Chapitre 3
Les modes d'authentification

1. Introduction

Vous allez découvrir dans ce chapitre les différents mécanismes qui permettent de gérer les comptes des utilisateurs.

Vous avez remarqué que des comptes prédéfinis sont créés lors de l'installation de GLPI, ce qui signifie que GLPI est capable de gérer l'authentification des utilisateurs au travers de sa propre base de comptes.

De nombreuses entreprises exploitent des solutions d'annuaires ou de comptes bureautiques. GLPI sait parfaitement s'appuyer sur ces éléments pour authentifier des utilisateurs et les ajouter dans la base des utilisateurs.

Vous apprendrez dans le chapitre sur les profils que ces données extérieures permettent d'aller au-delà de la simple authentification car elles permettent également de gérer dynamiquement les habilitations attribuées à ces utilisateurs.

La gestion de la base des comptes utilisateurs se fait dans le menu **Administration - Utilisateurs**, alors que la définition des éléments d'authentification externe se passe dans le menu **Configuration - Authentification**.

2. La base locale de comptes

Cette base de comptes sert à enregistrer les données relatives à tous les utilisateurs quel que soit leur mode d'authentification. Il est possible dans cette base de comptes de gérer manuellement l'ajout des utilisateurs.

La gestion de la base de comptes a lieu dans le menu **Administration - Utilisateurs**. Afin d'obtenir la visibilité et les droits sur ce menu, vous utiliserez le compte **glpi** qui possède les droits associés au profil Super-Admin.

Les comptes par défaut

Lors de l'installation de GLPI, cinq comptes utilisateurs prédéfinis sont créés :

– **glpi** (mot de passe **glpi**, profil associé **Super-Admin** sur l'**Entité Racine** récursif).

– **glpi-system** (ce nouvel utilisateur est spécial et est utilisé pour les actions automatiques).

– **normal** (mot de passe **normal**, profil associé **Observateur** sur l'**Entité Racine** récursif).

– **post-only** (mot de passe **postonly**, profil associé **Self-Service** sur l'**Entité Racine** récursif).

– **tech** (mot de passe **tech**, profil associé **Technicien** sur l'**Entité Racine** récursif).

Remarque

*La première chose à faire est de sécuriser l'accès à GLPI en mode **Super-Admin**.*

Sécurisation des comptes par défaut

Vous devez modifier le mot de passe du compte utilisateur **glpi** :

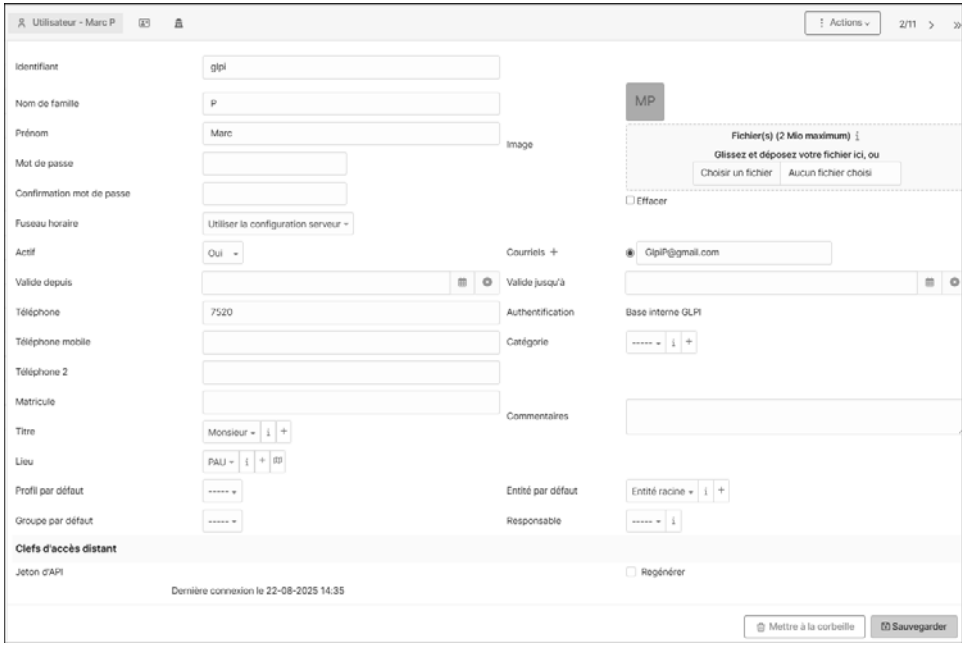
▶Placez-vous dans le menu **Administration - Utilisateurs**.

La liste des utilisateurs présents dans la base de comptes s'affiche.

▶Cliquez sur le nom du compte **glpi**.

La fiche de l'utilisateur s'affiche.

