Dell Encryption

Utilitaires administrateur

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Marques déposées et marques commerciales utilisées dans Dell Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise et dans la suite de documents Data Guardian : Dell™ et le logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® et KACE™ sont des marques commerciales de Dell Inc. Cylance®, CylancePROTECT et le logo Cylance sont des marques déposées de Cylance, Inc. aux États-Unis et dans d'autres pays. McAfee® et le logo McAfee sont des marques ou des marques déposées de McAfee, Inc. aux États-Unis et dans d'autres pays. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® et Xeon® sont des marques déposées d'Intel Corporation aux États-Unis et dans d'autres pays. Adobe®, Acrobat®, et Flash® sont des marques déposées d'Adobe Systems Incorporated. Authen Tec® et Eikon® sont des marques déposées d'Authen Tec. AMD® est une marque déposée d'Advanced Micro Devices, Inc. Microsoft®, Windows®, et Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, et Visual C++® sont des marques commerciales ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. VMware® est une marque déposée ou une marque commerciale de VMware, Inc. aux États-Unis ou dans d'autres pays. Box® est une marque déposée de Box. DropboxSM est une marque de service de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, et Google™ Play sont des marques commerciales ou des marques déposées de Google Inc. aux États-Unis et dans d'autres pays. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® et Siri® sont des marques de service, des marques commerciales ou des marques déposées d'Apple, Inc. aux États-Unis et/ou dans d'autres pays. GO ID®, RSA®, et SecurID® sont des marques déposées de Dell EMC. EnCase™ et Guidance Software® sont des marques commerciales ou des marques déposées de Guidance Software. Entrust® est une marque déposée d'Entrust®, Inc. aux États-Unis et dans d'autres pays. InstallShield® est une marque déposée de Flexera Software aux États-Unis, en Chine, dans l'Union européenne, à Hong Kong, au Japon, à Taïwan et au Royaume-Uni. Micron® et RealSSD® sont des marques déposées de Micron Technology, Inc. aux États-Unis et dans d'autres pays. Mozilla® Firefox® est une marque déposée de Mozilla Foundation aux États-Unis et/ou dans d'autres pays. IOS® est une marque commerciale ou une marque déposée de Cisco Systems, Inc. aux États-Unis et dans certains autres pays et elle est utilisée sous licence. Oracle® et Java® sont des marques déposées d'Oracle et/ou de ses sociétés affiliées. Les autres noms peuvent être des marques de leurs propriétaires respectifs. SAMSUNG™ est une marque commerciale de SAMSUNG aux États-Unis ou dans d'autres pays. Seagate® est une marque déposée de Seagate Technology LLC aux États-Unis et/ou dans d'autres pays. Travelstar® est une marque déposée de HGST, Inc. aux États-Unis et dans d'autres pays. UNIX® est une marque déposée de The Open Group. VALIDITY™ est une marque commerciale de Validity Sensors, Inc. aux États-Unis et dans d'autres pays. VeriSign® et d'autres marques connexes sont des marques commerciales ou des marques déposées de VeriSign, Inc. ou de ses filiales ou sociétés affiliées aux États-Unis et dans d'autres pays et dont la licence est octroyée à Symantec Corporation. KVM on IP® est une marque déposée de Video Products. Yahoo!® est une marque déposée de Yahoo! Inc. Ce produit utilise des parties du programme 7-Zip. Le code source est disponible à l'adresse 7-zip.org. L'octroi de licence est soumis à la licence GNU LGPL + aux restrictions unRAR (7-zip.org/license.txt).

Utilitaires administrateur

2017 - 08

Rév. A01

Table des matières

1

Introduction

Ce document décrit les utilitaires pour la récupération de clé de cryptage et l'accès aux fichiers. Les utilitaires offrent les fonctions suivantes :

Télécharger les clés : CMGAd permet à l'administrateur de télécharger le bundle de matériel clé afin de l'utiliser sur un ordinateur qui n'est pas connecté à un Dell Server.

