

McAfee Encrypted USB

Protection des données mobiles grâce aux périphériques McAfee® Encrypted USB

Des lecteurs USB de très petite taille mais de grande capacité permettent au personnel de transporter partout de grandes quantités de données d'entreprise confidentielles. Malheureusement, même les employés les mieux intentionnés ignorent souvent les coûts et les risques de sécurité élevés que la perte ou le vol de ces lecteurs fait courir à leur entreprise. Qui plus est, la majeure partie des lecteurs et clés USB n'est ni contrôlée ni gérée par le service informatique, et encore moins couverte par la stratégie de sécurité de l'entreprise, ce qui accroît le risque d'accès non autorisé, de fuites de données et de non-respect des exigences réglementaires. Dans les environnements mobiles actuels, il est vital d'intégrer le contrôle et la gestion des périphériques USB à la stratégie de sécurité d'entreprise pour garantir la sécurité des données.

Principaux avantages

- Conformité aux stratégies de sécurité de l'entreprise, aux lois relatives à la confidentialité des données et aux réglementations sectorielles grâce à l'utilisation de périphériques USB avec chiffrement matériel
- Mobilité des données assurée sans compromettre les stratégies de sécurité
- Suivi et gestion des périphériques USB chiffrés à l'échelle de l'entreprise via la plate-forme McAfee ePO pour bénéficier des fonctionnalités automatisées d'audit, de surveillance, d'administration des stratégies et de génération de rapports de sécurité
- Contrôle de l'accès aux données grâce à une authentification à deux ou à trois niveaux
- Sécurisation des données grâce à des validations et à des algorithmes de chiffrement de premier plan, dont AES-256 et FIPS 140-2, pour une protection robuste

Sécurisation des données

Toutes les informations copiées sur les périphériques McAfee Encrypted USB sont chiffrées et peuvent uniquement être lues par les personnes autorisées. Un contrôle d'accès utilisateur intégré et un chiffrement matériel des données puissants garantissent la sécurité des données sensibles, où qu'elles soient.

Gestion centralisée

Le déploiement et la gestion des périphériques de stockage portables au sein d'une entreprise peuvent s'avérer complexes et onéreux. Les lecteurs et clés USB n'étant généralement pas gérés par le service informatique, ils sont rarement couverts par les stratégies de sécurité de l'entreprise. La plate-forme McAfee ePolicy Orchestrator® (McAfee ePO™) offre une solution à ces problèmes en permettant le déploiement et la gestion centralisés des périphériques McAfee Encrypted USB depuis une console unique, ce qui améliore la sécurité de l'entreprise tout en réduisant le coût total de possession. Il suffit pour cela que les utilisateurs initialisent les périphériques en les branchant sur un ordinateur managé par McAfee ePO.

Chiffrement matériel puissant

Toutes les données stockées sur des périphériques McAfee Encrypted USB sont chiffrées à l'aide des plus puissants algorithmes de chiffrement matériel standard disponibles (notamment AES-256) et des certifications reconnues par le secteur telles que FIPS 140-2 (Federal Information Processing Standards).

Grâce aux fonctionnalités intégrées de chiffrement matériel, de génération de clés et de stockage de certificats, il est impossible d'obtenir ou de copier les clés de chiffrement puisqu'elles ne quittent jamais le périphérique USB. Il est en outre possible de stocker d'autres clés de chiffrement et/ou des certificats d'infrastructure de clés publiques (PKI).

Pour accéder aux données stockées sur les périphériques McAfee Encrypted USB, les utilisateurs doivent s'authentifier à l'aide d'un mot de passe ou d'une empreinte digitale, ce qui empêche les accès non autorisés aux données. Pour une sécurité optimale, une authentification à deux niveaux peut être utilisée. Si l'utilisateur a oublié le mot de passe ou s'il n'est pas en mesure d'effectuer une authentification biométrique, il peut aisément accéder aux données par le biais d'une réinitialisation centralisée du mot de passe ou de la fonction d'autorécupération proposée par le logiciel McAfee ePO.

Démonstration de la conformité réglementaire

Dans la mesure où ils sont intégrés avec la console de gestion McAfee ePO, les périphériques McAfee Encrypted USB soutiennent vos efforts en matière de conformité aux stratégies de sécurité de l'entreprise, aux réglementations sectorielles ou encore aux lois relatives à la confidentialité des données. Vous pouvez prouver que les données stockées sur un périphérique USB perdu ou volé étaient chiffrées, et générer des rapports détaillant les accès aux données et l'utilisation du périphérique USB à des fins d'audit.

