

1.2 Sécurité

- **Restriction IP par plage CIDR** : il est désormais possible de limiter l'accès à **Keatic ERP** à des plages d'adresses IP spécifiques (ex : 192.168.1.0/24), plutôt que seulement à des adresses IP uniques.
- Le niveau de protection CSRF passe de 2 à 3 (**MAIN_SECURITY_CSRF_WITH_TOKEN**), renforçant la vérification des tokens anti-falsification sur les formulaires.
- L'option **MAIN_DISALLOW_UNSECURED_SELECT_INTO_EXTRAFIELDS_FILTER** est activée par défaut et déplacée dans le fichier conf.php, bloquant les filtres non sécurisés sur les extrachamps et évitant des injections SQL potentielles.
- L'éditeur riche (**WYSIWYG**) est désactivé par défaut sur les pages publiques pour limiter les risques XSS sur les formulaires ouverts à l'extérieur.
- Début d'implémentation de **MAIN_RESTRICTHTML_ONLY_VALID_HTML=2** pour bloquer les balises HTML dangereuses dans les zones de contenu riche.
- Amélioration des outils de vérification d'intégrité des fichiers **Keatic ERP** (contrôle des checksums des fichiers du core).
- **L'API de connexion (/login) est désactivée par défaut** : l'API doit être utilisée avec un Bearer token (token API utilisateur). Pour réactiver les endpoints de login, ajouter **API_ENABLE_LOGIN_API=1** dans la configuration.

NOTE : Zone IA et vulnérabilités : l'intégration de l'IA dans Keatic ERP nécessite une vigilance particulière sur les données transmises aux fournisseurs d'IA tiers. L'utilisateur du serveur MCP doit impérativement avoir des droits minimaux (lecture seule).

Revision #3

Created 2026-07-08 12:28:22 UTC by InfraS

Updated 2026-07-08 13:38:56 UTC by InfraS