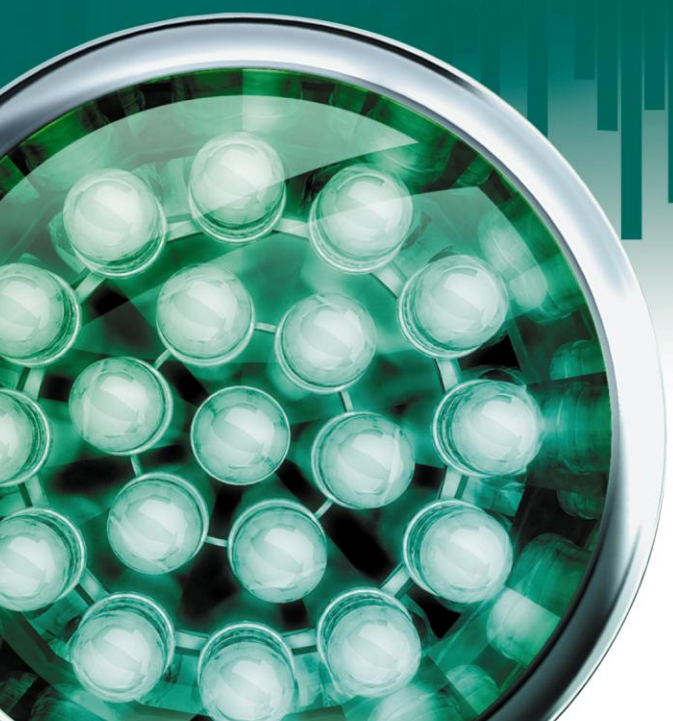
Kaspersky Password Manager

MANUEL DE L'UTILISATEUR



KASPERSKY lab

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que cette documentation vous sera utile et qu'elle répondra aux questions que vous pourriez avoir sur le logiciel.

Date d'édition : 11/11/09

http://www.kaspersky.com/fr
http://www.kaspersky.com/fr/support

TABLE DES MATIERES

KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager enregistre et protège toutes vos données personnelles (par exemple mots de passe, noms d'utilisateur, identifiants de messageries instantanées, données de contact, numéros de téléphone, etc.). Kaspersky Password Manager établit un lien entre vos mots de passe / Comptes et les applications Microsoft Windows ou pages Web dans lesquelles ils sont utilisés. Toutes les informations stockées sont cryptées dans une base de mots de données dont l'accès est protégé au moyen d'un Mot de passe principal. Une fois la base de mots de passe déverrouillée, vos données personnelles sont facilement accessibles. Après avoir lancé la page Web ou l'application, Kaspersky Password Manager renseigne à votre place le mot de passe, l'Identifiant et les autres données personnelles dans les champs correspondants. De cette manière, il vous suffit de retenir un seul mot de passe.

Par défaut, Kaspersky Password Manager est lancé automatiquement au démarrage du système d'exploitation. Le composant s'intègre dans les applications qui permettent de gérer des données personnelles directement depuis la fenêtre de l'application.

Kaspersky Password Manager surveille l'activité des applications ayant trait aux mots de passe et offre une protection contre l'interception et le vol de données personnelles. Le composant analyse les programmes qui utilisent des mots de passe ou interrogent le mot de passe d'autres programmes et vous propose ensuite de décider d'autoriser ou d'interdire l'action suspecte.

En outre, Kaspersky Password Manager permet de :

- enregistrer et utiliser vos mots de passe (cf. page 13) ;
- rechercher des comptes utilisateur, des mots de passe, des noms d'utilisateur et d'autres informations personnelles dans la base de mots de passe (cf. page 14) ;
- générer des mots de passe complexes (cf. p. 40) lors de la création de comptes utilisateur ;
- enregistrer tous les mots de passe sur un support amovible (cf. p. 41) ;
- restaurer la base de mots de passe depuis la copie de sauvegarde (cf. p. 25) ;
- protéger les mots de passe contre l'accès non autorisé (cf. p. 12).

Pour lancer Kaspersky Password Manager, procédez comme suit :

1. Cliquez avec le bouton gauche de la souris sur l'icône de Kaspersky Password Manager dans la zone de notification de la barre des tâches.
2. Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel qui s'ouvre.

INSTALLATION DE KASPERSKY PASSWORD MANAGER SUR L'ORDINATEUR

Kaspersky Password Manager s'installe sur l'ordinateur en mode interactif à l'aide de l'Assistant d'installation, qui se lance à l'ouverture du fichier d'installation.

Avant l'installation de Kaspersky Password Manager il est recommandé de fermer toutes les applications.

Pour installer Kaspersky Password Manager sur votre ordinateur, lancer le fichier de distribution (fichier avec extension *.exe), téléchargé via Internet. Ensuite, l'Assistant d'installation de Kaspersky Password Manager est lancé.

L'Assistant d'installation se compose de la suite des fenêtres (étapes). Afin d'administrer le processus d'installation, chaque fenêtre contient un ensemble de boutons. Pour naviguer parmi les écrans, utilisez les boutons **Suivant** et **Précédent**. Pour interrompre l'assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**. À la fin de l'assistant, cliquez sur le bouton **Installer**. Examinons en détail chacune des étapes de la procédure d'installation.

DANS CETTE SECTION

ÉTAPE 1. LECTURE DU CONTRAT DE LICENCE

Avant l'installation de l'application il vous sera proposé de prendre connaissance du contrat de licence qui est conclu entre Kaspersky Lab et vous. Le contrat de licence contient la liste des droits d'utilisateur sur l'utilisation du logiciel acheté. Sans l'acceptation du contrat de licence l'installation ne sera pas possible.

Lisez-le attentivement et si vous n'avez aucune objection à formuler, sélectionnez l'option **J'accepte les termes du contrat de licence**. L'installation de l'application sur votre ordinateur se poursuivra.

Pour ne pas appliquer l'installation de l'application, cliquez sur le bouton **Annuler**.

ÉTAPE 2. SELECTION DU REPERTOIRE D'INSTALLATION

Cette étape vous permet de sélectionner le dossier de destination, dans lequel Kaspersky Password Manager sera installé. Par défaut, le chemin d'installation est suivant : **<disque> \ Program Files \ Kaspersky Password Manager**.

Pour modifier le dossier de destination cliquez sur le bouton **Parcourir** et dans la fenêtre ouverte indiquez le dossier nécessaire sur votre ordinateur. Vous pouvez aussi indiquer le nouveau chemin d'installation, en le saisissant dans le champ correspondant. Pour prendre une décision sur le dossier de destination, en bas de la fenêtre vous pouvez indiquer la place libre sur le disque pour installer l'application.

N'oubliez pas que si vous saisissez manuellement le chemin d'accès complet au dossier d'installation, le nom ne pourra pas compter plus de 200 caractères ni contenir des caractères spéciaux.

Cliquez sur le bouton **Suivant**, afin de poursuivre l'installation.

ÉTAPE 3. EMPLACEMENT DE L'APPLICATION DANS LE MENU DEMARRER DANS LA BARRE DES TACHES MICROSOFT WINDOWS

Cette étape vous permet d'indiquer le chemin pour lancer l'application depuis le menu **Démarrer** dans la barre des tâches Microsoft Windows. Par défaut, dans le menu **Démarrer** dans la barre des tâches Microsoft Windows l'application sera accessible selon le chemin suivant : menu **Démarrer** → **Toutes les applications** → **Kaspersky Password Manager**.

Pour modifier le chemin d'accès à l'application cliquez sur le bouton **Parcourir** et dans la fenêtre ouverte sélectionnez un autre dossier dans le menu **Démarrer**.

Cliquez sur **Suivant**. L'installation se poursuit.

ÉTAPE 4. CREATION DU RACCOURCI KASPERSKY PASSWORD MANAGER SUR LE BUREAU

Pour lancer rapidement Kaspersky Password Manager, cette étape vous propose de créer un raccourci de l'application sur le bureau. Pour ce faire, cochez la case ☑ **Créer un raccourci sur le bureau**.

Cliquez sur le bouton **Suivant**, afin de poursuivre l'installation.

ÉTAPE 5. ANALYSE FINALE AVANT L'INSTALLATION DE KASPERSKY PASSWORD MANAGER

Avant l'installation il vous sera proposé de consulter et de modifier, si nécessaire, les paramètres d'installation sélectionnés.

Pour modifier les paramètres sélectionnés, retournez aux étapes précédentes à l'aide du bouton **Précédent**.

Si tous les paramètres sont justes, cliquez sur le bouton **Installer**.

ÉTAPE 6. FIN D'INSTALLATION DE KASPERSKY PASSWORD MANAGER

La dernière fenêtre de l'Assistant vous signale la fin de l'installation du programme. Pour commencer le fonctionnement de Kaspersky Password Manager, assurez-vous que la case ☑ **Lancer Kaspersky Password Manager** est cochée et cliquez sur le bouton **Terminer**.

L'Assistant de configuration Kaspersky Password Manager se lancera automatiquement.

ACTIVATION DE L'APPLICATION

La procédure d'activation de l'application consiste en la saisie du code d'activation dans le produit. A la base de la clé de licence le droit d'utilisation de la version actuelle de l'application est défini en fonction de ce code.

A chaque version de l'application correspond sa propre clé de licence, qui se compose d'une suite unique des caractères. Vous recevez le code d'activation via le courrier électronique à l'achat de Kaspersky Password Manager.

Le code d'activation est utilisé par la version actuelle de l'application, ainsi que pour toutes ses mises à jour.

Avant l'installation de mises à jour de la version actuelle de l'application assurez-vous que la clé de licence a été sauvegardée.

Kaspersky Password Manager fonctionne dans sa version complète pendant 30 jours à partir de son installation. Une fois la période d'évaluation terminée, certaines fonctions de l'application sont inaccessibles. Vous pouvez activer la licence pendant la configuration initiale de Kaspersky Password Manager dans la fenêtre de l'Assistant de configuration des paramètres (cf. page 12), ainsi qu'à n'importe quel moment pendant les 30 jours de fonctionnement de la version d'évaluation. Si vous n'avez pas acheté la licence de l'application avant l'activation, vous pouvez passer à l'achat de la licence pendant l'activation de l'application.

Vous pouvez acheter une licence Kaspersky Password Manager par l'un des moyens suivants :

- sur la boutique en ligne de Kaspersky Lab ;
- dans le menu contextuel de Kaspersky Password Manager : pour ce faire, dans le menu contextuel de l'application, sélectionnez l'option **Activation** ;
- dans la fenêtre d'informations sur l'application : pour ce faire, dans le menu contextuel de l'application sélectionnez l'option **Aide** → **A propos du logiciel** ;
- lors du déblocage de la base de mots de passe par le mot de passe principal : pour ce faire, dans la fenêtre de déblocage cliquez sur le lien **Acheter une licence en ligne** ;
- le bouton de lancement rapide : pour ce faire, dans le menu du bouton de lancement rapide sélectionnez le point **Activation**.

Vous pouvez activer l'application avec l'un des moyens suivants :

- Par le menu contextuel de l'application. Pour ce faire, choisissez l'option **Aide** → **Activer à l'aide du code d'activation** dans le menu contextuel de l'application.
- Dans la fenêtre d'informations sur l'application. Pour ce faire, choisissez l'option **Aide** → **A propos de Kaspersky Password Manager** dans le menu contextuel de l'application.
- Lors du déblocage de la base de mots de passe par le mot de passe principal. Pour ce faire, dans la fenêtre de déblocage cliquez sur le lien **Activez votre licence**.

Pour activer l'application, procédez comme suit :

1. Dans le menu contextuel de Kaspersky Password Manager, consultez l'option **Aide** → **Activer à l'aide du code d'activation**.
2. Dans la fenêtre ouverte passez, si nécessaire, à l'achat d'une licence. Pour ce faire, cliquez sur le lien **Acheter une licence en ligne**. Après avoir obtenu la licence, saisissez le code d''activation et confirmez-la.

INTERFACE DE KASPERSKY PASSWORD MANAGER

L'interface de Kaspersky Password Manager est simple et conviviale. Ce chapitre est consacré aux principes de base de fonctionnement de l'application.

Kaspersky Password Manager dispose d'extensions (modules externes) s'intégrant dans les programmes exigeant une authentification. Vous pouvez installer indépendamment ces modules externes pour chaque Navigateur Internet que vous utilisez. Les modules externes installés garantissent l'accès aux fonctions de Kaspersky Password Manager depuis l'interface de l'application / du navigateur Internet.

Le pointeur de Kaspersky Password Manager vous permet de sélectionner rapidement un programme / une page Web où des données personnelles doivent être remplies automatiquement.

DANS CETTE SECTION

ICONE DANS LA ZONE DE NOTIFICATION DE LA BARRE DES TACHES

L'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows directement après son lancement.

En fonction de la situation, l'icône de Kaspersky Password Manager prend différents aspects :

-  actif (vert) – Kaspersky Password Manager est déverrouillé, l'accès aux données personnelles est autorisé ;
-  inactif (rouge) – Kaspersky Password Manager est verrouillé, les données sont inaccessibles ;

En outre, lorsque vous cliquez sur l'icône, vous pouvez accéder aux éléments suivants de l'interface :

- menu contextuel (cf. p. 10) ;
- fenêtre principale de l'application (cf. p. 10) ;
- pointeur de Kaspersky Password Manager (cf. p. 41).

