Dell Encryption

Utilità di amministrazione

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

Utilità di amministrazione

2017 - 08

Rev. A01

Sommario

1

Introduzione

Questo documento descrive le utilità per il recupero delle chiavi di crittografia e per l'accesso ai file. Le utilità offrono le seguenti funzioni:

Download delle chiavi: il comando **CMGAd** consente agli amministratori di scaricare il bundle del materiale delle chiavi per l'uso in un computer non collegato a un Dell Server.

Avvio dei processi: il comando **CMGAlu** consente agli amministratori di sbloccare i file crittografati utente o comuni in un computer mentre è in esecuzione un processo.

Sblocco di file: il comando **CMGAu** consente agli amministratori di accedere a file crittografati utente, comuni o SDE in un'unità secondaria, un computer avviato in un ambiente preinstallato o in un computer in cui un utente attivato non ha eseguito l'accesso.

Contattare Dell ProSupport

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Assicurarsi di avere a portata di mano il Codice di servizio per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono esterni agli Stati Uniti, controllare Numeri di telefono internazionali di Dell ProSupport.

Administrative Download Utility (CMGAd)

Questa utilità consente il download di un bundle di materiale delle chiavi da usare in un computer non connesso a un Dell Server. Le utilità di amministrazione possono quindi usare questi bundle non in linea.

Questa utilità usa uno dei seguenti metodi per scaricare un bundle di chiavi, a seconda del parametro della riga di comando trasferito all'applicazione:

- **Modalità Forensic** - Usata se **-f** viene trasferito alla riga di comando o se non viene usato alcun parametro della riga di comando.
- **Modalità Amministratore** - Usata se **-a** viene trasferito alla riga di comando.

I file di registro sono disponibili al percorso C:\ProgramData\CmgAdmin.log

Utilizzo della modalità Forensic

1 Fare doppio clic su **cmgad.exe** per avviare l'utilità o aprire un prompt dei comandi in cui si trova CMGAd e digitare **cmgad.exe -f** (o **cmgad.exe**).

2 Immettere le seguenti informazioni (alcuni campi possono essere già popolati).

Parametri della modalità Forensic	Descrizione
URL del Device Server	URL completo del Security Server (Device Server). Il formato è https://securityserver.domain.com:8443/xapi/. Se il Dell Server in uso è precedente alla versione v7.7, il formato è https://deviceserver.domain.com:8081/xapi (numero di porta diverso, senza barra finale).
Amministratore Dell	Nome dell'amministratore con credenziali di amministratore Forensic, ad esempio jdoe (attivato nella Management Console)
Password	Password dell'amministratore Forensic
MCID	ID della macchina, come IDmacchina.dominio.com
DCID	Prime otto cifre dell'ID dello Shield a 16 cifre

SUGGERIMENTO:
Solitamente, è sufficiente specificare l'MCID o il DCID. Tuttavia, se sono noti, è utile immetterli entrambi. Ogni parametro contiene informazioni diverse utilizzate da questa utilità.

Fare clic su **Avanti**.

3 Nel campo *Passphrase*, digitare una passphrase per proteggere il file di download. La passphrase deve contenere almeno otto caratteri, di cui almeno uno alfabetico e uno numerico. Confermare la passphrase.

Accettare il nome e il percorso predefiniti in cui salvare il file, oppure fare clic sui tre puntini ("...") per selezionare un percorso diverso.

Fare clic su **Avanti**.

Viene visualizzato un messaggio che indica che il materiale delle chiavi è stato sbloccato. È ora possibile accedere ai file.

4 Al termine fare clic su **Fine**.

Utilizzo della modalità Amministratore

Il Security Management Server Virtual non usa il Key Server, quindi non è possibile usare la modalità Amministratore per ottenere un bundle di chiavi da un Security Management Server Virtual. Usare la modalità Forensic per ottenere il bundle di chiavi se il client è attivato per un Security Management Server Virtual.

1 Aprire un prompt dei comandi dove si trova CMGAd e digitare **cmgad.exe -a**.

2 Immettere le seguenti informazioni (alcuni campi possono essere già popolati).

Parametri della modalità Amministratore	Descrizione
Server:	Nome host completo del Key Server, come serverchiavi.dominio.com.
Numero di porta	La porta predefinita è 8050
Account server	L'utente del dominio in cui è in esecuzione Key Server. Il formato è DOMINIO\Nome utente. L'utente del dominio in cui l'utilità è in esecuzione deve essere autorizzato ad effettuare il download dal Key Server.
MCID	ID della macchina, come IDmacchina.dominio.com
DCID	Prime otto cifre dell'ID dello Shield a 16 cifre

SUGGERIMENTO:

Solitamente, è sufficiente specificare l'MCID *o* il DCID. Tuttavia, se sono noti, è utile immetterli entrambi. Ogni parametro contiene informazioni diverse utilizzate da questa utilità.

