

TECHNISCHES

Konfigurieren einer Moodle-Instanz

07.03.2022 – Version 1.0

1.	Ziel des Dokuments	2
2.	Vorbedingungen	2
3.	Vollständiger Ablauf	2
4.	Konfiguration des simpleSAMLphp-Plugins in Moodle für Edulog	3
4.1	Zur Konfigurationsseite des Plugins gehen:	3
4.2	Konfiguration des SAML-Endpoints:	4
4.3	Das Zertifikat des SP generieren	5
4.4	Konformitätsprüfung des Zertifikats	5
4.5	«EdulogPersonTechID» als Attribut für das Moodle-Benutzerfeld konfigurieren	6
4.6	Das «Mapping» der Moodle-Attribute mit denen von Edulog konfigurieren	7
5.	Übermittlung der Metadaten-Datei des SAML2-Plugins von Moodle an den technischen Partner der Föderation	8
6.	Verbindungstests	9

1. Ziel des Dokuments

Dieses Dokument erklärt Dienstleistungsanbietern (SP), wie sie eine Moodle-Instanz für die Föderation mit Edulog konfigurieren.

Dieses Dokument erklärt weder die Installation von Moodle noch die Installation des Plugins *simpleSAMLphp*.

2. Vorbedingungen

Dieser Leitfaden kann nur verwendet werden, wenn die folgenden technischen Anforderungen erfüllt sind:

- Der SP nutzt - in seiner eigenen Infrastruktur - einen Server mit einer Moodle-Instanz¹.
- Der SP verwendet ein Plugin für das SAML-Protokoll, um die Moodle-Instanz mit einem IdP zu verbinden. Hierfür existieren mehrere Plugins. Im Folgenden beschreiben wir die notwendige Konfiguration mit *simpleSAMLphp*².
- Die digitalen Zertifikate, die bei der Konfiguration der Moodle-Instanz und der Signatur ihrer «SAML Request»-Anfragen verwendet werden, erfüllen die Sicherheitsanforderungen von Edulog.

3. Vollständiger Ablauf

Folgende technische Schritte³ sind von einem SP (mit der zuvor erwähnten Infrastruktur) zu erledigen, um die notwendige Konfiguration beim *Onboarding* mit Edulog durchzuführen:

Nr.	Zu erledigende Arbeiten	Moment
1	Die Moodle-Instanz einrichten und das SAML2-Plugin installieren	Voraussetzung
2	Das SAML2-Plugin in Moodle konfigurieren	Kapitel 4
3	ELCA die Metadaten-Datei des SAML2-Plugins mitteilen	Kapitel 5
4	Login-Tests mit Benutzern durchführen	Kapitel 6

Dieses Dokument behandelt die Punkte 2 bis 4.

