LIVRE BLANC

RDX® PowerEncrypt

Le chiffrement des données avec RDX PowerEncrypt garantit la sécurité des informations stockées sur les supports RDX lors de leur transfert ou de leur archivage hors site en les protégeant contre les accès non autorisés.

Présentation de RDX PowerEncrypt

Le chiffrement de données avec RDX PowerEncrypt peut être incorporé à n'importe quel support RDX. Les données inscrites sur les supports RDX sont chiffrées selon les normes XTS AES-256 et l'accès aux données est sécurisé au moyen d'une clé avec mot de passe déployée via le logiciel RDX Manager. En l'absence de clé d'accès, les données résidant sur le support RDX ne sont consultables par aucun utilisateur non autorisé, ce qui rend les données et le support inutilisables. Avec RDX PowerEncrypt, vous avez l'assurance que vos données sont parfaitement protégées.

L'accès aux supports RDX cryptés requiert l'installation de RDX Manager sur le système. RDX Manager facilite l'accès aux supports et aux données et incorpore des outils d'effacement, de partitionnement et de formatage. En outre, lors de l'utilisation de RDX Manager pour supprimer le chiffrement, un effacement sécurisé du support a lieu automatiquement.

La dernière version du logiciel RDX Manager incluant la fonctionnalité RDX PowerEncrypt est téléchargeable depuis la page Web du produit RDX QuikStor. Il est vivement conseillé d'installer RDX Manager lorsque les fonctionnalités RDX sont utilisées, afin de faciliter l'accès à toutes les fonctions RDX telles que l'éjection de support en toute sécurité, les changements de mode, la préparation de supports, les diagnostics, les mises à niveau de micrologiciel et, désormais, les fonctions RDX PowerEncrypt.

Valeur de PowerEncrypt

RDX PowerEncrypt apporte une valeur complémentaire intégrée aux unités SATA III RDX QuikStor utilisant les versions 0253 et ultérieures du micrologiciel. Sa disponibilité prochaine pour les autres lecteurs RDX est également prévue, conformément à notre plan de développement de produits.

La prise en charge de RDX PowerEncrypt est assurée par l'unité RDX SATA III certifiée FIPS 140-2. Les données résidant sur les supports RDX peuvent désormais être chiffrées en toute confiance pour chaque situation nécessitant une sécurisation des données. Les clients ayant besoin d'exploiter l'unité RDX SATA III en mode FIPS 140-2 peuvent commander un kit d'inviolabilité auprès d'Overland-Tandberg.

