

Encryption DataPort User's Manual



Manuel d' utilisation



www.CRU-DataPort.com

À propos de CRU-DataPort

Fondée en 1986 et implantée à Vancouver, dans l'État de Washington, la société CRU-DataPort développe et commercialise des périphériques de sécurité et de stockage des données informatiques. Avec plus de 2 000 000 unités installées de par le monde, DataPort™, la marque de modules de stockage amovibles de la société, s'est imposée de fait comme un modèle en matière de sécurité des données et de modules de stockage amovibles pour les services gouvernementaux, le secteur de l'enseignement et les services informatiques des sociétés. Les ports d'accès sont définis pour 25 000 insertions et sont dotés de ventilateurs afin de protéger le lecteur de disque.

Les produits CRU-DataPort sont disponibles auprès des principaux distributeurs, fabricants de matériel informatique d'origine, distributeurs à valeur ajoutée ainsi que de nombreux revendeurs et intégrateurs de système dans le monde entier. Pour plus d'informations sur CRU-DataPort, visitez notre site Web à l'adresse www.CRU-DataPort.com.

Table des matières

À propos de CRU-DataPort	i
Description générale	1
À propos du cryptage	1
Fonctionnalité DES (de l'anglais Data Encryption Standard, Norme de cryptage des données)	1
Fonctionnalité TDES (de l'anglais Triple DES, Norme de cryptage triple des données)	1
Fonctionnalités de Encryption DataPort	1
Contenu du coffret Encryption DataPort V "Plus"	3
Avant toute installation	4
Installation du châssis	4
Installation du disque dur	6
Fonctionnement	8
Utilisation des clés de sécurité	8
Étapes à suivre pour faire fonctionner le système	9
Fonctions des voyants DEL	10
Alarme signalant une défaillance du ventilateur	10
Résolution des problèmes	11
Support technique	12
Garantie limitée du produit	12
Réclamations concernant le produit	12
Limitations de responsabilité	12

Description générale

Le module de stockage amovible CRU-DataPort permet de retirer facilement un disque dur de 3,5 po de votre ordinateur de bureau, de votre Macintosh, de votre poste de travail ou d'un sous-système de groupe de disques.

Il comprend un châssis et un support avec des protections inférieure et supérieure emboîtables. Le châssis peut être inséré dans n'importe quelle baie de lecteur d'une demi-hauteur de 5,25 po. Les modèles DataPort sont compatibles avec les interfaces Serial ATA, IDE et SCSI, et peuvent être configurés de façon à disposer d'un verrou à clé ou d'un loquet. Il existe également des modèles Encryption DataPort pour l'interface IDE, avec plusieurs niveaux de puissance de clé de cryptage (40, 64, 128 et 192 bits).

À propos du cryptage

Fonctionnalité DES (de l'anglais Data Encryption Standard, Norme de cryptage des données)

Le module Encryption DataPort V "Plus" utilise l'algorithme DES ou TDES pour crypter tout le disque dur. Un algorithme DES avec une clé électronique secrète à 64 bits est appelé un crypteur. Il code mathématiquement les données initiales à l'aide de sa clé électronique secrète à 64 bits (ou supérieure). Le résultat d'un cryptage DES est appelé texte crypté. Une opération DES inverse est appelée décryptage. Toutefois, pour récupérer les données initiales lors d'une procédure de décryptage, il faut utiliser une clé électronique secrète appropriée (avec une correspondance de bit à bit). Si la clé utilisée pour le décryptage n'est pas la bonne, les données seront illisibles.

Fonctionnalité TDES (de l'anglais Triple DES, Norme de cryptage triple des données)

L'algorithme Triple DES (ou TDES) consiste en trois (3) opérations DES successives. À la première étape, l'algorithme DES crypte les données avec une clé électronique secrète (clé 1). À la deuxième étape, les données cryptées lors de la première étape sont traitées avec une deuxième clé électronique secrète (clé 2). À la troisième étape, les données de la deuxième étape sont cryptées avec une troisième clé électronique secrète (clé 3).

