

Dell Data Protection

Guida al ripristino per crittografia di file/cartelle,  
Hardware Crypto Accelerator,  
unità autocrittografanti  
e General Purpose Key  
v8.10



---

© 2016 Dell Inc.

Marchi registrati e marchi commerciali usati nella suite di documenti di Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools e Dell Data Protection | Cloud Edition: Dell™ e il logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ sono marchi commerciali di Dell Inc. Cylance® e il logo Cylance sono marchi registrati di Cylance, Inc. negli Stati Uniti e in altri Paesi. McAfee® e il logo McAfee sono marchi commerciali o marchi registrati di McAfee, Inc. negli Stati Uniti e in altri Paesi. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® sono marchi registrati di Intel Corporation negli Stati Uniti e in altri Paesi. Adobe®, Acrobat® e Flash® sono marchi registrati di Adobe Systems Incorporated. Authen Tec® ed Eikon® sono marchi registrati di Authen Tec. AMD® è un marchio registrato di Advanced Micro Devices, Inc. Microsoft®, Windows® e 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® e Visual C++® sono marchi commerciali o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. VMware® è un marchio registrato o marchio commerciale di VMware, Inc. negli Stati Uniti o in altri Paesi. Box® è un marchio registrato di Box. Dropbox<sup>SM</sup> è un marchio di servizio di Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play sono marchi commerciali o marchi registrati di Google Inc. negli Stati Uniti e in altri Paesi. Apple®, Aperture®, App Store<sup>SM</sup>, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud<sup>SM</sup>, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® sono marchi di servizio, marchi commerciali o marchi registrati di Apple, Inc. negli Stati Uniti e/o in altri Paesi. GO ID®, RSA® e SecurID® sono marchi registrati di EMC Corporation. EnCase™ e Guidance Software® sono marchi commerciali o marchi registrati di Guidance Software. Entrust® è un marchio registrato di Entrust®, Inc. negli Stati Uniti e in altri Paesi. InstallShield® è un marchio registrato di Flexera Software negli Stati Uniti, in Cina, nella Comunità Europea, ad Hong Kong, in Giappone, a Taiwan e nel Regno Unito. Micron® e RealSSD® sono marchi registrati di Micron Technology, Inc. negli Stati Uniti e in altri Paesi. Mozilla® Firefox® è un marchio registrato di Mozilla Foundation negli Stati Uniti e/o in altri Paesi. iOS® è un marchio commerciale o marchio registrato di Cisco Systems, Inc. negli Stati Uniti e in alcuni altri Paesi, ed è concesso in licenza. Oracle® e Java® sono marchi registrati di Oracle e/o sue affiliate. Altri nomi possono essere marchi commerciali dei rispettivi proprietari. SAMSUNG™ è un marchio commerciale di SAMSUNG negli Stati Uniti o in altri Paesi. Seagate® è un marchio registrato di Seagate Technology LLC negli Stati Uniti e/o in altri Paesi. Travelstar® è un marchio registrato di HGST, Inc. negli Stati Uniti e in altri Paesi. UNIX® è un marchio registrato di The Open Group. VALIDITY™ è un marchio commerciale di Validity Sensors, Inc. negli Stati Uniti e in altri Paesi. VeriSign® e altri marchi correlati sono marchi commerciali o marchi registrati di VeriSign, Inc. o sue affiliate o filiali negli Stati Uniti e in altri Paesi, e sono concessi in licenza a Symantec Corporation. KVM on IP® è un marchio registrato di Video Products. Yahoo!® è un marchio registrato di Yahoo! Inc.

In questo prodotto vengono utilizzate parti del programma 7-Zip. Il codice sorgente è disponibile all'indirizzo [www.7-zip.org](http://www.7-zip.org). La gestione delle licenze è basata sulla licenza GNU LGPL + restrizioni unRAR ([www.7-zip.org/license.txt](http://www.7-zip.org/license.txt)).

07-2016

Protetto da uno o più brevetti statunitensi, tra cui: numero 7665125; numero 7437752; e numero 7665118.

Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso.

# Sommario

1	Guida introduttiva	5
2	Ripristino della crittografia di file/cartelle	7
	<b>Requisiti per il ripristino</b>	7
	<b>Panoramica del processo di ripristino</b>	7
	<b>Effettuare il ripristino di FFE</b>	8
	Ottenerne il file di ripristino - Computer gestito in remoto	8
	Ottenerne il file di ripristino - Computer gestito localmente	9
	Effettuare il ripristino	9
3	Ripristino dell'Hardware Crypto Accelerator	11
	<b>Requisiti per il ripristino</b>	11
	<b>Panoramica del processo di ripristino</b>	11
	<b>Effettuare il ripristino dell'HCA</b>	12
	Ottenerne il file di ripristino - Computer gestito in remoto	12
	Ottenerne il file di ripristino - Computer gestito localmente	13
	Effettuare il ripristino	13
4	Ripristino dell'unità autocrittografante (SED)	15
	<b>Requisiti per il ripristino</b>	15
	<b>Panoramica del processo di ripristino</b>	15
	<b>Effettuare il ripristino dell'unità autocrittografante</b>	16
	Ottenerne il file di ripristino - Client dell'unità autocrittografante gestito in remoto	16
	Ottenerne il file di ripristino - Client dell'unità autocrittografante gestito localmente	16
	Effettuare il ripristino	16
5	Ripristino della General Purpose Key	17
	<b>Ripristinare la GPK</b>	17
	Ottenerne il file di ripristino	17
	Effettuare il ripristino	18

6	Ripristino dei dati delle unità crittografate .....	19
	<b>Ripristinare i dati delle unità crittografate</b> .....	<b>19</b>
7	Ripristino di BitLocker Manager .....	21
	<b>Ripristinare i dati</b> .....	<b>21</b>
	Appendice A - Masterizzare l'ambiente di ripristino .....	23
	<b>Masterizzare l'ISO dell'ambiente di ripristino su CD/DVD</b> .....	<b>23</b>
	<b>Masterizzare l'ambiente di ripristino su un supporto rimovibile</b> .....	<b>23</b>

## Guida introduttiva

Questa sezione descrive in dettaglio ciò che è necessario per creare l'ambiente di ripristino.

- Copia scaricata del software dell'ambiente di ripristino: si trova nella cartella Windows Recovery Kit nel supporto di installazione di Dell Data Protection
- Supporti CD-R o DVD-R, o supporto USB formattato
  - Se si masterizza un CD o DVD, fare riferimento a [Appendice A - Masterizzare l'ambiente di ripristino](#) per i dettagli.
  - Se si usa un supporto USB, fare riferimento a [Appendice A - Masterizzare l'ambiente di ripristino](#) per i dettagli.
- Pacchetto di ripristino per dispositivo guasto
  - Per client gestiti in remoto, le istruzioni qui di seguito spiegano come recuperare un pacchetto di ripristino dal proprio Dell Data Protection Server.
  - Per client gestiti localmente, il pacchetto di ripristino è stato creato nel corso dell'installazione in un'unità di rete condivisa o in un supporto esterno. Individuare tale pacchetto prima di procedere.



## Ripristino della crittografia di file/cartelle

Con il ripristino della crittografia di file/cartelle (FFE, File/Folder Encryption), è possibile ripristinare l'accesso a quanto segue:

- Un computer che non si avvia e che visualizza una richiesta per eseguire il ripristino SDE.
- Un computer in cui non è possibile accedere ai dati crittografati o modificare i criteri.
- Un server in cui è in esecuzione Dell Data Protection | Server Encryption che soddisfa una delle due condizioni precedenti.
- Un computer in cui è necessario sostituire la scheda dell'Hardware Crypto Accelerator o la scheda madre/il TPM.

