

TECHNIQUE

Configuration d'une instance Moodle

07.03.2022 – Version 1.0

1.	But du document	2
2.	Prérequis	2
3.	Procédure complète	2
4.	Configuration du plugin simpleSAMLphp sous Moodle	3
4.1	Aller à la page de configuration du plugin :	3
4.2	Configurer le SAML-Endpoint:.....	4
4.3	Générer le certificat du SP	5
4.4	Vérifier la conformité du certificat	5
4.5	Configurer «EdulogPersonTechID» comme attribut pour le champ utilisateur de Moodle	6
4.6	Configurer le «mapping» des attributs de Moodle avec ceux d'Edulog	7
5.	Communication du fichier Metadata du plugin SAML2 de Moodle au partenaire technique de la Fédération.....	8
6.	Tests de connexion	9

1. But du document

Ce document explique aux fournisseurs de services (SP) comment configurer une instance Moodle pour se fédérer avec Edulog.

Ce document n'explique pas l'installation de Moodle, ni l'installation du plugin *simpleSAMLphp*.

2. Prérequis

Ce guide ne peut être utilisé que si les exigences techniques suivantes sont respectées :

- Le SP utilise – dans sa propre infrastructure – un serveur avec une instance Moodle¹.
- Le SP utilise un plugin pour mettre en œuvre le protocole SAML pour connecter l'instance Moodle avec un IdP. Lorsque plusieurs plugins existent, nous montrons la configuration nécessaire avec *simpleSAMLphp*².
- Les certificats digitaux utilisés dans la configuration de l'instance Moodle et la signature de ses requêtes « SAML Request » vérifient les exigences de sécurité d'Edulog.

3. Procédure complète

Nous rappelons ici les étapes techniques³ nécessaires à un SP (avec l'infrastructure précédemment citée) pour réaliser la configuration nécessaire à l'*onboarding* avec Edulog :

N°	Actions à réaliser	Moment
1	Configurer l'instance Moodle et installer le plugin SAML2	Prérequis
2	Configurer le plugin SAML2 de Moodle	Chapitre 4
3	Communiquer à ELCA le fichier Metadata du plugin SAML2 de Moodle	Chapitre 5
4	Réaliser les tests de connexion avec des utilisateurs	Chapitre 6

Ce document traite les points 2 à 4.

¹ <https://download.moodle.org/>

² <https://simplesamlphp.org/>

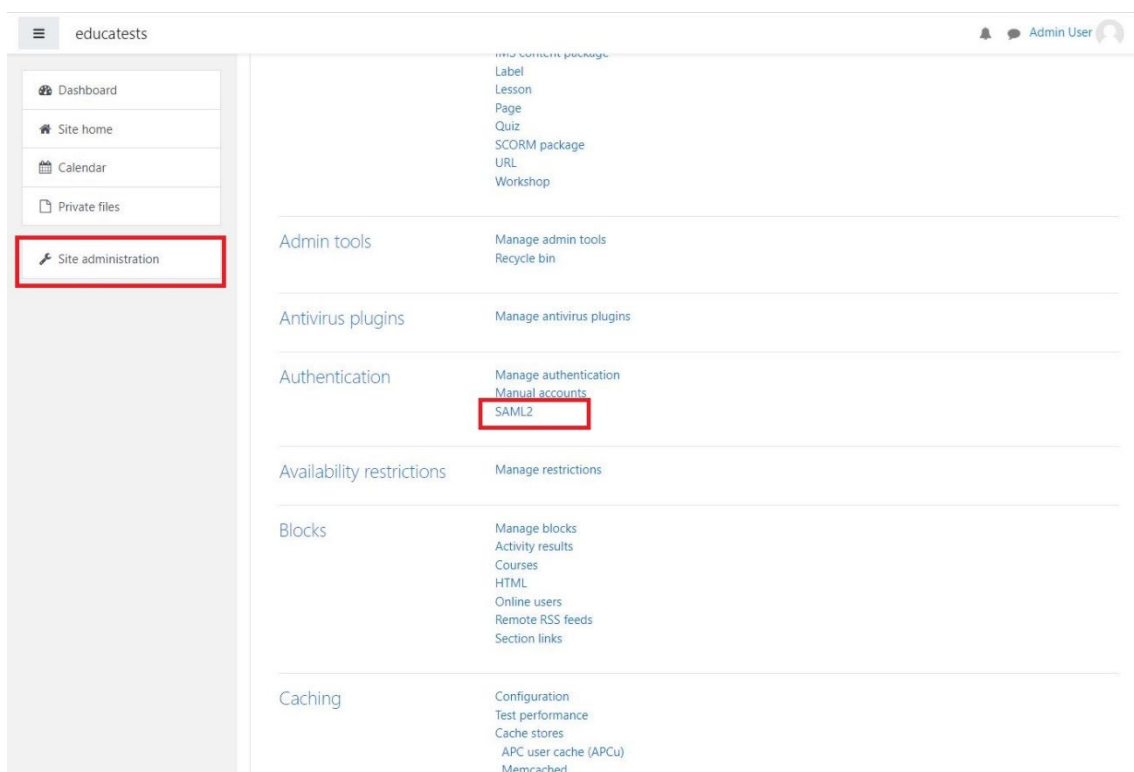
³ D'autres étapes non-techniques (contrats, etc.) sont nécessaires pour l'intégration dans la Fédération. Elles ne sont pas traitées dans ce document.