Fonctionnalités de Encryption DataPort

Félicitations pour l'achat du produit CRU-DataPort Encryption DataPort V "Plus". Vous possédez maintenant un système à haute performance pour le cryptage et le contrôle de l'accès, lequel vous permettra de protéger la confidentialité de vos données. La technologie de pointe proposée par Encryption DataPort V "Plus" offre une protection équivalente à celle utilisée par les forces armées des États-Unis. Le système Encryption DataPort V "Plus" dispose d'un processeur en temps réel pour crypter tout le contenu du disque dur, bit par bit, y compris le secteur d'amorçage, les fichiers temporaires, les fichiers d'échange et le système d'exploitation, sans ralentir les performances.

Le système Encryption DataPort V "Plus" est totalement transparent pour les utilisateurs ; il n'y a aucune commande ni interface utilisateur graphique à prendre en considération. Le système est extrêmement rapide et capable de traiter des opérations au rythme de 1,6 giga-octets par seconde sans accaparer un surplus de temps du processeur et de ressources système. En outre, le système fonctionne sous tous les systèmes d'exploitation et ne requiert aucun pilote de périphérique.

Le système Encryption DataPort V "Plus" utilise un moteur de cryptage et de décryptage en temps réel basé matériel DES à 64 bits et TDES à 128/192 bits certifié par NIST (National Institute of Standards and Technology, l'institut national des normes en technologie). Ces algorithmes sont garantis de fournir une sécurité fiable ; il est quasiment impossible de deviner ou de trouver par déduction la clé TDES correcte pour accéder aux données cryptées. Étant donné que tout le contenu du disque est crypté, vos données sont en sécurité même si des intrus essaient d'amorcer le système à partir de leur propre disque ou de transférer les données de votre disque sur une machine non protégée.

Le système Encryption DataPort V "Plus" a été conçu pour fonctionner avec des châssis standard DataPort V & V "Plus" (version IDE). Comme le moteur de cryptage du matériel se trouve sur le support, un support comportant un lecteur crypté peut être utilisé avec des châssis DataPort V et V "Plus" existants qui sont déjà installés. Le support et la clé de sécurité (qui fournit le code électronique secret) utilisée pour crypter le disque dur peuvent être utilisés dans plusieurs châssis DataPort V ou V "Plus", de sorte qu'un support comportant un disque dur crypté peut facilement être utilisé avec plusieurs ordinateurs. De plus, plusieurs utilisateurs peuvent en toute sécurité utiliser le même ordinateur en ayant chacun leur propre support Encryption DataPort V "Plus" avec une clé de sécurité unique. La conception du système Encryption DataPort V "Plus" vous permet de crypter vos données tout en conservant la mobilité et la sécurité fournies par votre DataPort.

Contenu du coffret Encryption DataPort V "Plus"

Le coffret DataPort inclut tout le matériel nécessaire à l'installation d'un disque dur de 3,5 po dans une baie de lecteur de 5,25 po. Avant de procéder à l'installation, vérifiez si les éléments suivants sont bien inclus dans le coffret.

Quantité	Description
1	Ensemble du châssis DataPort V "Plus"
1	Ensemble du support DataPort V "Plus"
2	Protections métalliques
4	Vis à tête plate 6-32 x 3/8 po pour le montage du disque dur
4	Vis cruciforme à tête cylindrique M3 x 10 mm pour le montage du châssis
2	Clé de sécurité pour le cryptage (un double de la clé)
2	Clé pour le verrou à clé

Si l'un des éléments indiqués ci-dessus est absent du coffret ou si vous avez besoin de pièces spéciales, contactez votre revendeur ou CRU-DataPort pour obtenir les instructions nécessaires en cas de remplacement de pièces ou pour assistance. Vous pouvez commander des supports ou des châssis Encryption DataPort supplémentaires pour plusieurs systèmes de lecteurs.