Lancer des tâches : la commande **CMGAlu** permet aux administrateurs de déverrouiller les fichiers cryptés communs ou utilisateurs sur un ordinateur lorsqu'un processus est en cours d'exécution.

Déverrouiller les fichiers : CMGAu permet à un administrateur d'accéder à des fichiers cryptés par SDE, à des fichiers utilisateurs ou communs sur un lecteur esclave, un ordinateur démarré dans un environnement pré-installé, ou sur un ordinateur où aucun utilisateur activé n'est pas connecté.

Contacter Dell ProSupport

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24h/24, 7j/7 une assistance téléphonique concernant votre produit Dell.

Un support en ligne pour les produits Dell est en outre disponible à l'adresse dell.com/support. Le support en ligne englobe les pilotes, les manuels, des conseils techniques et des réponses aux questions fréquentes et émergentes.

Aidez-nous à vous mettre rapidement en contact avec l'expert technique approprié en ayant votre Code de service à portée de main lors de votre appel.

Pour les numéros de téléphone en dehors des États-Unis, consultez Numéros de téléphone internationaux Dell ProSupport.

2

Utilitaire de téléchargement administratif (CMGAd)

Cet utilitaire permet de télécharger un bundle de matériel clé à utiliser sur un ordinateur non connecté à un Dell Server. L'utilitaire Admin peut ensuite utiliser ces ensembles hors ligne).

Cet utilitaire utilise l'une des méthodes suivantes pour télécharger un ensemble clé, selon le paramètre de ligne de commande passé à l'application :

- Mode d'analyse approfondie : utilisé si **-f** est passé sur la ligne de commande ou si aucun paramètre de ligne de commande n'est utilisé.
- **Mode Admin** : utilisé si **-a** est passé sur la ligne de commande.

Les fichiers journaux sont disponibles à l'adresse C:\ProgramData\CmgAdmin.log

Utilisation du mode Analyse approfondie

1 Double-cliquez sur **cmgad.exe** pour lancer l'utilitaire, ou ouvrez une invite de commande où se trouve CMGAd et saisissez **cmgad.exe -f** (ou **cmgad.exe**).

2 Entrez les informations suivantes (certains champs peuvent être déjà renseignés).

Paramètres du mode d'analyse approfondie	Description
URL serveur du périphérique	URL complète du serveur Security Server (Device Server). Le format est le suivant https://securityserver.domain.com:8443/xapi/. Si la version de votre Dell Server est antérieure à v7.7, le format est https://deviceserver.domain.com:8081/xapi (numéro de port différent, sans barre oblique).
Dell Admin	Nom de l'administrateur avec les informations d'identification de l'administrateur d'analyse approfondie comme jdupont (activé dans la console de gestion)
Mot de passe	Mot de passe administrateur d'analyse approfondie
MCID	ID de la machine, tel que IDmachine.domaine.com
DCID :	Les huit premiers caractères de l'ID de Bouclier comportant 16 caractères

CONSEIL:
Généralement, il suffit de spécifier MCID ou DCID. Cependant, si les deux sont connus, il peut être utile de les entrer tous les deux. Chaque paramètre contient différentes informations utilisées par cet utilitaire.

Cliquez sur **Suivant**.

3 Dans le champ *Phrase de passe*, entrez la phrase de passe pour protéger le fichier de téléchargement. La phrase de passe doit contenir au moins huit caractères, au moins un caractère alphabétique et un caractère numérique. Confirmer la phrase de passe.

Acceptez le nom et l'emplacement par défaut auquel le fichier sera enregistré, ou cliquez sur ... pour sélectionner un emplacement différent.

Cliquez sur **Suivant**.

Le message qui s'affiche indique que le matériel clé a été déverrouillé avec succès. Les fichiers sont désormais accessibles.

4 Cliquez sur **Terminer** lorsque vous avez terminé.

Utilisation du mode Admin

Le mode Admin ne peut pas être utilisé pour l'obtention d'un ensemble de clés depuis un Security Management Server Virtual, car le Security Management Server Virtual n'utilise pas le Key Server. Utilisez le mode Analyse approfondie pour obtenir l'ensemble de clés si le client est activé par rapport à un Security Management Server Virtual.