4. Configuration du plugin simpleSAMLphp sous Moodle

La configuration du plugin SAML de Moodle doit suivre un certain nombre de règles. Nous explicitons ici les différentes étapes nécessaires.

4.1 Aller à la page de configuration du plugin :

- Se connecter à l'instance Moodle en tant qu'administrateur;
- Sélectionner «Site administration», puis «Plugins», puis cliquer sur «SAML2» dans la section «Authentication».



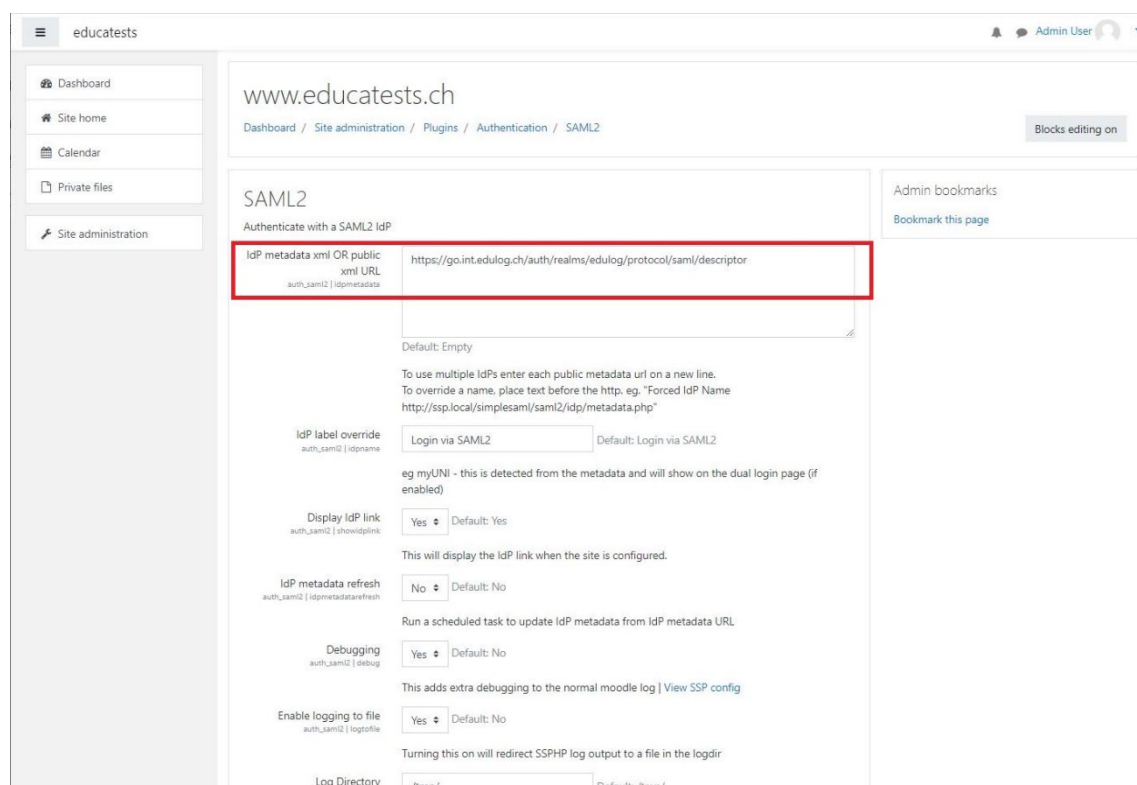
4.2 Configurer le SAML-Endpoint:

Dans l'exemple ci-dessous, l'instance Moodle est fédérée avec l'instance de test d'EduLog, le lien délivrant le fichier metadata d'EduLog est donc:

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

Dans le cas de la mise en production de l'instance, le lien est :

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



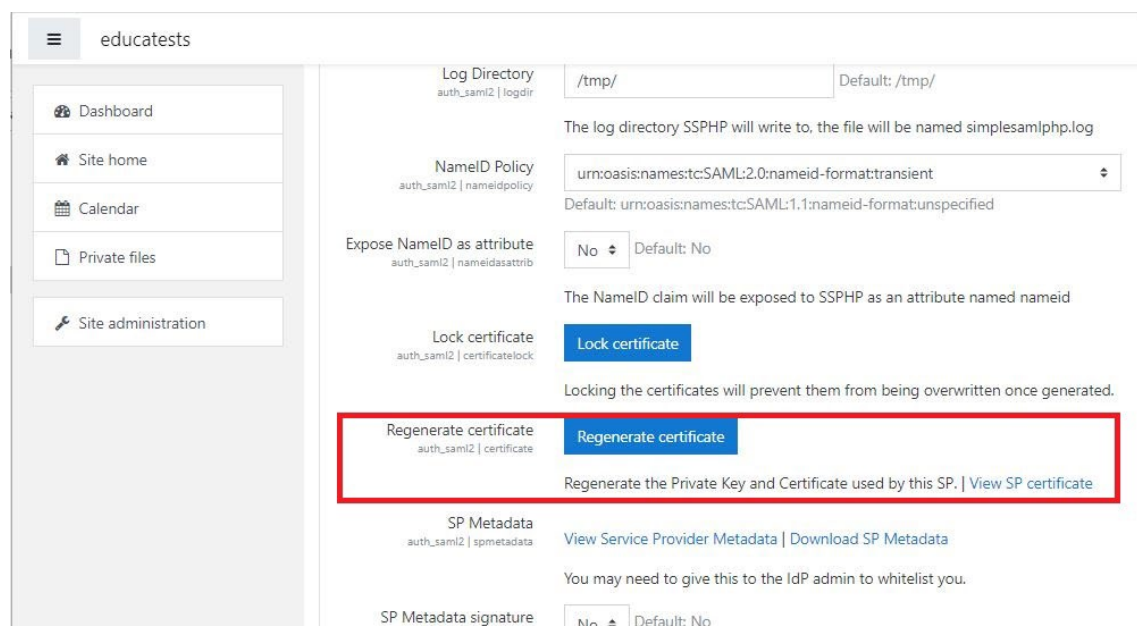
The screenshot shows the Moodle administration interface for the site 'educatests'. The left sidebar contains navigation links: Dashboard, Site home, Calendar, Private files, and Site administration. The main content area is titled 'SAML2' and 'Authenticate with a SAML2 IdP'. A red box highlights the '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 other configuration options:

- 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 | logfile): 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.