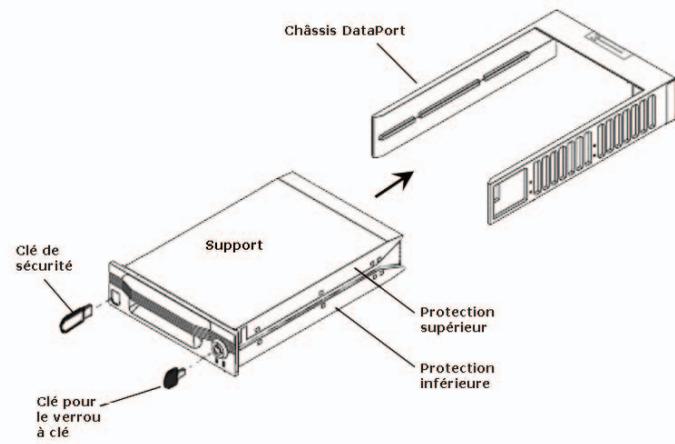


Figure 1 - Contenu du coffret

Avant toute installation

1. Avant d'installer ou d'utiliser le périphérique DataPort, lisez attentivement ce manuel afin d'éviter toute perte de données.
2. Touchez une partie métallique du châssis de l'ordinateur avant de toucher tout équipement électrique afin de décharger l'électricité statique qui pourrait endommager l'ordinateur. CRU-DataPort n'est en aucun cas responsable des dégâts causés par une décharge d'électricité statique.
3. Rassemblez les outils et les éléments nécessaires suivants :
 - Tournevis cruciforme
 - Petit tournevis pour vis à tête plate
 - Manuel d'utilisation de l'ordinateur
 - Manuel d'utilisation du lecteur de disque dur pour régler le cavalier principal

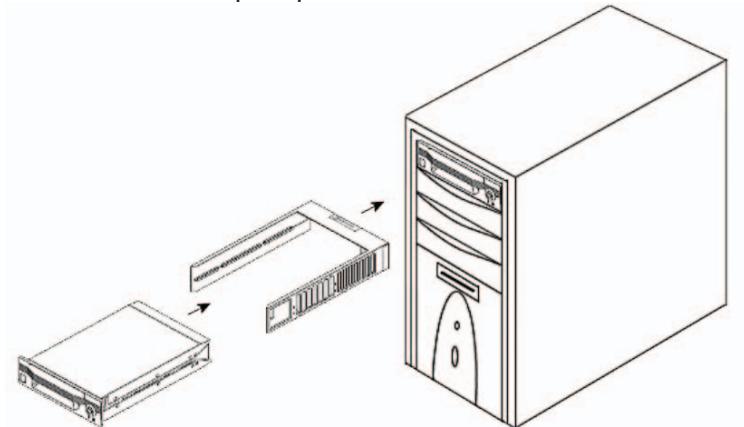


Figure 2 - Vue d'ensemble

Installation du châssis

1. Éteignez l'ordinateur et débranchez le câble d'alimentation de la prise électrique. Avant de commencer à travailler sur votre ordinateur, patientez une minute afin que toute énergie résiduelle se dissipe.
2. Retirez le couvercle de l'ordinateur.
3. Localisez une baie équipée d'un lecteur 5,25 po dotée d'un accès externe.
4. Si la baie du lecteur requiert des rails de montage, installez-en un de chaque côté du châssis. Les rails de montage doivent être fournis avec le système informatique.
5. Montez l'ensemble du châssis en insérant le châssis dans la baie 5,25 po. Fixez le châssis de manière sécurisée avec les vis fournies.

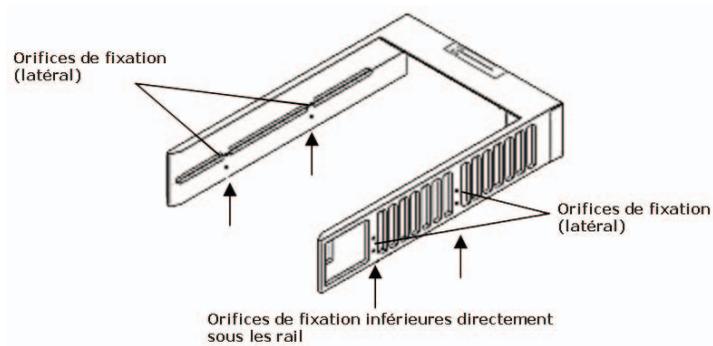


Figure 3 - Position des fentes de montage du châssis

6. Branchez un câble d'alimentation c.c. sur le châssis, trouvez un câble adéquat à 4 broches disponible sur le bloc d'alimentation de l'ordinateur et branchez-le sur la prise de courant femelle du châssis (voir Figure 4).
7. Branchez le câble des données sur le châssis.

