Shibboleth team
- download from

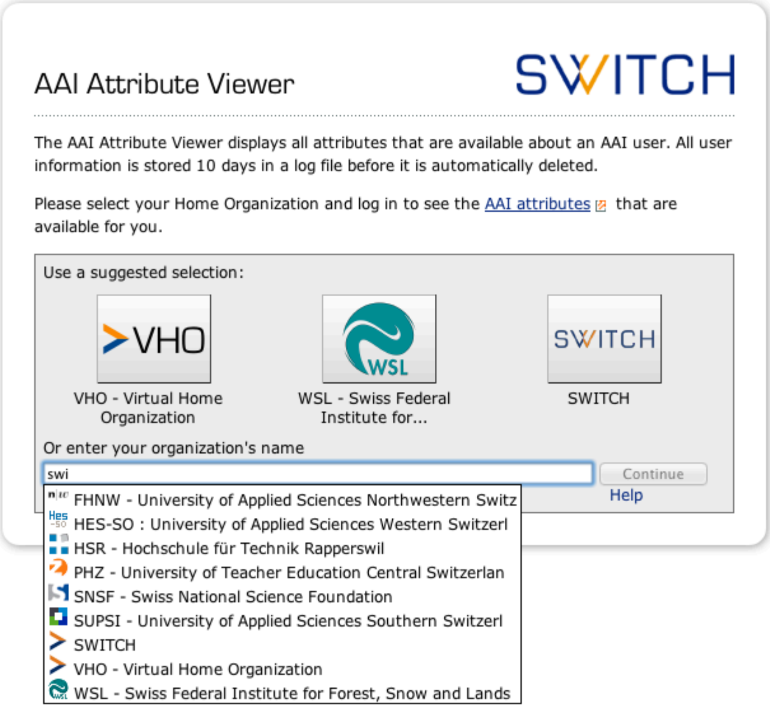
https://shibboleth.net/downloads/embedded-discovery-service/latest/

- Documentation can be found at:

https://wiki.shibboleth.net/confluence/display/EDS10/Embedded+Discovery+Service

Embedded Discovery Service

EDS



AAI Attribute Viewer

The AAI Attribute Viewer displays all attributes that are available about an AAI user. All user information is stored 10 days in a log file before it is automatically deleted.

Please select your Home Organization and log in to see the AAI attributes that are available for you.

Use a suggested selection:

VHO - Virtual Home Organization
WSL - Swiss Federal Institute for...
SWITCH

Or enter your organization's name

swi

- FHNW - University of Applied Sciences Northwestern Switz
- HES-SO : University of Applied Sciences Western Switzerl
- HSR - Hochschule für Technik Rapperswil
- PHZ - University of Teacher Education Central Switzerlan
- SNSF - Swiss National Science Foundation
- SUPSI - University of Applied Sciences Southern Switzerl
- SWITCH
- VHO - Virtual Home Organization
- WSL - Swiss Federal Institute for Forest, Snow and Lands

Embedded WAYF vs Embedded DS

Properties	Login Link	Embedded WAYF SWITCH	EDS Shibboleth
Independent from central server	✓		✓
Display only “valid” IdPs for SP		(✓)	✓
Search as you type feature		✓	✓
Show Home Org Logo	(✓)	✓	✓
Very easy deployment	✓	✓	✓
Can be used with old SPs (<2.4)	✓	(✓)	
Categories supported	(✓)	✓	
Uses cached recent IdP selection across different services		✓	

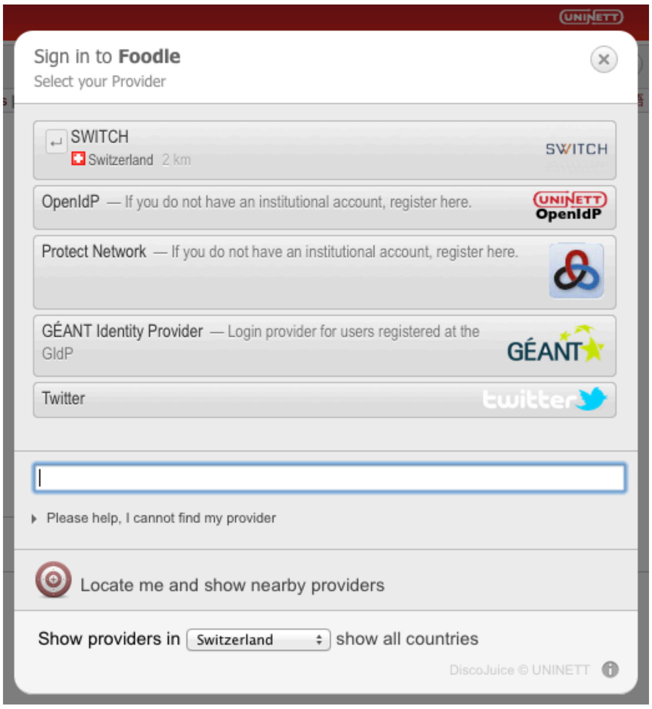
When to use what ?

Numbers of IdPs	Login Link(s)	Embedded WAYF SWITCH	EDS Shibboleth.
1 - 5	✓	✓	✓
1 - 500		✓	✓

To mention: Disco Juice

- Very comprehensive Discovery Service
- Well suited for services with users from many IdPs
- Search-as-you-type only
- Uses Geo IP and metric to guess user's IdP
- Based on PHP and JS

http://discojuice.org/



Sign in to **Foodle**

Select your Provider

SWITCH
Switzerland 2 km

OpenIdP — If you do not have an institutional account, register here.

Protect Network — If you do not have an institutional account, register here.

GÉANT Identity Provider — Login provider for users registered at the GIdP

Twitter

Please help, I cannot find my provider

Locate me and show nearby providers

Show providers in Switzerland show all countries

DiscoJuice © UNINETT