Spécifications

Remarque : la configuration système varie en fonction des périphériques choisis par votre entreprise.

McAfee Encrypted USB Standard

- Systèmes d'exploitation : Microsoft Windows XP, Windows Vista et Windows 7 (32 et 64 bits)
- Matériel : capacité de stockage de 1 à 64 Go

McAfee Encrypted USB Bio

- Systèmes d'exploitation : Microsoft Windows XP, Windows Vista et Windows 7 (32 et 64 bits) ; Mac OS 10.5 et 10.6¹
- Matériel : capacité de stockage de 1 à 64 Go

McAfee Encrypted USB Hard Disk

- Systèmes d'exploitation : Microsoft Windows XP, Windows Vista et Windows 7 (32 et 64 bits) ; Mac OS 10.5 et 10.6³
- Matériel : capacité de stockage de 250 à 750 Go

McAfee Encrypted USB Hard Disk Non-Bio

- Systèmes d'exploitation : Microsoft Windows XP, Windows Vista et Windows 7 (32 et 64 bits)
- Matériel : capacité de stockage de 250 à 750 Go

Principales caractéristiques

- Implémentation d'un contrôle d'accès robuste pour le stockage sur périphérique USB amovible et chiffrement matériel des données à l'aide d'AES-256 (Advanced Encryption Standard)
- Définition d'un nombre maximal de tentatives de saisie du mot de passe ou d'authentification biométrique pour contrer les attaques en force avec des options de restauration utilisateur ou de destruction des données
- Souplesse maximale grâce à une technologie sans client, et sécurité garantie indépendamment du système d'exploitation ; aucune installation de logiciel ni aucun droit d'administrateur ne sont requis, un port USB suffit
- Blocage des accès non autorisés aux données grâce à une authentification à deux niveaux nécessitant que les utilisateurs s'authentifient à l'aide d'un mot de passe ou d'une empreinte digitale
- Installation et exécution d'applications directement et en toute sécurité à partir du périphérique USB (de type « computer-on-a-Stick », navigateur Internet, client léger, etc.)² ; les utilisateurs peuvent exécuter des applications en toute simplicité et de façon sûre, où qu'ils soient

- Génération de clés de chiffrement intégrée et stockage de certificats, qui empêchent de copier ces clés puisqu'elles ne quittent jamais la clé USB ; et possibilité de stocker d'autres clés de chiffrement et/ou des certificats d'infrastructure de clés publiques (PKI)
- Protection intégrée contre les logiciels malveillants (*malwares*) des lecteurs et clés USB, ainsi que des ordinateurs et réseaux auxquels ils se connectent, grâce à un moteur d'analyse antimalware qui détecte et bloque automatiquement les menaces véhiculées par les périphériques USB (plate-forme de gestion McAfee ePO requise)

Périphériques McAfee Encrypted USB

Le tableau ci-dessous répertorie les principales caractéristiques des périphériques de la gamme McAfee Encrypted USB. La capacité de stockage s'étend de 1 à 64 Go pour les clés USB et de 250 à 750 Go pour les disques durs USB.

Tableau de synthèse des fonctionnalités

	McAfee Encrypted USB Standard	McAfee Encrypted USB Bio	McAfee Encrypted USB Hard Disk Non-Bio	McAfee Encrypted USB Hard Disk
Mot de passe ou authentification par carte CAC/PIV	●	●	●	●
Authentification biométrique		●		●
Chiffrement matériel AES-256	●	●	●	●
Possibilité de virtualisation (de type « computer-on-a-Stick ») ²	En option	En option	En option	En option
Certification FIPS 140-2	●	●	●	●
Gestion centralisée via McAfee ePolicy Orchestrator (McAfee ePO)	●	●	●	●
Protection antimalware de McAfee	●	●	●	●

¹ Prise en charge de Mac OS X pour les périphériques managés après initialisation sur un poste client Windows géré via McAfee ePO et pour les périphériques non managés uniquement dans le cadre d'une authentification biométrique (autonome, biométrique).

² Logiciel d'éditeur tiers requis entraînant des frais supplémentaires.

³ Prise en charge de Mac OS X pour les périphériques managés après initialisation sur un poste client Windows géré via McAfee ePO et pour les périphériques non managés uniquement dans le cadre d'une authentification biométrique (autonome, biométrique).

Pour en savoir plus sur les périphériques McAfee Encrypted USB, visitez notre site à l'adresse : www.mcafee.com/fr/products/data-protection/index.aspx.

