4.10 Sécurité

Chemin : Administration > Configuration > Sécurité Accès : Administrateurs uniquement Cette page regroupe l'ensemble des paramètres de sécurité de ***Dolibarr***™, organisés en 8 onglets depuis la v24.

> **Important :** Chaque onglet dispose de son propre bouton de sauvegarde (MODIFIER ou ENREGISTRER). Les modifications sont effectives immédiatement pour tous les utilisateurs.

Onglet 1 – Divers

Paramètre	Constante	Défaut
Utiliser les autorisations avancées des modules	MAIN_USE_ADVANCED_PERMS	Off
Délai expiration des sessions (secondes)	MAIN_SESSION_TIMEOUT	1440 s
Nombre max. d'images dans un champ HTML	MAIN_SECURITY_MAX_IMG_IN_HTML_CONTENT	0
Nombre max. de publications par IP en un mois	MAIN_SECURITY_MAX_POST_ON_PUBLIC_PAGES_BY_IP_ADDRESS	200
Nombre max. de fichiers joints dans un formulaire	MAIN_SECURITY_MAX_ATTACHMENT_ON_FORMS	10
Nombre max. d'échecs d'authentification en 24h	MAIN_SECURITY_MAX_NUMBER_FAILED_AUTH	100

☑ ***Comment configurer le délai d'expiration des sessions ?***

Rendez-vous dans ***Administration > Configuration > Sécurité > Onglet 1 — Divers*** et renseignez le champ Délai expiration des sessions (constante **MAIN_SESSION_TIMEOUT**). La valeur par défaut est 1440 secondes (24 minutes). Si ce champ n'est pas surchargé, ***Dolibarr***™ suit la valeur session.gc_maxlifetime définie dans la configuration PHP de votre serveur. Cliquez sur MODIFIER pour appliquer immédiatement le nouveau délai à tous les utilisateurs.

☑ ***Comment configurer les autorisations avancées dans l'onglet Divers ?***

Activez l'option Utiliser les autorisations avancées des modules (constante **MAIN_USE_ADVANCED_PERMS**) dans l'onglet Divers. Cela débloque un niveau de droits supplémentaire et plus granulaire : les permissions standard se limitent à « Lire », « Créer/Modifier », « Supprimer », tandis que les permissions avancées ajoutent des droits précis comme « Valider », « Envoyer par email », « Clôturer »... Une fois activée, rendez-vous dans Accueil > Utilisateurs & Groupes pour attribuer ces nouvelles permissions fines depuis l'onglet Permissions de chaque utilisateur ou groupe.

Onglet 2 – Captcha

Protège les formulaires publics de ***Dolibarr***™ contre les robots. Les options disponibles dépendent des modules actifs.

Formulaire protégé	Constante
Page de connexion	MAIN_SECURITY_ENABLECAPTCHA
Formulaire public de contact tiers	MAIN_SECURITY_ENABLECAPTCHA_THIRDPARTY
Création de ticket public	MAIN_SECURITY_ENABLECAPTCHA_TICKET
Adhésion publique	MAIN_SECURITY_ENABLECAPTCHA_MEMBER
Formulaire de don public	MAIN_SECURITY_ENABLECAPTCHA_DONATION
Formulaire de recrutement public	MAIN_SECURITY_ENABLECAPTCHA_RECRUITMENT

Si au moins un CAPTCHA est activé, une seconde section permet de choisir le moteur de génération (handler). Le moteur disponible par défaut est Standard (image générée en interne — la bibliothèque PHP GD est requise). Constante du handler : **MAIN_SECURITY_ENABLECAPTCHA_HANDLER**.

Quelles sont les limites contre les attaques par force brute ?