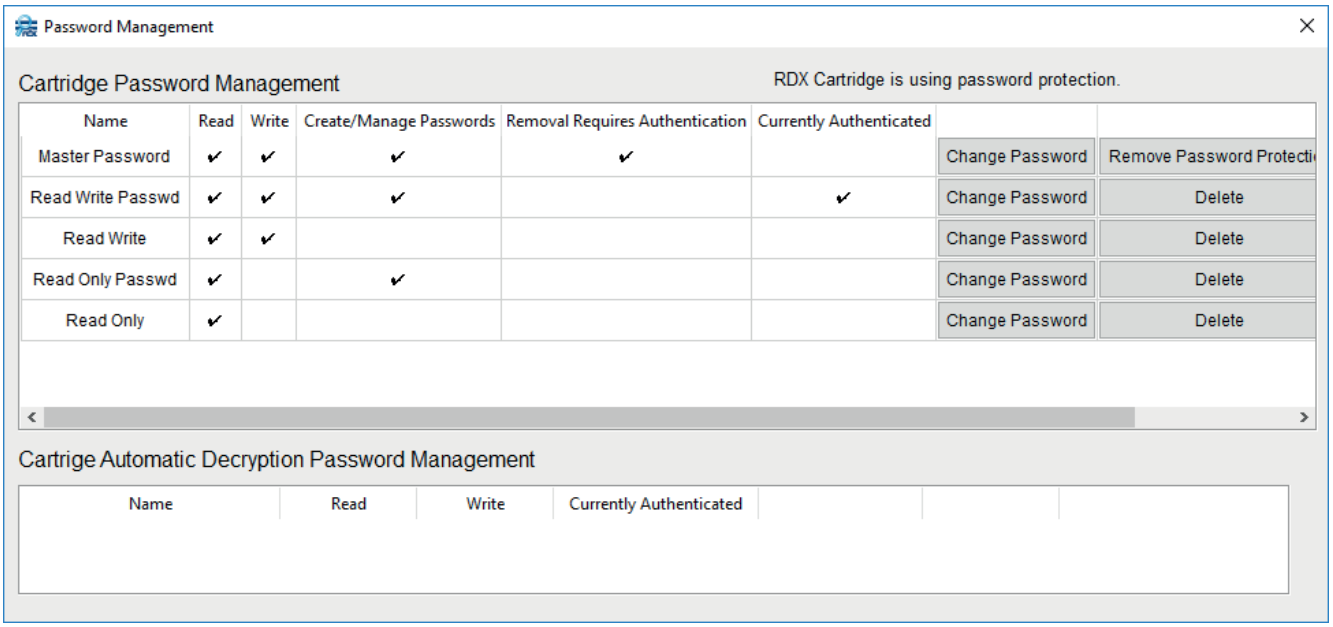
Modes de fonctionnement et options

RDX PowerEncrypt propose deux modes de protection des données : par mot de passe seul ou par mot de passe avec chiffrement.

Protection basique par mot de passe (sans chiffrement)

RDX PowerEncrypt prend en charge jusqu'à huit mots de passe avec quatre options de droit d'accès et capacités de gestion différentes. Ces quatre niveaux d'autorisation sont les suivants :

- Accès en lecture seule
- Accès en lecture seule avec gestion par mot de passe
- Accès en lecture/écriture
- Accès en lecture/écriture avec gestion par mot de passe



L'illustration indique les combinaisons de mots de passe utilisées dans la protection de base

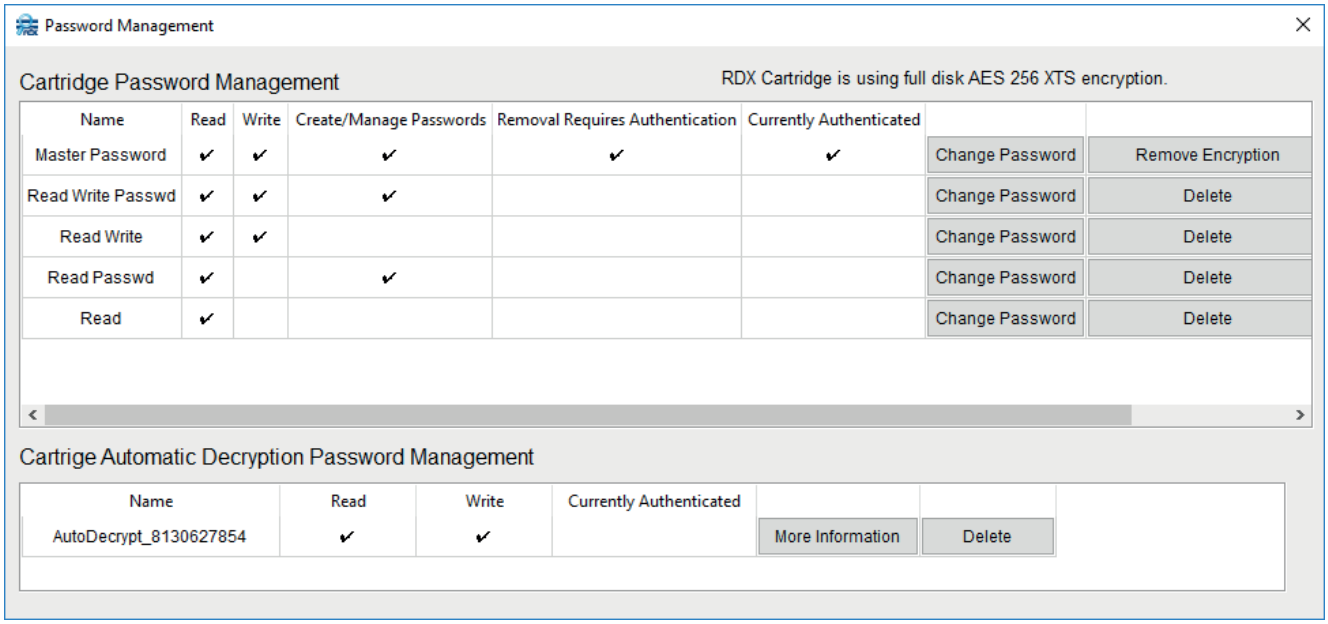
En outre, un mot de passe principal avec accès en lecture/écriture et gestion de mot de passe est automatiquement fourni. Ce mot de passe principal sert à administrer la protection des supports RDX.