¹ <https://download.moodle.org/>

² <https://simplesamlphp.org/>

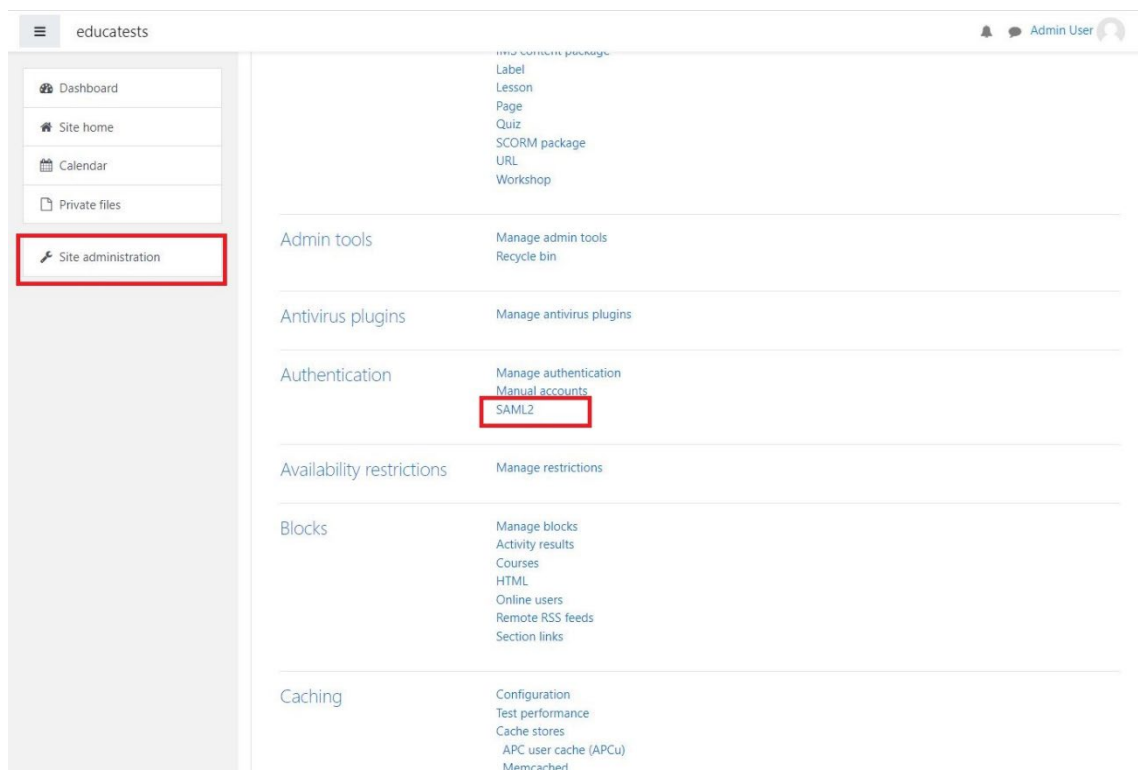
³ Weitere nicht-technische Schritte (Vertrag, etc.) sind für die Aufnahme in die Föderation notwendig. Sie werden in diesem Dokument nicht behandelt.

4. Konfiguration des simpleSAMLphp-Plugins in Moodle für Edulog

Die Konfiguration des SAML-Plugins für Moodle muss eine Reihe von Regeln befolgen. Wir erläutern hier die einzelnen notwendigen Schritte.

4.1 Zur Konfigurationsseite des Plugins gehen:

- Melden Sie sich bei der Moodle-Instanz als Administrator an;
- Wählen Sie «Site administration», dann «Plugins» und klicken Sie im Bereich «Authentication» auf «SAML2».



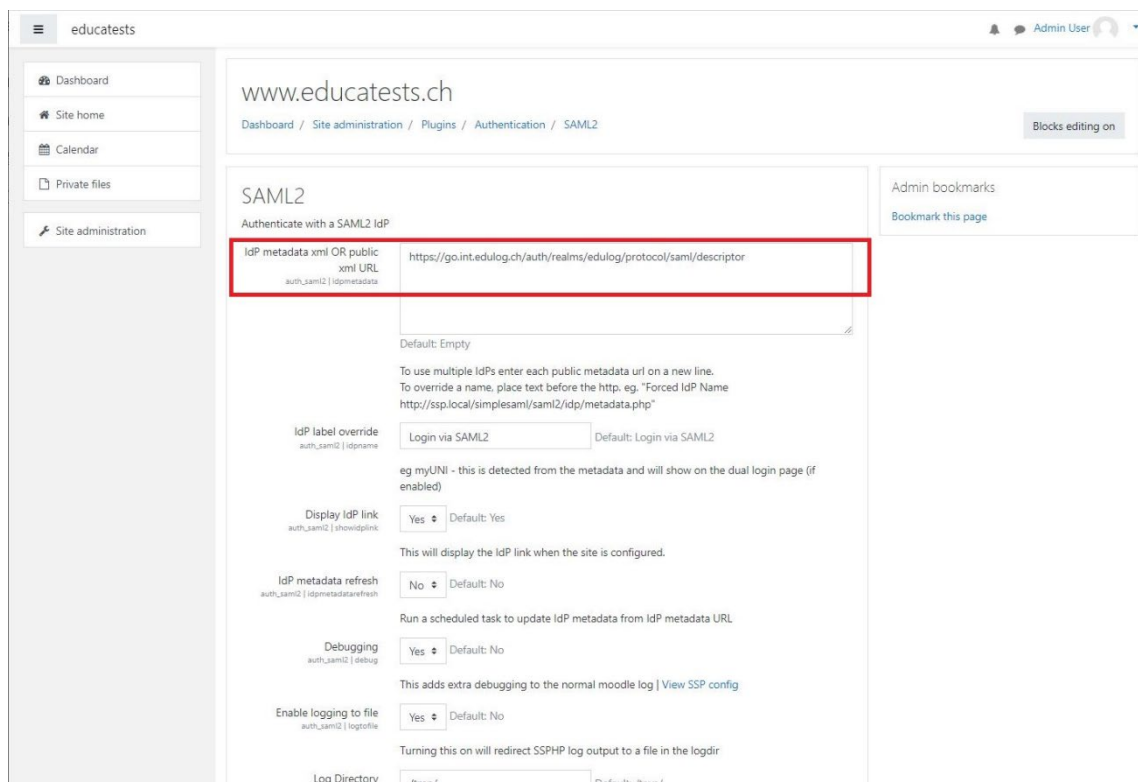
4.2 Konfiguration des SAML-Endpoints:

