Dell Data Protection | Encryption

Administrator-Dienstprogramme

2014-05

Inhalt

1

Administrator-Download-Dienstprogramm

Mit diesem Dienstprogramm können Sie Schlüsseldatenpakete zur Verwendung auf einem Computer herunterladen, der nicht mit einem Unternehmensserver 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 Schlüsseldatenpaketen:

- **Admin-Modus**: wird bei Ausführung des Befehlszeilenparameters **-a** verwendet oder wenn keine Befehlszeilenparameter übergeben werden.
- **Forensischer Modus**: wird bei Ausführung des Befehlszeilenparameters **-f** verwendet.

Die Protokolldateien befinden sich hier:

Windows XP – C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\CmgAdmin.log

Windows 7, Windows 8, und Windows 8.1 - C:\ProgramData\CmgAdmin.log

Verwenden des Administrator-Download-Dienstprogramms im Admin-Modus

1. Doppelklicken Sie auf **cmgad.exe**, um das Dienstprogramm zu starten.

   Alternative:

   Öffnen Sie am Speicherort des Administrator-Download-Dienstprogramms eine Eingabeaufforderung und geben Sie **cmgad.exe -a** (oder cmgad.exe) ein.

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

Server:	Vollständiger Hostname des Key Server, 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:	Geräte-ID, z. B. machineID.domain.com
DCID:	Die ersten acht Stellen der 16-stelligen Shield-ID

   Klicken Sie auf **Weiter >**

3. Geben Sie in das Feld **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.

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

4. Klicken Sie nach Abschluss des Vorgangs auf **Fertigstellen**.

Verwenden des Administrator-Download-Dienstprogramms im forensischen Modus

1. Öffnen Sie am Speicherort des Administrator-Download-Dienstprogramms eine Eingabeaufforderung und geben Sie **cmgad.exe -f** ein.
2. Geben Sie die folgenden Informationen ein (einige Felder sind möglicherweise bereits ausgefüllt).

   URL für Device Server: Vollständige URL des Device Servers

   Bei älteren Versionen als Enterprise Server v7.7 gilt das Format https://deviceserver.domain.com:8081/xapi.

   Bei Versionen ab Enterprise Server v7.7 gilt das Format https://deviceserver.domain.com:8443/xapi/.

   Dell Admin: Name des Administrators mit forensischen Zugriffsrechten (aktiviert im Enterprise Server), z. B. „hschmidt“

   Passwort: Passwort des forensischen Administrators

   MCID: Geräte-ID, z. B. machineID.domain.com

   DCID: Die ersten acht Stellen der 16-stelligen Shield-ID

   Klicken Sie auf **Weiter >**
3. Geben Sie in das Feld **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.

   Eine Meldung zeigt an, dass die Schlüsseldaten erfolgreich entsperrt wurden. Die Dateien sind jetzt frei zugänglich.
4. Klicken Sie nach Abschluss des Vorgangs auf **Fertigstellen**.

2

Administrator-Ausführungsdienstprogramm

Dieses Befehlszeilendienstprogramm 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 Clientcomputer 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:

- Admin-Modus: Kein Programmschalter erforderlich.
- Forensischer Modus: wird bei Ausführung des Befehlszeilenparameters **-f** verwendet.
- Sicherungsdatei Modus: wird bei Ausführung des Befehlszeilenparameters **-b** verwendet.

Die Protokolldateien befinden sich hier:

Windows XP – C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\CmgAdmin.log

Windows 7, Windows 8, und Windows 8.1 - C:\ProgramData\CmgAdmin.log

Verwenden des Administrator-Ausführungsdienstprogramms im Admin-Modus

Syntax für den Admin-Modus

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

Parameter für den Admin-Modus	Erläuterung
-k	Gibt an, dass Kerberos (Admin-Modus) verwendet werden soll. CmgAlu benötigt die option-k um im Admin-Modus zu arbeiten.
X	Protokollebene. 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.

Parameter für den Admin-Modus	Erläuterung
SCID	Shield-ID für das zu entsperrende Gerät. SCID wird auch als DCID oder Wiederherstellungs-ID bezeichnet.
-?	Befehlszeilenhilfe.