Fare clic su **Avanti**.

3 Nel campo *Passphrase*, digitare una passphrase per proteggere il file di download. La passphrase deve contenere almeno otto caratteri, di cui almeno uno alfabetico e uno numerico.

Confermare la passphrase.

Accettare il nome e il percorso predefiniti in cui salvare il file, oppure fare clic sui tre puntini ("...") per selezionare un percorso diverso.

Fare clic su **Avanti**.

Viene visualizzato un messaggio che indica che il materiale delle chiavi è stato sbloccato. È ora possibile accedere ai file.

4 Al termine fare clic su **Fine**.

3

Administrative Launch Utility (CMGAlu)

Questa utilità consente agli amministratori di sbloccare i file crittografati utente o comuni in un computer mentre è in esecuzione un processo.

Questa utilità viene usata per avviare i processi da una console di gestione. L'utilità deve essere copiata nel computer di destinazione e qualsiasi processo che richieda l'accesso a file crittografati utente o comuni deve essere modificato per eseguire questa utilità, trasferendo la riga di comando per il processo di gestione all'utilità. Dopo la chiusura del processo, l'utilità si interrompe.

Questa utilità usa uno dei seguenti metodi per sbloccare i file, a seconda del parametro della riga di comando trasferito all'applicazione:

- **Modalità Forensic** - Usata se **-f** viene trasferito alla riga di comando o se non viene trasferito alcun parametro alla riga di comando.
- **Modalità amministratore** - Usata se **-k** viene trasferito alla riga di comando.
- **Modalità File di backup** - Usata se **-b** viene trasferito alla riga di comando.

I file di registro sono disponibili al percorso C:\ProgramData\CmgAdmin.log

Utilizzo della modalità Forensic

Sintassi della modalità Forensic

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

Parametri della modalità Forensic	Descrizione
-f	Indica che deve essere usata la modalità Forensic.
-vX	X indica il livello del registro. I livelli di registro sono da 0 a 5 (0 è nessun file di registro/5 è livello di debug).
AdminPwd	Password dell'amministratore Forensic
AdminName	Nome utente dell'amministratore con le credenziali di amministratore Forensic
-r	Ordina all'utilità di caricare l'URL e l'MCID (o SCID) del Device Server del computer dal registro. Se -r non è specificato, devono essere forniti l'URL/Server e l'MCID (o SCID).
URL	URL completo del Device Server Se la versione del Dell Server in uso è precedente alla 7.7, il formato sarà https://deviceserver.domain.com:8081/xapi Se la versione del Dell Server in uso è la 7.7 o successiva, il formato sarà https://deviceserver.domain.com:8443/xapi/
MCID	L'ID dispositivo per il dispositivo da sbloccare.

Parametri della modalità Forensic	Descrizione
	L'MCID è anche noto come l'ID univoco o il nome host del dispositivo.
SCID	ID Shield per il dispositivo da sbloccare. Lo SCID è anche noto come DCID o ID ripristino.
-?	Guida della riga di comando.

Utilizzo della modalità Amministratore

Sintassi della modalità Amministratore

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

Parametri della modalità Amministratore	Descrizione
-k	Indica che è necessario utilizzare Kerberos (modalità Amministratore). CmgAlu richiede il flag -k per il funzionamento in modalità Amministratore.
-vX	X indica il livello del registro. I livelli di registro sono da 0 a 5 (0 è nessun file di registro/5 è livello di debug).
ServerPrincipal	AD Account (account del dominio) sotto cui il Key Server è in esecuzione.
Porta	Porta TCP cui connettere il Key Server.
Server	Nome/indirizzo IP del Key Server.
-r	Ordina all'utilità di caricare il nome e l'MCID (o SCID) del Key Server del computer dal registro. Se –r non è specificato, devono essere forniti il nome del Key Server e l'MCID (o SCID).
MCID	L'ID dispositivo per il dispositivo da sbloccare. L'MCID è anche noto come l'ID univoco o il nome host del dispositivo.
SCID	ID Shield per il dispositivo da sbloccare. Lo SCID è anche noto come DCID o ID ripristino.
-?	Guida della riga di comando.

Utilizzo della modalità file di backup

Sintassi della modalità file di backup

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

Parametri della modalità File di backup	Descrizione
-vX	X indica il livello del registro. I livelli di registro sono da 0 a 5 (0 è nessun file di registro/5 è livello di debug).
-b"FilePath"	Il percorso del file system per il file di backup, tipicamente un file di ripristino LSA o un file di output scaricato da CMGAd.
-BackupPwd	La password usata per creare il file di backup.
-?	Guida della riga di comando.