Im folgenden Beispiel ist die Moodle-Instanz mit der Testinstanz von Edulog verbunden, der Link, der die Metadaten-Datei von Edulog liefert, lautet also:

<https://go.int.edulog.ch/auth/realms/edulog/protocol/saml/descriptor>

Im Falle der Produktionsfreigabe der Instanz lautet der Link so:

<https://go.edulog.ch/auth/realms/edulog/protocol/saml/descriptor>



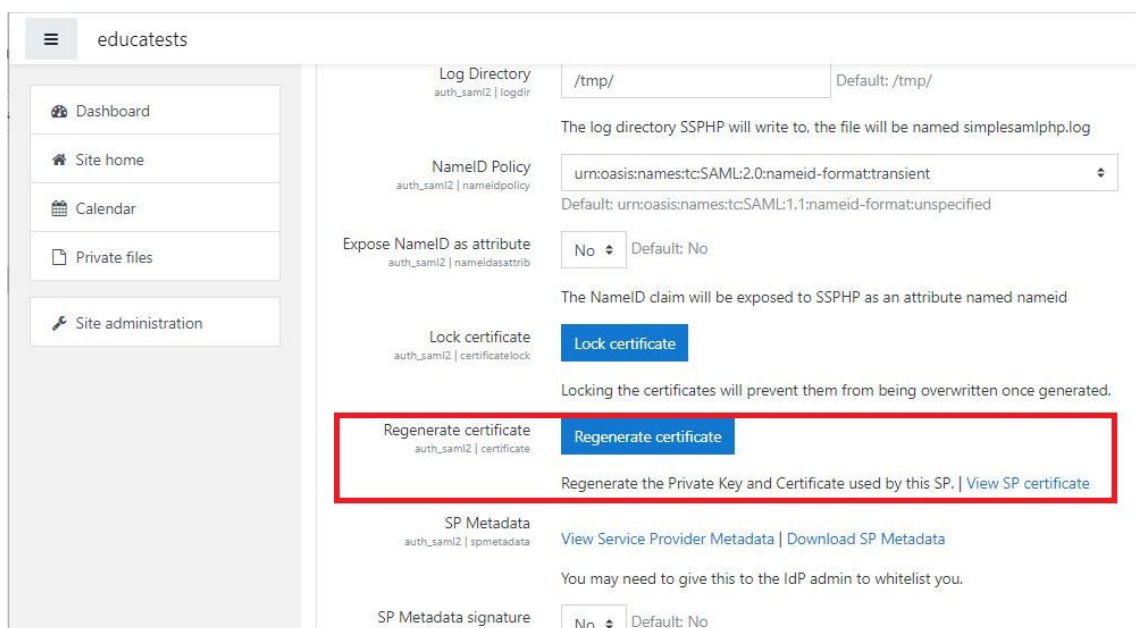
The screenshot shows the Moodle administration interface for the site 'educatests'. The left sidebar contains navigation links: Dashboard, Site home, Calendar, Private files, and Site administration. The main content area is titled 'SAML2' and 'Authenticate with a SAML2 IdP'. A red box highlights the 'IdP metadata xml OR public xml URL' field, which contains the URL <https://go.int.edulog.ch/auth/realms/edulog/protocol/saml/descriptor>. Below this field, there are several configuration options with dropdown menus and checkboxes:

- IdP label override** (auth_saml2 | idpname): A text input field containing 'Login via SAML2'.
- Display IdP link** (auth_saml2 | showidplink): A dropdown menu set to 'Yes'.
- IdP metadata refresh** (auth_saml2 | idpmetadatarefresh): A dropdown menu set to 'No'.
- Debugging** (auth_saml2 | debug): A dropdown menu set to 'Yes'.
- Enable logging to file** (auth_saml2 | logtofile): A dropdown menu set to 'Yes'.
- Log Directory**: A text input field containing '/tmp/'.