Pour faire apparaître le menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de Kaspersky Password Manager.

Par défaut en double-cliquant vous pouvez verrouiller / déverrouiller l'application.

Pour utiliser le pointeur de Kaspersky Password Manager, déplacez le curseur de la souris sur l'icône actif de l'application et patientez quelques secondes. Le pointeur de Kaspersky Password Manager sera disponible sous l'icône de l'application.

MENU CONTEXTUEL DE KASPERSKY PASSWORD MANAGER

Les fonctions principales de Kaspersky Password Manager sont accessibles depuis le menu contextuel de l'application. Le menu de Kaspersky Password Manager contient les éléments suivants :

- **Verrouillage / Déverrouillage** – interdit / autorise l'accès à vos données personnelles.
- Liste des Comptes favoris - permet d'accéder rapidement à un des Comptes favoris. Cette liste est établie automatiquement en fonction de la fréquence d'utilisation des Comptes. La liste est présente si son affichage dans le menu contextuel a été configuré (cf. p. 28). Lors du premier démarrage de l'application, la liste est vide car aucun compte n'a pu être utilisé.
- **Comptes** – affiche la liste des tous les comptes afin de pouvoir y accéder rapidement. Le nombre de Comptes présents dans la base de mots de passe est affiché entre parenthèses.
- **Ajouter un Compte** – raccourci vers l'ajout d'un nouveau Compte dans Kaspersky Password Manager.
- **Gestionnaire de mots de passe** – passage à la fenêtre principale de l'application (cf. p. 10).
- **Configuration** – raccourci vers la configuration des paramètres de l'application.
- **Version portable** – lance l'assistant de création d'une version portable de Kaspersky Password Manager.
- **Générateur de mots de passe** – raccourci vers l'outil de génération de mots de passe.
- **Aide** – démarre l'aide en ligne de l'application.
- **Terminer** - arrêt du fonctionnement de l'application (si vous choisissez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).

Si le programme est verrouillé, vous ne pourrez pas accéder à vos données personnelles. Dans ce cas, seuls les entrées suivantes apparaîtront dans le menu contextuel: **Verrouillage / Déverrouillage**, **Générateur de mots de passe** et **Terminer**.

FENETRE DE KASPERSKY PASSWORD MANAGER

Il est possible d'ouvrir la fenêtre principale de l'application depuis le menu contextuel de Kaspersky Password Manager (cf. p. 10). Pour ce faire, sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.

Vous pouvez également configurer l'ouverture de la fenêtre principale de Kaspersky Password Manager d'un double-clic sur l'icône de Kaspersky Password Manager dans la zone de notification de la barre des tâches.

La fenêtre **Gestionnaire de mots de passe** peut être divisée en deux parties:

- la partie supérieure de la fenêtre permet de sélectionner rapidement les fonctions de Kaspersky Password Manager et d'effectuer les tâches de base ;
- la partie inférieure de la fenêtre contient la liste de tous les comptes ainsi que les autres données personnelles. Elle permet également de gérer les informations personnelles.

Vous pouvez également utiliser la zone de recherche pour retrouver des données personnelles dans la base de mots de passe. La zone de recherche se situe dans la partie inférieure de la fenêtre principale de l'application.

FENETRE DE CONFIGURATION DES PARAMETRES

Vous pouvez ouvrir la fenêtre de configuration des paramètres de Kaspersky Password Manager depuis le menu contextuel de Kaspersky Password Manager (cf. p. 10). Pour ce faire, sélectionnez l'entrée **Configuration** dans le menu de Kaspersky Password Manager.

La fenêtre de configuration contient deux parties:

- la partie gauche de la fenêtre contient la liste des fonctions de l'application ;
- la partie droite de la fenêtre reprend les paramètres propres à la fonction, à la tâche ... sélectionnée.

BOUTON D'ACCES RAPIDE

Le Bouton d'accès rapide permet d'utiliser vos données personnelles depuis la fenêtre de l'application / de la page Web. Ce bouton se situe dans le coin supérieur droit de l'application.

Le Bouton d'accès rapide n'est actif  que lorsque la base de mots de passe est déverrouillée. Il vous permet d'accéder aux fonctions suivantes :

- **Ajouter un compte** – raccourci vers l'ajout d'un nouveau Compte.
- **Modifier un compte** – raccourci vers l'ajout d'un Identifiant / la modification d'un Compte activé. L'entrée n'est présente dans le menu que si le Compte est actif.
- **Compte Internet** – affiche la liste de tous les comptes Internet et permet de lancer l'un d'entre eux. Le nombre de Comptes présents dans la base de mots de passe est affiché entre parenthèses.
- **Liste des Comptes favoris** – lancement d'un Compte depuis la liste. Cette liste est établie automatiquement en fonction de la fréquence d'utilisation des Comptes. La liste figure dans le menu si son affichage a été configuré (cf. p. 28).
- **Identité** – affiche la liste des identités déjà créées et permet d'appliquer l'une d'entre elles à un formulaire d'enregistrement.
- **Aide** – raccourci vers l'aide de l'application.

Le Bouton d'accès rapide n'est actif  que lorsque la base de mots de passe est déverrouillée. Dans ce cas, il n'est pas possible d'accéder aux fonctions mentionnées ci-dessus en cliquant sur le bouton. Lorsqu'il est inactif, le bouton apparaît dans la fenêtre de l'application si les paramètres du Bouton d'accès rapide le spécifient (cf. p. 39).

PREMIERE UTILISATION

Kaspersky Password Manager garantit la protection de vos données personnelles et permet de les gérer facilement.

La configuration optimale des paramètres lors de la première utilisation constitue l'une des particularités de l'application. Afin de rendre l'utilisation plus conviviale, les étapes de configuration initiale ont été regroupées au sein d'un Assistant de Configuration de l'application (cf. p. 12) qui démarre lors du premier lancement de l'application. Grâce aux instructions de l'Assistant, vous pouvez créer le Mot de passe principal, définir les paramètres d'accès à l'application et configurer les paramètres de protection de vos données.

Pour prévenir tout accès à vos données personnelles par des inconnus lorsque vous n'êtes pas devant votre ordinateur, Kaspersky Password Manager prévoit un verrouillage automatique de la base de mots de passe. Pour utiliser vos données personnelles, déverrouillez Kaspersky Password Manager (cf. p. 12).

Kaspersky Password Manager ne facilite pas seulement l'utilisation (cf. p. 13) de vos données personnelles mais également leur organisation. Pour trouver n'importe quelle information conservée, lancez la recherche de mots de passe (cf. p. 14).

DANS CETTE SECTION

ASSISTANT DE CONFIGURATION DES PARAMETRES

L'Assistant de Configuration des paramètres de l'application est lancé au premier démarrage de Kaspersky Password Manager. Son rôle est de vous aider à réaliser la configuration initiale des paramètres de Kaspersky Password Manager en fonction de vos préférences personnelles et des tâches que vous devrez effectuer.

L'assistant se présente sous la forme d'une succession d'écrans (étapes): Pour naviguer parmi les écrans, utilisez les boutons **Suivant** et **Précédent**. Pour interrompre l'assistant à n'importe quelle étape, cliquez sur le bouton **Fermer**. À la fin de l'assistant, cliquez sur le bouton **Terminer**. Nous détaillerons plus loin chaque étape de l'assistant.

ACCES A LA BASE DE MOTS DE PASSE

Toutes vos données personnelles sont stockées de manière cryptée dans la base de mots de passe. Pour les utiliser, la base de mots de passe doit être déverrouillée. Pour accéder à la base de mots de passe, vous pouvez choisir parmi les méthodes d'authentification suivantes :

- **Protection par Mot de passe principal**. L'accès à la base de mots de passe s'effectue via le Mot de passe principal.
- **Périphérique USB**. L'accès à la base de mots de passe s'effectue via un périphérique à interface USB connecté à l'ordinateur. Lorsque le périphérique USB est déconnecté, la base de mots de passe est automatiquement verrouillée.
- **Périphérique Bluetooth**. L'accès à la base de mots de passe s'effectue via un périphérique Bluetooth connecté à l'ordinateur. Lorsque le périphérique Bluetooth est déconnecté, la base de mots de passe est automatiquement verrouillée.

- **Sans authentification**. L'accès à la base de mots de passe n'est pas protégé.

La protection activée par défaut est celle par Mot de passe principal qui vous permet de ne retenir qu'un seul mot de passe pour accéder à tous les autres.

Mot de passe principal – il s'agit de la méthode de base pour protéger vos données personnelles. Si vous avez opté pour la méthode d'authentification par périphérique et que par la suite vous n'avez pas ce périphérique sous la main (ou par exemple qu'il a été perdu), vous pouvez utiliser le Mot de passe principal pour accéder à vos données personnelles.

Par défaut, Kaspersky Password Manager verrouille la base de mots de passe au lancement de l'application ainsi qu'après une durée déterminée (cf. p. 34) d'inactivité de l'ordinateur. L'utilisation de l'application n'est possible que lorsque la base de mots de passe est déverrouillée.

Vous pouvez également déverrouiller / verrouiller la base de mots de passe par les moyens suivants :

- périphérique USB ou Bluetooth – uniquement possible lorsque le mode d'authentification par périphérique USB ou Bluetooth est activé ;
- pour ce faire, la fonction d'activation par double-clic doit être activée (cf. p. 37) ;
- menu contextuel de Kaspersky Password Manager ;
- combinaison de touches CRTL+ALT+L (cf. p. 30).

Pour saisir le Mot de passe principal, vous pouvez utiliser le Clavier virtuel. Celui-ci vous permet d'introduire des mots de passe sans risque d'interception des frappes sur le clavier.

Pour verrouiller l'application depuis le menu contextuel, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône de Kaspersky Password Manager dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez l'entrée **Verrouiller**.

Pour déverrouiller l'application depuis le menu contextuel, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône de Kaspersky Password Manager dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez l'entrée **Déverrouiller**.
3. Introduisez le Mot de passe principal dans la boîte de dialogue.

UTILISATION DES DONNEES PERSONNELLES

Kaspersky Password Manager établit un lien entre vos comptes et les applications ou pages Web dans lesquelles ils sont utilisés. Lors du lancement d'une application / d'une page Web, Kaspersky Password Manager recherche automatiquement un Compte associé dans la base de mots de passe. En cas de recherche fructueuse, les données personnelles sont complétées automatiquement. Si aucun compte utilisateur n'est trouvé dans la base de mots de passe, Kaspersky Password Manager vous propose de l'ajouter (cf. p. 17)

Certaines applications / pages Web peuvent utiliser plusieurs noms d'utilisateur. Kaspersky Password Manager vous permet de conserver plusieurs noms d'utilisateur pour un seul Compte. En cas d'introduction d'un nouveau nom d'utilisateur lors de l'authentification, Kaspersky Password Manager vous propose de l'ajouter au compte utilisateur (cf. p. 21) pour l'application / la page Web en cours d'utilisation. Par la suite, lors du lancement de l'application / de la page Web, une fenêtre reprenant la liste des noms d'utilisateur correspondant au Compte s'affiche en regard des champs de saisie des données personnelles.

Outre l'Identifiant et le mot de passe permettant l'identification, les sites Web utilisent souvent d'autres données personnelles (par exemple le nom complet, le sexe, le pays, la ville, l'adresse de courrier électronique, etc.). Kaspersky

Password Manager conserve toutes ces données dans une base de mots de passe cryptée sous la forme d'identités. Afin de séparer les informations professionnelles et privées, il est possible de créer plusieurs identités (cf. p. 22) De cette manière, lorsque vous vous enregistrez dans l'application / sur un site Web, Kaspersky Password Manager complète automatiquement les champs du formulaire d'enregistrement en se basant sur l'Identité sélectionnée. L'utilisation d'identités vous fait gagner du temps lors du remplissage de formulaires identiques.

Lorsque vous vous authentifiez dans une application / sur une page Web, Kaspersky Password Manager ne complétera automatiquement les données personnelles que si la base de mots de passe est déverrouillée.

Vous pouvez utiliser le Compte d'une des manières suivantes :

- Lancer l'application / la page Web. Le formulaire d'authentification sera automatiquement complété sur la base des données du Compte.
- Utiliser le pointeur de Kaspersky Password Manager. Pour ce faire, déplacez le curseur sur l'icône de l'application situé dans la zone de notification de la barre des tâches et activez le Compte en "glissant-déposant" le pointeur de Kaspersky Password Manager dans la fenêtre de l'application / sur la page Web concernée.
- Choisir le compte utilisateur dans la liste des comptes les plus fréquemment utilisés. Pour ce faire, accédez au menu contextuel de Kaspersky Password Manager et choisissez le compte approprié dans le groupe des comptes les plus fréquemment utilisés.
- Utiliser le menu contextuel de Kaspersky Password Manager. Pour ce faire, accédez au menu contextuel de Kaspersky Password Manager et choisissez l'entrée **Comptes** → **<Intitulé du Compte>**.

Pour utiliser une Identité, procédez comme suit :

1. Dans le coin supérieur droit de l'écran de l'application / du navigateur Internet, cliquez sur le Bouton d'accès rapide.
2. Dans la fenêtre qui s'ouvre, choisissez l'option **Identités** → **<Nom de l'identité>**. Kaspersky Password Manager complète automatiquement les champs du formulaire d'enregistrement en se basant sur les données de l'Identité.