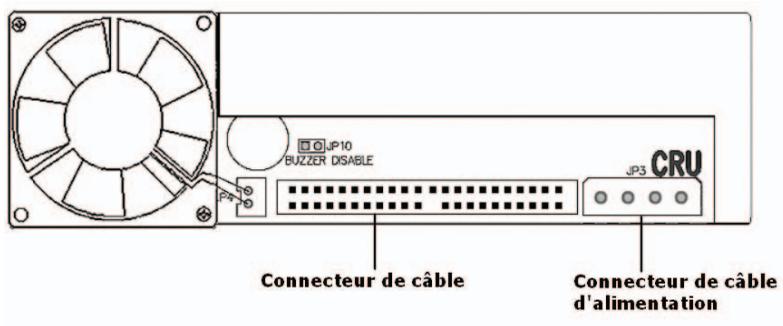


Figure 4 - Vue arrière du périphérique DataPort

L'installation du châssis est désormais terminée.

Installation du disque dur

IMPORTANT ! À lire avant d'effectuer l'installation.

Pour éviter toute perte de données, veuillez lire les sections suivantes avant d'installer votre système Encryption DataPort V "Plus".

Attention ! Veuillez toujours sauvegarder vos données avant d'installer tout matériel.

Pour installer le système Encryption DataPort V "Plus", vous devez formater votre disque dur. À la suite du formatage, toutes les données de votre disque dur seront perdues. Vous devez donc sauvegarder toutes les données que vous souhaitez garder avant de formater votre disque dur. Cette opération doit être effectuée avant d'installer votre lecteur de disque dur dans le système DataPort.

1. Retirez les protections supérieure et inférieure. Pour effectuer cette opération, utilisez l'outil fourni ou un petit tournevis pour vis à tête plate.

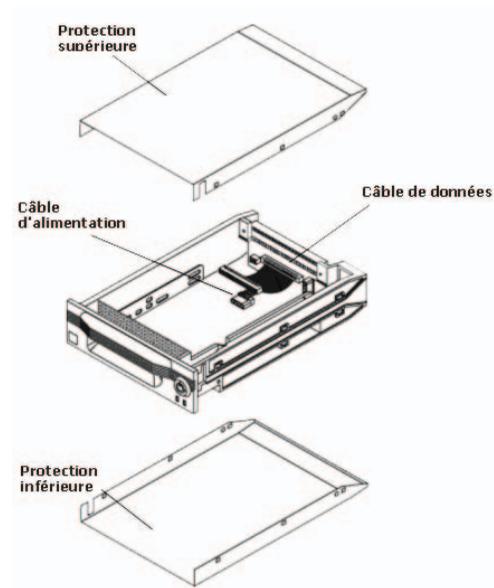


Figure 5 - Vue intérieure du support

- Configurez le cavalier maître/esclave sur le lecteur avant de placer ce dernier dans le support. Reportez-vous au manuel de l'utilisateur du lecteur de disque dur pour déterminer comment configurer le cavalier du lecteur en position « maître » ou « esclave ». Assurez-vous que le cavalier du support est correctement configuré avant d'insérer le lecteur.
- Configurez les cavaliers sur le support du périphérique Encryption DataPort V "Plus".

Il y a 3 différentes positions de cavaliers sur le support du périphérique Encryption DataPort V "Plus". Le système Encryption DataPort V "Plus" est configuré par défaut pour utiliser des lecteurs « maîtres ». Reportez-vous à la Figure 6 pour les autres configurations appropriées à votre lecteur.

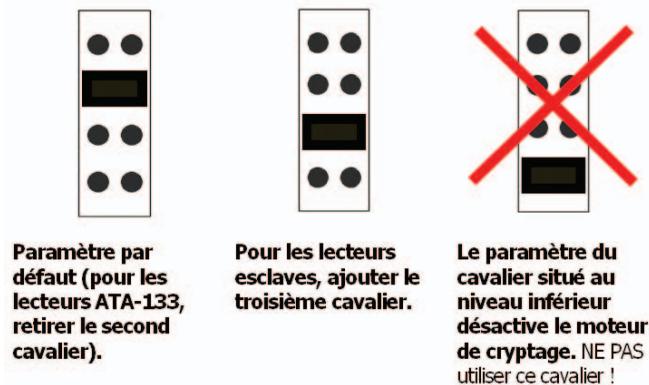


Figure 6 - Positions des cavaliers

Remarque : le cavalier situé au niveau inférieur est réservé aux tests propriétaires de CRU-DataPort. Si vous utilisez ce cavalier, vous empêcherez le cryptage de vos données.

