Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNISCHES

Konfigurieren einer Moodle-Instanz

07.03.2022 – Version 1.0

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-Instanz[1].
- 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 Schritte [3] 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.

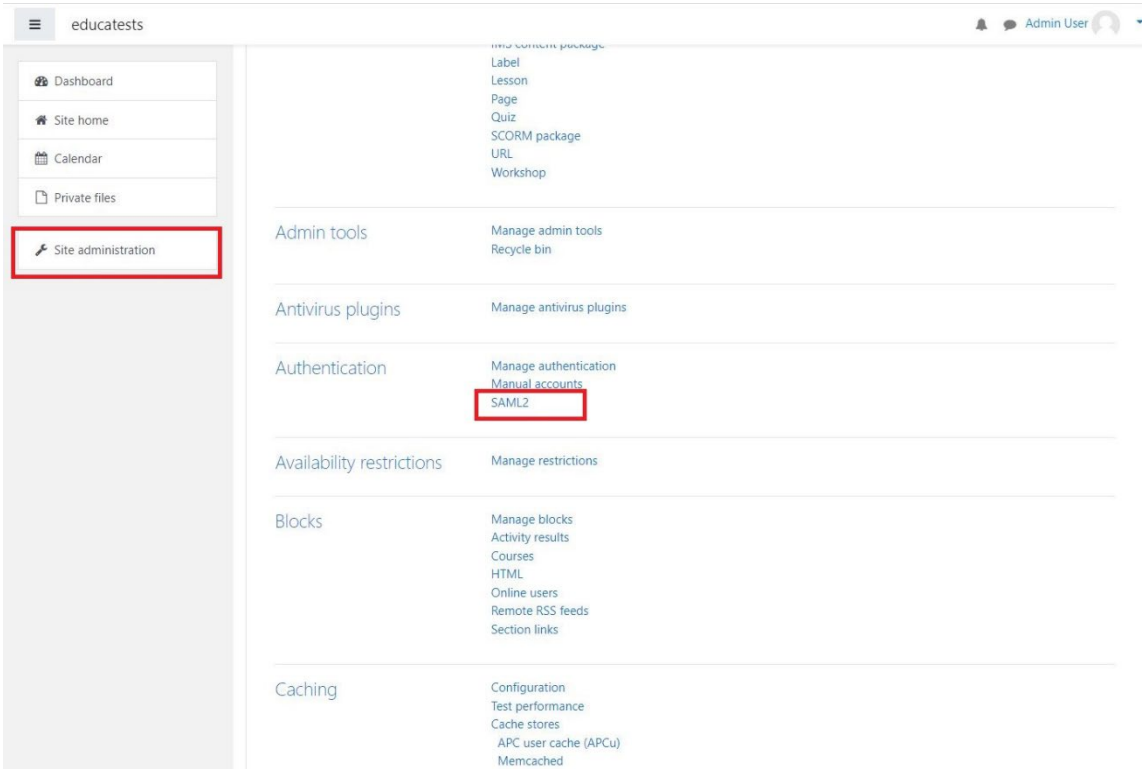
[1] https://download.moodle.org/
[2] https://simplesamlphp.org/
[3] Weitere nicht-technische Schritte (Vertrag, etc.) sind für die Aufnahme in die Föderation notwendig. Sie werden in diesem Dokument nicht behandelt.

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:

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



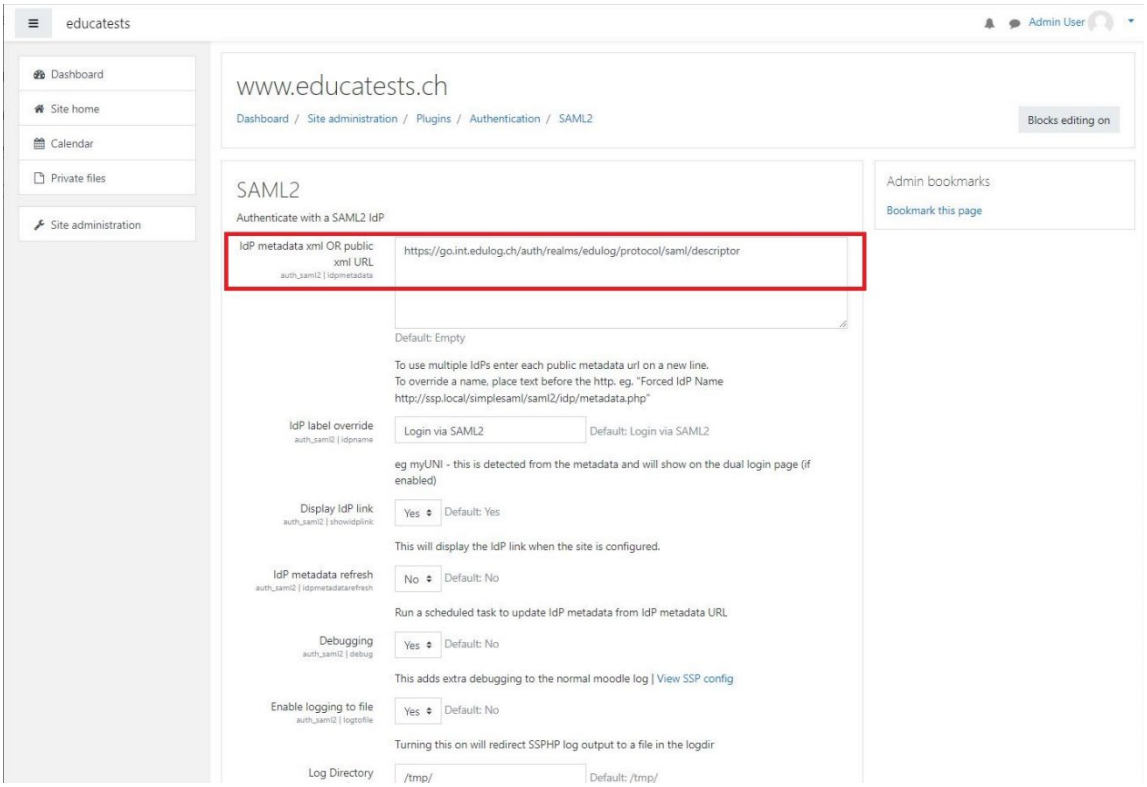
4.2 Konfiguration des SAML-Endpoints:

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

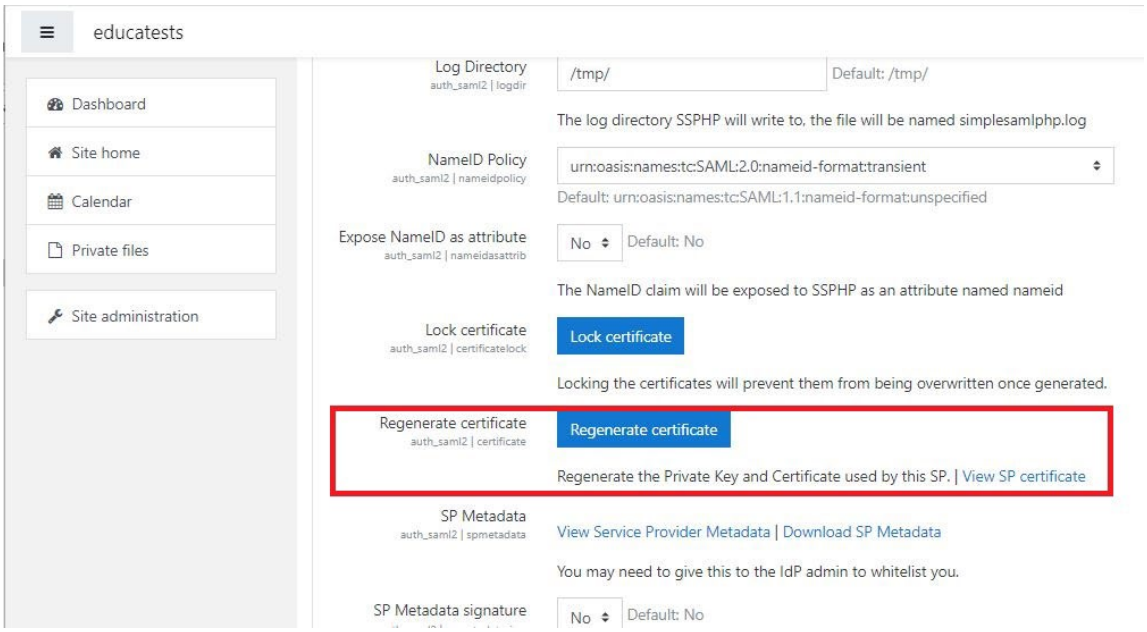
Im Falle der Produktionsfreigabe der Instanz lautet der Link so:

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



4.3 Das Zertifikat des SP generieren

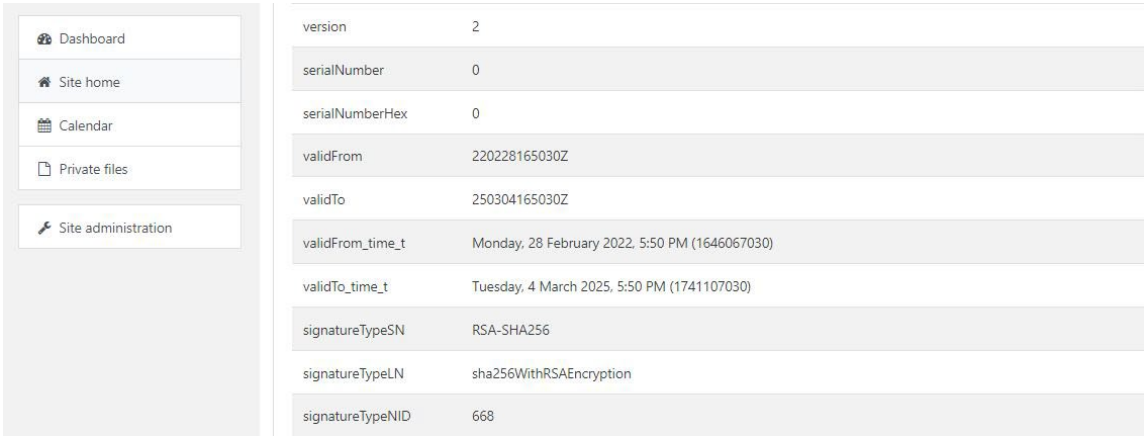
Klicken Sie auf die Schaltfläche «Regenerate certificate» und füllen Sie die für die Generierung erforderlichen Felder aus.