1 Ouvrez une invite de commande à l'emplacement de CMGAd et saisissez **cmgad.exe -a**.

2 Entrez les informations suivantes (certains champs peuvent être déjà renseignés).

Paramètres du mode Admin	Description
Serveur :	Nom d'hôte complet du Key Server, tel que keyserver.domaine.com.
Numéro de port	Le port par défaut est 8050
Compte du serveur	L'utilisateur de domaine sous le nom duquel le Key Server s'exécute. Le format est DOMAINE\Nom d'utilisateur. L'utilisateur de domaine qui exécute l'utilitaire doit être autorisé à effectuer le téléchargement depuis le Key Server.
MCID	ID de la machine, tel que IDmachine.domaine.com
DCID :	Les huit premiers caractères de l'ID de Bouclier comportant 16 caractères

CONSEIL:
Généralement, il suffit de spécifier MCID *ou* DCID. Cependant, si les deux sont connus, il peut être utile de les entrer tous les deux. Chaque paramètre contient différentes informations utilisées par cet utilitaire.

Cliquez sur **Suivant**.

3 Dans le champ *Phrase de passe*, entrez la phrase de passe pour protéger le fichier de téléchargement. La phrase de passe doit contenir au moins huit caractères, au moins un caractère alphabétique et un caractère numérique.
Confirmer la phrase de passe.

Acceptez le nom et l'emplacement par défaut auquel le fichier sera enregistré, ou cliquez sur ... pour sélectionner un emplacement différent.

Cliquez sur **Suivant**.

Le message qui s'affiche indique que le matériel clé a été déverrouillé avec succès. Les fichiers sont désormais accessibles.

4 Cliquez sur **Terminer** lorsque vous avez terminé.

Lancer l'utilitaire administratif (CMGAlu)

Cet utilitaire permet aux administrateurs de déverrouiller les fichiers cryptés communs ou utilisateurs sur un ordinateur lorsqu'un processus est en cours d'exécution.

Cet utilitaire est utilisé pour lancer des tâches à partir d'une console de gestion. L'utilitaire doit être copié sur l'ordinateur cible et toute tâche qui nécessite l'accès aux fichiers cryptés communs ou utilisateurs est modifiée pour exécuter cet utilitaire, en faisant passer la ligne de commande pour le travail de gestion à l'utilitaire. Une fois que le processus se ferme, l'utilitaire se termine.

Cet utilitaire utilise l'une des méthodes suivantes pour déverrouiller les fichiers, selon le paramètre de ligne de commande passé à l'application :

- **Mode d'analyse approfondie** : utilisé si **-f** est passé sur la ligne de commande ou si aucun paramètre de ligne de commande n'est passé.
- **Mode Admin** : utilisé si **-k** est passé sur la ligne de commande.
- **Mode Fichier de sauvegarde** : utilisé si **-b** est passé sur la ligne de commande.

Les fichiers journaux sont disponibles à l'adresse C:\ProgramData\CmgAdmin.log

Utilisation du mode Analyse approfondie

Syntaxe du mode Analyse approfondie

```
CmgAlu -f -vX -aAdminName -AAdminPwd [-r] [-XURL [-dMCID] [-sSCID]] "command"
```

Paramètres du mode d'analyse approfondie	Description
-f	Indique que le mode d'analyse approfondie doit être utilisé.
-vX	X indique le niveau de journalisation. Les niveaux de journaux sont 0 à 5 (0 correspondant à « pas de journal »/5 à « niveau de débogage »).
AdminPwd	Mot de passe administrateur d'analyse approfondie
AdminName	Nom d'utilisateur de l'administrateur avec les informations d'identification de l'administrateur d'analyse approfondie
-r	Indique à l'utilitaire la manière de charger l'adresse URL du serveur de périphérique et de l'identifiant MCID (ou SCID) de l'ordinateur depuis le registre. Si -r n'est pas spécifié, l'URL/serveur et MCID (ou SCID) doivent être fournis..
URL	Adresse URL du serveur du périphérique complet Si vous utilisez une version du serveur Serveur Dell antérieure à 7.7, le format est le suivant : https://deviceserver.domain.com:8081/xapi Si vous utilisez une version 7.7 ou supérieure du serveur Serveur Dell, le format est le suivant : https://deviceserver.domain.com:8443/xapi/

