Auth NetYpareo: requests and data flows

This page describes the exchanges between Moodle and NetYpareo (Yparéo) carried out by the authentication plugin `auth_netypareo`: who calls whom, with which method, which requests are issued and which data flows in each direction. It is intended for the security and compliance officers of the organisations using the plugin.

Overview

Exchanges take place in **three distinct contexts**:

Context	Trigger	Direction	Data
Single sign-on (SSO)	The user clicks from NetYpareo	NetYpareo → browser → Moodle, then Moodle → NetYpareo	A validation token, then the user's identity
Scheduled synchronisation	Moodle scheduled tasks, at night	Moodle → NetYpareo (read requests)	Users, sites, groups, periods, training courses
Document feedback	A document is generated in Moodle	Moodle → NetYpareo (upload)	A learner's PDF document

In all cases **Moodle is the client**: the plugin opens no entry point allowing NetYpareo to read from or write to Moodle. The only element received from NetYpareo is the login token, passed on by the user's browser.

Protocol and transport security

- **Main protocol: REST** (JSON) on the base URL of the NetYpareo instance (*baseurl* setting). A **SOAP** variant remains available (*protocol* setting) and also serves as a fallback for token validation.
- **Authentication of Moodle against NetYpareo**: with REST, a web service token is sent in the `X-Auth-Token` HTTP header of each request (*authwsresttoken* setting). With SOAP, service credentials (login and password) are used, distinct for each service (authentication, users, Pareo, EDM).
- **Licence levels**: the usual read functions use the “basic” licence. Uploading documents and reading document folders require the “expert” licence.
- **Encoding**: texts sent to NetYpareo are converted from UTF-8 to ISO-8859-15 (document name).
- **Proxy**: the HTTP proxy configured in Moodle is used if there is one.
- **Timeout**: adjustable connection timeout (*defaulttimeout*, 10 seconds by default).
- **TLS certificate verification**: in the current version of the REST client, verification of the NetYpareo server certificate is disabled (`CURLOPT_SSL_VERIFYPEER` set to false). See the

Points of attention section.

1. Single sign-on (token SSO)

1. The user is logged in to NetYpareo and opens Moodle from a link that adds a `token` parameter to the Moodle login URL.
2. The plugin reads this parameter when the login page is displayed. Without a token, it does nothing and the other login methods apply.
3. If several NetYpareo instances are configured (PRO version), the originating instance is identified by the *Referer* HTTP header. A Moodle site without HTTPS may not receive this header.
4. Moodle calls NetYpareo to validate the token:

```
GET {baseurl}/r/v1/authentification-jeton/utilisateur/{jeton}
Header: X-Auth-Token: <service token>
```

1. If the REST call fails, a second attempt is made using SOAP (token authentication service).
2. The response gives the user type (learner, staff, tutor/company) and the identity: last name, first name, email address and NetYpareo internal code.
3. Moodle looks up the existing account by its **identification number** (`idnumber`, in the form *{instance}_{NetYpareo code}*). If the account exists and is not suspended, the session is opened and the user is redirected to the home page. **No account is created at this step**: accounts are created by the scheduled synchronisation.
4. The password is neither transmitted nor stored by this flow.

2. Scheduled synchronisation

Scheduled tasks query NetYpareo in read-only mode. Default schedules (editable in the Moodle administration):

Task	Schedule	REST requests issued
Sites	00:30	`GET /r/v1/sites`
Reference data caches	00:05	statuses, situations, training courses, diplomas, subjects, business sectors, countries, periods, companies (`GET /r/v1/statuts`, `/situations`, `/formations`, `/diplomes-prepares`, `/matieres`, `/secteurs-activite`, `/pays`, `/periodes`, `/entreprises`)
Trainers (staff)	01:00	`GET /r/v1/utilisateur/personnels/{site}`
Tutors and companies	01:10	`GET /r/v1/entreprises`
Learners	01:20	`GET /r/v1/utilisateur/apprenants/{site}`
Groups	02:30	`GET /r/v1/formation-longue/groupes` (parameters: periods, sites)
Short training groups	04:30	`GET /r/v1/formation-courte/{…}/groupes`

Detail requests are also available for a learner, a group or a staff member (`/r/v1/apprenants/{code}`, `/r/v1/groupes/{code}`, `/r/v1.1/personnels/{code}`, `/r/v1/formation-longue/apprenants`, `/r/v1/groupes/{code}/apprenants`, `/r/v1/formation-courte/…/apprenants`, `/r/v1/apprenants/frequentes`, `/r/v1/document/apprenants/{code}/photo`). *To be checked: which of these functions are*

actually called by the tasks of the delivered version.