4.4 Konformitätsprüfung des Zertifikats

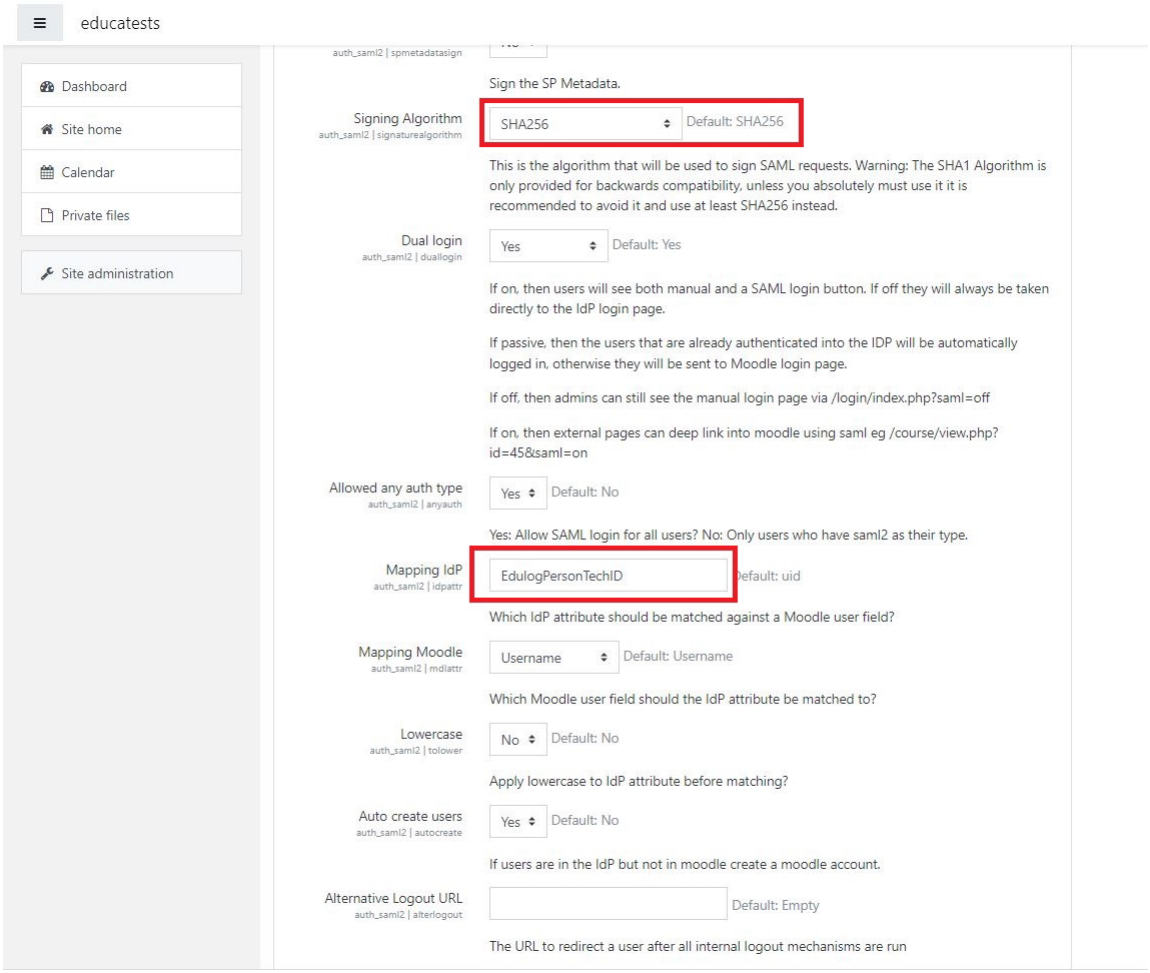
Klicken Sie auf "View SP certificate".

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



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.