▶Dans le champ **Mot de passe**, saisissez le nouveau mot de passe, puis ressaisissez-le dans le champ **Confirmation mot de passe**. Afin de respecter la politique de sécurité des mots de passe mise en place, celle-ci est rappelée à côté de ces champs.



▶Validez la modification en cliquant sur le bouton **Sauvegarder**.

L'accès à la configuration de GLPI est maintenant protégé par un mot de passe sur les comptes par défaut.

L'ajout de nouveaux utilisateurs

Pour ajouter manuellement un compte :

▶Placez-vous dans le menu **Administration - Utilisateurs**.

La liste des utilisateurs présents dans la base de comptes s'affiche.

▶Cliquez sur le bouton 

(bleu).

Remarque

Pour l'ajout de nouveaux utilisateurs, un bouton spécifique est disponible : 

▶Renseignez les différents champs :

Identifiant : ce champ permet de définir le login de l'utilisateur.

Si vous envisagez de mettre en place une authentification externe, il est fortement recommandé de choisir pour l'utilisateur en cours de création un login correspondant à l'identifiant que renvoie l'authentification externe. Ainsi, lorsque l'authentification externe sera en place, GLPI authentifiera l'utilisateur à partir de la source externe mais préservera pour l'utilisateur la configuration et les habilitations placées manuellement sur ce compte.

Courriels : ce champ est très important car il permet l'émission de messages dans le cadre du suivi des demandes d'assistance.

Remarque

Il est possible d'enregistrer et de gérer plusieurs adresses de messagerie en cliquant sur le ⊞ *situé à côté de "courriels" et en cochant l'adresse à prendre en compte.*

Nom de famille, **Prénom**, **Téléphone**, **Téléphone mobile**, **Téléphone 2**, **Matricule**, **Titre** : ces champs sont à remplir avec les informations concernant l'utilisateur et n'appellent aucun commentaire particulier.

Remarque

Attention, la loi française encadre strictement l'utilisation de données nominatives. Il convient de ne pas utiliser GLPI pour stocker des données nominatives dont l'utilité serait éloignée de l'objectif initial de l'application.

Mot de passe : ce champ permet de définir un mot de passe pour l'utilisateur courant. Dans tous les cas, si vous utilisez la base de comptes locale, la définition d'un mot de passe est obligatoire. Si vous mettez en place une authentification externe, celle-ci devient prioritaire sur le mot de passe local.

Remarque

Les mots de passe ne sont pas stockés en clair dans la base de données : seul le hash MD5 du mot de passe est stocké. L'authentification se fait par comparaison de ce hash avec le MD5 du mot de passe saisi.

Confirmation mot de passe : ce champ permet de s'assurer de la bonne saisie du mot de passe.

Fuseau horaire : ce champ peut permettre d'affecter un fuseau horaire propre à l'utilisateur. Les différents affichages et notifications contenant des dates et heures seront convertis dans le fuseau de l'utilisateur.

Actif : ce champ permet de rendre actif ou inactif un compte utilisateur.

Valide depuis et **Valide jusqu'à** : ces deux champs permettent de positionner une date de début et/ou une date de fin d'activité pour ce compte utilisateur. Utile, par exemple, pour la création d'un compte utilisateur « Stagiaire ».

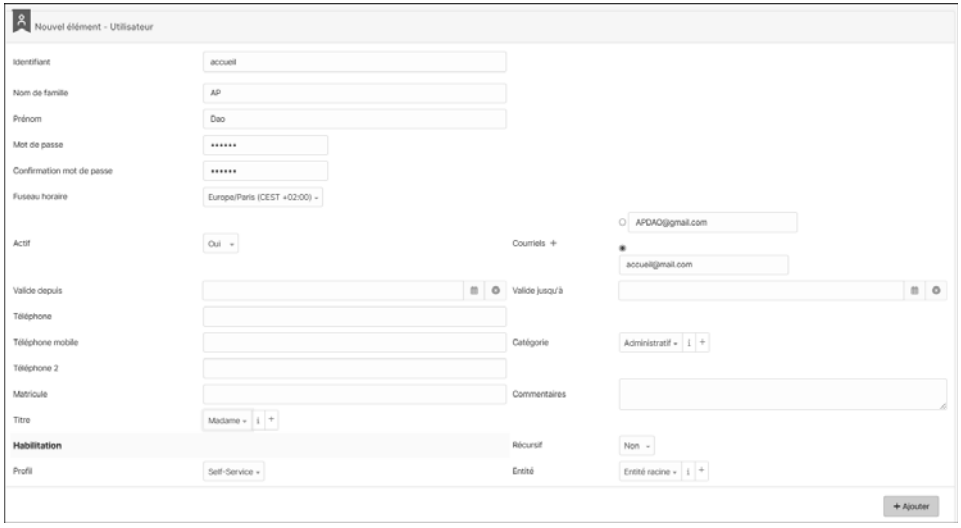
Catégorie : il est possible de définir des catégories d'utilisateurs. Cette gestion se fait dans le menu **Configuration - Intitulés**, **Types d'utilisateurs**.