Each task can be disabled by a setting (*syncstudents*, *syncteachers*, *synctutors*, *syncsites*, *syncgroups*, *syncpdgroups*). Filters (PRO version) allow restricting the import to the desired sites, periods or groups.

Data imported into Moodle

Default mapping for a **learner** (NetYpareo fields → Moodle fields):

NetYpareo data	**Moodle field**
`prenom` / `nom`	First name / Last name
`email` (or `adresse.email`)	Email address
`login`	Username (prefixed with the instance number)
`codeApprenant`	Identification number (`idnumber`, prefixed with the instance number)
`codeSite`	Home site (profile field)
`compteExpireLe`	Account expiry date
`adresse.ville`, `nomPays`	City, country
`nomEtabOrigine`, `departement`	Institution, department
`tel1`, `tel2`	Phone numbers
`estMajeur`	“Adult” profile field
`codeStatut`, `codeDiplome`, `codeFormation`, `codeAnnee`	Profile fields: status, curriculum, programme, programme year

For a **trainer**: first name, last name, username, email, staff code, home site (name and code). For a **tutor or company**: first name, last name, username, email, contact code, company name.

For **groups**: name, site, training year, lead trainer, action category, assessment mode, teaching and entry/exit arrangements.

Accounts have the authentication method `netypareo`. Former accounts that no longer appear in NetYpareo can be suspended or deleted depending on the *deleteoldusers*, *deleteoldsites* and *deleteoldcachedata* settings.

To be checked: the exact field mapping can be adapted per instance (PRO version); the tables above are those of the default configuration.

3. Sending documents to NetYpareo

When the *sendpdcertificates* setting is active and a certificate is generated in Moodle (*pdcertificate* module), the plugin sends the PDF document to the EDM folder of the learner concerned:

```
POST {baseurl}/r/v1/document/apprenant/{codeApprenant}/document[/{folder}]
Header: X-Auth-Token: <service token>
Corps JSON : contenu (base64), nomDocument, extension, mimeType,
dateCreation
```

- Only users whose identification number matches a NetYpareo learner are concerned.
- The document sent is the one Moodle has just generated for that learner. No other data is attached.
- Sending training session reports (*sendtrainingsessionreports*) is provided for in the configuration but is **not implemented** in the current version.

What the plugin does not send

- No Moodle password.
- No tracking, grade or progress data: only the documents mentioned above are transmitted, and only as a result of the document being generated. *To be checked:* sendlearningtimechecks *setting (not linked to any upload in the code that was read).*

Storage in Moodle

Imported data is stored in Moodle's standard tables (`user`, `user_info_data` for profile fields, cohorts and groups) and in the plugin's own tables (instances, reference data caches: sites, statuses, situations, training courses, diplomas). Synchronisation logs are written to the configured log directory (*logdir*); their content may include user names and identifiers.

Points of attention

- **TLS certificate**: never tick *Do not verify the TLS certificate* in production. A self-signed certificate or an internal authority must be declared in the Moodle server's certificate store.
- **Token in the URL**: the login token travels in the URL of the login page; it is for validation use only and must not be kept in intermediate access logs.
- **GDPR declaration**: :a faire: The GDPR provider must be reviewed to take into account the identity data flows passing through it.
- **Technical account**: the service token must be limited to the required read functions and to the required licence.

Back to the component index - Back to the plugin index - Back to the catalog

From:
https://docsen.activeprolearn.com/ - **Documentation Moodle ActiveProLearn**

Permanent link:
https://docsen.activeprolearn.com/doku.php?id=auth:netypareo:dataflow

Last update: **2026/11/13 22:01**