4

Administrative Unlock Utility (CMGAu)

Questa utilità consente l'accesso a file crittografati utente, comuni o tramite SDE in un'unità secondaria, un computer avviato in un ambiente preinstallato, o in un computer in cui un utente attivato non ha eseguito l'accesso.

Questa utilità usa il metodo seguente per scaricare un bundle di materiale delle chiavi:

- **Modalità Forensic** - Usata se **-f** viene trasferito alla riga di comando o se non viene usato alcun parametro della riga di comando.
- **Modalità Amministratore** - Usata se **-a** viene trasferito alla riga di comando.

I file di registro sono disponibili al percorso C:\ProgramData\CmgAdmin.log

Modalità di lavoro non in linea con un file scaricato in precedenza

Se si sceglie di lavorare in modalità non in linea con un file scaricato in precedenza, CMGAu funziona allo stesso modo, indipendentemente dal modo in cui viene avviato, ossia il funzionamento è lo stesso, che si faccia doppio clic sul file .exe per avviare l'utilità, che si avvii senza alcuna opzione in una riga di comando o che si avvii con l'opzione -f nella riga di comando.

1. Aprire il prompt dei comandi dove si trova CMGAu e digitare **cmgau.exe**.
2. Selezionare **Sì**, **lavora in modalità non in linea con un file scaricato in precedenza**. Fare clic su **Avanti >**.
3. Nel campo *File scaricato*, individuare il percorso del materiale delle chiavi salvato. Questo file è stato salvato quando è stata usata l'utilità di download amministrativa.

   Nel campo *Passphrase*, immettere la passphrase che è stata usata per proteggere i file del materiale delle chiavi. La passphrase è stata impostata quando è stata usata l'utilità di download amministrativa.

   Fare clic su **Avanti >**.

   Viene visualizzato un messaggio che indica che il materiale delle chiavi è stato sbloccato. È ora possibile accedere ai file.
4. **Una volta terminato il lavoro con i file crittografati**, fare clic su **Fine**. *Dopo aver fatto clic su Fine, i file crittografati non sono più disponibili.*

Esecuzione di un download immediato nella modalità Forensic

1. Aprire il prompt dei comandi dove si trova CMGAu e digitare **cmgau.exe**.
2. Selezionare **No, esegui il download da un server ora**. Fare clic su **Avanti >**.
3. Immettere le seguenti informazioni (alcuni campi possono essere già popolati).

Opzione	Descrizione
URL del Device Server:	URL completo del Device Server. Se la versione del Dell Server in uso è precedente alla 7.7, il formato sarà https://deviceserver.domain.com:8081/xapi

Opzione	Descrizione
	Se la versione del Dell Server in uso è la 7.7 o successiva, il formato sarà https://deviceserver.domain.com:8443/xapi/
Amministratore Dell:	Nome dell'amministratore con credenziali di amministratore Forensic, ad esempio jdoe (attivato nella Management Console)
Password:	Password dell'amministratore Forensic
MCID:	ID della macchina, come IDmacchina.dominio.com
DCID:	Prime otto cifre dell'ID dello Shield a 16 cifre

Fare clic su **Avanti >.**

Viene visualizzato un messaggio che indica che il materiale delle chiavi è stato sbloccato. È ora possibile accedere ai file.

4 **Una volta terminato il lavoro con i file crittografati**, fare clic su **Fine**. *Una volta selezionato **Fine**, i file crittografati non saranno più disponibili.*

Esecuzione di un download immediato nella modalità Amministratore

1 Aprire il prompt dei comandi dove si trova CMGAu e digitare **cmgau.exe -a**.

2 Selezionare **No, esegui il download da un server ora**. Fare clic su **Avanti >**.

3 Immettere le seguenti informazioni (alcuni campi possono essere già popolati).

Parametri della modalità Amministratore	Descrizione
Server:	nome host completo del Key Server, come serverchiavi.dominio.com
Numero di porta:	La porta predefinita è 8050
Account server:	L'utente del dominio in cui è in esecuzione Key Server. Il formato è DOMINIO\Nome utente. L'utente del dominio in cui l'utilità è in esecuzione deve essere autorizzato ad effettuare il download dal Key Server.
MCID:	ID della macchina, come IDmacchina.dominio.com
DCID:	Prime otto cifre dell'ID dello Shield a 16 cifre

Fare clic su **Avanti >**.

Viene visualizzato un messaggio che indica che il materiale delle chiavi è stato sbloccato. È ora possibile accedere ai file.

4 **Una volta terminato il lavoro con i file crittografati**, fare clic su **Fine**. *Una volta selezionato **Fine**, i file crittografati non saranno più disponibili.*