4.3 Générer le certificat du SP

Cliquer sur le bouton «Regenerate certificate» et remplir les champs nécessaires pour la génération.



educatests

- Dashboard
- Site home
- Calendar
- Private files
- Site administration

Log Directory
auth_saml2 | logdir /tmp/ Default: /tmp/
The log directory SSPHP will write to, the file will be named simplesamlphp.log

NameID Policy
auth_saml2 | nameidpolicy urn:oasis:names:tc:SAML:2.0:nameid-format:transient
Default: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Expose NameID as attribute
auth_saml2 | nameidasattrib No Default: No
The NameID claim will be exposed to SSPHP as an attribute named nameid

Lock certificate
auth_saml2 | certificatelock Lock certificate
Locking the certificates will prevent them from being overwritten once generated.

Regenerate certificate
auth_saml2 | certificate Regenerate certificate
Regenerate the Private Key and Certificate used by this SP. | View SP certificate

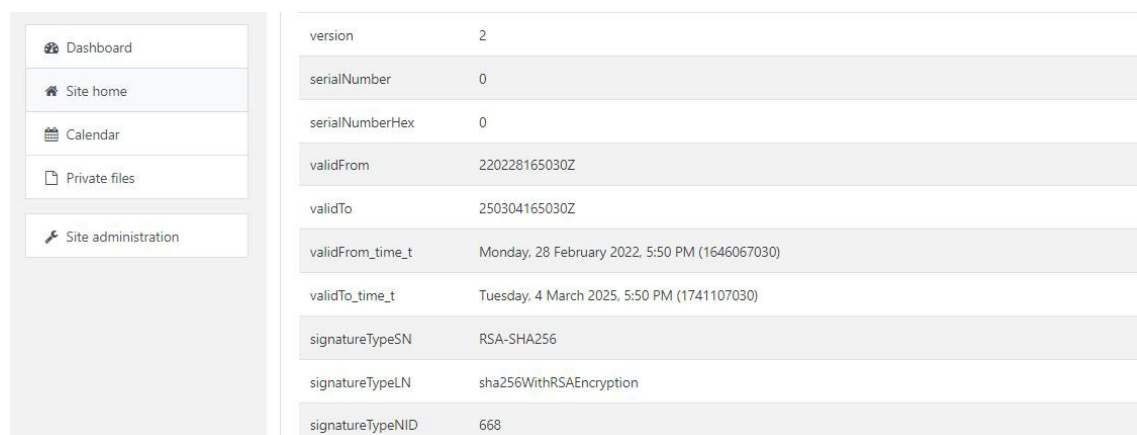
SP Metadata
auth_saml2 | spmetadata View Service Provider Metadata | Download SP Metadata
You may need to give this to the IdP admin to whitelist you.

SP Metadata signature No Default: No

4.4 Vérifier la conformité du certificat

Cliquer sur «View SP certificate».

Vérifier que la validité du certificat est bien de 3 ans et que le type de signature est sha256WithRSAEncryption.



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

Attention ! A chaque fois que le certificat est régénéré, le fichier metadata de votre instance change, ce qui peut poser problème avec la Fédération qui ne pourra vérifier la signature de vos requêtes SAML.