RECHERCHE DE MOTS DE PASSE

La recherche de données personnelles peut être difficile dans les cas suivants :

- certains mots de passe ne sont pas liés à des programmes / pages Web ;
- la base de mots de passe contient un nombre important de comptes.

Kaspersky Password Manager permet de retrouver rapidement des mots de passe sur la base des paramètres suivants :

- intitulé du Compte ;
- nom de l'utilisateur ;
- les paramètres de recherche sur mots-clés (cf. p. 18) sont accessoires et propres à chaque nom d'utilisateur) ;
- URL (pour les pages Web).

La recherche s'opère sur l'ensemble du nom ou sur la base des premières lettres et de n'importe quel caractère dans le nom du compte utilisateur ou du lien.

Pour trouver un compte / mot de passe, procédez comme suit :

1. Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.

2. Introduisez le texte à rechercher dans le champ correspondant de la boîte de dialogue **Gestionnaire de mots de passe**.

   Pour visualiser les données du Compte dont le mot de passe, appuyez sur la touche **Entrée**.

GESTION DE LA BASE DE MOTS DE PASSE

La base de mots de passe conserve tous les comptes des programmes et pages Web ainsi qu'un ou plusieurs noms d'utilisateurs et même vos identités (contenant p.ex. des données de contact, numéros de téléphone, identifiants de messageries, etc.).

La base de mots de passe ne peut être utilisée que lorsqu'elle est déverrouillée (cf. p. 12). Avant toute modification de la base de mots de passe, il est recommandé de configurer les paramètres de copie de sauvegarde de la base (cf. p. 32). Si vos données ont été malencontreusement modifiées ou supprimées, utilisez la fonction de restauration de la base de mots de passe (cf. p. 25).

Vous pouvez exécuter les opérations suivantes :

- ajouter (cf. p. 16), modifier (cf. p. 22), supprimer (cf. p. 23) des données personnelles ;
- importer/exporter (cf. p. 23), restaurer (cf. p. 25) la base de mots de passe.

DANS CETTE SECTION

AJOUT DE DONNEES PERSONNELLES

L'ajout de données personnelles est possible si la base de mots de passe n'est pas verrouillée (cf. p. 12). Lors du lancement d'une application / d'une page Web, un nouveau compte est automatiquement identifié lorsqu'il ne se trouve pas dans la base de mots de passe. Après vous être authentifié dans l'application / sur la page Web, Kaspersky Password Manager vous propose d'ajouter automatiquement vos données personnelles dans la base de mots de passe.

Les données personnelles suivantes peuvent être ajoutées dans la base de mots de passe :

- **Compte utilisateur** (cf. p. 17).
- **Nom d'utilisateur** (cf. p. 21). Par défaut, Kaspersky Password Manager vous propose de créer un Compte avec un seul Identifiant. Les noms d'utilisateurs multiples s'utilisent lorsque les programmes ou pages Web permettent de créer plusieurs noms d'utilisateur pour accéder à leurs ressources.
- **Identités** (cf. p. 22). Les Identités permettent de conserver des données telles que le sexe, la date de naissance, les données de contact, le numéro de téléphone, le lieu de travail, l'identifiant de messagerie instantanée, l'URL de votre page d'accueil, etc. Afin de séparer les informations professionnelles et privées, vous pouvez créer plusieurs identités.
- **Groupe de comptes** (cf. p. 22). S'utilise pour organiser de manière plus commode les comptes dans la base de mots passe.

COMPTE

Kaspersky Password Manager identifie automatiquement un nouveau Compte lorsqu'il ne le trouve pas dans la base de mots de passe. Après vous être authentifié dans l'application / sur la page Web, Kaspersky Password Manager vous propose d'ajouter les données dans la base de mots de passe. Vous pouvez également ajouter manuellement un Compte dans la base de mots de passe.

Un Compte se compose des données suivantes :

- nom / plusieurs noms d'utilisateur ;
- mot de passe ;
- emplacement de l'application / URL de la page Web ;
- paramètres définissant le lien entre le Compte et l'objet ;
- paramètres d'activation du compte ;
- commentaires ;
- paramètres de remplissage de champs supplémentaires pour la pages Web.

Kaspersky Password Manager permet d'utiliser un ou plusieurs Comptes pour un programme / un site Web. Kaspersky Password Manager permet de spécifier la zone d'utilisation de chaque compte utilisateur sur la base du chemin d'accès à l'application/de l'URL de la page Web.

Il existe plusieurs manières d'ajouter un Compte :

- via le Bouton d'accès rapide – pour ce faire, sélectionnez l'entrée **Ajouter un Compte** dans le menu du Bouton d'accès rapide ;
- depuis le menu contextuel de Kaspersky Password Manager – pour ce faire, sélectionnez l'entrée **Ajouter un Compte** dans le menu contextuel de Kaspersky Password Manager ;
- depuis la fenêtre principale de Kaspersky Password Manager.

Pour ajouter un nouveau Compte, procédez comme suit :

1. Dans le menu contextuel de l'application, sélectionnez l'option **Gestionnaire de mots de passe**.
2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, cliquez sur le bouton **Ajouter un Compte**.
3. Dans le champ **Nom** de la boîte de dialogue, introduisez l'intitulé du nouveau Compte (par exemple, nom de l'application / de la page Web).
4. Sous l'onglet **Identifiant**, introduisez l'Identifiant et le mot de passe.

   L'Identifiant peut se composer d'un ou plusieurs caractères. Pour spécifier les mots-clés (cf. p. 18) associés au nom d'utilisateur, cliquez sur le bouton  .

   Pour copier l'Identifiant / mot de passe dans le Presse-papiers, utilisez le bouton  .

   Pour créer automatiquement un mot de passe, cliquez sur le lien **Nouveau mot de passe** (cf. p. 40).
5. Sous l'onglet **Liens**, spécifiez l'emplacement de l'application / de la page Web ainsi que les paramètres d'utilisation du compte.
6. Sous l'onglet **Modification avancée**, configurez si nécessaire les paramètres de remplissage des champs complémentaires de la page Web.

7. Sous l'onglet **Commentaires**, introduisez si nécessaire un texte complémentaire décrivant le compte. Pour afficher les commentaires dans les notifications après activation du compte, cochez la case **Afficher les commentaires dans les notifications**.

DEFINITION DE MOTS-CLES POUR LA RECHERCHE

Pour rechercher rapidement des données personnelles dans la base de mots de passe, vous pouvez utiliser des mots-clés. Vous pouvez en spécifier pour chaque Identifiant. Il est conseillé de définir des mots clés lors de l'ajout d'un compte utilisateur (cf. p. 17) / nom d'utilisateur (cf. p. 21).

Pour associer des mots-clés à un Identifiant, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.

2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, sélectionnez l'Identifiant dans la liste **Base de données** et cliquez ensuite sur **Modifier** pour accéder à sa fenêtre de modification.

3. Dans la boîte de dialogue, cliquez sur le bouton en regard du champ **Identifiant** et complétez le champ **Description**.

   En cas de sélection d'un Compte associé à un seul Identifiant, cliquez sur le bouton sous l'onglet **Identifiant** de la fenêtre **Compte associé à un seul Identifiant**.

AJOUT DE L'EMPLACEMENT DE L'APPLICATION / DE LA PAGE WEB

Les données personnelles du Compte sont automatiquement introduites dans les champs d'authentification de la page Web / de l'application. L'emplacement de la page Web / de l'application se définit par le biais d'un lien. Pour les pages Web, il s'agit d'une URL et pour les applications, du chemin du fichier exécutable de l'application. Sans ces données, le Compte ne peut être associé au programme / à la page Web.

Pour associer un Compte à un programme / à une page Web, vous pouvez procéder de différentes manières :

- sélectionnez le lien en cliquant sur le bouton dans les favoris de votre navigateur Internet ou dans la liste des programmes installés sur votre ordinateur ;
- spécifiez manuellement l'emplacement de l'application / de la page Web ;
- utilisez le pointeur de Kaspersky Password Manager.

Pour vérifier que le lien introduit est correct, ouvrez le programme / la page Web via le bouton .

Pour associer un lien à un compte déterminé, procédez comme suit :

1. Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.

2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, cliquez sur le bouton **Ajouter un Compte**.

3. Dans le champ **Lien** de l'onglet **Liens** de la boîte de dialogue, cliquez sur le bouton .

4. Dans le champ **Lien** de la boîte de dialogue, saisissez l'emplacement de l'application / de la page Web.

   Pour sélectionner une page Web à partir de la liste des pages Web sauvegardées (Favoris), sélectionnez une page dans la liste **Onglets** et cliquez ensuite sur le lien **Copier le lien de la Sélection**. Pour copier l'emplacement de la page Web depuis la fenêtre du navigateur Internet, cliquez sur le lien **Utiliser le chemin à l'application couplée**.

   Pour sélectionner le lien vers un programme, spécifiez son emplacement sur l'ordinateur dans le champ **Lien** en cliquant sur le bouton .

Pour spécifier manuellement l'emplacement d'un programme / d'une page Web, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.
2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, cliquez sur le bouton **Ajouter un Compte**.
3. Dans le champ **Lien** de l'onglet **Liens** de la boîte de dialogue, saisissez l'emplacement de l'application / l'URL de la page Web. L'URL de la page Web doit commencer par http://www.

Pour définir l'emplacement d'un programme / d'une page Web à l'aide du pointeur de Kaspersky Password Manager, procédez comme suit :

1. Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.
2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, cliquez sur le bouton **Ajouter un Compte**.
3. Dans le champ **Lien** de l'onglet **Liens** de la boîte de dialogue, spécifiez l'emplacement de l'application / l'URL de la page Web en déplaçant le pointeur de Kaspersky Password Manager dans la fenêtre de l'application / du navigateur Internet.

SELECTION DU MODE DE LIAISON DU COMPTE

Pour déterminer le Compte dont les données doivent être utilisées pour le remplissage automatique lors du lancement d'un programme / d'une page Web, Kaspersky Password Manager utilise l'emplacement de l'application / l'URL de la page Web.

Étant donné que Kaspersky Password Manager permet d'utiliser plusieurs Comptes pour un seul programme / site Web, la zone d'utilisation de chaque Compte doit être définie.

Kaspersky Password Manager permet d'établir la zone d'utilisation d'un Compte sur la base de l'emplacement de l'application introduit / de l'URL de la page Web introduite. Les paramètres de la zone sont configurés lors de la création d'un compte utilisateur (cf. p. 17). Il est toutefois possible d'en modifier ultérieurement la valeur.

En fonction de l'objet (programme ou site Web), l'utilisation du Compte est différente.

Pour un programme, les options possibles sont les suivantes :

- Utiliser le Compte pour le programme. Le Compte sera utilisé pour toutes les fenêtres de l'application prévoyant l'introduction de données personnelles.
- Identifier selon le titre de la fenêtre. Le Compte ne sera utilisé que pour la fenêtre spécifiée de l'application.

  Par exemple, un programme peut utiliser plusieurs Comptes. Au sein de ce programme, le seul élément permettant de distinguer le compte à utiliser est le titre de la fenêtre. Kaspersky Password Manager complétera automatiquement les données du Compte en fonction du titre de la fenêtre de l'application.

Pour une page Web, les utilisations possibles du Compte sont les suivantes :

- Uniquement pour la page Web spécifiée. Kaspersky Password Manager ne procédera au remplissage automatique de l'Identifiant et du mot de passe que si la page Web correspond à l'URL définie.

  Par exemple, si le compte utilisateur est associé à l'URL http://www.web-site.com/login.html, celui-ci ne sera pas actif pour les autres pages du même site (par exemple pour l'URL http://www.web-site.com/index.php).
- Pour les pages Web d'un répertoire. Kaspersky Password Manager ne procédera au remplissage automatique de l'Identifiant et du mot de passe que si la page Web appartient au dernier niveau de répertoire.

  Par exemple, si l'URL introduite est http://www.web-site.com/cgi-bin/login.html, le compte utilisateur spécifié sera utilisé pour toutes les pages Web situées dans le répertoire *cgi-bin*.
- Pour un site Web: <nom de domaine de troisième niveau et inférieur>. Le Compte spécifié est utilisé pour n'importe quelle page du domaine (domaine de troisième niveau et inférieur).

Par exemple, Kaspersky Password Manager complète automatiquement les données d'identification pour les pages Web: http://www.domain1.domain2.web-site.com/login.html ou http://www.domain1.domain2.web-site.com/index.php. Cependant, le compte utilisateur spécifié ne sera pas utilisé pour les pages Web dont les URL ont un domaine de quatrième niveau différent : http://www.domain3.domain2.web-site.com/index.php ou http://www.domain4.domain2.web-site.com/index.php.

- Pour un site Web: <nom du site Web>. Le Compte spécifié sera utilisé pour toutes les pages du site Web prévoyant l'introduction d'un Identifiant et d'un mot de passe.

  Par exemple, Kaspersky Password Manager complètera automatiquement les données d'identification pour les pages Web: http://www.domain1.domain2.web-site.com/login.html, http://www.domain2.domain2.web-site.com/index.php, http://www.domain3.domain2.web-site.com/index.php ou http://www.domain4.domain2.web-site.com/index.php.

Pour spécifier les paramètres d'utilisation d'un Compte, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.
2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, sélectionnez le Compte dans la liste **Base de données** et cliquez ensuite sur **Modifier** pour accéder à sa fenêtre de modification.
3. Sous l'onglet **Liens** de la boîte de dialogue, sélectionnez l'une des options d'utilisation du compte.