Dolibarr™ propose plusieurs mécanismes complémentaires :

1. Limitation des échecs : après 100 échecs en 24h (constante MAIN_SECURITY_MAX_NUMBER_FAILED_AUTH, onglet Divers), la connexion est systématiquement refusée pour le compte concerné.
2. CAPTCHA : activez-le sur la page de connexion pour bloquer les soumissions automatisées par des scripts malveillants.
3. Complexité des mots de passe : forcez des règles dans l'onglet Mots de passe pour rendre les attaques par dictionnaire beaucoup plus longues.
4. Délégation OIDC : en utilisant OpenID Connect, vous déléguez l'authentification à un fournisseur externe (Google, Keycloak...) qui dispose de ses propres systèmes de détection de force brute.

5. Journal d'audit : l'onglet Événements de sécurité trace les échecs de connexion (USER_LOGIN_FAILED), permettant de surveiller et analyser les tentatives d'attaque.

Onglet 3 – Mots de passe

Règle de génération — un seul handler actif à la fois (interrupteur radio) :

Handler	Description	Longueur min.	Constante
Perso	Règles personnalisables	Selon config	USER_PASSWORD_GENERATED = Perso
Standard	12 caractères, algorithme interne	12	USER_PASSWORD_GENERATED = Standard
None	Aucune suggestion (saisie libre)	0	USER_PASSWORD_GENERATED = None

Configuration du handler Perso (constante **USER_PASSWORD_PATTERN**, format : longueur;majMin;numMin;speMin;consec) :

Champ	Description
Longueur minimale	Nombre minimum de caractères (min 1)
Nb min. majuscules/minuscules	Nombre de changements de casse requis
Nb min. chiffres	Nombre de chiffres requis
Nb min. caractères spéciaux	Nombre de symboles requis
Nb max. caractères consécutifs identiques	Limite les répétitions (ex. « aaa »)
Pas de caractères ambigus	Exclut les caractères difficiles à distinguer (0/O, 1/l…)

Paramètres de chiffrement :

Paramètre	Description
Chiffrer les mots de passe en base	Hash MD5/bcrypt — irréversible une fois activé
Masquer le mot de passe BDD dans conf.php	Chiffre dolibarr_main_db_pass dans le fichier de configuration
Cacher le lien « Mot de passe oublié »	Masque le lien de réinitialisation sur la page de connexion (**MAIN_SECURITY_DISABLEFORGETPASSLINK**)

Comment définir des règles de complexité pour les mots de passe ?

1. Rendez-vous dans Administration > Configuration > Sécurité > Onglet 3 — Mots de passe.
2. Activez le handler Perso pour définir vos propres critères via la constante USER_PASSWORD_PATTERN.
3. Renseignez : longueur minimale, nb min. de majuscules, de chiffres, de caractères spéciaux, nombre max. de caractères consécutifs identiques, et si vous souhaitez exclure les caractères ambigus (0/O, 1/l…).
4. Il est fortement recommandé d'activer aussi Chiffrer les mots de passe en base (hash bcrypt)

Attention, cette action est irréversible.

1. Cliquez sur le bouton de sauvegarde pour que ces nouvelles règles s'appliquent immédiatement à tous les utilisateurs.

Comment activer le chiffrement de la base de données dans conf.php ?

1. Rendez-vous dans Administration > Configuration > Sécurité > Onglet 3 — Mots de passe.
2. Localisez la ligne Masquer le mot de passe BDD dans conf.php et cliquez sur Activer.
3. ***Dolibarr***™ transforme la variable $dolibarr_main_db_pass de votre fichier htdocs/conf/conf.php en une version chiffrée. Note importante : avant d'effectuer cette opération, assurez-vous que votre fichier conf.php est temporairement accessible en écriture par le serveur web. Une fois l'activation terminée, remettez le fichier en lecture seule.

Onglet 4 – Fichiers

Paramètre	Constante	Défaut
Taille maximale des fichiers téléchargés (Ko)	MAIN_SECURITY_MAXFILESIZE_DOWNLOADED	—
Taille maximale des fichiers envoyés (Ko)	MAIN_UPLOAD_DOC	2048 Ko
Masque des nouveaux fichiers (Unix/Linux)	MAIN_UMASK	0660
Extensions interdites au téléversement	MAIN_FILE_EXTENSION_UPLOAD_RESTRICTION	htm,html,php,js,py,cgi…
Utiliser l'antivirus sur les fichiers téléversés	MAIN_ANTIVIRUS_UPLOAD_ON	Off

> **Astuce :** La taille maximale des fichiers envoyés ne peut pas dépasser la limite définie dans votre php.ini (paramètre upload_max_filesize).