RDX PowerEncrypt permet de déployer les options et fonctions sélectionnables pour différents clients ou membres du personnel de l'entreprise afin de sécuriser l'échange de données. Selon le niveau d'autorisation, les caractéristiques peuvent être grisées et non sélectionnables.

La configuration de l'accès aux données en lecture seule protège les données contre les virus et rançongiciels. Le mode lecture seule signifie que les données ne peuvent être modifiées, supprimées ou chiffrées par aucun utilisateur en l'absence du mot de passe approprié.

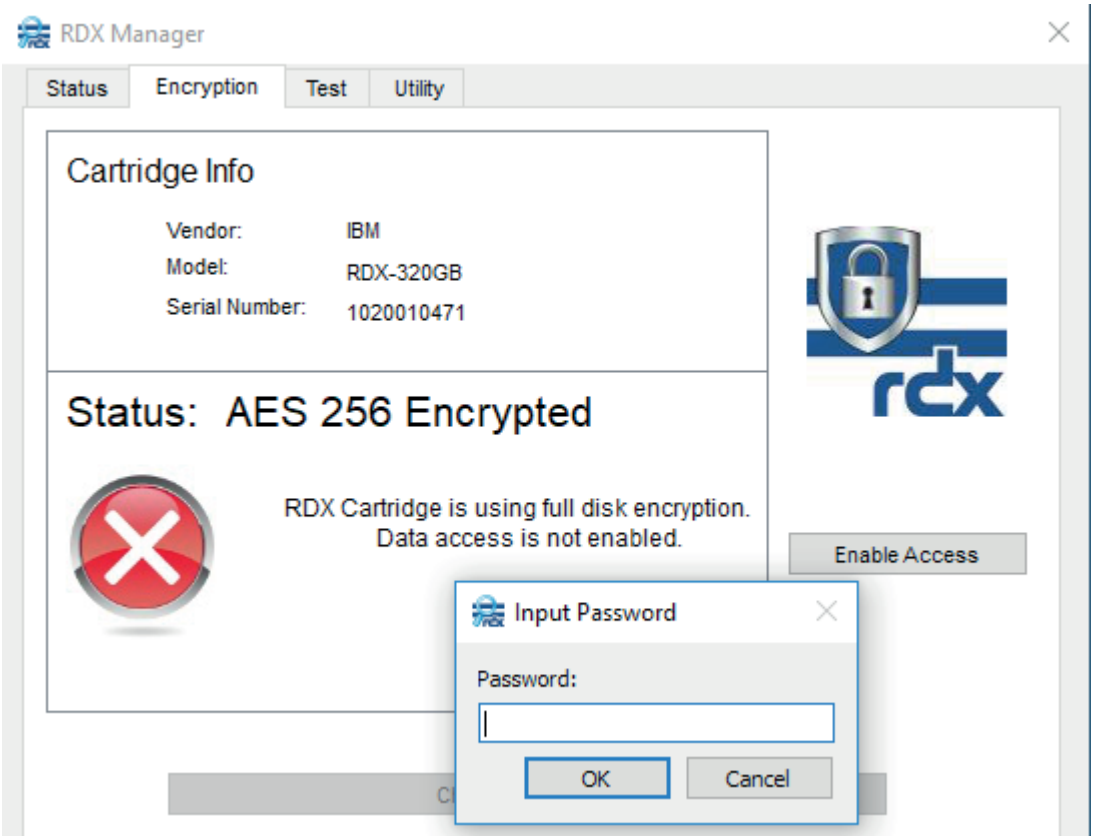
Chiffrement de disque intégral XTS AES-256

