Dell Encryption

Administrator-Dienstprogramme

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Administrator-Dienstprogramme

2017 - 08

Rev. A01

Inhaltsverzeichnis

1

Einleitung

Dieses Dokument beschreibt Dienstprogramme zum Abrufen des Verschlüsselungsschlüssels und zum Zugriff auf Dateien. Die Dienstprogramme bieten die folgenden Funktionen:

Schlüssel herunterladen – Mit **CMGAd** können Administratoren Schlüsseldatenpakete zur Verwendung auf einem Computer herunterladen, der nicht mit einem Server verbunden ist.

Jobs starten – Der Befehl **CMGAlu** erlaubt es Administratoren, während eines laufenden Prozesses benutzer- oder allgemein verschlüsselte Dateien auf einem Computer zu entsperren.

Dateien entsperren – Der Befehl **CMGAu** gewährt Administratoren Zugriff auf benutzer-, allgemein oder mit SDE verschlüsselte Dateien auf einem Slave-Laufwerk, einem Computer, der in einer vorinstallierten Umgebung hochgefahren wurde, oder einem Computer, bei dem kein aktivierter Benutzer angemeldet ist.

Kontaktaufnahme mit dem Dell ProSupport

Telefonischen Support rund um die Uhr für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Halten Sie bei Ihrem Anruf Ihren Service Code bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport – Internationale Telefonnummern.

2

Administrator-Download-Dienstprogramm (CMGAd)

Mit diesem Dienstprogramm können Sie Schlüsseldatenpakete zur Verwendung auf einem Computer herunterladen, der nicht mit einem Dell Server verbunden ist. Diese Offline-Pakete können von den Administrator-Dienstprogrammen verwendet werden.

Je nachdem, welche Befehlszeilenparameter an die Anwendung übergeben werden, verwendet das Dienstprogramm eine der folgenden Methoden zum Herunterladen von Schlüsselpaketen:

- **Forensischer Modus** – wird bei Ausführung des Befehlszeilenparameters **-f** verwendet oder wenn kein Befehlszeilenparameter verwendet wird.
- **Admin-Modus** – wird bei Ausführung des Befehlszeilenparameters **-a** verwendet.

Die Protokolldateien befinden sich unter C:\ProgramData\CmgAdmin.log

Verwenden des forensischen Modus

1 Doppelklicken Sie auf **cmgad.exe** beim Start des Dienstprogramms oder öffnen Sie eine Eingabeaufforderung, wo sich CMGAd befindet, und geben Sie **cmgad.exe -f** (oder **cmgad.exe**) ein.

2 Geben Sie die folgenden Informationen ein (einige Felder sind möglicherweise bereits ausgefüllt).

Parameter für den forensischen Modus	Beschreibung
URL des Geräteservers:	Vollständig qualifizierte URL des Security Servers (Device Servers). Das Format lautet: https://securityserver.domain.com:8443/xapi/. Bei älteren Versionen als Dell Server v7.7 gilt das Format https://deviceserver.domain.com:8081/xapi (andere Portnummer, ohne den nachfolgenden Schrägstrich).
Dell Admin:	Name des Administrators mit forensischen Zugriffsrechten, z. B. „hschmidt“ (aktiviert in der Verwaltungskonsole)
Passwort	Passwort des forensischen Administrators.
MCID	Rechner-ID, z. B. rechnerID.domain.com
DCID	Die ersten acht Stellen der 16-stelligen Shield-ID.

TIPP:
In der Regel genügt es, entweder die MCID oder die DCID anzugeben. Wenn jedoch beide Werte bekannt sind, empfiehlt es sich, beide einzugeben. Jeder Parameter enthält verschiedene Informationen, die von diesem Dienstprogramm verwendet werden.

Klicken Sie auf **Weiter**.

3 Geben Sie unter *Passphrase* eine Passphrase ein, um die heruntergeladene Datei zu schützen. Die Passphrase muss mindestens acht Zeichen enthalten, darunter mindestens einen Buchstaben und eine Ziffer. Bestätigen Sie die Passphrase.

Akzeptieren Sie entweder die Standardwerte für Dateinamen und Speicherort oder klicken Sie auf ..., um einen anderen Speicherort auszuwählen.

Klicken Sie auf **Weiter**.

Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.

