

# Interfederation Attributes

And how to use the Shibboleth Attribute Checker



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Recommended Interfederation Attributes

EduGAIN recommends these attributes for each user:

Friendly name	Defined in	Example
<b>displayName</b>	eduPerson	Beatrice Huber
<b>common name (cn)</b>	eduPerson	Beatrice Huber
mail	eduPerson	bea.huber@switch.ch
eduPersonAffiliation <b>eduPersonScopedAffiliation</b>	eduPerson	staff staff@switch.ch
<b>eduPersonPrincipalName</b>	eduPerson	234cd8z239@switch.ch
<b>schacHomeOrganization</b>	SCHAC	switch.ch
<b>schacHomeOrganizationType</b>	SCHAC	urn:mace:terena.org:schac:home OrganizationType:int:NREN
eduPersonTargetedID / Persistent Name ID	eduPerson	https://aai-logon.switch.ch/idp/ shibboleth!https://sp.example.org/ shibboleth!2389cdhu3e-sda7323

## eduGAIN-specific Attributes

- Difference **commonName/displayName**:  
The same but commonName might be multi-valued
- **eduPersonScopedAffiliation**:  
Like eduPersonAffiliation but with domain name appended
- **eduPersonPrincipalName**:  
Like swissEduPersonUniqueID but not opaque
- **schacHomeOrganization**:  
Domain name (like swissEduPersonHomeOrganisation)
- **schacHomeOrganizationType**:  
Not very well defined yet unfortunately...

## Make SP eduGAIN attributes

- The attributes in bold blue letters are normally not used in SWITCHaai
- To make SP support them, the attribute-map.xml must be adapted to contain their definition
- SWITCHaai configuration guide can do that for you:  
Choose "Interfederation/eduGAIN Support" during configuration to include definitions automatically

### Advanced Configuration Options

Enable SWITCHtoolbox Tool Support:  Configure Service Provider as SWITCHtoolbox Tool. [More ...](#)

Enable Interfederation/eduGAIN Support:  Configure Service Provider for Interfederation. [More ...](#)

[Update Configuration Guide with above Data](#)

## Missing Attributes on SP

- Attribute release in other federations unfortunately is often a manual process
  - Identity Providers in other federations often don't release attributes
  - Not so much an issue in SWITCHaai thanks to Resource Registry
- Consequence: SPs sometimes don't get required attributes
  - Users will get some error from application or SP
- Ideally, application shows an error that tells what attributes are missing
- But Shibboleth SP can do that too

## Check Available Attributes

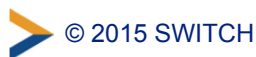
- In `<ApplicationDefaults>` or `<ApplicationOverride>` add the configuration option:  
`sessionHook="#URL#"`
- User is redirected to this (absolute or relative) URL
  - Before he is redirected to page requested initially
  - Page should check if all attributes are available and show error if not
  - Page therefore needs access to user's attributes!
- Standard page provided by Shibboleth would be:  
`sessionHook="/Shibboleth.sso/AttrChecker"`
  - Can use boolean expressions to check attributes

# Attribute Checker Example

If condition is not met:

- Shows an error message
- Flushes the Shibboleth session

```
<Handler type="AttributeChecker" flushSession="true"
  Location="/AttrChecker" template="attrChecker.html">
  <OR>
    <Rule require="displayName"/>
    <AND>
      <Rule require="givenName"/>
      <Rule require="surname"/>
    </AND>
  </OR>
</Handler>
```



© 2015 SWITCH

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPHandler>

# Standard Error Message

- Template is: `/etc/shibboleth/attrChecker.html`
- Ideally mention which attributes are missing

SWITCHaai

**We're sorry, but you cannot access this service at this time.**

This service requires information about you that your identity provider did not release. To gain access to this service, your identity provider must release the required information.

You were trying to access the following URL:

For more information about this service, including what user information is required for access, please visit [our information page](#).



© 2015 SWITCH