4.5 Configurer «EdulogPersonTechID» comme attribut pour le champ utilisateur de Moodle

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

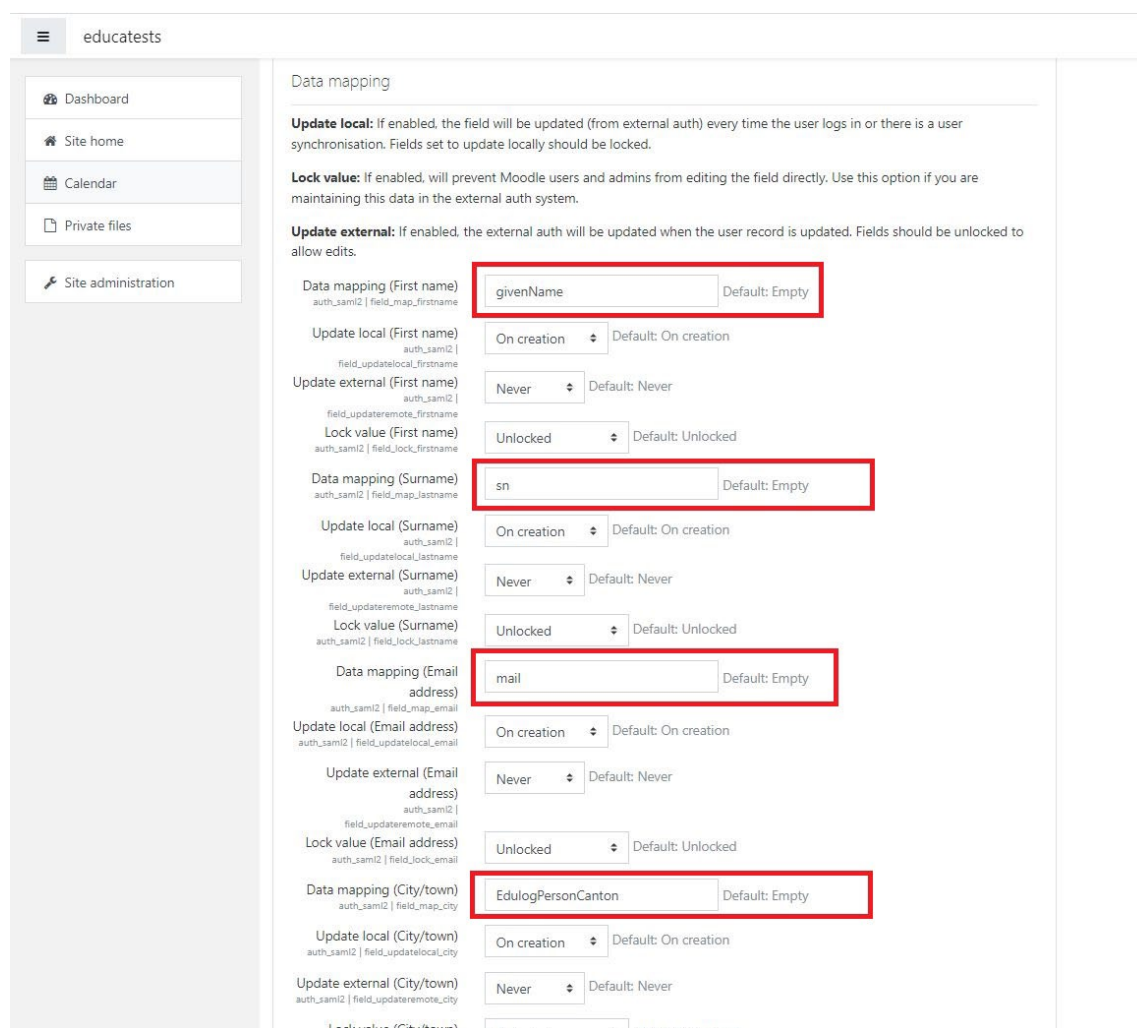
Default: Empty

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

L'attribut «EdulogPersonTechID» est un identifiant unique des identités d'Edulog. Le test réalisé permet de créer directement les utilisateurs d'Edulog dans l'instance Moodle en leur pré-remplissant certains attributs.

4.6 Configurer le «mapping» des attributs de Moodle avec ceux d'Edulog

Il est nécessaire d'expliciter quels attributs dans Moodle vont recevoir les données venant d'Edulog. Pour cela, on doit mettre en relation certains attributs de Moodle avec certains des attributs d'Edulog.



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.

