Shibboleth-aware Applications

Some Examples

SWITCH

SWITCHaai Team
lukas.haemmerle@switch.ch

Applications already Shibboleth-ready

- Official list: https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled
  - List is not always up-to-date
  - Applications that make use of HTTP Basic Auth (e.g. Nagios) are not listed even though they are very easy to "shibbolethize" using the REMOTE_USER attribute
  - Often it is more useful to google for "application Shibboleth"

- (Hosted) services as well as products to download

- What does Shibboleth-enabled mean exactly?
  - Especially commercial products often "exaggerate" to sell more
  - Many products rely on Shibboleth, other's implement a tiny fraction of the SAML standard
  - Often, only authentication makes use of AAI but not authorisation

Shibboleth-enabled out-of-the-box?

- Most Shibboleth/SAML-enabled application depend on:
  - Shibboleth Service Provider: Recommended for SWITCHaai
  - SimpleSAML PHP: Popular PHP-only alternative implementation
  - **Careful:** Most commercial web-hosters don't support Shibboleth SP! Often they only allow PHP applications.
- Some applications support SAML natively:
  - OCLC EZproxy: Popular proxy for accessing e-journals
  - Microsoft ADFS: Required for Sharepoint
- Non-Shibboleth SAML implementations often are not fully interoperable or have a limited feature set

Example: Moodle

- Popular e-Learning application in SWITCHaai (>40SPs)
- Requires installation of a Shibboleth Service Provider
  - Use our installation and configuration guide
  - Then follow the instructions in the README of the Moodle Shibboleth plug-in to protect `/auth/shibboleth/index.php`
- Configuration is done via web interface:
  - Site Administration – Plugins – Authentication – Shibboleth
- SWITCH heavily contributed to initial version of plugin

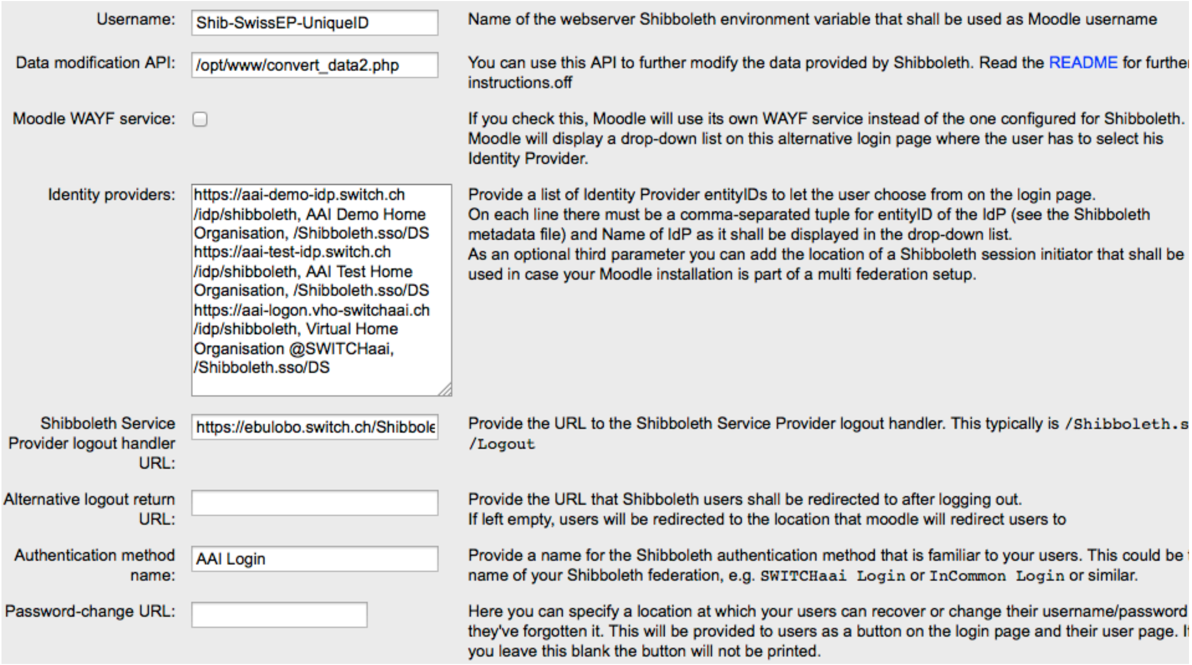
Moodle Configuration

- Configuration is done via web interface:
  Site Administration – Plugins – Authentication – Shibboleth