Quelles sont les extensions de fichiers interdites au téléversement ?

Par défaut, les extensions suivantes sont refusées pour empêcher l'envoi de scripts malveillants :

- Web et Scripts : htm, html, js
- Programmation et Exécutables : php, py (Python), cgi
- Extensions supplémentaires (selon les versions récentes) : shtml, phar, php3, php4, php5. La liste est stockée dans la constante MAIN_FILE_EXTENSION_UPLOAD_RESTRICTION. L'administrateur peut la personnaliser en ajoutant ou supprimant des extensions, séparées par des virgules.

Comment fonctionne l'antivirus pour les fichiers téléversés ?

Lorsqu'un utilisateur ajoute un document, ***Dolibarr***™ intercepte le fichier avant son enregistrement définitif et l'envoie pour analyse au logiciel de sécurité configuré. Si le moteur antivirus détecte une menace, le téléversement est immédiatement refusé. Configuration (onglet 4 — Fichiers) :

1. Activation : basculez **MAIN_ANTIVIRUS_UPLOAD_ON** sur ON.
2. Commande antivirus : indiquez le chemin complet vers l'exécutable (ex. /usr/bin/clamscan pour ClamAV sous Linux, ClamWin sous Windows).
3. Paramètres antivirus : saisissez les arguments nécessaires (ex. --no-summary -r).
4. Test : un formulaire de test d'envoi de fichier est disponible en bas de la page pour vérifier la configuration en conditions réelles. ***Dolibarr***™ ne fournit pas son propre moteur de détection — il pilote l'appel à l'outil système lors de chaque téléversement.

Onglet 5 – Accès externes (Proxy)

Si le serveur ***Dolibarr***™ doit passer par un proxy pour accéder à Internet (mises à jour, cours des devises, météo…), configurez ici les paramètres de connexion.

Paramètre	Constante	Défaut
Timeout de connexion (secondes)	MAIN_USE_CONNECT_TIMEOUT	10
Délai expiration de réponse (secondes)	MAIN_USE_RESPONSE_TIMEOUT	30
Utiliser un serveur proxy	MAIN_PROXY_USE	Non
Nom/Adresse du proxy	MAIN_PROXY_HOST	–
Port du proxy	MAIN_PROXY_PORT	0
Identifiant proxy	MAIN_PROXY_USER	–
Mot de passe proxy	MAIN_PROXY_PASS	–

Onglet 6 – Événements de sécurité

Active l'enregistrement d'un journal d'audit pour les événements de sécurité sensibles. Chaque événement s'active individuellement.

> **Avertissement :** Cette fonctionnalité peut générer un volume important de données en base selon le nombre d'événements activés et l'activité de votre instance.

Événement	Description	Constante
USER_LOGIN	Connexion réussie	MAIN_LOGEVENTS_USER_LOGIN
USER_LOGIN_FAILED	Échec de connexion	MAIN_LOGEVENTS_USER_LOGIN_FAILED
USER_LOGOUT	Déconnexion	MAIN_LOGEVENTS_USER_LOGOUT
USER_CREATE	Création d'un utilisateur	MAIN_LOGEVENTS_USER_CREATE
USER_MODIFY	Modification d'un utilisateur	MAIN_LOGEVENTS_USER_MODIFY
USER_NEW_PASSWORD	Nouveau mot de passe généré	MAIN_LOGEVENTS_USER_NEW_PASSWORD
USER_ENABLEDISABLE	Activation/désactivation d'un compte	MAIN_LOGEVENTS_USER_ENABLEDISABLE
USER_DELETE	Suppression d'un utilisateur	MAIN_LOGEVENTS_USER_DELETE
USERGROUP_CREATE	Création d'un groupe	MAIN_LOGEVENTS_USERGROUP_CREATE
USERGROUP_MODIFY	Modification d'un groupe	MAIN_LOGEVENTS_USERGROUP_MODIFY
USERGROUP_DELETE	Suppression d'un groupe	MAIN_LOGEVENTS_USERGROUP_DELETE

Où consulter le journal d'audit des événements de sécurité ?