Outre la protection basique par mot de passe des supports RDX, le logiciel RDX PowerEncrypt permet de chiffrer les données à l'aide de l'algorithme XTS AES-256. Ce mode de chiffrement est hautement recommandé lorsque le support RDX est destiné à être stocké hors site ou délocalisé. Tout comme pour la fonction de protection basique par mot de passe RDX, jusqu'à huit mots de passe avec des droits d'accès aux données dédiés et une gamme de fonctions peuvent être assignés selon les niveaux d'accès.



L'illustration indique les combinaisons de mots de passe utilisées pour le chiffrement XTS AES-256

La facilité d'utilisation est renforcée par l'option de génération de mot de passe automatique pour les unités et supports RDX. Cette option autorise l'accès aux données dès l'insertion de la cartouche dans une unité configurée avec cette option. Cette fonctionnalité est idéale pour les situations de sauvegarde impliquant une rotation de supports, ou lors des récupérations de type BMR (Bare Metal Restore) ne permettant pas d'utiliser RDX Manager pour assurer la protection des données par mot de passe. Le mot de passe stocké sur l'unité est utilisable sur des composants RDX multiples afin de répartir les restaurations entre plusieurs cartouches RDX. Le mot de passe peut être extrait de l'unité à tout moment si nécessaire.



Si le décryptage automatique est désactivé, un mot de passe est requis pour accéder aux données contenues sur le support RDX

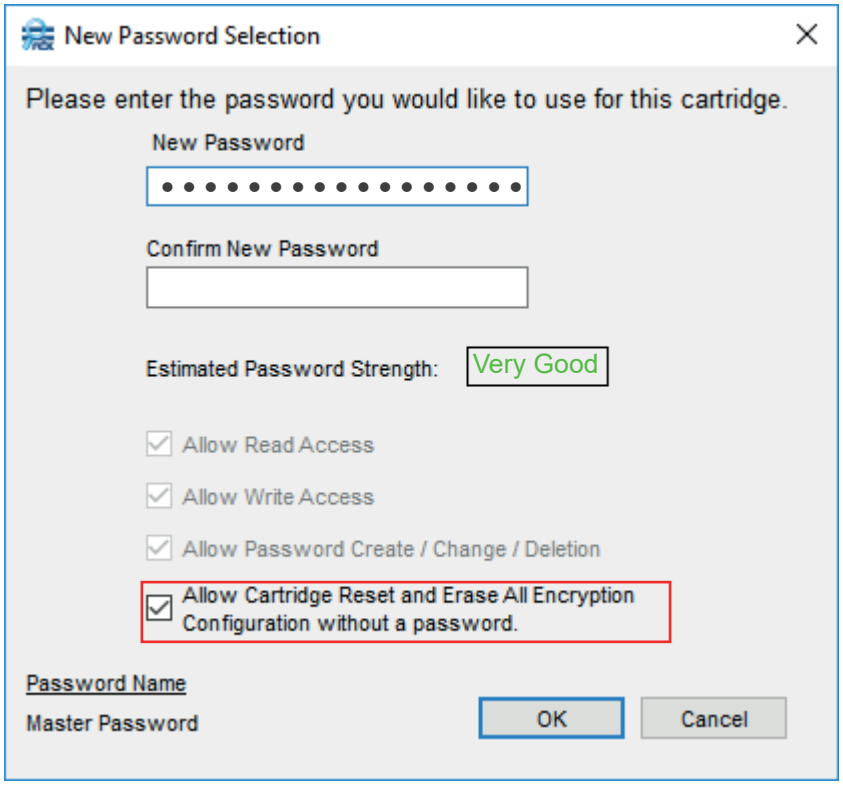
Autrement, lors du transfert de données inter-sites, l'accès automatique par les unités RDX serait permis par l'activation de l'option de mot de passe, tandis qu'un rejet automatique aurait lieu pour tout autre lecteur RDX sur lequel l'option de mot de passe n'a pas été activée. Cette configuration permet d'assurer que les données sont à la fois sécurisées et chiffrées sur votre support RDX. Un autre avantage pratique est la possibilité de dispenser les utilisateurs de saisir un mot de passe lorsque cette option est activée, ce qui permet un accès rapide aux données. Si le décryptage automatique est désactivé, un mot de passe est requis pour accéder aux données contenues sur le support RDX.