ACTIVATION AUTOMATIQUE D'UN COMPTE

L'option d'activation automatique d'un Compte est activée par défaut. Kaspersky Password Manager se contente alors d'introduire l'Identifiant et le mot de passe dans les champs d'identification. Vous pouvez configurer des paramètres complémentaires d'activation du compte utilisateur (cf. p. 17).

Pour les pages Web, il est en outre possible de spécifier une série d'URL pour lesquelles l'activation automatique doit s'appliquer.

Les différentes possibilités d'activation d'un Compte sont les suivantes :

- Pour la page Web sélectionnée. Le Compte ne sera activé que pour la page Web spécifiée.
- Pour un site Web. Le Compte sera activé pour toutes les pages du site Web.

Pour sélectionner l'activation automatique d'un Compte, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option **Gestionnaire de mots de passe**.
2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, sélectionnez le Compte dans la liste **Mes Mots de passe** et cliquez ensuite sur **Modifier** pour accéder à sa fenêtre de modification.
3. Sous l'onglet **Liens** de la boîte de dialogue, cochez la case ☑ **Activation automatique du Compte**.

   Choisissez également l'un des modes d'activation du compte pour la page Web.

REMPLISSAGE DE CHAMPS COMPLEMENTAIRES

Lors de l'authentification sur une page Web, des données autres que l'Identifiant et le mot de passe doivent parfois être complétées. Kaspersky Password Manager offre une fonction de remplissage automatique des champs complémentaires. Vous avez la possibilité de configurer les paramètres de remplissage des champs complémentaires pour un Compte.

La configuration des paramètres de remplissage des champs complémentaires est possible lorsque l'emplacement de l'application / l'URL de la page Web est spécifiée pour le Compte.

Pour configurer ces champs, Kaspersky Password Manager télécharge provisoirement la page Web et en analyse ensuite tous les champs et boutons. Les champs et boutons sont inclus dans un groupe propre à chaque page Web.

Lors du traitement de la page Web téléchargée, Kaspersky Password Manager en stocke temporairement les fichiers et images sur votre ordinateur.

Pour configurer les paramètres de remplissage automatique des champs complémentaires, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.
2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, sélectionnez le Compte dans la liste **Mes Mots de passe** et cliquez ensuite sur le bouton **Modifier** pour accéder à sa fenêtre de modification.
3. Sous l'onglet **Modification avancée** de la boîte de dialogue, cliquez sur le lien **Ouvrez l'édition avancée de formulaire**.
4. Dans la boîte de dialogue **Modification avancée**, cochez la case ☑ en regard du champ / bouton à modifier.
5. Activez le champ **Valeur** pour le champ / bouton sélectionné par un double-clic de la souris et saisissez ensuite la valeur du champ.

   Pour revenir à la liste des champs / boutons, cliquez sur le bouton **Modifier le champ**. Pour supprimer la valeur, cliquez sur le bouton **Supprimer**. Pour modifier à nouveau la valeur d'un champ / bouton, cliquez sur le bouton **Modifier**.

IDENTIFIANT

Certaines applications / pages Web utilisent plusieurs noms d'utilisateur. Kaspersky Password Manager vous permet de conserver plusieurs noms d'utilisateur pour un seul Compte. Kaspersky Password Manager détecte automatiquement le nouvel Identifiant lors de sa première utilisation et vous propose de l'ajouter au Compte pour l'application / la page Web concernée. Vous pouvez ajouter manuellement un nouveau nom d'utilisateur pour un compte utilisateur et par la suite le modifier (cf. p. 22).

Il existe plusieurs manières d'ajouter un Identifiant pour un Compte déterminé :

- Via le Bouton d'accès rapide. Pour ce faire, sélectionnez l'entrée **Modifier le Compte** → **Ajouter l'Identifiant** dans le menu du Bouton d'accès rapide.
- Depuis la fenêtre principale de l'application.

Pour ajouter un nouvel Identifiant pour un Compte déterminé, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.
2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, sélectionnez le Compte dans la liste **Mes Mots de passe** et cliquez ensuite sur le bouton **Ajouter l'Identifiant**.
3. Dans la boîte de dialogue, spécifiez l'Identifiant et le mot de passe. L'Identifiant peut se composer d'un ou plusieurs caractères. Pour spécifier les mots-clés associés à l'Identifiant, cliquez sur le bouton et complétez ensuite le champ **Description**.

   Pour copier l'Identifiant / mot de passe dans le Presse-papiers, utilisez le bouton . Pour créer un mot de passe automatiquement, cliquez sur le lien **Nouveau mot de passe** (cf. p. 40).

IDENTITE

Outre l'Identifiant et le mot de passe, certaines données personnelles sont souvent nécessaires pour s'enregistrer sur un site Web, par exemple le nom complet, l'année de naissance, le sexe, l'adresse de courrier électronique, le numéro de téléphone, la ville de résidence, etc. Kaspersky Password Manager permet de conserver toutes ces données de manière cryptée dans la base de mots de passe sous la forme d'identité. Lorsque vous vous enregistrez sur un nouveau site Web, Kaspersky Password Manager complète automatiquement le formulaire d'enregistrement en se basant sur les données de l'Identité sélectionnée. Afin de séparer les informations professionnelles et privées, il est possible d'utiliser plusieurs identités. Par la suite, vous pourrez modifier (cf. p. . 22) les paramètres de l'identité.

Pour créer une Identité, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.
2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, cliquez sur le bouton **Ajouter une identité**.
3. Dans le champ **Nom** de la boîte de dialogue, introduisez l'intitulé de l'Identité.
4. Saisissez une valeur dans les champs obligatoires en les activant via un double-clique.

GROUPE DE COMPTES

Les groupes de Comptes permettent d'organiser les informations dans la base de mots de passe. Un groupe se compose d'un dossier dans lequel sont ajoutés des Comptes.

Les groupes créés sont affichés dans le menu contextuel de Kaspersky Password Manager: entrée **Comptes** → **<Intitulé du groupe>**.

Pour créer un groupe de Comptes, procédez comme suit :

1. Dans le menu contextuel de l'application, sélectionnez l'option **Gestionnaire de mots de passe**.
2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, cliquez sur le bouton **Ajouter un groupe**.
3. Donnez un nom au dossier créé.
4. Glissez-déposez les Comptes à ajouter depuis la liste **Base de données** vers le dossier créé.

MODIFICATION DE DONNEES PERSONNELLES

Toutes les données personnelles stockées dans la base de mots de passe peuvent être modifiées: Compte, Identifiant, identité ou groupe de Comptes. Les modifications suivantes sont possibles pour chaque élément :

- Pour le Compte :
  - s'il s'agit d'un Compte associé à un seul Identifiant, modifier l'intitulé du Compte ainsi que l'Identifiant et le mot de passe ;
  - modifier l'emplacement de l'application / de la page Web associée à un Compte déterminé ;
  - créer des règles d'utilisation ;
  - configurer l'activation automatique ;
  - modifier les champs complémentaires du Compte ;

- modifier les commentaires du Compte.

- Pour l'Identifiant - modifier l'Identifiant et le mot de passe.

- Pour l'Identité - modifier l'intitulé de l'Identité et la valeur des champs obligatoires.

- Pour le groupe de Comptes - modifier l'intitulé et l'icône de groupe.

Étant donné que Kaspersky Password Manager est intégré à la fenêtre des programmes et pages Web qui l'utilisent, vous pouvez modifier les paramètres du Compte ou de l'Identifiant directement depuis la fenêtre de l'application / de la page Web.

Pour modifier les paramètres du Compte ou de l'Identifiant, procédez comme suit :

- Au départ du menu contextuel. Pour ce faire, ouvrez le menu contextuel de l'application et sélectionnez l'entrée **Comptes** → **<Intitulé du groupe de Comptes>** → **<Intitulé du Compte>** → **Modification du Compte**.

- Depuis la fenêtre principale de l'application.

- Via le Bouton d'accès rapide. Pour ce faire, sélectionnez l'entrée **Modifier le Compte** → **Modification du Compte** dans le menu du Bouton d'accès rapide.

Pour modifier la valeur des champs ainsi que les paramètres depuis la fenêtre principale de l'application, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.

2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, sélectionnez l'entrée **Base de données** dans la liste.

3. Dans la boîte de dialogue, modifiez les paramètres souhaités.

SUPPRESSION DE DONNEES PERSONNELLES

Avant toute modification de vos données personnelles, Kaspersky Password Manager crée automatiquement une copie de sauvegarde de la base de mots de passe. Si vos données ont été malencontreusement modifiées ou supprimées, utilisez la fonction de restauration de la base de mots de passe (cf. p. 25). Il est possible de supprimer un élément ou tous les éléments de la base de mots de passe.

Pour supprimer un élément de la base de mots passe, procédez comme suit :

1. Dans la Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.

2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, sélectionnez l'élément souhaité dans la liste **Mes Mots de passe** et cliquez ensuite sur le bouton **Supprimer** ou sur la touche **DEL** du clavier.

Pour supprimer tous les éléments de la base de mots passe, procédez comme suit :

1. Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.

2. Sous l'onglet **Modification** de la boîte de dialogue **Gestionnaire de mots de passe**, cliquez sur le bouton **Supprimer tout**.

IMPORTATION / EXPORTATION DE MOTS DE PASSE

Kaspersky Password Manager prévoit la possibilité d'importer et d'exporter vos mots de passe.

L'application permet d'ajouter des mots de passe provenant d'une base non protégée (non cryptée). Vous pouvez importer des mots de passe depuis d'autres programmes de gestion de mots de passe (par exemple, Internet Explorer, Mozilla Firefox, Keypass) ou des mots de passe préalablement exportés depuis Kaspersky Password Manager. L'importation de mots de passe s'effectue depuis des fichiers au format xml ou ini.

Kaspersky Password Manager permet d'exporter la base de mots de passe dans un fichier au format xml, html ou txt. La fonction d'exportation peut s'avérer utile lorsque vous devez partager les mots de passe, imprimer la base de mots de passe ou en effectuer une copie de sauvegarde dans un fichier d'un format différent de celui de Kaspersky Password Manager.

Les mots de passe exportés sont sauvegardés dans des fichiers non cryptés et par conséquent non protégés contre l'accès non autorisé. C'est pourquoi il est recommandé de réfléchir préalablement aux moyens de protéger les données exportées.

Lors de l'importation, la base de mots de passe subit des modifications. Vous aurez alors la possibilité de choisir parmi différentes actions:

- **Écraser**. La base de mots de passe actuelle est remplacée par la base importée (tous les mots de passe sauvegardés dans la base Kaspersky Password Manager avant l'importation seront supprimés).
- **Fusionner**. Les mots de passe importés depuis l'autre application sont ajoutés à la base de mots passe. Lors d'une fusion, il vous est proposé de choisir les Comptes à importer dans Kaspersky Password Manager.
- **Annuler**. L'importation des mots de passe est annulée.

Pour remplacer la base de mots de passe actuelle par la base importée depuis une autre application, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.
2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, sous l'onglet **Sauvegarde**, cliquez sur le bouton **Importer**.
3. Dans la boîte de dialogue **Importation des mots de passe**, sélectionnez l'application depuis laquelle seront importés les mots de passe. Cliquez ensuite sur le bouton **Charger les mots de passe**.
4. Dans la boîte de dialogue **Fichier Kaspersky Password Manager**, sélectionnez le fichier contenant les mots de passe à importer et cliquez sur le bouton **Ouvrir**. Pour annuler la sélection, cliquez sur **Annuler**.
5. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Écraser**.

Pour fusionner la base de mots de passe actuelle avec la base importée depuis une autre application, procédez comme suit :

1. Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.
2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, sous l'onglet **Sauvegarde**, cliquez sur le bouton **Importation**.
3. Dans la boîte de dialogue **Importation des mots de passe**, sélectionnez l'application depuis laquelle seront importés les mots de passe. Cliquez ensuite sur le bouton **Charger les mots de passe**.
4. Dans la boîte de dialogue **Fichier Kaspersky Password Manager**, sélectionnez le fichier contenant les mots de passe à importer et cliquez sur le bouton **Ouvrir**. Pour annuler la sélection, cliquez sur **Annuler**.
5. Dans la boîte de dialogue **Chargement Kaspersky Password Manager**, cliquez sur le bouton **Fusionner**.
6. Dans la fenêtre **Importation des mots de passe**, cochez la case ☑ en regard des Comptes à importer et cliquez sur le bouton **Importation**.

   Pour sélectionner tous les comptes de la liste, cochez la case ☑ en regard de l'application choisie.

Pour exporter la base de mots passe, procédez comme suit :

1. Sélectionnez l'entrée **Gestionnaire de mots de passe** dans le menu contextuel de l'application.
2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, sous l'onglet **Sauvegarde**, cliquez sur le bouton **Exportation vers un fichier texte**.
3. Confirmez l'exportation de la base de mots de passe en cliquant sur le bouton **OK**. Pour ne plus devoir confirmer à l'avenir l'exportation de la base de mots de passe, cochez la case **Ne plus montrer ce message à l'avenir**.
4. Dans la boîte de dialogue **Exportation de la base de mots de passe dans un fichier non protégé**, spécifiez l'emplacement, le nom et le format du fichier.