- Branchez le câble d'alimentation c.c. sur le lecteur : branchez le câble d'alimentation c.c. à 4 broches sur le connecteur d'alimentation du lecteur et vérifiez s'il est complètement enfoncé.
- Branchez le câble des données sur le lecteur.
- Installez le lecteur : mettez-le en place dans le support et utilisez les quatre vis fournies pour le monter. Insérez les câbles dans le support de façon à ce qu'ils soient complètement intégrés au support.
- À l'aide d'un ruban adhésif, fixez le capteur de refroidissement du contrôle de température (TCCS) sur la partie supérieure du disque dur.
- Après avoir vérifié toutes les connexions de câbles, emboîtez les protections supérieure et inférieure du support.

Fonctionnement

Les étapes à suivre pour faire fonctionner le système se trouvent après la section ci-dessous sur l'utilisation des clés de sécurité. Veuillez lire la section traitant des clés de sécurité avant de démarrer le système.

Utilisation des clés de sécurité

Votre système Encryption DataPort V "Plus" est fourni avec des clés de sécurité qui permettent de vous authentifier en tant qu'utilisateur autorisé et d'activer le cryptage/décryptage. Sans la clé de sécurité fournie, votre ordinateur NE pourra PAS démarrer et/ou les données du disque dur NE pourront PAS être lues. Après avoir installé le système Encryption DataPort, testez la seconde clé pour vous assurer qu'elle fonctionne correctement.

IMPORTANT !

N'insérez jamais la clé de sécurité dans un port FireWire ! Si vous insérez votre clé de sécurité dans un port FireWire, la clé de cryptage sera endommagée, et vous ne pourrez pas l'utiliser, ce qui causera une perte de données.

Veuillez toujours garder le double de la clé de sécurité en un endroit sûr !

La clé de sécurité contient la clé électronique secrète du moteur de cryptage en temps réel DES/TDES. Sans cette clé électronique secrète unique, vous ne pourrez pas accéder aux données de votre lecteur de disque dur crypté. Il est extrêmement important de conserver le double de la clé à un endroit sécurisé où celle-ci peut être récupérée au cas où la clé d'origine serait perdue.

Si les deux clés de sécurité sont perdues, il devient virtuellement impossible de récupérer vos données.

Aucun contournement n'est possible avec le système Encryption DataPort V "Plus". En ce qui concerne les clés de sécurité, la société CRU-DataPort ne conserve aucun dossier sur les clés électroniques secrètes. Celles-ci sont fournies au hasard ; par conséquent, la société ne peut pas fournir de clés de remplacement. CRU-DataPort propose un service de duplication des clés de sécurité, dans la mesure où la clé de sécurité d'origine est en votre possession, et si vous l'envoyez à CRU-DataPort.

Chaque périphérique Encryption DataPort V "Plus" est livré entièrement testé pour répondre aux exigences de qualité auxquelles les utilisateurs s'attendent de la part de CRU-DataPort. Toutefois, en cas de défaut de fabrication du périphérique Encryption DataPort V "Plus", retournez tout simplement le support à CRU-DataPort. Les données présentes sur le lecteur de disque dur ne seront pas perdues dans la mesure où la clé de sécurité d'origine est en votre possession.

Étapes à suivre pour faire fonctionner le système

1. Insérez la clé de sécurité dans l'emplacement prévu à cet effet, sur le panneau frontal du périphérique Encryption DataPort V "Plus". La clé de sécurité doit être insérée avant d'activer le système Encryption DataPort V "Plus".

Sans la clé de sécurité appropriée, votre ordinateur NE pourra PAS démarrer et/ou les données du disque dur NE pourront PAS être lues.

2. Après avoir démarré l'ordinateur, retirez la clé de sécurité et gardez-la en un endroit sûr. Le fonctionnement de l'ordinateur ne sera pas affecté si la clé de sécurité est retirée une fois l'ordinateur démarré.