Considérations relatives aux mots de passe

Pour des raisons de sécurité, un mot de passe est exigé pour accéder aux données stockées sur un support RDX. En cas de perte ou d'oubli de ce mot de passe, les données contenues sur le support RDX chiffré deviennent inaccessibles à tout utilisateur.

Si la case ***Autoriser la réinitialisation de la cartouche et effacer toutes les configurations de chiffrement sans mot de passe*** n'est pas cochée et que vous perdez votre mot de passe, les données deviennent non seulement inaccessibles, mais le support RDX ne peut plus être reformaté et devient donc inutilisable. Veuillez noter que la perte de votre mot de passe n'est pas couverte par la garantie du support RDX.

La configuration d'un mot de passe fort est primordiale pour préserver la sécurité des données. Il est important de définir un mot de passe véritablement fort afin de déjouer les tentatives de décryptage par des pirates informatiques. Pour vous aider à créer un mot de passe fort, RDX PowerEncrypt analyse le mot de passe fourni et indique son niveau de puissance estimé (insuffisant, faible, correct, bon ou très bon).



Si la case n'est pas cochée et que le mot de passe a été oublié, le support devient inutilisable.

RDX PowerEncrypt évalue l'entropie d'un mot de passe d'après plusieurs algorithmes comprenant des mots communs, répétitions de caractères, formats de date, substitutions numériques (leet speak) et dispositions de clavier.

Pour définir un mot de passe fort dans RDX PowerEncrypt, nous vous recommandons d'appliquer les règles suivantes :

- Utilisez au moins six mots n'ayant aucun rapport entre eux
- Employez des majuscules placées de manière aléatoire dans les mots (par exemple la deuxième lettre de chaque mot)
- Symboles et chiffres comme séparateurs entre les mots

À titre de règle de bonne pratique, utilisez une phrase comportant au moins 6 mots.

En raison des progrès technologiques (processeurs plus rapides, attaques par force brute et par dictionnaire), le craquage de mots de passe devient de plus en plus facile. Aujourd'hui, les ordinateurs les plus puissants sont capables d'envoyer quelque 1 014 clés par seconde, et ce nombre ne peut qu'augmenter à l'avenir. Pour contrer cette évolution, RDX PowerEncrypt n'autorise qu'une seule tentative par seconde, ce qui ramène toutes les tentatives de craquage de mots de passe à un rythme de 60 tentatives par minute. Cette fonctionnalité réduit considérablement les risques de découverte d'un mot de passe sécurisé, et rend le logiciel si robuste qu'il peut même résister aux techniques d'attaque parallèles employées par les pirates pour réduire le temps de craquage.