Paramètres du mode d'analyse approfondie	Description
MCID	ID de périphérique pour le périphérique à déverrouiller. L'ID MCID est aussi connu comme l'identifiant unique de périphérique ou le nom d'hôte.
SCID	Protection de l'ID du périphérique à déverrouiller. SCID est également appelé l'identifiant DCID ou de restauration.
-?	Aide de la ligne de commande.

Utilisation du mode Admin

Syntaxe du mode Admin

```
CmgAlu -k -vX -aServerPrincipal -pPort [-r] [-XServer [-dMCID] [-sSCID]] "command"
```

Paramètres du mode Admin	Description
-k	Indique que Kerberos (mode Admin) est à utiliser. CmgAlu nécessite l'indicateur -k pour fonctionner en mode Admin.
-vX	X indique le niveau de journalisation. Les niveaux de journaux sont 0 à 5 (0 correspondant à « pas de journal »/5 à « niveau de débogage »).
ServerPrincipal	Compte de domaine sous lequel Key Server s'exécute.
Port	Port TCP à connecter au Key Server activé.
Serveur	Nom ou adresse IP du serveur Key Server
-r	Indique à l'utilitaire la manière de charger le nom du Key Server et l'identifiant MCID (ou SCID) de l'ordinateur depuis le registre. Si -r n'est pas spécifié, le nom du Key Server et l'identifiant MCID (ou SCID) doivent être fournis.
MCID	ID de périphérique pour le périphérique à déverrouiller. L'ID MCID est aussi connu comme l'identifiant unique de périphérique ou le nom d'hôte.
SCID	Protection de l'ID du périphérique à déverrouiller. SCID est également appelé l'identifiant DCID ou de restauration.
-?	Aide de la ligne de commande.

Utilisation du mode Fichier de sauvegarde

Syntaxe du mode Fichier de sauvegarde

```
CmgAlu -vX -b"FilePath" -ABackupPwd "command"
```

Paramètres du mode Fichier de sauvegarde	Description
-vX	X indique le niveau de journalisation. Les niveaux de journaux sont 0 à 5 (0 correspondant à « pas de journal »/5 à « niveau de débogage »).
-b « Filepath »	Généralement le chemin système vers le fichier de sauvegarde, soit un fichier de récupération LSA, soit un fichier de sortie téléchargé depuis CMGAd.
-BackupPwd	Le mot de passe utilisé pour créer le fichier de sauvegarde.
-?	Aide de la ligne de commande.

Utilitaire de déverrouillage administratif (CMGAu)

Cet utilitaire vous permet d'accéder aux fichiers cryptés par SDE, à des fichiers utilisateurs ou communs sur un lecteur esclave, un ordinateur démarré dans un environnement pré-installé, ou sur un ordinateur où aucun utilisateur activé n'est connecté.

Cet utilitaire utilise la méthode suivante pour télécharger un ensemble de matériel clé :

- **Mode d'analyse approfondie** : utilisé si **-f** est passé sur la ligne de commande ou si aucun paramètre de ligne de commande n'est utilisé.
- **Mode Admin** : utilisé si **-a** est passé sur la ligne de commande.

Les fichiers journaux sont disponibles à l'adresse C:\ProgramData\CmgAdmin.log

Travail hors connexion avec un fichier téléchargé précédemment

Si vous choisissez de travailler hors connexion avec un fichier téléchargé précédemment, CMGAu fonctionne de la même façon, peu importe la façon dont vous le lancez, ce qui veut dire que l'opération est la même si vous double-cliquez sur le fichier .exe pour lancer l'utilitaire, lancez celle-ci à l'aide de n'importe quel commutateur dans une ligne de commande ou lancez-le à l'aide du commutateur -f dans la ligne de commande.