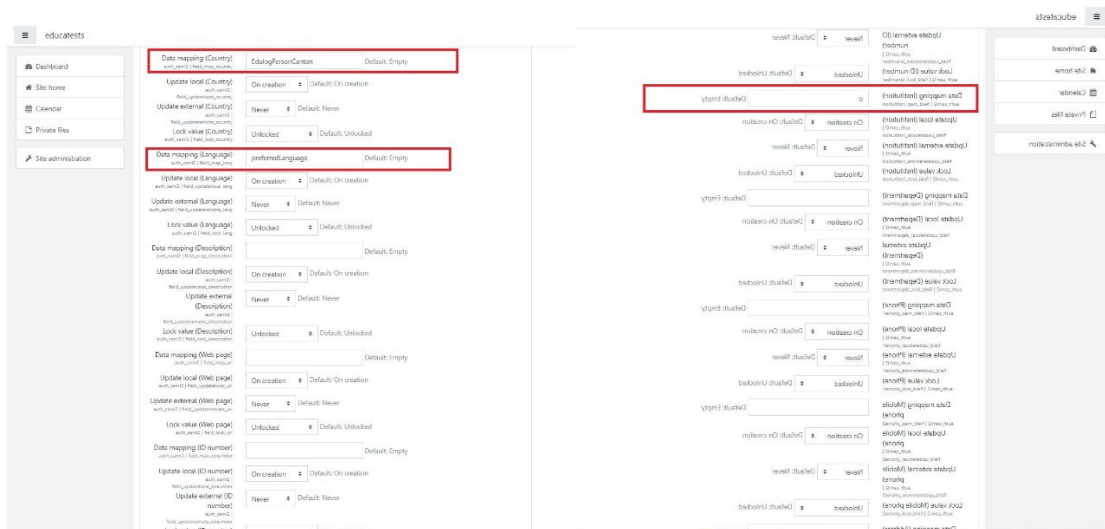
Update external: If enabled, the external auth will be updated when the user record is updated. Fields should be unlocked to allow edits.

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		Default: Unlocked

Seuls les attributs suivants d'Edulog sont facilement «mappés» dans l'instance Moodle de notre exemple :

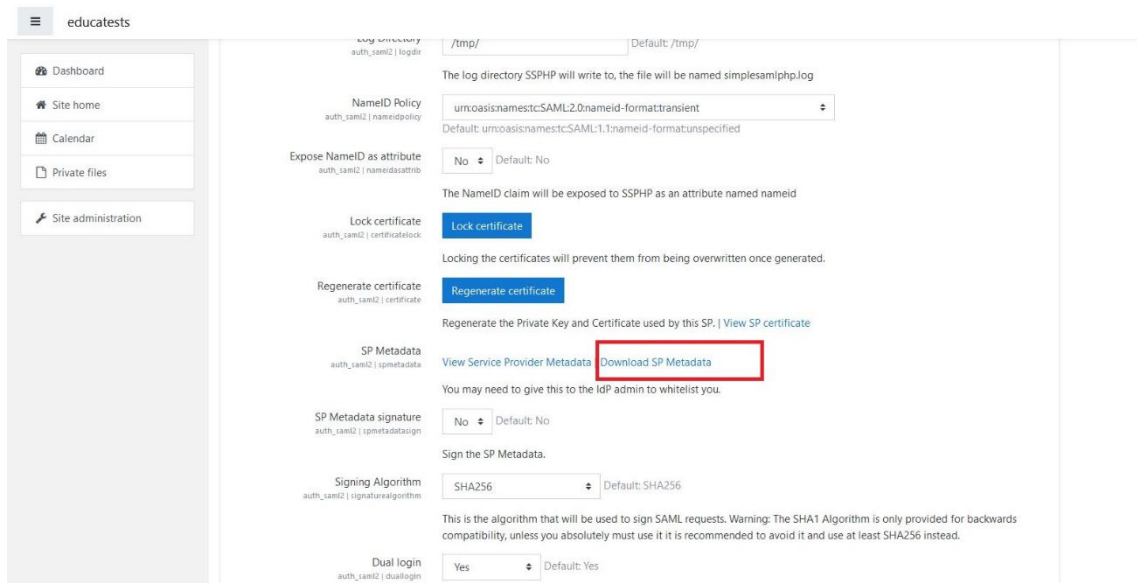
- «EdulogPersonTechID» avec «user» ;
- «givenName» avec «First name» ;
- «surname» avec «Surname» ;
- «mail» avec «email» ;
- «preferredLanguage» avec «Language» ;
- «o» avec «Institution».

