# SAML Authentifizierung in MOODLE konfigurieren



## Shibboleth Modul in Moodle konfigurieren

Dokumentation: http://docs.moodle.org/26/en/Shibboleth, auf jeden Fall empfehlenswert ist die README.txt Datei im Verzeichnis auth/shibboleth.

Hier ein grober Ablauf für den Umstieg der Authentifizierung in Moodle von LDAP auf Shibboleth: (am besten in einem Wartungsfenster und im Wartungsmodus durchführen)

1. In der Apache-Konfiguration einen Location-Eintrag setzen. Achtung: Dieser Eintrag muss nach dem Laden des Moduls mod_shib platziert werden.

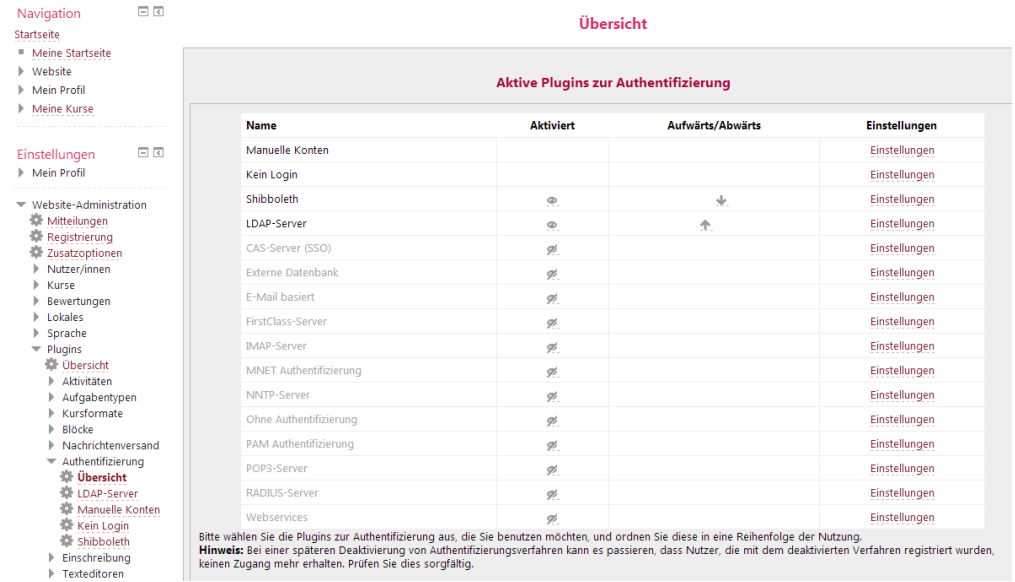
**alt: Apache 2.2**

```
<Location /moodle/auth/shibboleth/index.php>
    AuthType shibboleth
    ShibRequireSession On
    require valid-user
</Location>
```

**neu: DevOps Managed Server (Apache 2.4)**

```
<IfDefine ServerOptionShibboleth>
    Use ShibHeadersSession /moodle v-moodle
</IfDefine>
```

2. Apache durchstarten.
3. In Moodle einsteigen. Am besten temporär ein manuelles Konto verwenden, damit man sich ggf. nicht selbst aussperrt.
4. Authentifizierungsplugin Shibboleth aktivieren und an erste Position stellen:



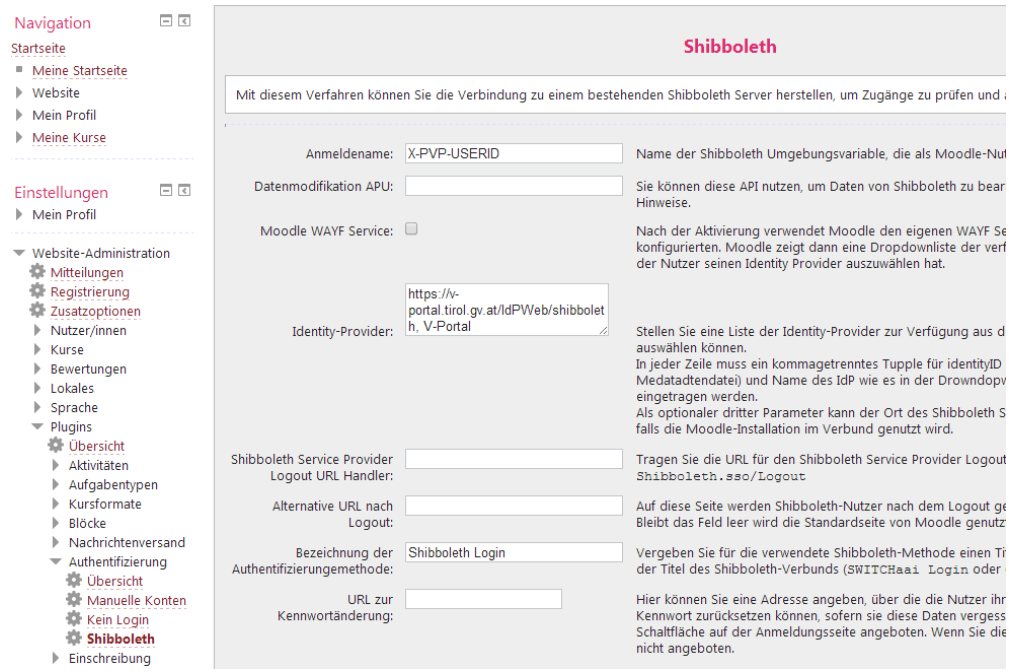

5. Authentifizierungsplugin Shibboleth einstellen: (Klick auf Einstellungen)

   Die SAML-Attribute haben unterschiedliche Namen, abhängig davon ob der Shibboleth Native-SP und Moodle innerhalb eines Apache (Verwendung von Environment-Variablen) oder getrennt

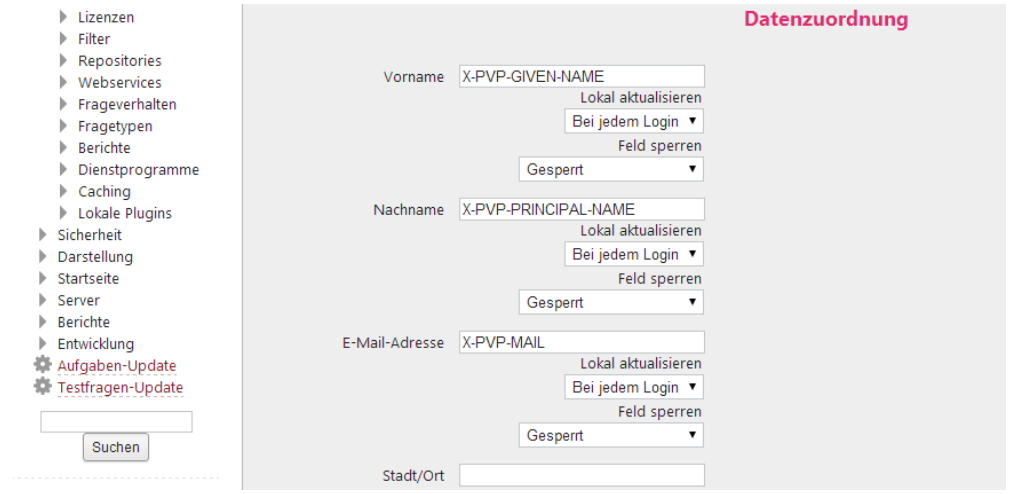
(Moodle im Backend; Verwendung von Request-Headern) läuft.
* Environment: wie in den Screenshots abgebildet, z.B. X-PVP-USERID
* Header: Attribute-Namen ergänzt um **HTTP**_ und Änderung von Bindestrich - zu Unterstrich_, z.B. HTTP_X_PVP_USERID

Für die Umsetzung von Moodle mit SAML (Shibboleth Native-SP und Shibboleth IDP) wird der (neue) IDP Version 3 verwendet. Daher ist noch folgende Einstellung anders als im Screenshot: Identity-Provider: **https://v-portal.tirol.gv.at/idp/shibboleth, V-Portal**

Der **Anmeldename** sollte mit jenem Attribut verknüpft werden, das sich mit dem Feld username in der Tabelle mdl_user deckt.




Dann können noch weitere Datenzuordnungen gemacht werden, je nach Belieben und Attributauswahl.




6. Änderungen speichern.
7. Zurück auf der Übersichtsseite kann eine URL für alternatives Login festgelegt werden. Falls Shibboleth als einzige Authentifzierungsmethode verwendet werden soll, ist in diesem Feld folgendes einzutragen:

```
/moodle/auth/shibboleth/index.php
```

8. Änderungen speichern.
9. Bestehende Benutzer sind jetzt aber noch in der Tabelle mdl_user mit der Authentifzierungsmethode

ldap verknüpft. Damit bestehende Benutzer sich nun mit Shibboleth authentifizieren können, muss in der Tabelle mdl_user der Wert für das Feld auth auf shibboleth aktualisiert werden und zwar für alle Datensätze, wo bisher der Wert ldap befüllt war.
Dies kann einfach mit einem Update-Statement durchgeführt werden:

```
UPDATE mdl_user SET auth = 'shibboleth' WHERE auth = 'ldap';
```

10. Mit der SAML Authentifizierung werden die Userids immer mit dem Postfix "@tsn.at" übertragen. Wenn in der Datenbank alte Userids von der TSN LDAP Authentifizierung vorhanden sind, müssen diese Userids aktualisiert werden, ansonst werden neue Benutzer angelegt und nicht die vorhandenen verwendet.
    Dies kann einfach mit einem Update-Statement durchgeführt werden:

    ```
    UPDATE mdl_user SET username = concat(username,'@tsn.at') WHERE
    auth = 'shibboleth' and username not like '%@tsn.at';
    ```

11. Jetzt sollte ein Login via Shibboleth möglich sein.