SAUVEGARDER / RESTAURER LA BASE DE MOTS DE PASSE

Avant toute modification de la base de mots de passe, une copie de sauvegarde est automatiquement créée. Un emplacement par défaut est défini pour l'enregistrement des copies de sauvegarde mais vous avez la possibilité de le modifier (cf. page 32). La sauvegarde des mots de passe peut s'avérer utile dans les cas suivants :

- pour annuler les dernières modifications ;
- lorsque la base de mots de passe a été écrasée ou supprimée ;
- lorsque la base de mots de passe est inaccessible / endommagée après une erreur matériel ou système.

Les données de la copie de sauvegarde sont entièrement cryptées. Kaspersky Password Manager enregistre toutes les modifications dans la base de mots de passe. Dans l'application, les copies de sauvegarde sont affichées dans une liste et triées par date de création, la plus récente en premier. Les informations suivantes sont spécifiées pour chaque copie de sauvegarde:

- emplacement ;
- date et heure de création ;
- modifications apportées par rapport à la version précédente.

Les différentes actions possibles sont les suivantes :

- sauvegarde de la base de mots de passe depuis une copie de sauvegarde spécifique ;
- suppression d'anciennes copies de sauvegarde ;
- modification de l'emplacement de l'enregistrement des copies de sauvegarde (cf. p. 32).

Pour restaurer la base de mots passe, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.
2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, sous l'onglet **Sauvegarde**, cliquez sur le bouton **Restaurer**.
3. Dans la boîte de dialogue **Sauvegarde**, sélectionnez la copie de sauvegarde dans la liste et cliquez sur le bouton **Restaurer**.
4. Dans la boîte de dialogue qui s'affiche, confirmez la sauvegarde à l'aide du bouton **OK**.

Pour supprimer une ancienne copie de sauvegarde devenue inutile, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Gestionnaire de mots de passe**.

2. Dans la boîte de dialogue **Gestionnaire de mots de passe**, sous l'onglet **Sauvegarde**, cliquez sur le bouton **Restaurer**.

3. Dans la boîte de dialogue **Sauvegarde**, sélectionnez dans la liste la copie de sauvegarde à supprimer. Pour sélectionner plusieurs versions, maintenez enfoncée la touche **CTRL**.

4. Cliquez sur le bouton **Supprimer**.

5. Confirmez la suppression des copies de sauvegarde à l'aide du bouton **OK**.

CONFIGURATION DES PARAMETRES DE L'APPLICATION

La configuration des paramètres de l'application n'est possible que lorsque la base de mots de passe est déverrouillée (cf. p. 12). La modification des paramètres recouvre les actions suivantes :

- définir l'heure de lancement de l'application (cf. p. 37) ;
- activer les notifications (cf. p. 37) ;
- définir le nom d'utilisateur (cf. p. 28), utilisé par défaut lors de la création d'un compte utilisateur ;
- définir la durée de conservation du mot de passe dans le Presse-papiers (cf. p. 38) ;
- configurer la liste des comptes souvent utilisés (cf. p. 28) ;
- établir la liste des sites Web interdits (cf. p. 29) pour lesquels les fonctions de Kaspersky Password Manager ne sont pas utilisées ;
- établir la liste des sites Web de confiance (cf. p. 29) pour lesquels Kaspersky Password Manager autorise le réadressage ;
- configurer les touches de raccourci pour l'appel des fonctions de Kaspersky Password Manager (cf. p. 30) ;
- modifier le chemin d'accès à la base des mots de passe (cf. p. 31), aux copies de sauvegarde (cf. p. 32) ;
- modifier la méthode de cryptage des données (cf. p. 33) ;
- configurer le verrouillage automatique de la base des mots de passe (cf. p. 34) ;
- modifier le mot de passe principal (cf. p. 36) ;
- configurer l'accès à la base de mots de passe (cf. p. 34) ;
- modifier la position du Bouton d'accès rapide, établir la liste des applications, supportant le Bouton d'accès rapide (cf. p 39) ;
- composer la liste des applications prises en charge (cf. p. 36).

Pour modifier les paramètres de fonctionnement de Kaspersky Password Manager, procédez comme suit :

1. Dans le menu de l'application, sélectionnez l'option **Configuration**.
2. Dans la boîte de dialogue **Configuration**, sélectionnez la section relative aux paramètres à modifier.
3. Dans la partie droite de la fenêtre, effectuez les modifications nécessaires au groupe de paramètres souhaité.

DANS CETTE SECTION

UTILISATION D'UN IDENTIFIANT PAR DEFAUT

Kaspersky Password Manager permet de spécifier l'Identifiant qui sera automatiquement affiché dans le champ **Identifiant** lors de la création d'un nouveau Compte (cf. p. 17).

Pour spécifier l'Identifiant par défaut, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration** qui s'ouvre, sélectionnez la section **Général**.
3. Dans la partie droite de la fenêtre, complétez le champ **Identifiant par défaut**.

LISTE DES COMPTES FAVORIS

Kaspersky Password Manager vous permet d'accéder rapidement à vos Comptes. Le menu de l'application contient une liste des Comptes favoris. Elle présente le nom des programmes / pages Web que vous lancez le plus souvent. Les éléments de la liste peuvent être triés par ordre alphabétique ou par fréquence d'utilisation.

La liste des Comptes favoris n'est accessible depuis le menu que si la base de mots de passe est déverrouillée (cf. p. 12).

Vous pouvez spécifier les paramètres de liste suivants :

- **Quantité d'éléments dans la liste** – nombre maximum de Comptes favoris pouvant être affichés dans le menu de l'application ;
- **Afficher les Comptes favoris dans le menu de la barre des tâches** – la liste des Comptes favoris sera accessible depuis le menu contextuel de Kaspersky Password Manager ;
- **Afficher les Comptes favoris dans le menu du Bouton d'accès rapide** – la liste des Comptes favoris sera accessible depuis le menu du Bouton d'accès rapide (dans la fenêtre de l'application / du navigateur Internet).

Pour afficher la liste des Comptes favoris, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Comptes favoris**.
3. Dans la partie droite de la fenêtre, cochez la case ☑ **Afficher les Comptes favoris dans le menu de la barre des tâches**.

   Pour afficher la liste des comptes fréquemment utilisés dans le menu du Bouton d'accès rapide, cochez en plus la case ☑ **Afficher les Comptes favoris dans le menu du Bouton d'accès rapide**.

   Si la case ☑ **Afficher les Comptes favoris dans le menu de la barre des tâches** n'est pas cochée, les autres paramètres de liste ne pourront être modifiés.
4. Spécifiez le nombre de Comptes dans le champ **Taille de la liste**.
5. Si nécessaire, modifiez manuellement la composition de la liste. Pour retirer un élément de la liste, sélectionnez le Compte souhaité et cliquez sur le bouton **Supprimer.** Pour supprimer tous les éléments de la liste, cliquez sur le bouton **Purger**.

LISTE DES URL IGNOREES

Généralement, lors de la première authentification sur un site Web, Kaspersky Password Manager vous propose d'ajouter un nouveau Compte. De cette manière, l'introduction des données personnelles s'effectuera automatiquement lors d'une visite ultérieure sur ce même site.

Pour introduire vous-mêmes vos données personnelles lors de l'authentification, vous pouvez établir une liste des URL pour lesquelles les fonctions de Kaspersky Password Manager doivent être désactivées. La fonction de remplissage automatique de l'Identifiant et du mot de passe sera inactive pour tous les sites Web appartenant à cette liste. De plus, Kaspersky Password Manager ne leur propose pas automatiquement la création d'un compte (cf. p. 17) / identifiant (cf. p. 21).

Pour constituer la liste des URL interdites, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **URL ignorées**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ajouter**, saisissez l'URL et appuyez sur la touche **ENTER**.

   Pour modifier une URL, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**. Pour supprimer une URL de la liste, sélectionnez-la et cliquez sur le bouton **Supprimer**.

LISTE DES URL DE CONFIANCE

Kaspersky Password Manager garantit la protection de vos données personnelles contre le phishing. Si lors d'une tentative d'authentification vous êtes redirigé vers un autre site Web, le programme vous en avise.

Les individus mal intentionnés utilisent souvent le réadressage à partir de sites Web qui accèdent à des comptes bancaires (il peut par exemple s'agir de banques sur Internet, de systèmes de paiement, etc.). Une fois sur la page d'authentification du site Web officiel de la société, un réadressage est effectué vers un site Web contrefait qui est visuellement identique à la page Web officielle. Toutes les données encodées sur la page contrefaite sont transmises aux individus mal intentionnés.

Les sites Web officiels utilisent régulièrement le réadressage. Pour éviter que Kaspersky Password Manager ne considère ce type de réadressage comme des tentatives de phishing, vous avez la possibilité d'établir une liste des URL de confiance. Cette liste doit contenir les sites Web vers lesquels sont transmises des données personnelles. Lors d'une authentification, Kaspersky Password Manager n'affiche pas de notification si des données personnelles sont transmises vers un site Web de confiance.

Kaspersky Password Manager autorise l'envoi de données personnelles vers un site Web de confiance. Avant d'ajouter un site Web dans la liste des URL de confiance, assurez-vous de sa fiabilité!

Vous pouvez ajouter un site Web dans la liste des URL de confiance de plusieurs manières :

- directement lors de l'authentification sur un site Web ;
- manuellement depuis la fenêtre **Configuration de Kaspersky Password Manager**.

Pour ajouter un site Web dans la liste des URL de confiance durant le processus d'authentification, attendez le réadressage d'un site Web à l'autre et cochez ensuite la case **Toujours faire confiance au site Web <intitulé du site Web>** dans la boîte de dialogue de Kaspersky Password Manager.

Pour constituer manuellement la liste des URL de confiance, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **URL de confiance**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ajouter**. Un champ devient accessible dans la liste **URL de confiance**. Saisissez l'URL et appuyez sur la touche **ENTER**.

   Pour modifier une URL, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**. Pour supprimer une URL, sélectionnez-la dans la liste et cliquez sur le bouton **Supprimer**.

RACCOURCIS DE L'APPLICATION

Pour appeler rapidement certaines fonctions de l'application, il peut s'avérer intéressant de les associer à des combinaisons de touches.

Vous pouvez spécifier une combinaison de touches pour les actions suivantes :

- Verrouiller/déverrouille Kaspersky Password Manager (cf. p. 12).
- Activer un mot de passe.
- Afficher le Clavier virtuel.

Un raccourci peut se composer d'une touche ou d'une combinaison de deux ou trois touches.

Évitez de spécifier une combinaison de touches déjà utilisée par Microsoft Windows.

Pour modifier une combinaison de touches, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Raccourcis clavier**.

3. Dans la partie droite de la fenêtre, spécifiez la combinaison de touches à associer à chaque action.

EMPLACEMENT DE LA BASE DE MOTS DE PASSE

Base de mots de passe Kaspersky Password Manager : il s'agit d'un fichier crypté (cf. p. 33) dans lequel sont conservées toutes vos données personnelles (comptes, noms d'utilisateur, mots de passe et identité).

Pour utiliser la base de mots de passe, il faut absolument la déverrouiller (cf. p. 12) (autoriser). Par défaut, l'accès aux données personnelles est protégé par un Mot de passe principal. En outre, Kaspersky Password Manager peut garantir la sécurité de la base de mots de passe au moyen d'un périphérique USB ou Bluetooth. Vous pouvez modifier les paramètres d'accès (cf. p. 34) pour chaque base de mots de passe.

Par défaut, le chemin d'accès à la base de mots de passe est le suivant (diffère selon la version de Microsoft Windows):

- pour Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Kaspersky Password Manager\ ;
- pour Microsoft Windows Vista: C:\Users\User_name\Documents\Kaspersky Password Manager\.

Votre base de mots de passe peut être stockée sur plusieurs supports différents: disque amovible, disque local ou disque réseau.

Lors de la modification du chemin d'accès à la base de mots de passe ou du nom de celle-ci, plusieurs actions sont possibles:

- **Copier** : une copie de la base de mots de passe est créée à l'emplacement indiqué. Cette copie devient la base de mots de passe active.
- **Replacer** : la base de mots de passe active est sauvegardée à l'emplacement indiqué.
- **Créer une base de mots de passe** : une copie vide de la base de mots de passe est créée, laquelle devient la base active.

Pour déplacer la base de mots de passe et modifier son nom, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Base de données**.
3. Dans la partie droite de la fenêtre, dans le groupe **Source**, cliquez sur le bouton  situé à droite du champ **Chemin**.
4. Dans la fenêtre **Sélection de la base de mots de passe**, spécifiez le chemin du fichier ainsi que son nom et cliquez ensuite sur le bouton **Ouvrir**.
5. Dans la fenêtre **Emplacement de la base de mots de passe**, sélectionnez l'action à effectuer et confirmez ensuite celle-ci à l'aide du bouton **OK**.
6. Dans la boîte de dialogue **Kaspersky Password Manager**, saisissez le Mot de passe principal pour confirmer les modifications.

Pour modifier la base de mots passe active, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Base de données**.
3. Dans la partie droite de la fenêtre, dans le groupe **Source**, cliquez sur le bouton  situé à droite du champ **Chemin**.

4. Dans la fenêtre **Sélection de base des mots de passe** sur le bouton **Ouvrir**.

5. Dans la boîte de dialogue **Kaspersky Password Manager**, saisissez le Mot de passe principal de la base que vous souhaitez ouvrir.