4 Klicken Sie anschließend auf **Fertig stellen**.

Verwenden des Admin-Modus

Der Security Management Server Virtual verwendet den Key Server nicht, d. h. im Admin-Modus kann kein Schlüsselpaket über den Security Management Server Virtual abgerufen werden. Verwenden Sie den forensischen Modus, um das Schlüsselpaket zu erhalten, wenn der Client auf einem Security Management Server Virtual aktiviert ist.

1 Öffnen Sie am Speicherort von CMGAd eine Befehlseingabe, und geben Sie **cmgad.exe -a** ein.

2 Geben Sie die folgenden Informationen ein (einige Felder sind möglicherweise bereits ausgefüllt).

Parameter für den Admin-Modus	Beschreibung
Server:	Vollständig qualifizierter Hostname des Key Servers, z. B. „keyserver.domain.com“
Portnummer	Der Standardport ist 8050.
Server-Konto	Der Domänenbenutzer, unter dem der Key Server ausgeführt wird. Das Format lautet DOMÄNE \Benutzername. Der Domänenbenutzer, der das Dienstprogramm ausführt, muss über die Berechtigung zum Download vom Key Server verfügen.
MCID	Rechner-ID, z. B. rechnerID.domain.com
DCID	Die ersten acht Stellen der 16-stelligen Shield-ID.

TIPP:
In der Regel genügt es, entweder die MCID *oder* die DCID anzugeben. Wenn jedoch beide Werte bekannt sind, empfiehlt es sich, beide einzugeben. Jeder Parameter enthält verschiedene Informationen, die von diesem Dienstprogramm verwendet werden.

Klicken Sie auf **Weiter**.

3 Geben Sie unter *Passphrase* eine Passphrase ein, um die heruntergeladene Datei zu schützen. Die Passphrase muss mindestens acht Zeichen enthalten, darunter mindestens einen Buchstaben und eine Ziffer.

Bestätigen Sie die Passphrase.

Akzeptieren Sie entweder die Standardwerte für Dateinamen und Speicherort oder klicken Sie auf ..., um einen anderen Speicherort auszuwählen.

Klicken Sie auf **Weiter**.

Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.

4 Klicken Sie anschließend auf **Fertig stellen**.

3

Administrator-Ausführungsdienstprogramm (CMGAlu)

Dieses Dienstprogramm erlaubt es Administratoren, während eines laufenden Prozesses benutzer- oder allgemein verschlüsselte Dateien auf einem Computer zu entsperren.

Mit diesem Dienstprogramm können Aufträge über eine Management Console gestartet werden. Das Dienstprogramm muss auf den Zielcomputer kopiert werden. Jeder Auftrag, für den der Zugriff auf benutzer- oder allgemein verschlüsselte Dateien erforderlich ist, wird so geändert, dass er die Befehlszeile für den Management-Auftrag an das Dienstprogramm übergibt und dieses so ausführt. Nach Abschluss des Prozesses wird auch das Dienstprogramm beendet.

Je nachdem, welche Befehlszeilenparameter an die Anwendung übergeben werden, verwendet das Dienstprogramm eine der folgenden Methoden zum Entsperren von Dateien:

- **Forensischer Modus** – wird bei Ausführung des Befehlszeilenparameters **-f** verwendet oder wenn kein Parameter an die Befehlszeile weitergeleitet wird.
- **Admin-Modus** – wird bei Ausführung des Befehlszeilenparameters **-k** verwendet.
- **Sicherungsdateimodus** – wird bei Ausführung des Befehlszeilenparameters **-b** verwendet.

Die Protokolldateien befinden sich unter C:\ProgramData\CmgAdmin.log

Verwenden des forensischen Modus

Syntax des forensischen Modus

```
CmgAlu -f -vX -aAdminName -AAdminPwd [-r] [-XURL [-dMCID] [-sSCID]] „Befehl“
```

Parameter für den forensischen Modus	Beschreibung
-f	Gibt an, dass der forensische Modus verwendet werden soll.
-vX	X steht für die Protokollierungsebene. Die Protokollebene ist ein Wert von 0 bis 5 (0 = keine Protokolle/5 = Debug-Ebene).
AdminPwd	Passwort des forensischen Administrators.
AdminName	Benutzername des Administrators mit den forensischen Administrator-Anmeldeinformationen
-r	Weist das Dienstprogramm an, die URL des Device Servers und die MCID (bzw. SCID) des Computers aus der Registrierung zu laden. Wenn „–r“ nicht angegeben wurde, müssen die URL des Servers und die MCID (bzw. SCID) angegeben werden.
URL	Vollständige URL des Geräteservers