Certification FIPS 140-2

La norme FIPS (Federal Information Processing Standard) 140 a été publiée par le NIST (National Institute of Standards and Technology) afin de coordonner les exigences et les normes des modules cryptographiques reposant à la fois sur des composants matériels et logiciels.

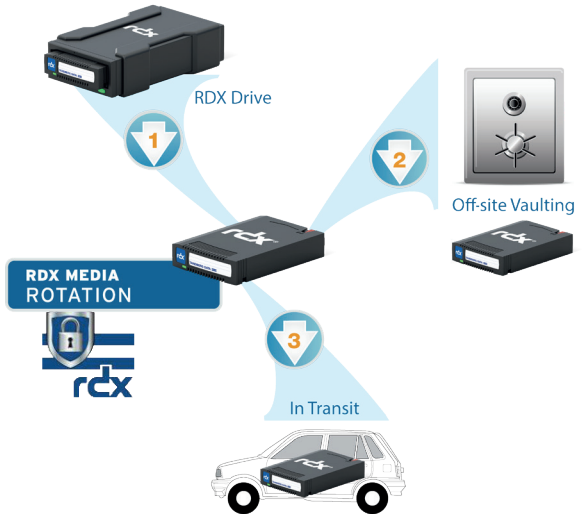
Le logiciel RDX PowerEncrypt utilise l'unité RDX SATA III certifiée FIPS 140-2 pour répondre aux normes des modules cryptographiques. Cette certification permet à l'unité RDX SATA III et au logiciel RDX PowerEncrypt de répondre aux exigences de provisionnement légales et de préserver la confidentialité et l'intégrité des informations protégées par le module.

La validation conformément à la norme FIPS 140-2 garantit que l'unité RDX SATA III et le logiciel RDX PowerEncrypt s'appuient sur des pratiques de sécurité robustes telles que des algorithmes et méthodes de chiffrement forts. Cette certification spécifie également le mode d'accréditation des individus ou processus, ainsi que la sécurisation des interactions des modules et composants avec d'autres systèmes. Pour être conformes à la norme FIPS 140-2, l'unité RDX SATA III et le logiciel RDX PowerEncrypt doivent respecter les exigences de conception et de mise en œuvre établies, et être testés et approuvés par l'un des 13 laboratoires indépendants accrédités par le NIST.

Applications

Sauvegarde et archivage

RDX PowerEncrypt est le choix idéal pour toutes les applications de sauvegarde et d'archivage. L'amovibilité du support RDX permet d'entreposer les sauvegardes hors site à des fins de récupération après sinistre et d'archivage, et d'appliquer un schéma de rotation des supports.



Pour protéger les sauvegardes contre l'accès non autorisé en cas de stockage délocalisé, RDX PowerEncrypt assure le plus haut niveau de protection et de sécurité des données sur l'ensemble des sauvegardes et archivages. La fonction d'accès par mot de passe automatique facilite l'usage du support chiffré en cas de récupération BMR.

Le support RDX garantit une capacité d'archivage à long terme éprouvée sur plus de 10 années et représente une solution idéale pour répondre aux exigences réglementaires et de conformité.

Avec RDX PowerEncrypt, vos données sont en sécurité et ne peuvent en aucun cas être lues, modifiées ou supprimées sans autorisation d'accès.

Nouvelles réglementations gouvernementales sur la protection des données

De nouvelles législations apparaissent, telles que le Règlement général sur la protection des données (RGPD). Le RGPD régit la manière dont les données personnelles des clients, fournisseurs et employés doivent être traitées, transformées et sécurisées dans notre monde numérisé afin de garantir la protection de la vie privée.

L'article 23 du RGPD concerne la restriction de l'accès aux données personnelles aux seuls individus en charge du traitement des données, exigeant ainsi que les données soient protégées contre tout accès non autorisé.