Le reste des attributs d'Edulog doivent être assignés par le SP, soit à d'autres attributs existants (voir exemple de l'attribut «EdulogPersonCanton» sur l'attribut de Moodle «City/Town»), soit à de nouveaux attributs (si possible).



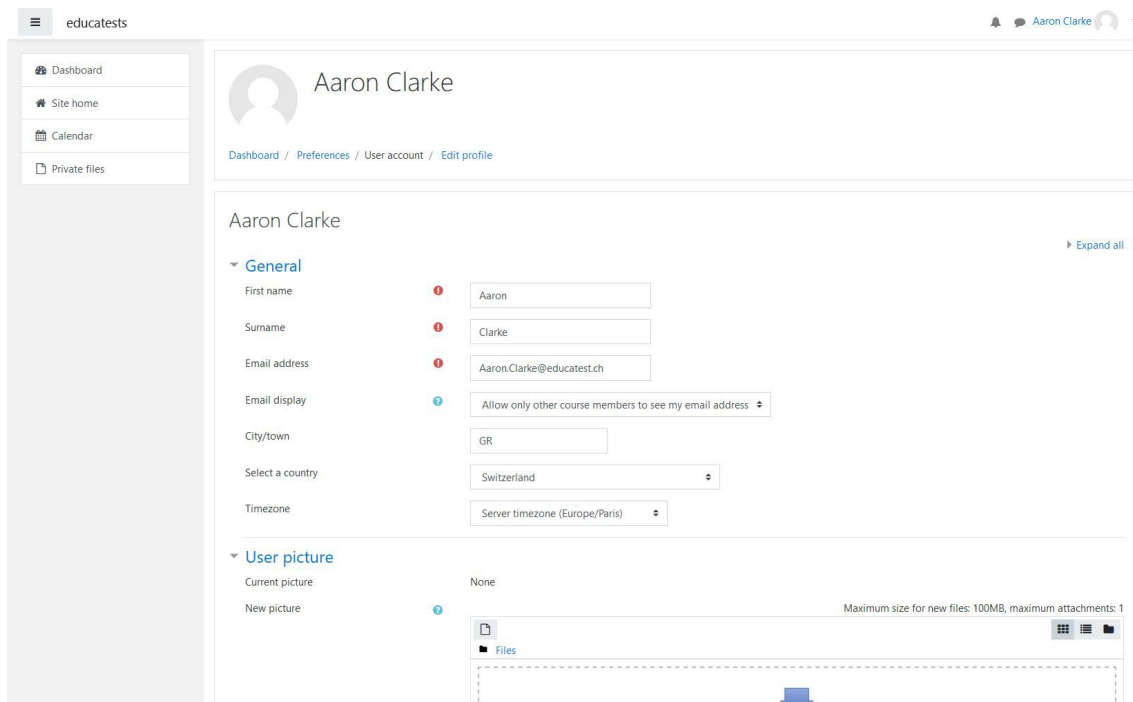
Ne pas oublier de sauvegarder la page avec les modifications.

5. Communication du fichier Metadata du plugin SAML2 de Moodle au partenaire technique de la Fédération



Une fois la configuration complétée, il faut récupérer la configuration SAML du *endpoint* créé par le plugin. Ce fichier sera après envoyé au partenaire technique de la Fédération qui pourra incorporer l'instance Moodle à Edulog.

6. Tests de connexion



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

Une fois la configuration du lien SAML terminé entre Edulog et le SP, on peut tester la connexion entre un utilisateur d'un IdP et l'instance Moodle. Si tout se passe bien, la première connexion de l'utilisateur créera un « profile » de l'utilisateur avec les attributs choisis au chapitre 4.