Remarque : la fente d'insertion de la clé de sécurité, située à l'avant du support DataPort, ne doit être utilisée que pour la clé de sécurité. Veuillez noter que cette fente, bien que physiquement identique à celle du IEEE-1394-FireWire, n'est pas une interface FireWire. Veuillez ne pas tenter d'enficher des produits FireWire standard dans la fente de la clé de sécurité.

3. Mettez le système en marche.

Le verrou du périphérique DataPort verrouille le support en place et sert également d'interrupteur de marche/arrêt. Tournez le verrou de 90 degrés vers la droite en position de marche (ON) avant d'allumer l'ordinateur.

4. Vous devez maintenant FORMATER le disque. Le formatage sert à préparer le disque à l'utilisation et à crypter à la fois le secteur d'amorçage et la table d'allocation des fichiers (FAT).

ATTENTION !

L'opération de FORMATAGE efface toutes les données du disque. Veuillez donc sauvegarder vos données avant de lancer cette opération. Le fabricant n'est en aucun cas responsable de la perte de données.

Le formatage de votre lecteur de disque dur efface toutes les données ; par conséquent, veuillez sauvegarder tout le contenu du lecteur avant d'effectuer le formatage. Avec le système Encryption DataPort V "Plus", l'opération de FORMATAGE doit toujours être exécutée sur le disque, que le lecteur soit nouveau ou ancien. Exécutez les commandes standard FDISK ou FORMAT, en fonction de votre système d'exploitation. Une fois l'opération terminée, chargez le système d'exploitation et les autres fichiers requis, y compris tous les fichiers que vous avez sauvegardés auparavant. (Contactez le Support technique de CRU-DataPort si vous avez besoin d'aide pour cette opération.)

L'installation est désormais terminée, et le périphérique DataPort est prêt à l'emploi.

Fonctions des voyants DEL

Le voyant DEL vert, lorsqu'il est allumé, indique que le périphérique DataPort est activé. Le voyant DEL rouge a une double fonction. Lorsqu'il reste allumé lors de l'amorçage, cela indique qu'il y a une erreur au niveau de votre clé de sécurité. La clé de sécurité ne peut pas être lue et ne parvient pas à crypter et décrypter les données. Après l'amorçage, le voyant DEL rouge fonctionne en tant que témoin DEL d'indication d'activité du disque dur.

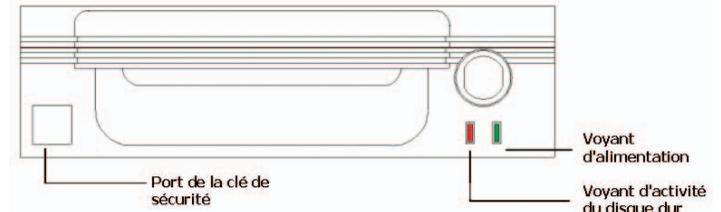


Figure 7 - Vue avant du périphérique DataPort

Alarme signalant une défaillance du ventilateur

La fonction d'alarme pour signaler un mauvais fonctionnement du ventilateur est une fonctionnalité standard du périphérique DataPort V "Plus". En cas de panne du ventilateur, une alarme sonore est émise, et le voyant DEL vert, situé dans l'angle inférieur droit de la fenêtre d'affichage DEL DataPort, clignote pour indiquer la défaillance.

IMPORTANT !

Avant de retirer le support, lisez les informations suivantes.

Il est déconseillé de retirer le support du périphérique DataPort pendant le fonctionnement de l'ordinateur. Toutefois, si cela s'avère nécessaire, observez les précautions suivantes :

- Patientez jusqu'à ce que le témoin d'activité (voyant rouge) du disque dur soit éteint et reste éteint, indiquant qu'aucune activité de lecture/d'écriture n'a lieu.
- Si le système utilise un programme de mise en cache des données du disque, vérifiez que toutes les données ont été gravées sur le disque dur.
- Éteignez le lecteur en tournant la clé sur la position d'arrêt (verticale). Le témoin d'alimentation (voyant vert) s'éteint, indiquant que le système n'est plus alimenté. Patientez 10 à 15 secondes pour permettre l'arrêt complet du lecteur, puis retirez le support.