CREATION D'UNE NOUVELLE BASE DE MOTS DE PASSE

Kaspersky Password Manager permet de travailler successivement avec plusieurs bases de mots de passe. La création d'une nouvelle base de mots de passe permet de séparer vos données personnelles en les répartissant dans deux ou plusieurs bases. Si nécessaire, il est possible de restaurer une ancienne base de mots de passe. Kaspersky Password Manager vous propose de créer une nouvelle base de mots de passe lorsque la base actuelle est endommagée ou qu'une copie de sauvegarde ne peut être restaurée.

Pour créer une nouvelle base de mots passe, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.

2. Dans la fenêtre **Configuration**, sélectionnez la section **Base de données**.

3. Dans la partie droite de la fenêtre, dans le groupe **Source**, cliquez sur le bouton  situé à droite du champ **Chemin**.

4. Dans la fenêtre **Sélection de la base de mots de passe**, définissez l'emplacement et le nom du fichier de la base de mots de passe et cliquez ensuite sur le bouton **Ouvrir**.

5. Dans la boîte de dialogue **Emplacement de la base de mots de passe**, sélectionnez l'action **Créer une base de mots de passe** et confirmez à l'aide du bouton **OK**.

6. Dans le groupe **Mot de passe** de la fenêtre **Nouvelle base de mots de passe**, spécifiez le mot de passe permettant d'accéder à la nouvelle base et confirmez celui-ci dans le champ **Confirmation du mot de passe**.

   Si le mot de passe introduit ne correspond pas au mot de passe de confirmation, ce dernier apparaîtra en rouge.

   Dans le groupe **Cryptage**, sélectionnez le fournisseur de services cryptographiques ainsi que le mode de cryptage souhaité (cf. p. 33).

7. Dans la boîte de dialogue, introduisez le nouveau Mot de passe principal afin de confirmer la création de la nouvelle base de mots de passe.

COPIE DE SAUVEGARDE

Avant de mémoriser les modifications apportées à vos données personnelles, Kaspersky Password Manager effectue automatiquement une copie de sauvegarde de la base de mots de passe. Cela permet de prévenir les pertes de données en cas de problèmes système ou techniques. Kaspersky Password Manager effectue une copie complète de la base de mots de passe juste avant d'enregistrer les dernières modifications. Si la base de mots de passe est endommagée, vous avez la possibilité de restaurer les données de la dernière copie de sauvegarde (cf. p. 25).

La copie de sauvegarde de votre base de mots de passe peut être stockée sur un disque local, un disque amovible ou un disque réseau.

L'emplacement par défaut de la copie de sauvegarde est le suivant (dépend du système d'exploitation):

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Kaspersky Password Manager\ ;

- Microsoft Windows Vista: C:\Users\User_name\Documents\Kaspersky Password Manager\.

Pour modifier l'emplacement de la copie de sauvegarde, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Base de données**.
3. Dans la partie droite de la fenêtre, dans le groupe **Copie de sauvegarde**, cliquez sur le bouton  situé à droite du champ **Chemin**.
4. Dans la boîte de dialogue **Parcourir**, sélectionnez le dossier de sauvegarde de la copie de sauvegarde de la base de mots de passe.

SELECTION DU MODE DE CRYPTAGE

But de la cryptographie – protéger vos informations de l'accès et de la diffusion non autorisés. Principale fonction du cryptage – brouiller la communication sur les canaux non protégés.

Les fonctions de cryptage et décryptage nécessitent des clés. Clé – paramètre indispensable pour le cryptage. Lorsque les fonctions de cryptage et décryptage mettent en œuvre une clé unique, l'algorithme est dit symétrique. Lorsqu'elles utilisent deux clés, on parle d'algorithme asymétrique. Le cryptage symétrique peut à son tour être par bloc ou par flot. Toute information (quel que soit le format des données originales) est interprétée en code binaire. Le cryptage par bloc part du principe que les données sont scindées en blocs et que chaque bloc est ensuite transformé de manière indépendante. Avec le cryptage par flot, l'algorithme de transformation s'applique à chaque bit d'information.

Kaspersky Password Manager propose les algorithmes de cryptage symétrique suivants :

- **DES**. Cryptage par bloc avec clé standard de 56 bits. Comparativement aux standards actuels, le DES n'offre pas un niveau de sécurité élevé. Cet algorithme s'utilise lorsque la fiabilité ne constitue pas l'exigence principale.
- **3DES**. Algorithme par bloc se basant sur le DES Cette version résout le principal défaut de l'algorithme précédent – la clé de petite taille. La clé du 3DES est trois fois plus grande que celle du DES (56*3=168 bits). Sa vitesse d'exécution est trois fois moins importante que celle du DES mais la sécurité est considérablement plus élevée. Le 3DES est plus fréquent que le DES car ce dernier n'est plus suffisamment complexe face aux technologies actuelles de piratage.
- **3DES TWO KEY**. Algorithme par bloc se basant sur le DES Algorithme 3DES avec clé de 112 bits (56*2).
- **RC2**. Algorithme de cryptage par bloc avec longueur de clé variable capable de traiter rapidement un grand volume d'informations. Algorithme plus rapide que le DES. Il équivaut au 3DES en termes de fiabilité et de résistance.
- **RC4**. Cryptage par flot avec longueur de clé variable. Celle-ci peut être comprise entre 40 et 256 bits. Avantages de cet algorithme – vitesse de traitement élevée et longueur de clé variable. Par défaut, Kaspersky Password Manager utilise l'algorithme RC4 pour le cryptage de vos données.
- **AES**. Algorithme symétrique à cryptage par bloc et clés de 128, 192 et 256 bits. Cet algorithme garantit une niveau de sécurité élevé et fait partie des algorithmes les plus répandus.

Sous Microsoft Windows, les opérations de cryptographie sont effectuées au moyen de fournisseurs de services cryptographiques. Chaque fournisseur supporte plusieurs algorithmes de cryptage avec une longueur de clé déterminée. Les fournisseurs de services cryptographiques intégrés à Microsoft Windows et utilisés par Kaspersky Password Manager sont les suivants :

- Microsoft Base Cryptographic Provider ;
- Microsoft Enhanced Cryptographic Provider ;
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype) ;
- Microsoft RSA/Schannel Cryptographic Provider ;

- Microsoft Strong Cryptographic Provider.

Pour modifier l'algorithme de cryptage, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Base de données**.
3. Dans la partie droite de la fenêtre, dans le groupe **Cryptage**, cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Algorithme de cryptage**, spécifiez les paramètres de l'algorithme de cryptage.

VERROUILLAGE AUTOMATIQUE LA BASE DE MOTS DE PASSE

Kaspersky Password Manager verrouille automatiquement la base de mots de passe après le lancement de l'application ainsi qu'après une durée déterminée d'inactivité de l'ordinateur. Vous pouvez déterminer vous-même la durée après laquelle se verrouille la base de mots de passe. Elle peut être comprise entre 1 et 60 minutes. Il est recommandé de verrouiller la base de mots de passe après 5-20 minutes d'inactivité de l'ordinateur. Vous pouvez également désactiver verrouillage automatique de la base de mots de passe.

Kaspersky Password Manager verrouille automatiquement la base de mots de passe après une durée déterminée d'inactivité de l'ordinateur. Si vous désactivez le verrouillage automatique de l'ordinateur, vos données personnelles ne seront pas protégées dans le cas où vous vous absenteriez de l'ordinateur sans verrouillage manuel préalable.

Pour modifier la durée après laquelle se verrouille la base de mots de passe, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Base de données**.
3. Dans la partie droite de la fenêtre, dans le groupe **Blocage automatique**, sélectionnez dans la liste la durée d'inactivité de l'ordinateur après laquelle Kaspersky Password Manager sera verrouillé.

   Pour désactiver le verrouillage de la base de mots de passe, sélectionnez la valeur **Jamais**.

MODE D'AUTHENTIFICATION DE KASPERSKY PASSWORD MANAGER

L'authentification permet de contrôler l'accès à vos données personnelles. Vous pouvez opter pour l'un des modes d'authentification suivants :

- **Mot de passe principal**. Le Mot de passe principal doit impérativement être introduit pour pouvoir déverrouiller la base de mots passe. Il s'agit du mode d'authentification par défaut.
- **Périphérique USB**. L'accès à la base de mots de passe s'effectue via un périphérique à interface USB connecté à l'ordinateur. Les périphériques USB compatibles sont notamment les unités à mémoire flash, les appareils photos, les baladeurs MP3 et les disques durs externes. Lorsque le périphérique USB est déconnecté, la base de mots de passe est automatiquement verrouillée.
- **Périphérique Bluetooth**. L'accès à la base de mots de passe s'effectue via un périphérique doté de la fonction Bluetooth. La fonction Bluetooth doit être disponible tant sur le téléphone portable que sur l'ordinateur où s'exécute Kaspersky Password Manager. La base de mots de passe est automatiquement déverrouillée lorsque la connexion Bluetooth est établie entre le téléphone portable et l'ordinateur. En cas de perte de connexion (par exemple si vous désactivez la fonction Bluetooth sur votre téléphone portable), la base de mots de passe est automatiquement verrouillée.

- **Sans authentification**. L'accès à la base de données n'est pas protégé.

  Sans authentification, vos données personnelles sont accessibles par tous les utilisateurs travaillant sur votre ordinateur.

Si vous optez pour l'authentification via périphérique USB ou Bluetooth, il est recommandé de retenir votre Mot de passe principal. Si vous n'avez pas votre périphérique d'authentification à portée de la main, Kaspersky Password Manager vous permet d'utiliser le Mot de passe principal pour accéder à vos données personnelles.

Pour modifier le mode d'authentification, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Mode d'autorisation**.
3. Dans la partie droite de la fenêtre, dans le groupe **Mode d'autorisation**, sélectionnez l'une des options d'authentification depuis le menu déroulant.

VOIR EGALEMENT :

Utilisation de périphériques USB ou Bluetooth 35

UTILISATION DE PERIPHERIQUES USB OU BLUETOOTH

Pour accéder à la base de mots de passe (cf. p. 34), Kaspersky Password Manager permet d'utiliser divers périphériques USB et Bluetooth.

Pour utiliser un périphérique USB afin d'accéder à la base de mots de passe, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Mode d'autorisation**.
3. Dans la partie droite de la fenêtre, dans le groupe **Mode d'autorisation**, sélectionnez la valeur **Périphérique USB** depuis le menu déroulant.
4. Connectez le périphérique portable à l'ordinateur.
5. Sélectionnez un périphérique dans la liste **Périphériques à disque** et cliquez sur le bouton **Installer**.

   L'icône apparaît en regard du périphérique sélectionné. Si le périphérique connecté n'est pas affiché dans la liste, cochez la case **Afficher tous les périphériques**. Si nécessaire, vous pouvez modifier le périphérique d'authentification en cliquant sur le bouton **Réinitialiser**.

Pour utiliser un périphérique Bluetooth afin d'accéder à la base de mots de passe, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Mode d'autorisation**.
3. Dans la partie droite de la fenêtre, dans le groupe **Mode d'autorisation**, sélectionnez la valeur **Périphérique Bluetooth** depuis le menu déroulant.
4. Activez la fonction Bluetooth sur votre ordinateur et ensuite sur votre périphérique.
5. Sélectionnez un périphérique dans la liste **Téléphones et modems** et cliquez sur le bouton **Installer**.

   L'icône apparaît en regard du périphérique sélectionné. Si nécessaire, il est possible de modifier le périphérique d'authentification en cliquant sur le bouton **Réinitialiser**.

MODIFICATION DU MOT DE PASSE PRINCIPAL

Kaspersky Password Manager vous permet d'utiliser le mot de passe principal pour accéder à votre base de mots de passe (cf. p. 34). De cette manière, il vous suffit de retenir un seul mot de passe. Le Mot de passe principal par défaut est créé au premier démarrage de Kaspersky Password Manager. Il est toutefois possible de le modifier ultérieurement. La sécurité de vos données personnelles dépend en grande partie de la fiabilité du Mot de passe principal. Lors de la création du Mot de passe principal, Kaspersky Password Manager en évalue automatiquement la fiabilité et lui attribue l'un des statuts suivants :

- faible ;
- normale ;
- haute.

Pour créer un mot de passe fiable, mélangez des caractères spéciaux, des chiffres, des lettres majuscules et des lettres minuscules. Il est déconseillé d'utiliser un mot de passe composé à partir de données faciles à deviner (par exemple, nom d'un membre de la famille ou date de naissance).

Lors de la modification du Mot de passe principal, Kaspersky Password Manager exige une confirmation du nouveau mot de passe (double introduction). Il est impossible d'enregistrer le nouveau mot de passe sans cette confirmation. Si le mot de passe introduit ne correspond pas au mot de passe de confirmation, ce dernier apparaîtra en rouge. Avant de mémoriser le nouveau mot de passe, un message d'avertissement est affiché.

Pour modifier le Mot de passe principal, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Mode d'autorisation**.
3. Dans la partie droite de la fenêtre, dans le groupe **Protection par mot de passe**, cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Protection par mot de passe**, introduisez le nouveau mot de passe et confirmez-le ensuite en l'introduisant une seconde fois dans le champ **Confirmation du mot de passe**.