- This plug-in only covers authentication!
  - Other plugins to enrol user based on Shibboleth attributes

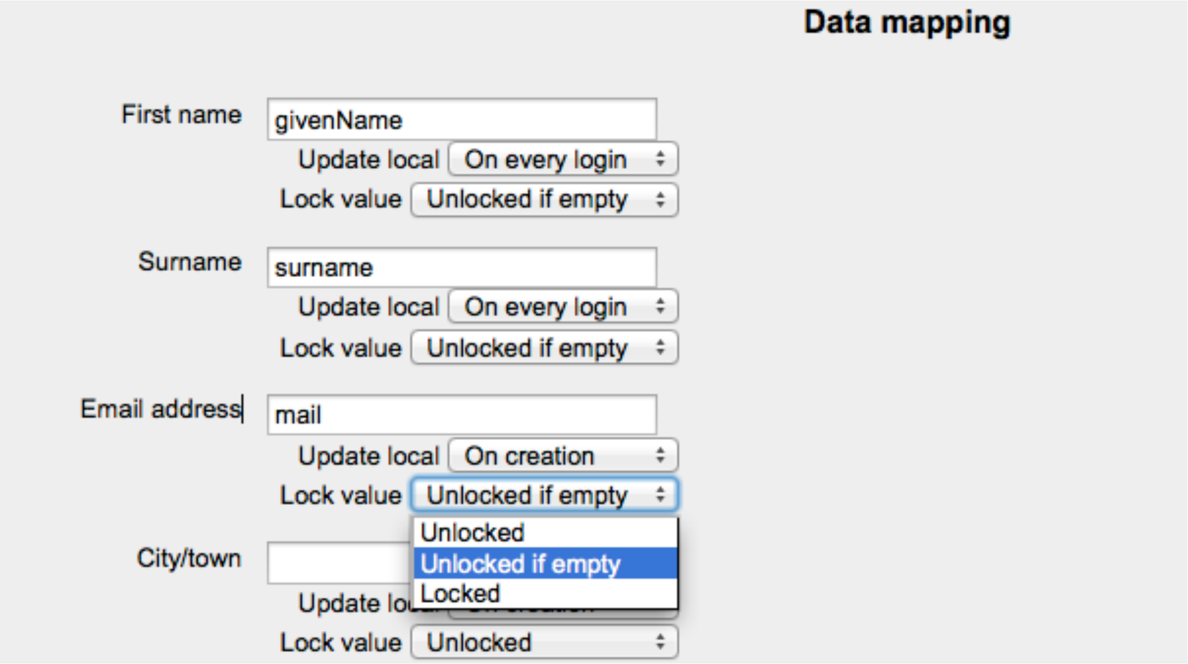
- Configuration defines:
  - Discovery Service: Use internal or external one
  - Alternative Login/Logout URLs: To further customize behavior
  - Attribute mapping: Shibboleth Attribute -> User profile field
  - Attribute update/locking: If and when to update user profile field
  - Data modification hook: To transform attributes before use in Moodle

Moodle Screenshot: Configuration I



Username:	Shib-SwissEP-UniqueID	Name of the webserver Shibboleth environment variable that shall be used as Moodle username
Data modification API:	/opt/www/convert_data2.php	You can use this API to further modify the data provided by Shibboleth. Read the README for furthe instructions.off
Moodle WAYF service:	□	If you check this, Moodle will use its own WAYF service instead of the one configured for Shibboleth. Moodle will display a drop-down list on this alternative login page where the user has to select his Identity Provider.
Identity providers:	https://aai-demo-idp.switch.ch/idp/shibboleth, AAI Demo Home Organisation, /Shibboleth.sso/DS https://aai-test-idp.switch.ch/idp/shibboleth, AAI Test Home Organisation, /Shibboleth.sso/DS https://aai-logon.vho-switchaai.ch/idp/shibboleth, Virtual Home Organisation @SWITCHaai, /Shibboleth.sso/DS	Provide a list of Identity Provider entityIDs to let the user choose from on the login page. On each line there must be a comma-separated tuple for entityID of the IdP (see the Shibboleth metadata file) and Name of IdP as it shall be displayed in the drop-down list. As an optional third parameter you can add the location of a Shibboleth session initiator that shall be used in case your Moodle installation is part of a multi federation setup.
Shibboleth Service Provider logout handler URL:	https://ebulobo.switch.ch/Shibbole	Provide the URL to the Shibboleth Service Provider logout handler. This typically is `/Shibboleth.s` `/Logout`
Alternative logout return URL:		Provide the URL that Shibboleth users shall be redirected to after logging out. If left empty, users will be redirected to the location that moodle will redirect users to
Authentication method name:	AAI Login	Provide a name for the Shibboleth authentication method that is familiar to your users. This could be name of your Shibboleth federation, e.g. `SWITCHaai Login` or `InCommon Login` or similar.
Password-change URL:		Here you can specify a location at which your users can recover or change their username/password they've forgotten it. This will be provided to users as a button on the login page and their user page. I you leave this blank the button will not be printed.

