Auth NetYpareo : requêtes et flux de données

Cette page décrit les échanges entre Moodle et NetYpareo (Yparéo) réalisés par le plugin d'authentification `auth_netypareo` : qui appelle qui, avec quelle méthode, quelles requêtes sont émises et quelles données circulent dans chaque sens. Elle s'adresse aux responsables de la sécurité et de la conformité des organismes utilisateurs.

Vue d'ensemble

Les échanges se font dans **trois contextes** distincts :

Contexte	Déclencheur	Sens	Données
Connexion unique (SSO)	L'utilisateur clique depuis NetYpareo	NetYpareo → navigateur → Moodle, puis Moodle → NetYpareo	Un jeton à usage de validation, puis identité de l'utilisateur
Synchronisation planifiée	Tâches planifiées Moodle, la nuit	Moodle → NetYpareo (requêtes de lecture)	Utilisateurs, sites, groupes, périodes, formations
Retour de documents	Génération d'un document dans Moodle	Moodle → NetYpareo (envoi)	Document PDF d'un apprenant

Dans tous les cas **Moodle est le client** : le plugin n'ouvre aucun point d'entrée permettant à NetYpareo de lire ou d'écrire dans Moodle. Le seul élément reçu de NetYpareo est le jeton de connexion, transmis par le navigateur de l'utilisateur.

Protocole et sécurité du transport

- **Protocole principal : REST** (JSON) sur l'URL de base de l'instance NetYpareo (réglage *baseurl*). Une variante **SOAP** reste disponible (réglage *protocol*) et sert aussi de secours pour la validation du jeton.
- **Authentification de Moodle auprès de NetYpareo** : en REST, un jeton de web service est envoyé dans l'en-tête HTTP `X-Auth-Token` de chaque requête (réglage *authwsresttoken*). En SOAP, des identifiants de service (login et mot de passe) sont utilisés, distincts par service (authentification, utilisateurs, Pareo, GED).
- **Niveaux de licence** : les fonctions de lecture usuelles utilisent la licence « basic ». L'envoi de documents et la lecture des répertoires de documents requièrent la licence « expert ».
- **Encodage** : les textes envoyés à NetYpareo sont convertis de UTF-8 vers ISO-8859-15 (nom de document).
- **Proxy** : le proxy HTTP configuré dans Moodle est utilisé s'il existe.
- **Délai** : délai de connexion réglable (*defaulttimeout*, 10 secondes par défaut).

- **Vérification du certificat TLS** : dans la version actuelle du client REST, la vérification du certificat du serveur NetYpareo est désactivée (`CURLOPT_SSL_VERIFYPEER` à faux). Voir la section *Points d'attention*.

1. Connexion unique (SSO par jeton)

1. L'utilisateur est connecté dans NetYpareo et ouvre Moodle depuis un lien qui ajoute un paramètre `token` à l'URL de connexion de Moodle.
2. Le plugin lit ce paramètre à l'affichage de la page de connexion. Sans jeton, il ne fait rien et les autres méthodes de connexion s'appliquent.
3. Si plusieurs instances NetYpareo sont configurées (version PRO), l'instance d'origine est identifiée par l'en-tête HTTP *Referer*. Un site Moodle sans HTTPS peut ne pas recevoir cet en-tête.
4. Moodle appelle NetYpareo pour valider le jeton :

```
GET {baseurl}/r/v1/authentification-jeton/utilisateur/{jeton}
En-tête : X-Auth-Token: <jeton de service>
```

1. En cas d'échec de l'appel REST, un second essai est fait en SOAP (service d'authentification par jeton).
2. La réponse indique le type d'utilisateur (apprenant, personnel, tuteur/entreprise) et l'identité : nom, prénom, adresse email et code interne NetYpareo.
3. Moodle recherche le compte existant par son **numéro d'identification** (`idnumber`, de la forme *{instance}_{code NetYpareo}*). Si le compte existe et n'est pas suspendu, la session est ouverte et l'utilisateur est redirigé vers l'accueil. **Aucun compte n'est créé à cette étape** : les comptes sont créés par la synchronisation planifiée.
4. Le mot de passe n'est ni transmis ni stocké par ce flux.