### Requisiti per il ripristino

Per il ripristino di FFE, sono necessari i seguenti componenti:

- Kit di ripristino di Windows per creare un disco di avvio speciale - Il kit contiene file che verranno usati per creare un'immagine di Windows PE (WinPE) e personalizzarla con driver e software Dell Data Protection. Il kit si trova nella cartella Windows Recovery Kit nel supporto di installazione di Dell Data Protection.

### Panoramica del processo di ripristino

Per ripristinare un sistema in errore:

- 1 Creare l'ISO di ripristino e masterizzarla in un CD/DVD oppure creare una USB avviabile. Consultare [Appendice A - Masterizzare l'ambiente di ripristino](#).
- 2 Ottenere il file di ripristino.
- 3 Effettuare il ripristino.

## Effettuare il ripristino di FFE

Seguire la procedura seguente per effettuare un ripristino di FFE.

### Ottenere il file di ripristino - Computer gestito in remoto

Per scaricare il file `LSARecovery_<machinename_domain.com>.exe`:

- 1 Aprire la Remote Management Console e, dal riquadro a sinistra, selezionare **Gestione > Ripristina endpoint**.
- 2 Nel campo Nome host, immettere il nome di dominio completo dell'endpoint e fare clic su **Cerca**.
- 3 Nella finestra Ripristino avanzato, immettere una password di ripristino e fare clic su **Scarica**.

**N.B.** È necessario ricordare questa password per avere accesso alle chiavi di ripristino.

- 4 Copiare il file `LSARecovery_<machinename_domain.com>.exe` in un percorso accessibile all'avvio in WinPE.



## Ottenere il file di ripristino - Computer gestito localmente

Per ottenere il file di ripristino di Personal Edition:

- 1 Individuare il file di ripristino denominato **LSARecovery\_<systemname>.exe**. Questo file è stato archiviato in un'unità di rete o in un dispositivo di archiviazione rimovibile durante la procedura di configurazione guidata relativa all'installazione di Personal Edition.
- 2 Copiare **LSARecovery\_<systemname>.exe** nel computer di destinazione (in cui ripristinare i dati).

## Effettuare il ripristino

- 1 Usando il supporto avviabile creato in precedenza, avviare da quel supporto in un sistema di ripristino o nel dispositivo con l'unità che si sta cercando di ripristinare. Si apre un ambiente WinPE.
  - 2 Immettere **x** e premere **Invio** per ottenere un prompt dei comandi.
  - 3 Individuare il file di ripristino e avviarlo.
  - 4 Selezionare un'opzione:
    - Il sistema non viene avviato e viene visualizzato un messaggio che richiede il ripristino SDE. Ciò consentirà di ricreare i controlli hardware che il Client di crittografia esegue all'avvio nel SO.
    - Il sistema non consente di accedere ai dati crittografati, modificare i criteri o è in fase di reinstallazione. Usare questa opzione se è necessario sostituire la scheda dell'Hardware Crypto Accelerator o la scheda madre/il TPM.
  - 5 Nella finestra di dialogo Informazioni di backup e ripristino, confermare che le informazioni sul computer client da ripristinare sono corrette e fare clic su **Avanti**.  
Quando si ripristinano computer non Dell, i campi SerialNumber e AssetTag saranno vuoti.
  - 6 Nella finestra di dialogo che elenca i volumi del computer, selezionare tutte le unità applicabili e fare clic su **Avanti**. Selezionare MAIUSC+clic o Ctrl+clic per evidenziare più unità.  
Se l'unità selezionata non è stata sottoposta alla crittografia di file/cartelle, non sarà possibile ripristinarla.
  - 7 Immettere la password di ripristino e fare clic su **Avanti**.  
Con un client gestito in remoto, è la password fornita al [Punto 3](#) in [Ottenere il file di ripristino - Computer gestito in remoto](#).  
In Personal Edition, la password è la Password di amministratore per crittografia impostata per il sistema quando le chiavi sono state depositate.
  - 8 Nella schermata Ripristino, fare clic su **Ripristina**. Viene avviato il processo di ripristino.
  - 9 Al completamento del ripristino, fare clic su **Fine**.
- N.B.** Assicurarsi di rimuovere eventuali supporti USB o CD/DVD usati per avviare il computer. In caso contrario è possibile che il computer venga avviato di nuovo nell'ambiente di ripristino.
- 10 Dopo il riavvio, il computer dovrebbe essere completamente funzionante. Se il problema persiste, contattare Dell ProSupport.