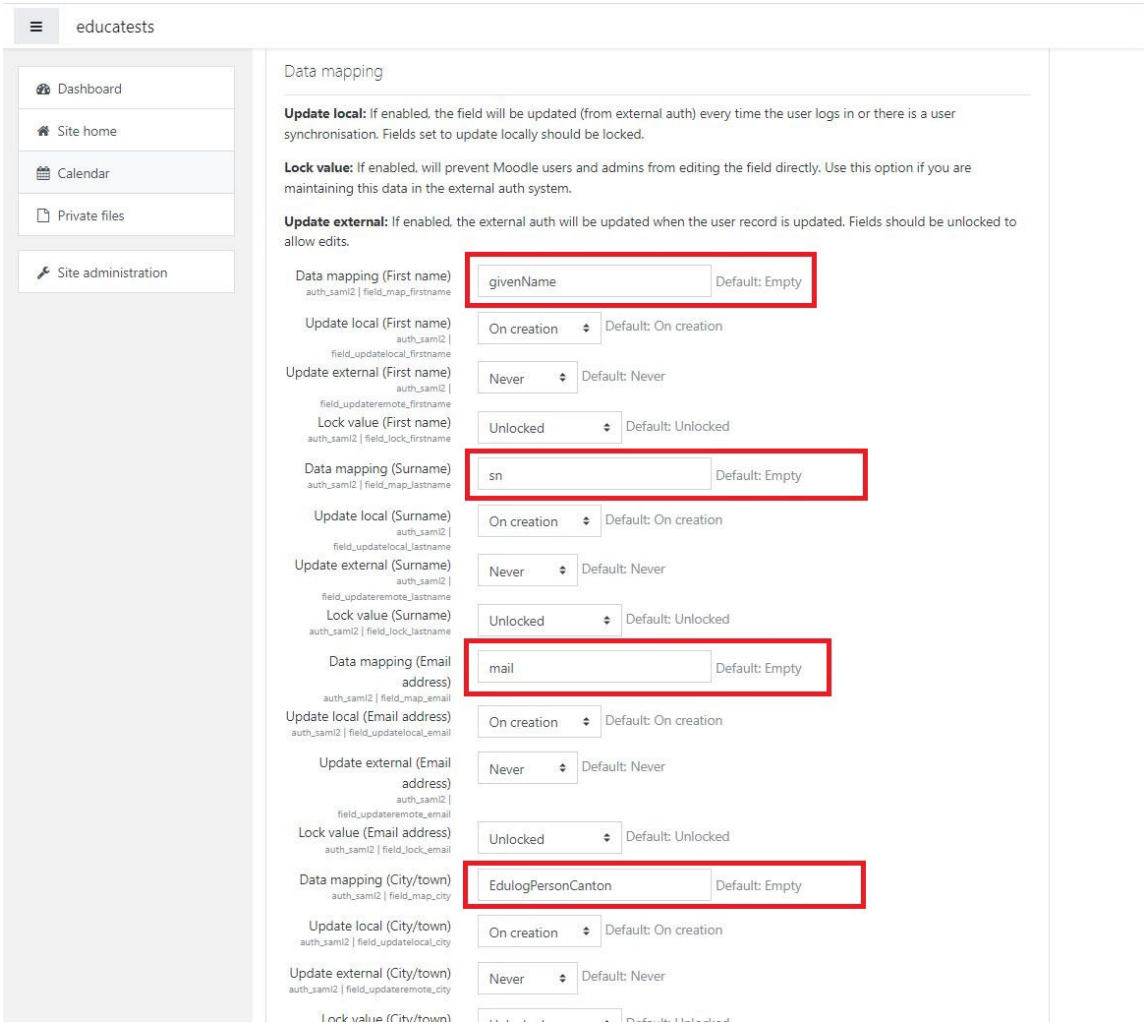
4.5 «EdulogPersonTechID» als Attribut für das Moodle-Benutzerfeld konfigurieren



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.



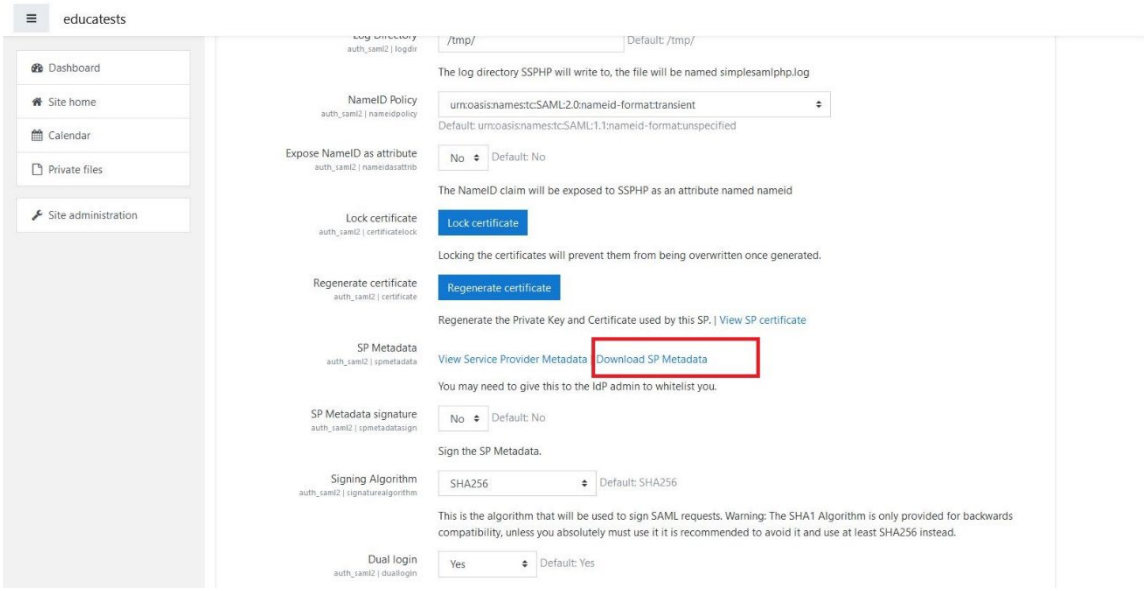
Nur die folgenden Attribute von Edulog lassen sich problemlos in die Moodle-Instanz unseres Beispiels "mappen" :