ÉTABLISSEMENT DE LA LISTE DES NAVIGATEURS INTERNET SUPPORTES

Pour garantir le bon fonctionnement de l'activation automatique du Compte et du Bouton d'accès rapide (cf. p. 39), Kaspersky Password Manager requiert l'installation d'extensions complémentaires (modules externes) pour certains navigateurs Internet. Par défaut, l'installation des extensions s'effectue lors du premier démarrage de Kaspersky Password Manager. Vous pouvez également installer le module externe requis.

Le programme prévoit une liste de navigateurs Internet qui sont chacun associés à l'état **Installé** / **Non installé** selon que leur module externe est ou non installé.

Avant d'installer des modules externes, il est recommandé de fermer tous les navigateurs Internet.

Pour installer le module externe d'un navigateur Internet, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Navigateurs compatibles**.
3. Dans la partie droite de la fenêtre, sélectionnez un navigateur Internet dans la liste **Navigateurs Internet pris en charge et extensions disponibles** et cliquez ensuite sur le bouton **Installer**.

4. Suivez les instructions de l'**Assistant d'installation**. Une fois le module externe installé, le navigateur Internet est automatiquement déplacé vers le groupe **Navigateurs installés**. Il est désormais associé au statut **Installé**. Vous pouvez désinstaller une extension en cliquant sur le bouton **Supprimer**.

PARAMETRES AVANCES

Kaspersky Password Manager vous permet de configurer certains paramètres avancés :

- heure de lancement de l'application (cf. p. 37) ;
- réception des notifications (cf. p. 37) ;
- durée de conservation du mot de passe dans le Presse-papiers (cf. p. 38) ;
- bouton d'accès rapide (cf. p. 39).

DEMARRAGE DE L'APPLICATION

Par défaut, Kaspersky Password Manager est lancé automatiquement au démarrage du système d'exploitation. Vous avez toutefois la possibilité de modifier les paramètres de lancement de l'application.

Pour lancer le programme manuellement, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration** qui s'ouvre, sélectionnez la section **Général**.
3. Dans la partie droite de la fenêtre, dans le groupe **Général**, décochez la case **Lancer Kaspersky Password Manager au démarrage de l'ordinateur**.

FONCTION D'ACTIVATION PAR DOUBLE-CLIQUE

Kaspersky Password Manager permet de définir la tâche qui sera exécutée lors d'un double-clique sur l'icône de l'application situé dans la zone de notification de la barre des tâches de Microsoft Windows. Il peut s'agir de l'une des tâches suivantes :

- ouvrir la fenêtre principale de Kaspersky Password Manager (cf. p. 10) ;
- verrouiller / déverrouiller Kaspersky Password Manager (action par défaut).

Pour configurer la tâche à lancer lors d'un double-clique sur l'icône de l'application situé dans la zone de notification de la barre des tâches, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration** qui s'ouvre, sélectionnez la section **Général**.
3. Dans la partie droite de la fenêtre, sélectionnez l'action à exécuter dans le menu déroulant **Double-clique sur l'icône pour**.

NOTIFICATIONS

Pendant le fonctionnement de Kaspersky Password Manager, divers types d'événements à caractère généralement informatif sont générés. Pour être informé de ces événements, utilisez le service de notification. Les utilisateurs sont notifiés par le biais d'avertissements et de messages contextuels.

Le programme prévoit les types de notification suivants :

- **Lancement de l'application**. Ce message apparaît lorsque le programme est lancé et que la base de mots de passe est déverrouillée.
- **Activation du compte**. Ce message apparaît lorsque le Compte est activé.
- **Purge du Presse-papiers**. Kaspersky Password Manager permet de conserver temporairement un mot de passe dans le Presse-papiers. Cela peut s'avérer utile lorsque des données doivent être copiées d'un champ à un autre. A la fin de la période définie (cf. p. 38), le mot de passe sera supprimé du Presse-papiers.
- **Verrouillage automatique de Kaspersky Password Manager**. Ce message apparaît lorsque Kaspersky Password Manager verrouille automatiquement la base de mots de passe. Par défaut, la base de mots de passe est automatiquement verrouillée au démarrage du système d'exploitation ainsi qu'après une durée définie (cf. p. 34) d'inactivité de l'ordinateur.
- **Exportation de données dans un fichier non protégé**. Message d'avertissement spécifiant que la fonction d'exportation sauvegardera vos mots de passe dans un fichier non crypté et qu'ils seront par conséquent accessibles par n'importe quel utilisateur travaillant sur votre ordinateur. Nous vous recommandons de réfléchir à la manière de protéger le fichier contenant les mots de passe avant de procéder à l'exportation des données.
- **Modification avancée**. Avant de modifier la configuration de champs complémentaires, le programme demande l'authentification d'utiliser le navigateur Internet par défaut. Ce message vous avertit que des images et fichiers système (cookies) seront sauvegardés sur votre ordinateur.
- **Problèmes lors du remplissage automatique de l'Identifiant pour le Compte**. Ce message vous avertit que les données n'ont pu être automatiquement complétées lors de l'authentification.

Pour recevoir les notifications, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration** qui s'ouvre, sélectionnez la section **Général**.
3. Dans la partie droite de la fenêtre, dans le groupe **Général**, cliquez sur le bouton **Notifications...**.
4. Dans la boîte de dialogue, cochez / décochez la case ☑ en regard des types de notification souhaités.

DUREE DE CONSERVATION D'UN MOT DE PASSE DANS LE PRESSE-PAPIERS

Kaspersky Password Manager vous permet de copier un mot de passe dans le Presse-papiers pour un laps de temps déterminé. Cela peut s'avérer intéressant lorsque le mot de passe ne doit être exploité que pour une courte durée (par exemple lors de l'enregistrement sur un site Web / dans un programme). Vous pouvez spécifier la durée de conservation du mot de passe dans le Presse-papiers. Une fois ce temps écoulé, le mot de passe est automatiquement supprimé du Presse-papiers. Cela permet d'éviter l'interception et le vol du mot de passe puisque celui-ci ne peut plus être récupéré dans le Presse-papiers après la durée définie.

Pour modifier la durée de conservation du mot de passe dans le Presse-papiers, procédez comme suit :

1. Sélectionnez l'entrée **Configuration** dans le menu contextuel de l'application.
2. Dans la fenêtre **Configuration** qui s'ouvre, sélectionnez la section **Général**.
3. Dans la partie droite de la fenêtre, dans le groupe **Presse-papiers**, spécifiez-la durée en secondes.

BOUTON D'ACCES RAPIDE

Kaspersky Password Manager permet de gérer les Comptes directement depuis la fenêtre de l'application / du navigateur Internet par le biais d'un Bouton d'accès rapide situé dans le coin supérieur droit de la fenêtre de l'application / du navigateur Internet. Après avoir cliqué sur le Bouton d'accès rapide, un menu apparaît avec la liste des noms d'utilisateur associés au programme / à la page Web. Lorsque vous sélectionnez un Identifiant, Kaspersky Password Manager complète automatiquement les champs d'authentification en fonction des données stockées dans la base de mots de passe.

Le bouton d'accès rapide est accessible si la base de mots de passe n'est pas verrouillée (cf. p. 12).

Si le programme que vous utilisez intègre le menu d'une application autre que Kaspersky Password Manager, vous avez la possibilité de spécifier la position du Bouton d'accès rapide par rapport aux autres boutons. Par ailleurs, il est possible de définir manuellement la liste des navigateurs Internet devant intégrer le Bouton d'accès rapide.

Pour modifier les paramètres du Bouton d'accès rapide, procédez comme suit :

1. Dans le menu contextuel de l'application, choisissez l'option. **Configuration**.
2. Dans la fenêtre **Configuration**, sélectionnez la section **Bouton d'accès rapide**.
3. Dans la partie droite de la fenêtre, dans le groupe **Affichage du Bouton d'accès rapide**, configurez les paramètres requis en fonction de la tâche à effectuer:
   - pour modifier la position du Bouton d'accès rapide, introduisez le numéro correspondant à la position du bouton dans le groupe **Affichage du Bouton d'accès rapide** (la position du Bouton d'accès rapide en commençant par la gauche) ;
   - pour empêcher l'affichage du Bouton d'accès rapide en cas de verrouillage de la base de mots de passe, cochez la case ☑ **Masquer le Bouton d'accès rapide si Kaspersky Password Manager est verrouillé** dans le groupe **Affichage du Bouton d'accès rapide**;
   - pour établir la liste des navigateurs Internet dans lesquels le Bouton d'accès rapide doit apparaître, cochez dans la liste du groupe **Afficher le Bouton d'accès rapide dans les navigateurs Internet suivants** la case ☑ en regard des navigateurs Internet concernés.

POSSIBILITES COMPLEMENTAIRES

Kaspersky Password Manager se compose d'une série d'outils et assistants complémentaires:

- **Le générateur de mots de passe** permet de créer des mots de passe complexes pour vos Comptes.
- **Le pointeur Kaspersky Password Manager** permet de sélectionner rapidement un programme / une page Web et ensuite d'appliquer une action à l'objet sélectionné.
- **L'assistant de création de la version portable de Kaspersky Password Manager** permet d'installer une version portable de l'application sur un support amovible.

DANS CETTE SECTION

GENERATEUR DE MOTS DE PASSE

La sécurité des données dépendent directement de la fiabilité des mots de passe. Les données sont sujettes à un risque dans les cas suivants :

- utilisation d'un mot de passe unique pour tous les comptes ;
- mot de passe simpliste ;
- mot de passe composé à partir de données faciles à deviner (par exemple, nom d'un membre de la famille ou date de naissance).

Pour garantir la sécurité des données, Kaspersky Password Manager vous permet de créer des mots de passe uniques et complexes pour vos Comptes. Kaspersky Password Manager conserve tous les mots de passe générés afin de ne pas devoir les retenir.

Un mot de passe est considéré comme complexe lorsqu'il se compose de plus de quatre caractères et qu'il mélange des caractères spéciaux, des chiffres, des lettres majuscules et des lettres minuscules.

Les paramètres suivants déterminent la fiabilité d'un mot de passe :

- **Longueur** – nombre de caractères composant le mot de passe. Elle peut être comprise entre 4 et 99 caractères. On considère que plus le mot de passe est long, plus il est complexe.
- **A-Z** – utilisation de lettres majuscules.
- **A-Z** – utilisation de lettres majuscules.
- **0-9** – utilisation de chiffres.
- **Caractères spéciaux** – utilisation de caractères spéciaux.
- **Ne pas utiliser deux fois le même caractère** – défense d'utiliser des caractères identiques dans le mot de passe.

Vous pouvez utiliser le générateur de mots de passe dans les situations suivantes :

- lors de la création d'un nouveau Compte dans l'application / sur un site Web.
- lors de l'ajout manuel d'un compte (cf. p. 17) / d'un nom d'utilisateur (cf. p. 21) à Kaspersky Password Manager.

Pour utiliser le générateur de mots de passe lors de la création d'un nouveau Compte dans l'application / sur un site Web, procédez comme suit :

1. Accédez au menu contextuel de Kaspersky Password Manager et sélectionnez l'entrée **Générateur de mots de passe**.
2. Dans le champ **Longueur du mot de passe** de la fenêtre **Générateur de mots de passe**, spécifiez le nombre de caractères devant composer le mot de passe.
3. Si vous le souhaitez, vous pouvez configurez les paramètres avancés du générateur de mots de passe. Pour ce faire, cochez / décochez la case ☑ en regard des paramètres à modifier dans le groupe **Paramètres avancés**.
4. Cliquez sur le bouton **Générer**. Le mot de passe généré s'affiche dans le champ **Mot de passe**. Pour visualiser le mot de passe créé, cochez la case ☑ **Afficher le mot de passe**.
5. Copiez le mot de passe dans le Presse-papiers à l'aide du bouton  , collez ensuite le mot de passe dans le champ de saisie du mot de passe de l'application / dans la page Web à l'aide de la combinaison de touche **CTRL+V**. Le mot de passe généré est conservé dans le Presse-papiers pendant la durée définie, après quoi il est supprimé.
6. Cochez la case ☑ **Par défaut** pour conserver les paramètres établis.

POINTEUR DE KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager vous permet d'utiliser facilement vos Comptes. Le pointeur de Kaspersky Password Manager permet de sélectionner rapidement une application / une page Web dans laquelle vous souhaitez introduire des données personnelles.

Lors du lancement d'une application / d'une page Web, Kaspersky Password Manager recherche automatiquement un Compte associé à la base de mots de passe. En cas de recherche fructueuse, les données personnelles sont automatiquement introduites dans les champs d'authentification. Si aucun Compte n'est trouvé, Kaspersky Password Manager vous propose de l'ajouter. La recherche des champs contenant un Identifiant ou un mot de passe est automatique. Lorsque la fenêtre de l'application / la page Web s'affiche, les champs sont automatiquement remplis avec les données retrouvées dans la base de mots de passe. Il ne vous reste qu'à remplir les champs vides.

Pour lancer Kaspersky Password Manager, procédez comme suit :

1. Déplacez le curseur de la souris sur l'icône Kaspersky Password Manager dans la zone de notification de la barre des tâches et patientez quelques secondes.
2. Une fois que le pointeur de Kaspersky Password Manager apparaît, déplacez-le dans la fenêtre de l'application / sur la page Web souhaitée. Kaspersky Password Manager détermine automatiquement l'action à exécuter pour l'application / la page Web sélectionnée.