Le journal d'audit est consultable dans Accueil > Outils d'administration > Événements de sécurité. L'activation de l'enregistrement se fait dans Administration > Configuration > Sécurité > Onglet 6 — Événements de sécurité (/admin/events.php). Dans les versions récentes (v23 et v24), le journal consigne également l'installation (ou la tentative d'installation) d'un module. Note : si vous utilisez le module Archives/Logs Inaltérables (conformité Loi Finance), les événements liés aux factures et paiements sont gérés dans un journal spécifique et distinct, accessible via le menu dédié à ce module.

Onglet 7 – Paramètres d'authentification OpenID Connect

Permet à ***Dolibarr***™ de déléguer l'authentification à un fournisseur d'identité OpenID Connect pour mettre en place du SSO (Single Sign-On). Lorsque l'option est activée (toggle ON/OFF), des champs de configuration supplémentaires apparaissent pour saisir les paramètres du fournisseur (URL, client ID, secret, etc.). Exemples de fournisseurs compatibles : Keycloak, Google, Microsoft Entra ID.

> Note : L'intégration native OpenID Connect est une nouveauté v24, remplaçant les anciens modules externes. Elle permet une authentification déléguée sans installation de module tiers.

Onglet 8 – En-têtes de sécurité HTTP

Réservé aux utilisateurs avancés. Un en-tête mal configuré peut rendre ***Dolibarr***™ inaccessible ou bloquer des ressources légitimes.

En-tête HTTP	Description	Constante
Referer-Policy	Contrôle les informations de référencement transmises lors des navigations	MAIN_SECURITY_FORCERP
Strict-Transport-Security (HSTS)	Force l'utilisation de HTTPS	MAIN_SECURITY_FORCESTS
Permissions-Policy	Contrôle l'accès aux API navigateur (caméra, micro…)	MAIN_SECURITY_FORCEPP
Content-Security-Policy (CSP)	Déclare les sources autorisées pour scripts, styles, images…	MAIN_SECURITY_FORCECSP

> **Astuce :** Le bouton + sur le champ CSP ouvre un assistant visuel pour ajouter des directives et sources sans saisie manuelle. ***Dolibarr***™ injecte automatiquement script-src 'self' 'unsafe-inline' et style-src 'self' 'unsafe-inline' pour ne pas bloquer son propre fonctionnement.

Permissions par défaut

Sous l'onglet Permissions par défaut, vous définissez les droits automatiquement attribués à chaque nouvel utilisateur créé. Cliquez sur + pour accorder une permission par défaut, et sur − pour la retirer.

> **Avertissement :** Ces réglages ne s'appliquent qu'aux nouveaux utilisateurs. Pour modifier les permissions d'un utilisateur ou groupe existant, allez sur sa fiche dans Accueil > Utilisateurs & Groupes.

Comment gérer les permissions par défaut des nouveaux utilisateurs ?

Rendez-vous dans Accueil > Configuration > Sécurité > Permissions par défaut. L'interface présente tous les modules activés avec leurs actions possibles.

- Cliquez sur + pour qu'une permission soit donnée par défaut à tous les futurs utilisateurs.
- Cliquez sur - pour supprimer cette permission de la configuration par défaut. Points importants : - Ces réglages n'ont aucun effet sur les utilisateurs déjà existants. - Configurez cette section après avoir activé tous les modules souhaités — la liste des droits disponibles dépend des modules actifs. - Si vous avez activé les autorisations avancées (onglet Divers), des permissions plus fines (valider, envoyer par mail…) apparaissent également dans cette liste.

Revision #7
Created 2026-07-06 10:54:36 UTC by InfraS
Updated 2026-09-28 07:13:02 UTC by Fallinah