Verwenden des Administrator-Ausführungsdienstprogramms im forensischen Modus

Syntax für den forensischen Modus

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

Parameter für den forensischen Modus	Erläuterung
-f	Gibt an, dass der forensische Modus verwendet werden soll.
AdminName	Benutzername des Administrators mit forensischen Zugriffsrechten.
AdminPwd	Passwort des forensischen Administrators.
URL	Vollständige URL des Device Servers. Bei älteren Versionen als Enterprise Server v7.7 gilt das Format https://deviceserver.domain.com:8081/xapi. Bei Versionen ab Enterprise Server v7.7 gilt das Format https://deviceserver.domain.com:8443/xapi/.
-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 übergeben wird, müssen die URL des Servers und die MCID (bzw. SCID) angegeben werden.
X	Protokollebene. Die Protokollebene ist ein Wert von 0 bis 5 (0 = keine Protokolle/5 = Debug-Ebene).
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 Administrator-Ausführungsdienstprogramms im Sicherungsdatei Modus

Syntax für den Sicherungsdatei Modus

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

Parameter für den Sicherungsdatei Modus	Erläuterung
X	Protokollebene. Die Protokollebene ist ein Wert von 0 bis 5 (0 = keine Protokolle/5 = Debug-Ebene).
-b"FilePath"	Das Dateisystem Pfad zur Sicherungsdatei, entweder ein LSA-Wiederherstellungsdatei oder eine Ausgabedatei von CmgAd heruntergeladen wurde.
BackupPwd	Das Passwort für die Sicherungsdatei zu erstellen.
-?	Befehlszeilenhilfe.

3

Administrator-Entsperrungsdienstprogramm

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.

Das Dienstprogramm verwendet eine der folgenden Methoden zum Herunterladen von Schlüsseldatenpaketen:

- Admin-Modus: Kein Programmschalter erforderlich. Dies ist der Standardmodus.
- Forensischer Modus: wird bei Ausführung des Befehlszeilenparameters **-f** verwendet.

Die Protokolldateien befinden sich hier:

Windows XP – C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\CmgAdmin.log

Windows 7, Windows 8, und Windows 8.1 - C:\ProgramData\CmgAdmin.log

Verwenden des Administrator-Entsperrungsdienstprogramms für die Offline-Bearbeitung 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. Doppelklicken Sie auf **cmgau.exe**, um das Dienstprogramm zu starten.
2. Wählen Sie **Ja, mit bereits heruntergeladener Datei offline arbeiten**. Klicken Sie auf **Weiter >**.
3. Wählen Sie im Feld **Heruntergeladene Datei:** den Speicherort der gespeicherten Schlüsseldaten aus. Diese Datei wurde beim Verwenden des Administrator-Download-Dienstprogramms gespeichert.

   Geben Sie in das Feld **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 **Fertigstellen**. *Nachdem Sie auf „Fertigstellen“ geklickt haben, sind die verschlüsselten Dateien nicht mehr verfügbar.*

Verwenden des Administrator-Entsperrungsdienstprogramms für den Download von einem Server im Admin-Modus

1. Doppelklicken Sie auf **cmgau.exe**, um das Dienstprogramm zu starten.

   Alternative:

   Öffnen Sie am Speicherort des Administrator-Entsperrungsdienstprogramms eine Eingabeaufforderung 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).

Server:	Vollständiger Hostname des Key Server, 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:	Geräte-ID, z. B. machineID.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 **Fertigstellen**. *Nachdem Sie auf „Fertigstellen“ geklickt haben, sind die verschlüsselten Dateien nicht mehr verfügbar.*

Verwenden des Administrator-Entsperrungsdienstprogramms für den Download von einem Server im forensischen Modus

1 Öffnen Sie am Speicherort des Administrator-Entsperrungsdienstprogramms eine Eingabeaufforderung und geben Sie **cmgau.exe -f** 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).

URL des Device Servers:	Vollständige URL des Device Servers. Bei älteren Versionen als Enterprise Server v7.7 gilt das Format https://deviceserver.domain.com:8081/xapi. Bei Versionen ab Enterprise Server v7.7 gilt das Format https://deviceserver.domain.com:8443/xapi/.
Dell Admin::	Name des Administrators mit forensischen Zugriffsrechten (aktiviert im Enterprise Server), z. B. „hschmidt“
Passwort:	Passwort des forensischen Administrators
MCID:	Geräte-ID, z. B. machineID.dell.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 **Fertigstellen**. *Nachdem Sie auf „Fertigstellen“ geklickt haben, sind die verschlüsselten Dateien nicht mehr verfügbar.*


0 XXXXXA0 X