On the right side of the page, there are 'Admin bookmarks' and a 'Bookmark this page' button. The top right corner shows the user 'Admin User' and a 'Blocks editing on' button.

4.3 Das Zertifikat des SP generieren

Klicken Sie auf die Schaltfläche «Regenerate certificate» und füllen Sie die für die Generierung erforderlichen Felder aus.



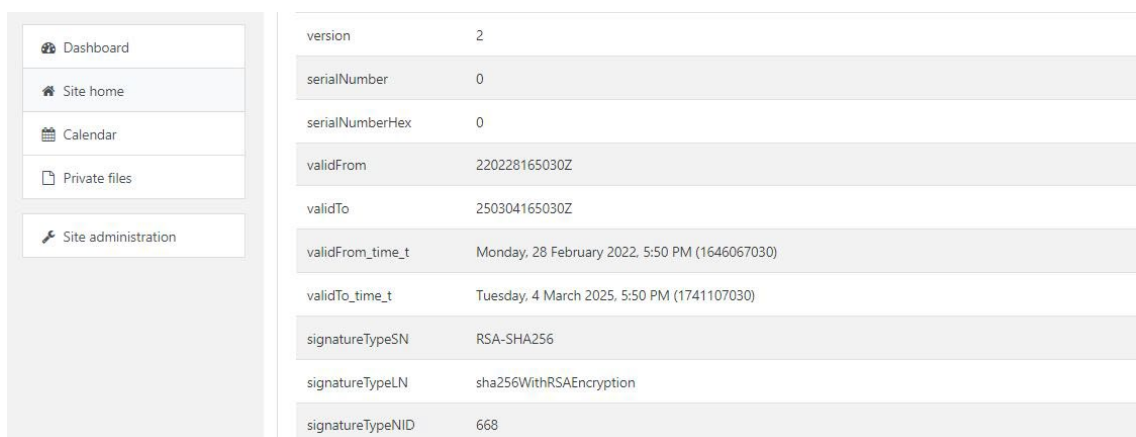
The screenshot shows the Moodle SAML configuration page for the 'educatests' instance. The left sidebar contains navigation links: Dashboard, Site home, Calendar, Private files, and Site administration. The main content area is divided into several sections:

- Log Directory:** Set to '/tmp/'. Description: 'The log directory SSPHP will write to, the file will be named simplesamlphp.log'.
- NamID Policy:** Set to 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient'. Default: 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified'.
- Expose NamID as attribute:** Set to 'No'. Default: 'No'. Description: 'The NamID claim will be exposed to SSPHP as an attribute named nameid'.
- Lock certificate:** A blue button labeled 'Lock certificate'. Description: 'Locking the certificates will prevent them from being overwritten once generated.'
- Regenerate certificate:** A blue button labeled 'Regenerate certificate' is highlighted with a red rectangle. Description: 'Regenerate the Private Key and Certificate used by this SP. | View SP certificate'.
- SP Metadata:** Links for 'View Service Provider Metadata' and 'Download SP Metadata'. Description: 'You may need to give this to the IdP admin to whitelist you.'
- SP Metadata signature:** Set to 'No'. Default: 'No'.

4.4 Konformitätsprüfung des Zertifikats

Klicken Sie auf "View SP certificate".

Überprüfen Sie, ob das Zertifikat 3 Jahre gültig ist und ob der Signaturtyp sha256WithRSAEncryption ist.



The screenshot shows the 'View SP certificate' section of the Moodle SAML configuration page. It displays a table with the following certificate metadata:

version	2
serialNumber	0
serialNumberHex	0
validFrom	220228165030Z
validTo	250304165030Z
validFrom_time_t	Monday, 28 February 2022, 5:50 PM (1646067030)
validTo_time_t	Tuesday, 4 March 2025, 5:50 PM (1741107030)
signatureTypeSN	RSA-SHA256
signatureTypeLN	sha256WithRSAEncryption
signatureTypeNID	668

Achtung: Jedes Mal, wenn das Zertifikat neu generiert wird, ändert sich die Metadaten-Datei Ihrer Instanz, was zu Problemen mit der Föderation führen kann, welche die Signatur Ihrer SAML-Anfragen nicht überprüfen kann.