## Ripristino dell'Hardware Crypto Accelerator

Con il ripristino dell'Hardware Crypto Accelerator (HCA) di Dell Data Protection, è possibile ripristinare l'accesso a quanto segue:

- File in un'unità con crittografia HCA - Questo metodo decrittografa l'unità usando le chiavi fornite. È possibile selezionare l'unità specifica da decrittografare durante il processo di ripristino.
- Un'unità con crittografia HCA dopo la sostituzione dell'hardware - Questo metodo è usato in seguito alla sostituzione della scheda dell'Hardware Crypto Accelerator o della scheda madre/del TPM. È possibile eseguire un ripristino per accedere nuovamente ai dati crittografati senza decrittografare l'unità.

### Requisiti per il ripristino

Per il ripristino dell'HCA, sono necessari i seguenti componenti:

- Accesso all'ISO di un ambiente di ripristino
- Supporto CD/DVD o USB avviabile

### Panoramica del processo di ripristino

Per ripristinare un sistema in errore:

- 1 Creare l'ISO di ripristino e masterizzarla in un CD/DVD oppure creare una USB avviabile. Consultare [Appendice A - Masterizzare l'ambiente di ripristino](#).
- 2 Ottenere il file di ripristino.
- 3 Effettuare il ripristino.

## Effettuare il ripristino dell'HCA

Seguire la procedura seguente per effettuare un ripristino dell'HCA.

### Ottenere il file di ripristino - Computer gestito in remoto

Per scaricare il file `LSARecovery_<nomecomputer_dominio.com>.exe` generato quando è stato installato Dell Data Protection:

- 1 Aprire la Remote Management Console e, dal riquadro a sinistra, selezionare **Gestione > Ripristina endpoint**.
- 2 Nel campo Nome host, immettere il nome di dominio completo dell'endpoint e fare clic su **Cerca**.
- 3 Nella finestra Ripristino avanzato, immettere una password di ripristino e fare clic su **Scarica**.

**N.B.** È necessario ricordare questa password per avere accesso alle chiavi di ripristino.

Viene scaricato il file `LSARecovery_<machinename_domain.com>.exe`.

## Ottenere il file di ripristino - Computer gestito localmente

Per ottenere il file di ripristino di Personal Edition:

- 1 Individuare il file di ripristino denominato **LSARecovery\_<systemname>.exe**. Questo file è stato archiviato in un'unità di rete o in un dispositivo di archiviazione rimovibile durante la procedura di configurazione guidata relativa all'installazione di Personal Edition.
- 2 Copiare **LSARecovery\_<systemname>.exe** nel computer di destinazione (in cui ripristinare i dati).

## Effettuare il ripristino

- 1 Usando il supporto avviabile creato in precedenza, avviare da quel supporto in un sistema di ripristino o nel dispositivo con l'unità che si sta cercando di ripristinare.  
Si apre un ambiente WinPE.
- 2 Digitare **x** e premere **Invio** per ottenere un prompt dei comandi.
- 3 Individuare il file di ripristino salvato e avviarlo.
- 4 Selezionare un'opzione:
  - Desidero decrittografare l'unità con crittografia HCA.
  - Desidero ripristinare l'accesso all'unità con crittografia HCA.
- 5 Nella finestra di dialogo Informazioni di backup e ripristino, confermare che il numero di Service Tag o di Asset sia corretto e fare clic su **Avanti**.
- 6 Nella finestra di dialogo che elenca i volumi del computer, selezionare tutte le unità applicabili e fare clic su **Avanti**. Selezionare **MAIUSC+clic** o **Ctrl+clic** per evidenziare più unità.  
Se l'unità selezionata non è crittografata con HCA, non sarà possibile ripristinarla.
- 7 Immettere la password di ripristino e fare clic su **Avanti**.  
In un computer gestito in remoto, è la password fornita al [Punto 3](#) in [Ottenere il file di ripristino - Computer gestito in remoto](#).  
In un computer gestito localmente, questa password è la Password di amministratore per crittografia impostata per il sistema in Personal Edition quando le chiavi sono state depositate.
- 8 Nella schermata Ripristino, fare clic su **Ripristina**. Viene avviato il processo di ripristino.
- 9 Quando richiesto, individuare il file di ripristino salvato e fare clic su **OK**.  
Se si sta effettuando una decrittografia completa, la seguente finestra di dialogo visualizza lo stato. Questo processo potrebbe richiedere del tempo.
- 10 Quando viene visualizzato il messaggio che indica che il ripristino è stato completato, fare clic su **Fine**. Il computer si riavvia.