Moodle Screenshot: Configuration I



Data mapping

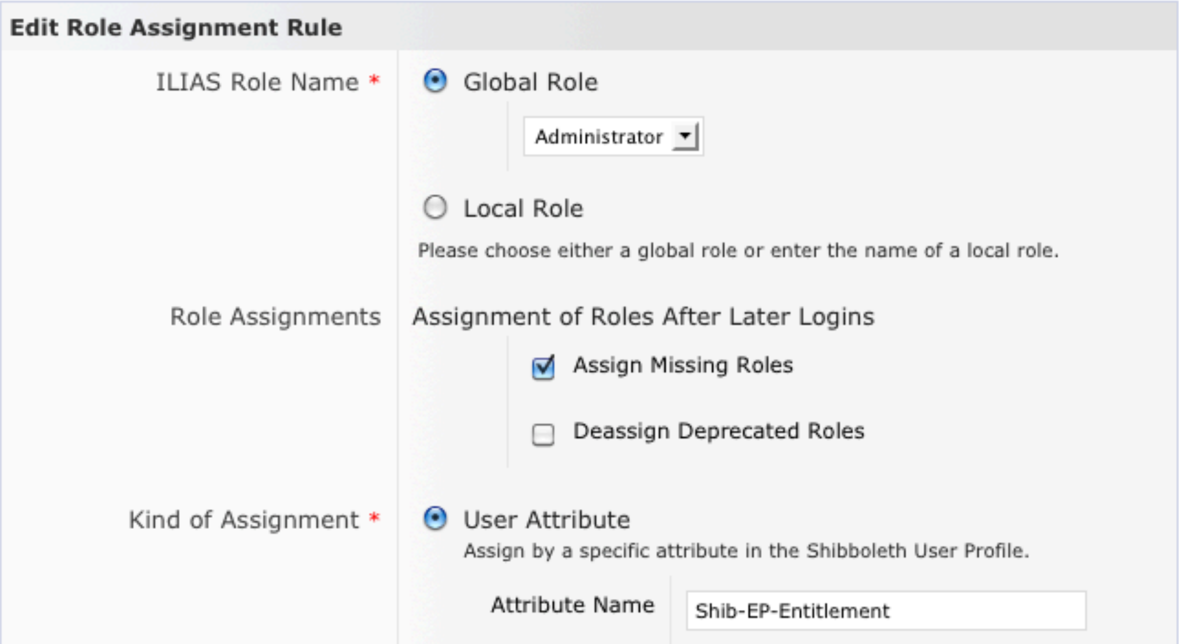
First name: givenName
Update local: On every login
Lock value: Unlocked if empty

Surname: surname
Update local: On every login
Lock value: Unlocked if empty

Email address: mail
Update local: On creation
Lock value: Unlocked if empty

City/town:
Update lo
Lock value: Unlocked

ILIAS Screenshot: Role Assignment



Edit Role Assignment Rule

ILIAS Role Name *
● Global Role
Administrator
○ Local Role
Please choose either a global role or enter the name of a local role.

Role Assignments
Assignment of Roles After Later Logins
☑ Assign Missing Roles
□ Deassign Deprecated Roles

Kind of Assignment *
● User Attribute
Assign by a specific attribute in the Shibboleth User Profile.
Attribute Name: Shib-EP-Entitlement