4.5 «EdulogPersonTechID» als Attribut für das Moodle-Benutzerfeld konfigurieren

educatests

Dashboard
Site home
Calendar
Private files
Site administration

auth_saml2 | spmetadatasign

Sign the SP Metadata.

Signing Algorithm

auth_saml2 | signaturealgorithm

SHA256

Default: SHA256

This is the algorithm that will be used to sign SAML requests. Warning: The SHA1 Algorithm is only provided for backwards compatibility, unless you absolutely must use it it is recommended to avoid it and use at least SHA256 instead.

Dual login

auth_saml2 | duallogin

Yes

Default: Yes

If on, then users will see both manual and a SAML login button. If off they will always be taken directly to the IdP login page.

If passive, then the users that are already authenticated into the IdP will be automatically logged in, otherwise they will be sent to Moodle login page.

If off, then admins can still see the manual login page via /login/index.php?saml=off

If on, then external pages can deep link into moodle using saml eg /course/view.php?id=45&saml=on

Allowed any auth type

auth_saml2 | anyauth

Yes

Default: No

Yes: Allow SAML login for all users? No: Only users who have saml2 as their type.

Mapping IdP

auth_saml2 | idpattr

EdulogPersonTechID

Default: uid

Which IdP attribute should be matched against a Moodle user field?

Mapping Moodle

auth_saml2 | mdlattr

Username

Default: Username

Which Moodle user field should the IdP attribute be matched to?

Lowercase

auth_saml2 | tolower

No

Default: No

Apply lowercase to IdP attribute before matching?

Auto create users

auth_saml2 | autcreate

Yes

Default: No

If users are in the IdP but not in moodle create a moodle account.