Dopo il riavvio, il computer dovrebbe essere completamente funzionante. Se il problema persiste, contattare Dell ProSupport.



## Ripristino dell'unità autocrittografante (SED)

Con Ripristino unità autocrittografante è possibile ripristinare l'accesso ai file in un'unità autocrittografante mediante i seguenti metodi:

- Effettuare un singolo sblocco dell'unità per escludere e rimuovere l'Autenticazione di preavvio (PBA).
  - Con un client dell'unità autocrittografante gestito in remoto, la PBA può essere abilitata nuovamente in seguito tramite la Remote Management Console.
  - Con un client dell'unità autocrittografante gestito localmente, la PBA può essere abilitata tramite la console di amministrazione di Security Tools.
- Sbloccare e rimuovere definitivamente la PBA dall'unità. Il Single Sign-On non funzionerà se la PBA è stata rimossa.
  - Con un client dell'unità autocrittografante gestito in remoto, la rimozione della PBA richiederà la disattivazione del prodotto dalla Remote Management Console se questa è necessaria per riabilitare la PBA in futuro.
  - Con un client dell'unità autocrittografante gestito localmente, la rimozione della PBA richiederà la disattivazione del prodotto nel SO se questo è necessario per riabilitare la PBA in futuro.

### Requisiti per il ripristino

Per il ripristino dell'unità autocrittografante, sono necessari i seguenti componenti:

- Accesso all'ISO dell'ambiente di ripristino
- Supporto CD/DVD o USB avviabile

### Panoramica del processo di ripristino

Per ripristinare un sistema in errore:

- 1 Creare l'ISO di ripristino e masterizzarla in un CD/DVD oppure creare una USB avviabile. Consultare [Appendice A - Masterizzare l'ambiente di ripristino](#).
- 2 Ottenere il file di ripristino.
- 3 Effettuare il ripristino.

# Effettuare il ripristino dell'unità autocrittografante

Seguire la procedura seguente per effettuare il ripristino dell'unità autocrittografante.

## Ottenere il file di ripristino - Client dell'unità autocrittografante gestito in remoto

- 1 Ottenere il file di ripristino.

Il file di ripristino può essere scaricato dalla Remote Management Console. Per scaricare il file *<nome host>-sed-recovery.dat* generato quando è stato installato Dell Data Protection:

- a Aprire la Remote Management Console e, dal riquadro a sinistra, selezionare **Gestione > Ripristina dati**, quindi selezionare la scheda **Unità autocrittografante**.
- b Nella schermata Ripristina dati, nel campo Nome host, immettere il nome di dominio completo dell'endpoint e fare clic su **Cerca**.
- c Nel campo Unità autocrittografante, selezionare un'opzione.
- d Fare clic su **Crea file di ripristino**.

Viene scaricato il file *<nome host>-sed-recovery.dat*.

## Ottenere il file di ripristino - Client dell'unità autocrittografante gestito localmente

- 1 Ottenere il file di ripristino.

Il file è stato generato ed è accessibile dal percorso di backup selezionato quando Dell Data Protection | Security Tools è stato installato nel computer. Il nome del file è *OpalSPkey<nome sistema>.dat*.

