Sécurité et identité : protéger les comptes et les sessions

Première connexion, mots de passe, double authentification, appareils actifs et journal de sécurité réunis dans une même administration.

Une sécurité organisée autour des identités

Portix rassemble les comptes administrateurs et membres dans le module Sécurité et identité. L’administrateur y contrôle l’état des mots de passe, les comptes désactivés, les appareils connectés, les alertes et les événements importants.

Première connexion contrôlée

Un mot de passe provisoire doit être remplacé avant l’accès normal au portail. Une fois un secret personnel enregistré, Portix autorise la navigation et peut proposer un rappel facultatif au maximum une fois tous les sept jours.

Règles appliquées

- changement obligatoire d’un mot de passe initial ou provisoire ;
- mot de passe personnel conservé lors des mises à jour ;
- invalidation des sessions après une modification sensible ;
- protection du dernier compte administrateur actif ;
- récupération par courriel ou procédure locale contrôlée.

Sessions et appareils

La page de gestion des sessions indique l’utilisateur, le navigateur, le système, une adresse IP masquée et la dernière activité. Une session précise peut être révoquée sans déconnecter les autres appareils du compte.

Double authentification

Les administrateurs peuvent activer une authentification TOTP et générer des codes de récupération à usage unique. Cette protection complète le mot de passe sans le remplacer.

AccèsAdministration -> Système -> Sécurité et identité. Article vérifié pour Portix.

Une protection organisée par couches

La sécurité ne repose pas sur une seule option. Portix combine les mots de passe, les sessions, les permissions, la protection des formulaires, la limitation des tentatives et la journalisation. Chaque couche répond à un risque différent : usurpation de compte, action non autorisée, automatisation abusive, fuite de données ou modification non traçable.

Des droits adaptés aux responsabilités

Les fonctions visibles et les routes accessibles doivent correspondre au rôle réel de l’utilisateur. Un membre ne doit pas atteindre l’administration, tandis qu’un responsable métier ne doit voir que les opérations nécessaires à sa mission. Le filtrage des menus

améliore la lisibilité, mais le contrôle côté serveur reste indispensable lorsqu'une adresse est saisie manuellement.

Surveiller sans exposer les données

Les journaux et la gestion des sessions doivent fournir assez d'informations pour comprendre un incident sans afficher inutilement des données sensibles. Les adresses réseau peuvent être masquées, les événements importants datés et les sessions révoquées individuellement. Cette approche facilite le diagnostic tout en limitant la diffusion d'informations personnelles.

Une maintenance régulière

Après chaque mise à jour, il faut vérifier les comptes administrateurs, les modules actifs, les permissions, les extensions PHP et les protections des répertoires privés. Une sauvegarde récente, un test de restauration et une revue périodique des journaux complètent le dispositif. La sécurité est un processus continu, pas une opération ponctuelle.

La sécurité inclut désormais la cohérence fonctionnelle

La protection d'un portail ne repose pas seulement sur les mots de passe. Portix contrôle aussi les routes, les permissions, les formulaires POST, les exemptions CSRF, l'état des modules et les zones de stockage. Les audits récents ont permis de vérifier que les chemins dynamiques de paiement, les fonctions administratives et les espaces membres restent soumis aux contrôles attendus.

Un changement de version doit laisser un état cohérent

Lorsqu'un module est désactivé, les anciens réglages hérités ne doivent pas continuer à présenter une fonction comme active. La synchronisation des services aligne désormais ces anciens paramètres sur le registre des modules au changement de version.