Alternative Logout URL

auth_saml2 | alterlogout

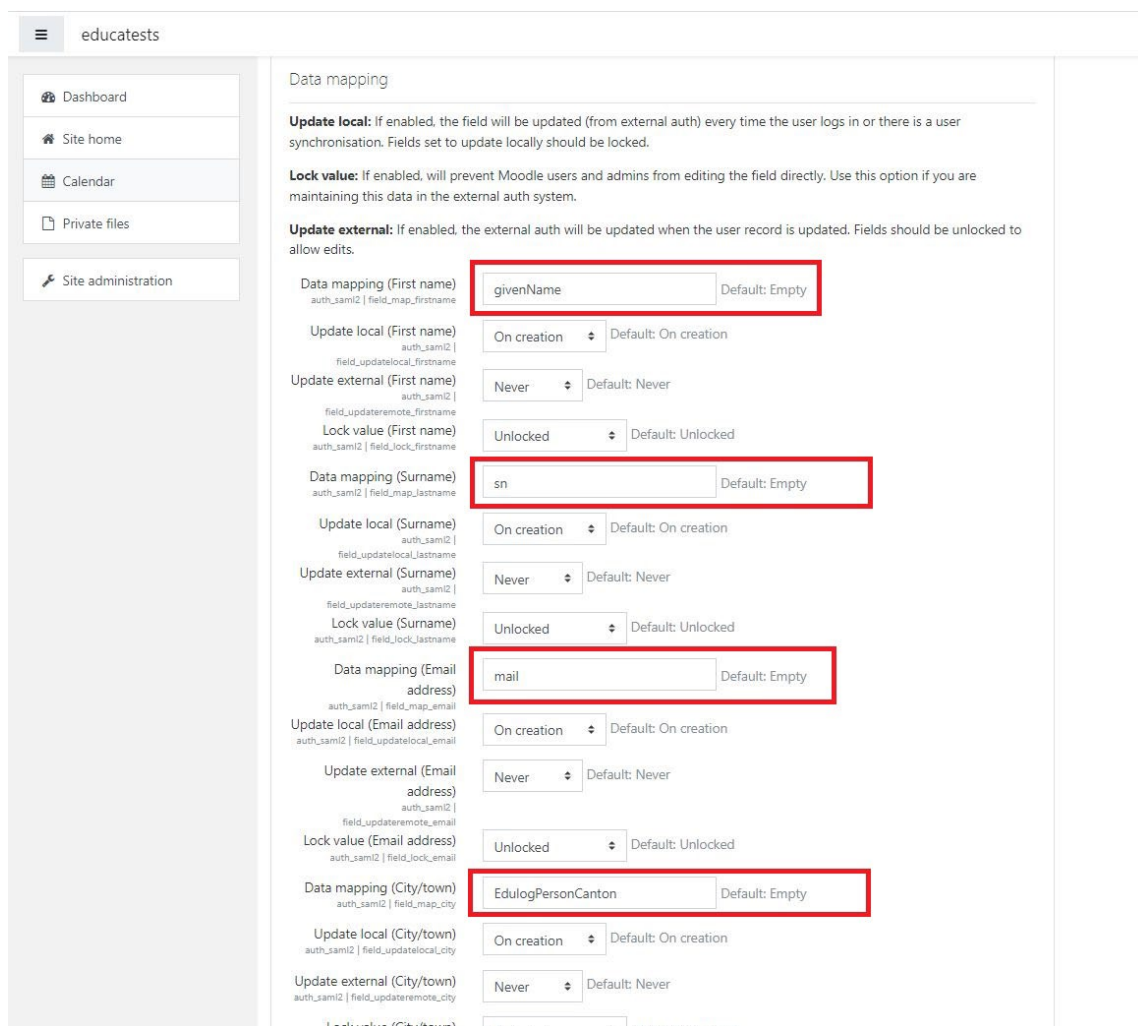
Default: Empty

The URL to redirect a user after all internal logout mechanisms are run

Das Attribut «EdulogPersonTechID» ist eine eindeutige Kennung der Edulog-Identitäten. Der durchgeführte Test ermöglicht es, Edulog-Benutzer direkt in der Moodle-Instanz zu erstellen, indem bestimmte Attribute vorausgefüllt werden.

4.6 Das «Mapping» der Moodle-Attribute mit denen von Edulog konfigurieren

Es ist notwendig zu erklären, welche Attribute in Moodle die Daten aus Edulog erhalten. Dazu müssen wir bestimmte Attribute in Moodle mit bestimmten Attributen in Edulog in Beziehung setzen.



Data mapping

Update local: If enabled, the field will be updated (from external auth) every time the user logs in or there is a user synchronisation. Fields set to update locally should be locked.

Lock value: If enabled, will prevent Moodle users and admins from editing the field directly. Use this option if you are maintaining this data in the external auth system.

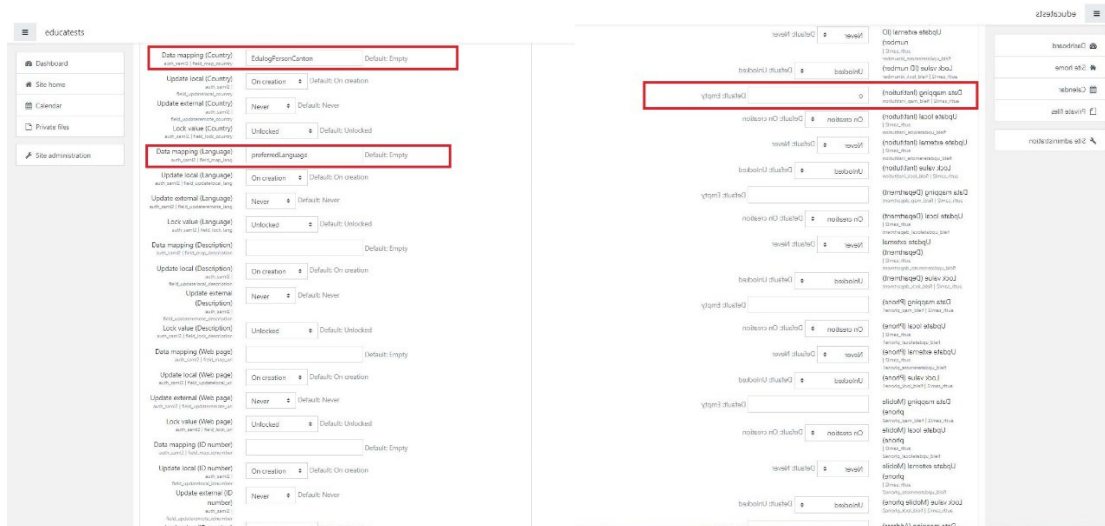
Update external: If enabled, the external auth will be updated when the user record is updated. Fields should be unlocked to allow edits.