Parameter für den forensischen Modus	Beschreibung
	Bei älteren Versionen als Dell Server v7.7 gilt das Format https://deviceserver.domain.com:8081/xapi. Bei Versionen ab Dell Server v7.7 gilt das Format https://deviceserver.domain.com:8443/xapi/.
MCID	Geräte-ID für das zu entsperrende Gerät. MCID wird auch als eindeutige Geräte-ID oder Hostname bezeichnet.
SCID	Shield-ID für das zu entsperrende Gerät. SCID wird auch als DCID oder Wiederherstellungs-ID bezeichnet.
-?	Befehlszeilenhilfe.

Verwenden des Admin-Modus

Syntax des Admin-Modus

```
CmgAlu -k -vX -aServerPrincipal -pPort [-r] [-XServer [-dMCID] [-sSCID]] „Befehl“
```

Parameter für den Admin-Modus	Beschreibung
-k	Gibt an, dass der Kerberos (Admin-Modus) verwendet werden soll. Für CmgAlu muss die -k-Kennzeichnung im Admin-Modus arbeiten.
-vX	X steht für die Protokollierungsebene. Die Protokollebene ist ein Wert von 0 bis 5 (0 = keine Protokolle/5 = Debug-Ebene).
ServerPrincipal	Das AD-Konto (Domänenkonto), unter dem der Key Server ausgeführt wird.
Port	Der TCP-Port für die Verbindung zum Key Server.
Server	Name/IP-Adresse des Key Server.
-r	Weist das Dienstprogramm an, den Namen des Key Server und die MCID (bzw. SCID) des Computers aus der Registrierung zu laden. Wenn –r nicht übergeben wird, müssen der Name des Key Server und die MCID (bzw. SCID) angegeben werden.
MCID	Geräte-ID für das zu entsperrende Gerät. MCID wird auch als eindeutige Geräte-ID oder Hostname bezeichnet.
SCID	Shield-ID für das zu entsperrende Gerät. SCID wird auch als DCID oder Wiederherstellungs-ID bezeichnet.
-?	Befehlszeilenhilfe.

Verwenden des Sicherungsdateimodus

Syntax des Sicherungsdateimodus

```
CmgAlu -vX -b"FilePath" -ABackupPwd „Befehl“
```

Parameter für den Sicherungsdateimodus	Beschreibung
-vX	X steht für die Protokollierungsebene. Die Protokollebene ist ein Wert von 0 bis 5 (0 = keine Protokolle/5 = Debug-Ebene).
-b"FilePath"	Der Dateisystempfad zur Sicherungsdatei; dabei handelt es sich in der Regel entweder um eine LSA-Wiederherstellungsdatei oder eine Ausgabedatei, die von CMGAd heruntergeladen wurden.
-BackupPwd	Das Passwort, das für die Erstellung der Sicherungsdatei verwendet wurde.
-?	Befehlszeilenhilfe.

Administrator-Entsperrungsdienstprogramm (CMGAu)

Dieses Dienstprogramm gewährt Zugriff auf benutzer-, allgemein oder mit SDE verschlüsselte Dateien auf einem Slave-Laufwerk, einem Computer, der in einer vorinstallierten Umgebung hochgefahren wurde, oder einem Computer, bei dem kein aktivierter Benutzer angemeldet ist.

Dieses Dienstprogramm verwendet die folgende Methode zum Herunterladen eines Schlüsseldatenpakets:

- **Forensischer Modus** – wird bei Ausführung des Befehlszeilenparameters **-f** verwendet oder wenn kein Befehlszeilenparameter verwendet wird.
- **Admin-Modus** – wird bei Ausführung des Befehlszeilenparameters **-a** verwendet.