- «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.

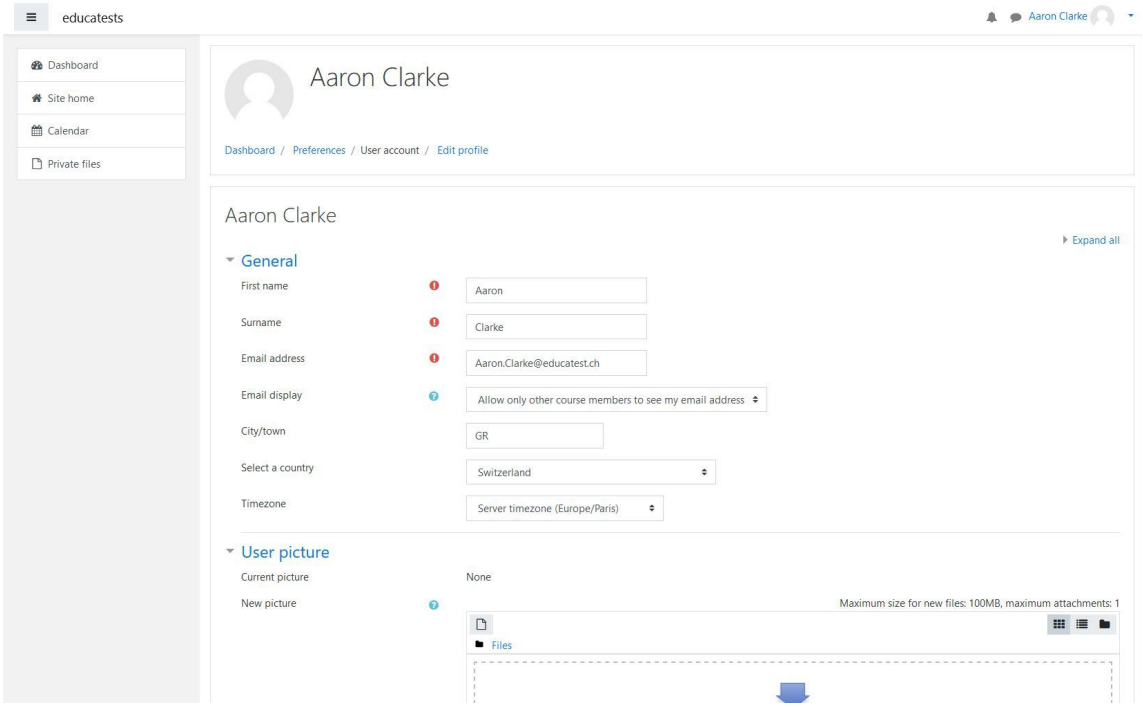
Vergessen Sie nicht, die Seite mit den Änderungen abschliessend zu speichern.

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



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.