Commentaires : ce champ permet de saisir des informations supplémentaires concernant l'utilisateur courant.

Profil : par défaut, huit profils ont été prédéfinis dans GLPI. Super-Admin / Admin / Supervisor / Technicien / Hotliner / Observateur / Self-Service / Read-Only. Nous les examinerons plus en détail dans le chapitre Les profils.

Récursif : Oui / Non. Principe de récursivité : permet de répercuter les droits liés au profil à toutes les entités filles de l'entité définie dans le champ suivant.

Entité : ce champ permet d'associer un utilisateur à une entité. En choisissant une entité fille, cet utilisateur aura des droits (pas obligatoirement identiques) sur plusieurs entités.



▶Validez l'ajout de l'utilisateur en cliquant sur le bouton + Ajouter (jaune).

Vous découvrirez dans le chapitre sur les profils les droits dont bénéficie par défaut un compte qui vient d'être créé et comment attribuer de nouveaux droits à un utilisateur.

Remarque

Si une connexion à une source d'authentification externe est présente dans la configuration de GLPI, il est possible d'importer des utilisateurs. Un bouton spécifique apparaît alors en haut de l'écran. En fonction du paramétrage existant, GLPI propose alors un import depuis les annuaires ou depuis les autres sources.

3. Les modes d'authentification externe

La possibilité qu'offre GLPI de gérer manuellement une base de comptes ne peut être considérée comme suffisante dès lors que le nombre d'utilisateurs devient trop important.

Il convient alors de s'appuyer sur une source externe de données pour valider le fait qu'un utilisateur a le droit de se connecter à l'application.

En fonction de la source de données externe choisie, GLPI proposera différents modes de fonctionnement. Il sera par exemple possible de choisir d'importer les données d'un annuaire pour alimenter la base locale de comptes. Cette solution simplifie bien sûr la gestion de la base de comptes mais reste un mode de gestion manuel.

GLPI propose donc de déléguer l'authentification à un outil externe. Les principaux outils sur lesquels peut s'appuyer GLPI sont :

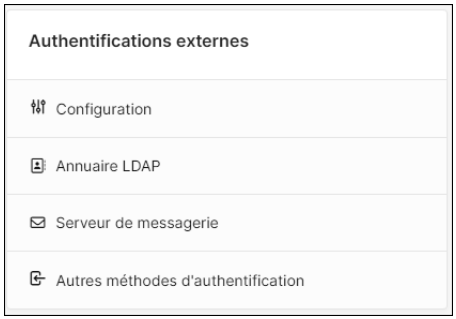
– un annuaire LDAP ;

– un serveur de messagerie.

Dès lors qu'un utilisateur sera authentifié au travers d'une source externe, il vous sera possible de l'ajouter automatiquement à la base de comptes de l'application.

Pour activer l'ajout des utilisateurs qui s'authentifient sur des ressources externes :

- Placez-vous dans le menu **Configuration - Authentification**.



- Cliquez sur le lien **Configuration**.

  La fenêtre de configuration des authentifications externes s'affiche.

- Placez le champ **Ajout automatique des utilisateurs à partir des sources externes d'authentification** sur **Oui**.

Les autres champs de cette fenêtre de configuration sont :

Ajouter un utilisateur sans habilitation depuis un annuaire LDAP : ce champ permet d'autoriser l'ajout d'un utilisateur dans la base de comptes locale, même si aucune règle ne lui donne d'habilitation.

Action lorsqu'un utilisateur est supprimé de l'annuaire LDAP : (Conserver / Désactiver / Désactiver + Retirer les groupes / Désactiver + Retirer les habilitations et les groupes (dynamiques) / Mettre à la corbeille / Retirer les habilitations et les groupes (dynamiques)). Ce champ permet de configurer le comportement de GLPI lors des synchronisations avec l'annuaire LDAP si un utilisateur a été supprimé de l'annuaire.

Action à réaliser quand un utilisateur est restauré dans l'annuaire LDAP : (Activer / Ne rien faire / Restaurer (sortir de la corbeille)). Ce champ permet de configurer le comportement de GLPI lors des synchronisations avec l'annuaire LDAP si un utilisateur est restauré dans l'annuaire.

Fuseau horaire du serveur GLPI : ce champ permet de configurer le décalage horaire qui pourrait exister entre le serveur sur lequel est installé GLPI et celui sur lequel est installé l'annuaire LDAP.

Enregistrez les modifications en cliquant sur le bouton **Sauvegarder**.

La question de l'intérêt de conserver ces comptes dans la base de comptes pourrait se poser dès lors que l'authentification externe permet de s'affranchir de cette gestion locale. L'intérêt réside dans la possibilité de leur associer des éléments de l'inventaire et d'effectuer un suivi de leurs demandes d'assistance.