1 Ouvrez une invite de commande à l'emplacement de CMGAu et saisissez **cmgau.exe**.
2 Sélectionnez **Yes (Oui)**, **travailler hors connexion avec un fichier téléchargé précédemment**. Cliquez sur **Suivant >**.
3 Dans *Fichier téléchargé*, accédez à l'emplacement du matériel clé enregistré. Ce fichier a été enregistré lors de l'utilisation de l'utilitaire de téléchargement administratif.

   Dans le champ *phrase de passe*, entrez la phrase de passe qui a été utilisée pour protéger le fichier matériel clé. Cette phrase de passe a été définie lors de l'utilisation de l'utilitaire de téléchargement administratif.

   Cliquez sur **Suivant >**.

   Le message qui s'affiche indique que le matériel clé a été déverrouillé avec succès. Les fichiers sont désormais accessibles.
4 **Une fois que vous avez fini d'utiliser les fichiers cryptés**, cliquez sur **Terminer**. *Une fois que vous avez cliqué sur Terminer, les fichiers cryptés ne sont plus disponibles.*

Opération Télécharger maintenant en mode Analyse approfondie

1 Ouvrez une invite de commande à l'emplacement de CMGAu et saisissez **cmgau.exe**.
2 Sélectionnez **Non, effectuer un téléchargement à partir d'un serveur maintenant**. Cliquez sur **Suivant >**.
3 Entrez les informations suivantes (certains champs peuvent être déjà renseignés).

Option	Description
URL serveur du périphérique :	Adresse URL du serveur du périphérique complet. Si vous utilisez une version du serveur Serveur Dell antérieure à 7.7, le format est le suivant : https://deviceserver.domain.com:8081/xapi

Option	Description
	Si vous utilisez une version 7.7 ou supérieure du serveur Serveur Dell, le format est le suivant : https://deviceserver.domain.com:8443/xapi/
Admin Dell :	Nom de l'administrateur avec les informations d'identification de l'administrateur d'analyse approfondie comme jdupont (activé dans la console de gestion)
Mot de passe :	Mot de passe administrateur d'analyse approfondie
MCID :	ID de la machine, tel que IDmachine.domaine.com
DCID :	Les huit premiers caractères de l'ID de Bouclier comportant 16 caractères

Cliquez sur **Suivant >.**

Le message qui s'affiche indique que le matériel clé a été déverrouillé avec succès. Les fichiers sont désormais accessibles.

4 **Une fois que vous avez fini d'utiliser les fichiers cryptés**, cliquez sur **Terminer**. *Une fois que vous avez cliqué sur **Terminer**, les fichiers cryptés ne sont plus disponibles.*

Opération Télécharger maintenant en mode Admin

1 Ouvrez une invite de commande à l'emplacement de CMGAu et saisissez **cmgau.exe -a**.

2 Sélectionnez **Non, effectuer un téléchargement à partir d'un serveur maintenant**. Cliquez sur **Suivant >**.

3 Entrez les informations suivantes (certains champs peuvent être déjà renseignés).

Paramètres du mode Admin	Description
Serveur :	Nom d'hôte complet du Key Server, tel que Key Server.domaine.com
Numéro de port :	Le port par défaut est 8050
Compte du serveur :	L'utilisateur de domaine sous le nom duquel le Key Server s'exécute. Le format est DOMAINE\Nom d'utilisateur. L'utilisateur de domaine qui exécute l'utilitaire doit être autorisé à effectuer le téléchargement depuis le Key Server.
MCID :	ID de la machine, tel que IDmachine.domaine.com
DCID :	Les huit premiers caractères de l'ID de Bouclier comportant 16 caractères

Cliquez sur **Suivant >**.

Le message qui s'affiche indique que le matériel clé a été déverrouillé avec succès. Les fichiers sont désormais accessibles.

4 **Une fois que vous avez fini d'utiliser les fichiers cryptés**, cliquez sur **Terminer**. *Une fois que vous avez cliqué sur **Terminer**, les fichiers cryptés ne sont plus disponibles.*