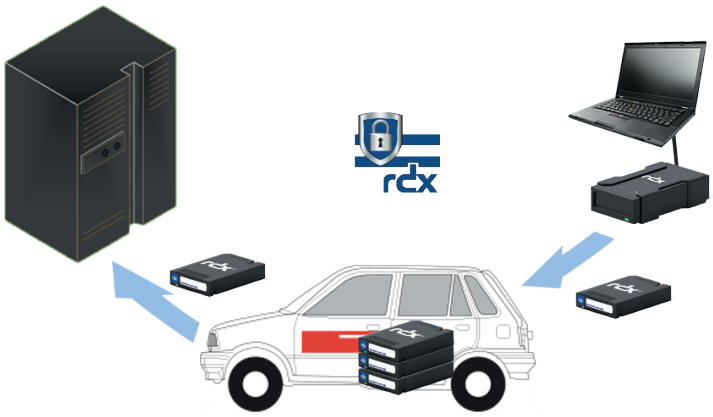
L'article 32, paragraphe 1 du RGPD décrit la sécurisation des données personnelles par l'emploi du chiffrement.

L'article 34, paragraphe 3 du RGPD décrit la manière dont les violations de données doivent être communiquées sans délai, sauf lorsque les données sont chiffrées. Grâce au chiffrement RDX, aucune communication de ce type n'est nécessaire.

Toutes ces fonctionnalités font partie intégrante du logiciel RDX PowerEncrypt. Le contrôle d'accès est garanti par les différents niveaux de droits d'accès avec protection par mot de passe, tandis que le chiffrement des données garantit un niveau de sécurité maximal.

Transfert et échange de données

La conception robuste du support RDX facilite son transport. Les cassettes RDX résistent aux vibrations, aux environnements hostiles et aux chutes d'une hauteur maximale d'un mètre sur un sol en béton. Les supports RDX peuvent être livrés aisément via les services postaux ou de transport classiques. L'ensemencement de données intensif depuis ou vers des ressources cloud représente un défi, compte tenu des taux de transfert des réseaux actuels. Une alternative aux faibles taux de transfert rencontrés sur les réseaux locaux ou étendus consiste à connecter le système RDX à un serveur local afin de bénéficier d'un débit beaucoup plus élevé.



De même, pour consolider les données volumineuses des multiples succursales vers un centre de données, la grande capacité du support RDX est une solution plus viable que les transferts en réseau.

En cas de vol du support RDX durant un transit, les données non chiffrées contenues sur ce support peuvent être accessibles. Les données sensibles des entreprises ou des instances publiques doivent être protégées. Le logiciel RDX PowerEncrypt constitue une solution puissante pour garantir leur protection.

Conclusion

Grâce à sa facilité d'administration et à ses fonctionnalités complètes, RDX PowerEncrypt peut être mis en oeuvre sur un large éventail d'applications individuelles, de PME ou de grandes entreprises. Cette fonctionnalité intégrée de protection par mot de passe est incluse sur les unités SATA III RDX QuikStor. PowerEncrypt RDX garantit le plus haut niveau de confiance en matière de protection des données grâce au chiffrement XTS AES-256, leader du marché et conforme aux exigences réglementaires, ainsi qu'à ses options de contrôle d'accès.

Certifié conforme aux normes de cryptographie FIPS 140-2, le logiciel RDX PowerEncrypt est une solution compatible avec les exigences des instances sectorielles internationales de réglementation en charge de la sécurité des données. RDX PowerEncrypt est compatible avec une large gamme d'applications, dont la sauvegarde, la restauration, l'archivage, le transport et l'échange de données.

RDX PowerEncrypt est actuellement disponible pour les unités de disque dur SATA III RDX QuikStor configurées avec le niveau de micrologiciel 0253 ou supérieur, ainsi qu'avec le nouveau logiciel utilitaire RDX Manager. Conformément à notre plan de développement étendu, il sera bientôt disponible pour d'autres produits RDX.

WP_v1_jun27_2019