VERSION PORTABLE DE KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager permet de sauvegarder tous vos mots de passe sur un support amovible (par exemple une unité de mémoire flash ou un téléphone portable si celui-ci peut être utilisé comme unité de mémoire flash). De cette manière, vous pouvez utiliser Kaspersky Password Manager sur des ordinateurs publics (par exemple dans un cybercafé ou une bibliothèque). Dès que le périphérique amovible est connecté à l'ordinateur public, Kaspersky Password Manager se lance automatiquement. Vos données personnelles sont très bien protégées car la version portable ne nécessite pas

d'installation ou de configuration préalable. Dès que le support amovible est déconnecté, Kaspersky Password Manager se ferme automatiquement en ne laissant aucune trace de vos données sur l'ordinateur public.

La version portable de l'application est créée sur votre ordinateur où est installée la version complète de Kaspersky Password Manager. La version portable de l'application possède toutes les fonctions de Kaspersky Password Manager.

Pour garantir le bon fonctionnement de la version portable de l'application, il est recommandé, pour autant que cela soit possible, d'installer une module complémentaire pour navigateur Internet sur l'ordinateur public.

Il est possible d'installer le module externe de plusieurs manières :

- depuis l'assistant d'installation du module externe. Pour ce faire, suivez les étapes de l'assistant d'installation du module externe qui se lance lors du premier démarrage de la version portable de Kaspersky Password Manager.

- depuis le menu du Bouton d'accès rapide situé dans la fenêtre du navigateur Internet. Pour ce faire, sélectionnez l'entrée **Module externe de remplissage automatique non installé** dans le menu du bouton d'accès rapide.

L'assistant d'installation de la version portable de Kaspersky Password Manager se lance automatiquement lors du premier démarrage sur l'ordinateur public. Vous avez alors la possibilité de modifier certains paramètres avancés de la version portable :

- créer sur le bureau un raccourci vers la version portable - permet de lancer ultérieurement le programme depuis le bureau de l'ordinateur en cours d'utilisation ;

- utiliser le Clavier virtuel – affiche un Clavier virtuel pour l'introduction des données personnelles.

Pour créer une version portable de Kaspersky Password Manager, procédez comme suit :

1. Dans le menu contextuel de Kaspersky Password Manager, sélectionnez l'entrée **Version portable**.

2. Dans la boîte de dialogue **Assistant de création de la version portable**, cliquez sur le bouton **Suivant** et sélectionnez ensuite dans la liste le périphérique sur lequel sera installée la version portable de Kaspersky Password Manager. Cliquez ensuite sur le bouton **Suivant**.

3. En fonction de l'action à effectuer, procédez comme suit :

   - pour mettre à jour la base de mots de passe sur le support amovible, cochez la case **Copier la base de mots de passe actuelle sur le disque amovible** ;

   - pour copier les dernières copies de sauvegarde, cochez la case **Copier les <quantité sélectionnée> dernières sauvegarde sur le disque amovible** et spécifiez le nombre de copies ;

   - pour éviter de devoir introduire le Mot de passe principal pour accéder à la version portable de Kaspersky Password Manager, cochez la case **Ne jamais demander le Mot de passe principal (déconseillé)**.

4. Cliquez sur le bouton **Installer**. Une fois l'installation achevée, cliquez sur le bouton **Terminer**.

   Pour revenir à l'étape précédente de l'installation, cliquez sur le bouton **Précédent**. Si vous souhaitez annuler la création de la version portable, cliquez à n'importe quelle étape sur le bouton **Annuler**.

Pour configurer les paramètres de la version portable de l'application lors du premier démarrage sur un ordinateur, procédez comme suit :

1. Connectez le périphérique amovible à l'ordinateur.

2. Lancez la version portable de Kaspersky Password Manager depuis le disque amovible sélectionné. Si l'option d'exécution automatique du système d'exploitation est active, la fenêtre **Disque amovible <intitulé du disque>** se lance automatiquement. Sélectionnez alors l'action **Démarrer le gestionnaire de mots de passe**.

3. Introduisez le Mot de passe principal dans la boîte de dialogue.

4. Pour garantir le bon fonctionnement de Kaspersky Password Manager, désactivez le gestionnaire de mots de passe de Microsoft Internet Explorer en cliquant sur le bouton **Oui** dans la boîte de dialogue.

5. Dans la boîte de dialogue, cochez la case ☑ en regard des paramètres avancés à modifier et cliquez ensuite sur le bouton **Terminer**.

Pour utiliser la version portable de l'application, procédez comme suit :

1. Connectez le périphérique amovible à l'ordinateur partagé.

2. Lancez la version portable de Kaspersky Password Manager depuis le disque amovible sélectionné. Si l'option d'exécution automatique du système d'exploitation est active, la fenêtre **Disque amovible <intitulé du disque>** se lance automatiquement. Sélectionnez alors l'action **Démarrer le gestionnaire de mots de passe**.

3. Introduisez le Mot de passe principal dans la boîte de dialogue.

KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux États-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches Anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les experts principaux de Kaspersky Lab siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malveillants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus® : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (États-Unis), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en ouvre et accompagnons les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez une réponse complète à vos questions.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
L'Encyclopédie des virus :	http://www.viruslist.com/fr
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

AVIS JURIDIQUE IMPORTANT À L'INTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT SUIVANT AVANT DE COMMENCER À UTILISER LE LOGICIEL.

LORSQUE VOUS CLIQUEZ SUR LE BOUTON D'ACCEPTATION DE LA FENÊTRE DU CONTRAT DE LICENCE OU SAISISSEZ LE OU LES SYMBOLES CORRESPONDANTS, VOUS CONSENTEZ À LIÉ PAR LES CONDITIONS GÉNÉRALES DE CE CONTRAT. **CETTE ACTION EST UN SYMBOLE DE VOTRE SIGNATURE, ET VOUS CONSENTEZ PAR LÀ À VOUS SOUMETTRE AUX CONDITIONS DE CE CONTRAT ET À ÊTRE PARTIE DE CELUI-CI, ET CONVENEZ QUE CE CONTRAT A VALEUR EXÉCUTOIRE AU MÊME TITRE QUE TOUT CONTRAT ÉCRIT, NÉGOCIÉ SIGNÉ PAR VOS SOINS.** SI VOUS N'ACCEPTEZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

APRÈS AVOIR CLIQUÉ SUR LE BOUTON D'ACCEPTATION DANS LA FENÊTRE DU CONTRAT DE LICENCE OU AVOIR SAISI LE OU LES SYMBOLES CORRESPONDANTS, VOUS POUVEZ VOUS SERVIR DU LOGICIEL CONFORMÉMENT AUX CONDITIONS GÉNÉRALES DE CE CONTRAT.

1. Définitions

1.1. On entend par **Logiciel** le logiciel et toute mise à jour, ainsi que tous les documents associés.

1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.

1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les « téléphones intelligents », les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.

1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, *« Vous »* signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme *« entité »,* sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limité, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.

1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.

1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patch, les modifications, les copies, les ajouts ou les packs de maintenance, etc.

1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

2. Concession de la Licence

2.1. Le Titulaire des droits convient par la présente de Vous accorder une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (« l'utilisation ») du Logiciel sur un nombre spécifié d'Ordinateurs pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions générales de ce Contrat (la « Licence ») et vous acceptez cette Licence :

Version de démonstration. Si vous avez reçu, téléchargé et/ou installé une version de démonstration du Logiciel et si l'on vous accorde par la présente une licence d'évaluation du Logiciel, vous ne pouvez utiliser ce Logiciel qu'à des fins d'évaluation et pendant la seule période d'évaluation correspondante, sauf indication contraire, à compter de la date d'installation initiale. Toute utilisation du Logiciel à d'autres fins ou au-delà de la période d'évaluation applicable est strictement interdite.

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre de licences que vous avez obtenues auprès du Titulaire des

droits, *sachant que,* sauf disposition contraire du contrat de licence, chaque licence achetée vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acheté sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.

2.3. Si le Logiciel a été acheté sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'achat de la Licence du Logiciel.

2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.

2.5. Vous pouvez transférer la licence non exclusive d'utilisation du Logiciel à d'autres personnes physiques ou morales dans la limite du champ d'application de la licence qui Vous est accordée par le Titulaire des droits, à condition que son destinataire accepte de respecter les conditions générales de ce Contrat et se substitue pleinement à vous dans le cadre de la licence que vous accorde le Titulaire des droits. Si Vous transférez intégralement les droits d'utilisation du Logiciel que vous accorde le Titulaire des droits, Vous devrez détruire toutes les copies du Logiciel, y compris la copie de sauvegarde. Si Vous êtes le destinataire du transfert d'une licence, Vous devez accepter de respecter toutes les conditions générales de ce Contrat. Si vous n'acceptez pas de respecter toutes les conditions générales de ce Contrat, Vous n'êtes pas autorisé à installer ou utiliser le Logiciel. Vous acceptez également, en qualité de destinataire de la licence transférée, de ne jouir d'aucun droit autre que ceux de l'Utilisateur final d'origine qui avait acheté le Logiciel auprès du Titulaire des droits.

2.6. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acheté sur un support physique) ou stipulée pendant l'achat (si le Logiciel a été acheté sur Internet) :

- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.

3.2. Si le Logiciel a été acheté sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.

3.3. Si le Logiciel a été acheté sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'achat.

3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.

3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.

3.6. Si vous avez acheté le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.

3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence d'utilisation du Logiciel sans rembourser le prix d'achat en tout ou en partie.

3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.

3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

4. Assistance technique

L'assistance technique décrite dans la Clause 2.6 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).

Service d'assistance technique : http://support.kaspersky.com

5. Recueil d'informations

5.1. Conformément aux conditions générales de ce Contrat, Vous consentez à communiquer au Titulaire des droits des informations relatives aux fichiers exécutables et à leurs sommes de contrôle pour améliorer Votre niveau de protection et de sécurité.

5.2. Pour sensibiliser le public aux nouvelles menaces et à leurs sources, et dans un souci d'amélioration de Votre sécurité et de Votre protection, le Titulaire des droits, avec votre consentement explicitement confirmé dans le cadre de la déclaration de recueil des données du réseau de sécurité Kaspersky, est autorisé à accéder à ces informations. Vous pouvez désactiver le réseau de sécurité Kaspersky pendant l'installation. Vous pouvez également activer et désactiver le réseau de sécurité Kaspersky à votre guise, à la page des options du Logiciel.

Vous reconnaissez par ailleurs et acceptez que toutes les informations recueillies par le Titulaire des droits pourront être utilisées pour suivre et publier des rapports relatifs aux tendances en matière de risques et de sécurité, à la seule et exclusive appréciation du Titulaire des droits.

5.3. Le Logiciel ne traite aucune information susceptible de faire l'objet d'une identification personnelle et ne combine les données traitées avec aucune information personnelle.

5.4. Si vous ne souhaitez pas que les informations recueillies par le Logiciel soient transmises au Titulaire des droits, n'activez pas ou ne désactivez pas le réseau de sécurité Kaspersky.

6. Limitations

6.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.

6.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.

6.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans la Clause 2.5 de ce Contrat.

6.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

6.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.

6.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.

6.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

7. **Garantie limitée et avis de non-responsabilité**

7.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que

possible après sa constation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.

7.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adaptés à Votre cas.

7.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.

7.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.6 de ce Contrat.

7.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.

7.6. LE LOGICIEL EST FOURNI « TEL QUEL » ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PARLA LÉGISLATION EN VIGUEUR, LE « COMMON LAW », LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

8. Exclusion et Limitation de responsabilité

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SERA LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT).

AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

9. Licence GNU et autres licences de tierces parties

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou

des portions de ceux-ci, et à accéder au code source (« Logiciel libre »). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel. Si une licence de Logiciel libre devait exiger que le Titulaire des droits accorde des droits d'utilisation, de reproduction ou de modification du programme de logiciel libre plus importants que les droits accordés dans le cadre de ce Contrat, ces droits prévaudront sur les droits et restrictions énoncés dans les présentes.

10. Droits de propriété intellectuelle

10.1 Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des Etats-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les « Marques de commerce »). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

10.2 Vous convenez que le code source, le code d'activation et/ou le fichier clé de licence sont la propriété exclusive du Titulaire des droits et constituent des secrets industriels dudit Titulaire des droits. Vous convenez de ne pas modifier, adapter, traduire le code source du Logiciel, de ne pas en faire l'ingénierie inverse, ni le décompiler, désassembler, ni tenter de toute autre manière de découvrir le code source du Logiciel.

10.3 Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

11. Droit applicable ; arbitrage

Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 11 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

12. Délai de recours.

Aucune action, quelle qu'en soit la forme, motivée par des transactions dans le cadre de ce Contrat, ne peut être intentée par l'une ou l'autre des parties à ce Contrat au-delà d'un (1) an à la suite de la survenance de la cause de l'action, ou de la découverte de sa survenance, mais un recours en contrefaçon de droits de propriété intellectuelle peut être intenté dans la limite du délai statutaire maximum applicable.

13. Intégralité de l'accord ; divisibilité ; absence de renoncement.

Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions

générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en equity de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

14. Service clientèle

Si vous souhaitez joindre le Titulaire des droits pour toute question relative à ce Contrat ou pour quelque raison que ce soit, n'hésitez pas à vous adresser à notre service clientèle aux coordonnées suivantes :

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie
Tél. :+7-495-797-8700
Fax : +7-495-645-7939
E-mail : info@kaspersky.com
Site Internet : www.kaspersky.com