2. Synchronisation planifiée

Les tâches planifiées interrogent NetYpareo en lecture seule. Horaires par défaut (modifiables dans l'administration Moodle) :

Tâche	Horaire	Requêtes REST émises
Sites	00h30	`GET /r/v1/sites`
Caches de référentiels	00h05	statuts, situations, formations, diplômes, matières, secteurs d'activité, pays, périodes, entreprises (`GET /r/v1/statuts`, `/situations`, `/formations`, `/diplomes-prepares`, `/matieres`, `/secteurs-activite`, `/pays`, `/periodes`, `/entreprises`)
Formateurs (personnels)	01h00	`GET /r/v1/utilisateur/personnels/{site}`
Tuteurs et entreprises	01h10	`GET /r/v1/entreprises`
Apprenants	01h20	`GET /r/v1/utilisateur/apprenants/{site}`
Groupes	02h30	`GET /r/v1/formation-longue/groupes` (paramètres : périodes, sites)
Groupes de formation courte	04h30	`GET /r/v1/formation-courte/{…}/groupes`

Les requêtes de détail sont également disponibles pour un apprenant, un groupe ou un personnel (`/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`). *À vérifier : lesquelles de ces fonctions sont effectivement appelées par les tâches de la version livrée.*

Chaque tâche peut être désactivée par un réglage (*syncstudents*, *syncteachers*, *synctutors*, *syncsites*, *syncgroups*, *syncpdgroups*). Des filtres (version PRO) permettent de restreindre l'import aux sites, périodes ou groupes souhaités.

Données importées dans Moodle

Correspondance par défaut pour un **apprenant** (champs NetYpareo → champs Moodle) :

Donnée NetYpareo	**Champ Moodle**
`prenom` / `nom`	Prénom / Nom
`email` (ou `adresse.email`)	Adresse email
`login`	Identifiant (préfixé du numéro d'instance)
`codeApprenant`	Numéro d'identification (`idnumber`, préfixé du numéro d'instance)
`codeSite`	Site de rattachement (champ de profil)
`compteExpireLe`	Date d'expiration du compte
`adresse.ville`, `nomPays`	Ville, pays
`nomEtabOrigine`, `departement`	Institution, département
`tel1`, `tel2`	Téléphones
`estMajeur`	Champ de profil « majorité »
`codeStatut`, `codeDiplome`, `codeFormation`, `codeAnnee`	Champs de profil : statut, cursus, programme, année du programme

Pour un **formateur** : prénom, nom, identifiant, email, code personnel, site de rattachement (nom et code). Pour un **tuteur ou entreprise** : prénom, nom, identifiant, email, code interlocuteur, nom de l'entreprise.

Pour les **groupes** : nom, site, année de formation, formateur référent, catégorie d'action, mode d'évaluation, modalités d'enseignement et d'entrée/sortie.

Les comptes ont pour méthode d'authentification `netypareo`. Les anciens comptes qui ne figurent plus dans NetYpareo peuvent être suspendus ou supprimés selon les réglages *deleteoldusers*, *deleteoldsites* et *deleteoldcachedata*.

À vérifier : la correspondance exacte des champs peut être adaptée par instance (version PRO) ; les tableaux ci-dessus sont ceux de la configuration par défaut.

3. Envoi de documents vers NetYpareo

Lorsque le réglage *sendpdcertificates* est actif et qu'un certificat est généré dans Moodle (module *pdcertificate*), le plugin envoie le document PDF dans le dossier GED de l'apprenant concerné :

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

- Seuls les utilisateurs dont le numéro d'identification correspond à un apprenant NetYpareo sont concernés.
- Le document envoyé est celui que Moodle vient de générer pour cet apprenant. Aucune autre donnée n'est jointe.
- L'envoi des rapports de sessions de formation (*sendtrainingsessionreports*) est prévu dans la configuration mais **n'est pas implémenté** dans la version actuelle.

Ce que le plugin n'envoie pas

- Aucun mot de passe Moodle.
- Aucune donnée de traces, de notes ou de progression : seuls les documents cités ci-dessus sont transmis, et uniquement à l'initiative de la génération du document. *À vérifier : réglage* sendlearningtimechecks *(non relié à un envoi dans le code lu).*

Stockage dans Moodle

Les données importées sont stockées dans les tables standard de Moodle (`user`, `user_info_data` pour les champs de profil, cohortes et groupes) et dans les tables propres au plugin (instances, caches de référentiels : sites, statuts, situations, formations, diplômes). Les journaux de synchronisation sont écrits dans le répertoire de journaux configuré (*logdir*) ; leur contenu peut inclure des noms et identifiants d'utilisateurs.

Points d'attention

- **Certificat TLS** : la vérification du certificat du serveur NetYpareo est désactivée dans le client REST actuel. Correctif prévu : l'activer par défaut avec une option de dérogation documentée.
- **Jeton dans l'URL** : le jeton de connexion circule dans l'URL de la page de connexion ; il est à usage de validation et ne doit pas être conservé dans les journaux d'accès intermédiaires.
- **Déclaration RGPD** : le fournisseur de confidentialité du plugin est déclaré « sans données » alors que le plugin importe des données personnelles et envoie des documents vers un système tiers. La déclaration doit être complétée.
- **Compte technique** : le jeton de service doit être limité aux fonctions de lecture nécessaires et à la licence requise.

Revenir à l'index du composant - Revenir à l'index des plugins - Revenir au catalogue

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

Permanent link:
https://docs.activeprolearn.com/doku.php?id=auth:netypareo:dataflow&rev=1792677161

Last update: **2026/10/22 15:52**