Data mapping (First name) auth_saml2 field_map_firstname	givenName	Default: Empty
Update local (First name) auth_saml2 field_updatelocal_firstname	On creation	Default: On creation
Update external (First name) auth_saml2 field_updateremote_firstname	Never	Default: Never
Lock value (First name) auth_saml2 field_lock_firstname	Unlocked	Default: Unlocked
Data mapping (Surname) auth_saml2 field_map_lastname	sn	Default: Empty
Update local (Surname) auth_saml2 field_updatelocal_lastname	On creation	Default: On creation
Update external (Surname) auth_saml2 field_updateremote_lastname	Never	Default: Never
Lock value (Surname) auth_saml2 field_lock_lastname	Unlocked	Default: Unlocked
Data mapping (Email address) auth_saml2 field_map_email	mail	Default: Empty
Update local (Email address) auth_saml2 field_updatelocal_email	On creation	Default: On creation
Update external (Email address) auth_saml2 field_updateremote_email	Never	Default: Never
Lock value (Email address) auth_saml2 field_lock_email	Unlocked	Default: Unlocked
Data mapping (City/town) auth_saml2 field_map_city	EdulogPersonCanton	Default: Empty
Update local (City/town) auth_saml2 field_updatelocal_city	On creation	Default: On creation
Update external (City/town) auth_saml2 field_updateremote_city	Never	Default: Never
Lock value (City/town) auth_saml2 field_lock_city	Unlocked	Default: Unlocked

Nur die folgenden Attribute von Edulog lassen sich problemlos in die Moodle-Instanz unseres Beispiels "mappen" :

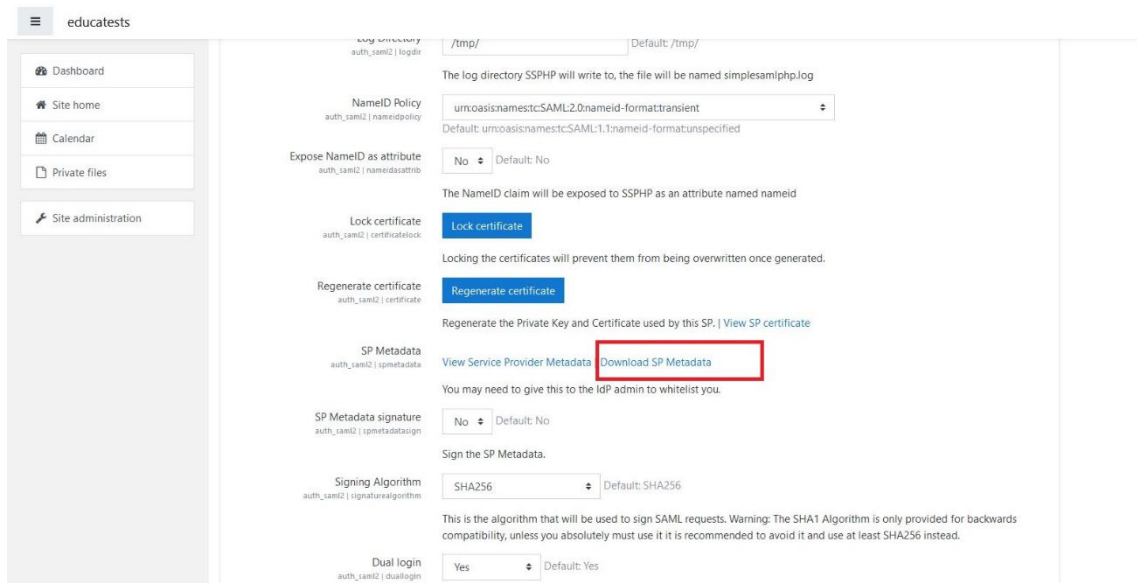
- «EdulogPersonTechID» mit «user» ;
- «givenName» mit «First name»;
- «surname» mit «Surname»;
- «mail» mit «email»;
- «preferredLanguage» mit «Language» ;
- «o» mit «Institution».