Die Protokolldateien befinden sich unter C:\ProgramData\CmgAdmin.log

Offline Arbeiten mit einer bereits heruntergeladenen Datei

Wenn Sie mit einer bereits heruntergeladenen Datei offline arbeiten, funktioniert CMGAu ungeachtet des Startverfahrens wie gewohnt. Der Ablauf ist immer gleich, egal, ob Sie das Dienstprogramm per Doppelklick auf die EXE-Datei, ohne Programmschalter in einer Befehlszeile oder unter Verwendung des -f-Programmschalters in der Befehlszeile starten.

1 Öffnen Sie am Speicherort von CMGAu eine Befehlseingabe und geben Sie **cmgau.exe** ein.

2 Wählen Sie **Ja, mit bereits heruntergeladener Datei offline arbeiten** aus. Klicken Sie auf **Weiter >**.

3 Wählen Sie unter *Heruntergeladene Datei* den Speicherort der gespeicherten Schlüsseldaten aus. Diese Datei wurde beim Verwenden des Administrator-Download-Dienstprogramms gespeichert.

   Geben Sie unter *Passphrase* die Passphrase ein, mit der die Schlüsseldaten geschützt wurden. Diese Passphrase wurde beim Verwenden des Administrator-Download-Dienstprogramms eingerichtet.

   Klicken Sie auf **Weiter >**.

   Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.

4 **Wenn Sie die Bearbeitung der verschlüsselten Dateien abgeschlossen haben**, klicken Sie auf **Fertig stellen**. *Nachdem Sie auf Fertigstellen geklickt haben, sind die verschlüsselten Dateien nicht mehr verfügbar.*

Ausführen von „Jetzt Herunterladen“ im forensischen Modus

1 Öffnen Sie am Speicherort von CMGAu eine Befehlseingabe und geben Sie **cmgau.exe** ein.

2 Wählen Sie **Nein, Download von einem Server jetzt durchführen**. Klicken Sie auf **Weiter >**.

3 Geben Sie die folgenden Informationen ein (einige Felder sind möglicherweise bereits ausgefüllt).

Option	Beschreibung
Device Server-URL:	Vollständige URL des Geräteservers. Bei älteren Versionen als Dell Server v7.7 gilt das Format https://deviceserver.domain.com:8081/xapi. Bei Versionen ab Dell Server v7.7 gilt das Format https://deviceserver.domain.com:8443/xapi/.
Dell Admin:	Name des Administrators mit forensischen Zugriffsrechten, z. B. „hschmidt“ (aktiviert in der Verwaltungskonsole)
Passwort:	Passwort des forensischen Administrators.
MCID:	Rechner-ID, z. B. rechnerID.domain.com
DCID:	Die ersten acht Stellen der 16-stelligen Shield-ID.

Klicken Sie auf **Weiter >.**

Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.

4 **Wenn Sie die Bearbeitung der verschlüsselten Dateien abgeschlossen haben**, klicken Sie auf **Fertig stellen**. *Nachdem Sie auf **Fertigstellen** geklickt haben, sind die verschlüsselten Dateien nicht mehr verfügbar.*

Ausführen von „Jetzt herunterladen“ im Admin-Modus

1 Öffnen Sie am Speicherort von CMGAu eine Befehlseingabe und geben Sie **cmgau.exe -a** ein.

2 Wählen Sie **Nein, Download von einem Server durchführen**. Klicken Sie auf **Weiter >**.

3 Geben Sie die folgenden Informationen ein (einige Felder sind möglicherweise bereits ausgefüllt).

Parameter für den Admin-Modus	Beschreibung
Server:	Vollständig qualifizierter Hostname des Key Servers, z. B. keyserver.domain.com
Portnummer:	Der Standardport ist 8050.
Serverkonto:	Der Domänenbenutzer, unter dem der Key Server ausgeführt wird. Das Format lautet DOMÄNE \Benutzername. Der Domänenbenutzer, der das Dienstprogramm ausführt, muss über die Berechtigung zum Download vom Key Server verfügen.
MCID:	Rechner-ID, z. B. rechnerID.domain.com
DCID:	Die ersten acht Stellen der 16-stelligen Shield-ID.

Klicken Sie auf **Weiter >**.

Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.

4 **Wenn Sie die Bearbeitung der verschlüsselten Dateien abgeschlossen haben**, klicken Sie auf **Fertig stellen**. *Nachdem Sie auf **Fertigstellen** geklickt haben, sind die verschlüsselten Dateien nicht mehr verfügbar.*