CRU-DataPort n'est en aucun cas responsable de pertes de données éventuelles. Il est de la responsabilité de l'utilisateur de respecter ces procédures importantes pour la sauvegarde des données.

Résolution des problèmes

Problème	Solution
Absence d'alimentation	<ul style="list-style-type: none"> · Vérifiez si le verrou du périphérique DataPort est en position de marche (horizontale) et si le voyant DEL vert est allumé. · Vérifiez la connexion d'alimentation c.c. à 4 broches sur le support et à l'arrière du châssis.
Erreur de la clé de sécurité	<ul style="list-style-type: none"> · Le voyant DEL rouge a une double fonction. Lorsqu'il reste allumé lors de l'amorçage, cela indique qu'il y a une erreur au niveau de votre clé de sécurité. La clé de sécurité ne peut pas être lue, et le processeur de cryptage ne parvient ni à crypter, ni à décrypter les données. · Vérifiez si vous avez inséré la clé de sécurité dans la fente réservée à cet effet. Si la clé de sécurité appropriée n'est pas insérée correctement, votre lecteur de disque ne peut ni être amorcé, ni détecté par le système.
Lecteur non reconnu par l'ordinateur	<ul style="list-style-type: none"> · Commencez par vérifier le branchement de tous les câbles et la configuration des cavaliers. · Vérifiez le paramètre du mode maître/esclave du lecteur. · Vérifiez si le support et le châssis sont complètement emboîtés, et si aucune des broches ne s'est pliée lors de l'insertion du support. · Vérifiez s'il n'y a aucune indication d'erreur de clé de sécurité. · De plus, si vous utilisez plusieurs périphériques DataPort cryptés, assurez-vous que vous utilisez la clé appropriée.
Défaillance du ventilateur	<ul style="list-style-type: none"> · En cas de panne du ventilateur, contactez le Support technique de DataPort, au 800.260.9800 (aux États-Unis)

Support technique

Pour obtenir une assistance technique, prenez d'abord contact avec votre revendeur. Si cela ne suffit pas, contactez le service de support technique de CRU-DataPort, sur le site Web à l'adresse URL <http://www.CRU-DataPort.com>, ou en envoyant un courriel à support@CRU-DataPort.com.

Garantie limitée du produit

CRU-DataPort garantit, pendant une période de trois (3) ans à compter de la date d'achat initiale, que les périphériques Encryption DataPort V "Plus" sont exempts de vices de matériel et de fabrication.

Réclamations concernant le produit

En cas de rupture de garantie, il est de l'entière responsabilité de CRU-DataPort et du recours exclusif de l'acquéreur initial, et à la seule décision de CRU-DataPort, de (a) rembourser la totalité du prix, ou de (b) réparer ou remplacer le matériel, à la seule condition que ce dernier soit renvoyé à CRU-DataPort accompagné d'une copie du bordereau de vente ou de la documentation applicable. Tout remplacement de matériel sera garanti jusqu'à la date de terminaison de la garantie initiale.

Ces recours sont inapplicables si la défectuosité du matériel est le résultat d'un accident, d'une utilisation abusive, d'une utilisation incorrecte ou d'une modification. (Cette situation sera déterminée par CRU-DataPort.)

Limitations de responsabilité

Seules les garanties spécifiées dans le présent accord sont valides. CRU-DataPort rejette expressément toute autre garantie, y compris, sans que cela ait un caractère limitatif, les garanties implicites de qualité marchande et de conformité pour un but spécifique et le non-respect des droits des tiers en ce qui concerne la documentation et le matériel. Aucun des revendeurs, agents ou employés de CRU-DataPort n'est autorisé à modifier de quelque façon que ce soit ou étendre les termes définis dans la présente garantie.

CRU-DataPort ou ses fournisseurs d'informations ou de données, de dysfonctionnement de l'ordinateur, ou de tout autre dommage spécial, indirect ou consécutif découlant de la vente, de l'utilisation ou de l'impossibilité d'utiliser tout produit ou service de CRU-DataPort, même si CRU-DataPort a été prévenu de ces dommages éventuels. La responsabilité de CRU-DataPort ne doit en aucun cas dépasser le prix réel payé pour les produits en question.