Die restlichen Attribute von Edulog müssen vom SP entweder anderen bereits existierenden Attributen (siehe Beispiel des Attributs «EdulogPersonCanton» auf dem Moodle-Attribut «City/Town») oder neuen Attributen (falls möglich) zugewiesen werden.



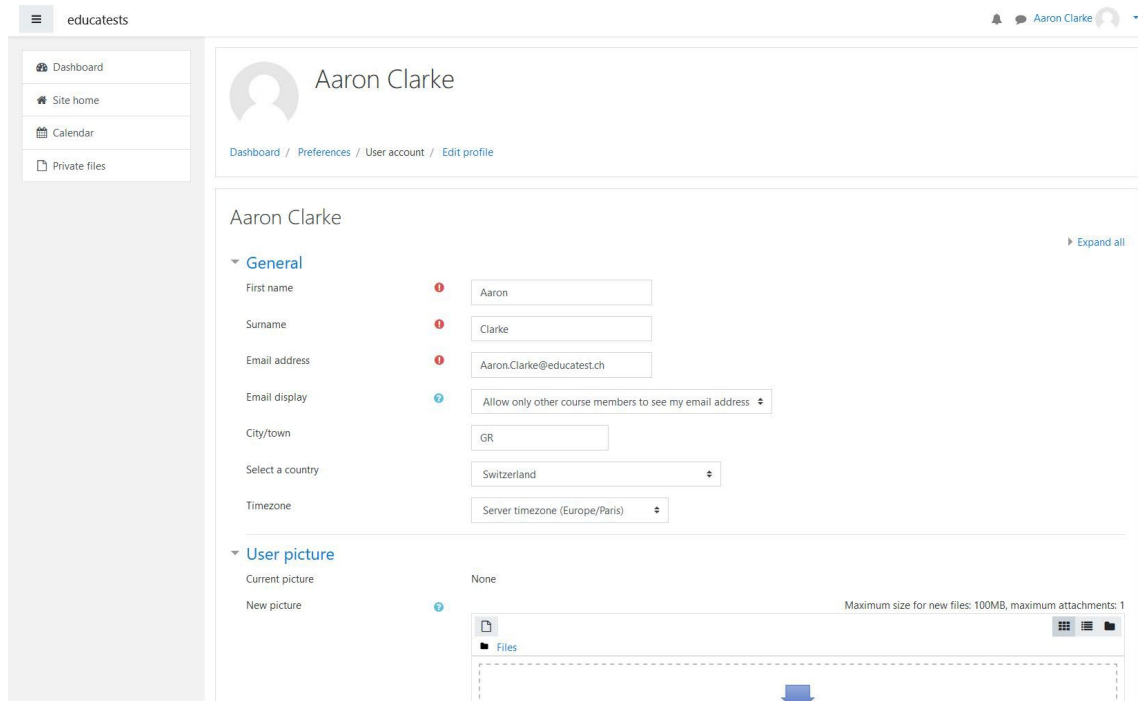
Vergessen Sie nicht, die Seite mit den Änderungen abschliessend zu speichern.

5. Übermittlung der Metadaten-Datei des SAML2-Plugins von Moodle an den technischen Partner der Föderation



Sobald die Konfiguration abgeschlossen ist, muss die SAML-Konfiguration des vom Plugin erstellten Endpunkts heruntergeladen werden. Diese Datei wird anschliessend an den technischen Partner der Föderation geschickt, der die Moodle-Instanz in Edulog einbindet.

6. Verbindungstests



educatests

Aaron Clarke

Dashboard / Preferences / User account / Edit profile

Aaron Clarke

Expand all

General

First name: Aaron

Surname: Clarke

Email address: Aaron.Clarke@educatest.ch

Email display: Allow only other course members to see my email address

City/town: GR

Select a country: Switzerland

Timezone: Server timezone (Europe/Paris)

User picture

Current picture: None

New picture: Maximum size for new files: 100MB, maximum attachments: 1

Files

Nachdem die Konfiguration der SAML-Verbindung zwischen Edulog und dem SP abgeschlossen ist, können Sie die Verbindung zwischen einem Benutzer eines IdP und der Moodle-Instanz testen. Wenn alles klappt, wird beim ersten Einloggen des Benutzers ein Benutzerprofil mit den in Kapitel 4 ausgewählten Attributen erstellt.