## Effettuare il ripristino

- 1 Usando il supporto avviabile creato, avviare da quel supporto in un sistema di ripristino o nel dispositivo con l'unità che si sta cercando di ripristinare. Con l'applicazione di ripristino si apre un ambiente WinPE.
  - 2 Scegliere l'opzione uno e premere **Invio**.
  - 3 Selezionare **Sfogliare**, individuare il file di ripristino e fare clic su **Apri**.
  - 4 Selezionare un'opzione e fare clic su **OK**.
    - **Singolo sblocco dell'unità** - Questo metodo esclude e rimuove la PBA. Successivamente potrà essere abilitata nuovamente tramite la Remote Management Console (per un client dell'unità autocrittografante gestito in remoto) o tramite la console di amministrazione di Security Tools (per un client dell'unità autocrittografante gestito localmente).
    - **Sblocca l'unità e rimuovi la PBA** - Questo metodo sblocca e rimuove definitivamente la PBA dall'unità. La rimozione della PBA richiederà la disattivazione del prodotto dalla Remote Management Console (per un client dell'unità autocrittografante gestito in remoto) o nel SO (per un client dell'unità autocrittografante gestito localmente) se questo è necessario per riabilitare la PBA in futuro. Il Single Sign-On non funzionerà se la PBA è stata rimossa.
  - 5 Il ripristino è ora completo. Premere un tasto per tornare al menu.
  - 6 Premere **r** per riavviare il sistema.
- N.B.** Assicurarsi di rimuovere eventuali supporti USB o CD/DVD usati per avviare il sistema. In caso contrario è possibile che il computer venga avviato di nuovo nell'ambiente di ripristino.
- 7 Dopo il riavvio, il computer dovrebbe essere completamente funzionante. Se il problema persiste, contattare Dell ProSupport.



## Ripristino della General Purpose Key

La General Purpose Key (GPK) è usata per crittografare parte del registro per gli utenti del dominio. Tuttavia, durante il processo di avvio, in rari casi potrebbe corrompersi e non rimuovere il seal. In tal caso, vengono visualizzati i seguenti errori nel file CMGShield.log nel computer client:

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]
[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure
[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

Se la GPK non rimuove il seal, deve essere ripristinata estraendola dal bundle di ripristino scaricato dal server.

### Ripristinare la GPK

#### Ottenere il file di ripristino

Per scaricare il file `LSARecovery_<nomecomputer_dominio>.exe` generato quando è stato installato Dell Data Protection:

- 1 Aprire la Remote Management Console e, dal riquadro a sinistra, selezionare **Gestione > Ripristina endpoint**.
- 2 Nel campo Nome host, immettere il nome di dominio completo dell'endpoint e fare clic su **Cerca**.

**3** Nella finestra Ripristino avanzato, immettere una password di ripristino e fare clic su **Scarica**.

**N.B.** È necessario ricordare questa password per avere accesso alle chiavi di ripristino.

Viene scaricato il file `LSARecovery_<machinename_domain.com>.exe`.

### **Effettuare il ripristino**

**1** Usando il supporto avviabile creato in [Appendice A - Masterizzare l'ambiente di ripristino](#), avviare da quel supporto in un sistema di ripristino o nel dispositivo con l'unità che si sta cercando di ripristinare.

Si apre un ambiente WinPE.

**2** Immettere **x** e premere **Invio** per ottenere un prompt dei comandi.

**3** Individuare il file di ripristino e avviarlo.

Si apre la finestra di dialogo della diagnostica del Client di crittografia mentre il file di ripristino viene generato in background.

**4** Al prompt dei comandi di amministrazione, eseguire `LSARecovery_<machinename_domain.com>.exe -p <password> -gpk`

Questo restituisce il file `GPKRCVR.txt` per il computer.

**5** Copiare il file `GPKRCVR.txt` nella directory principale dell'unità del SO del computer.

**6** Riavviare il sistema.

Il file `GPKRCVR.txt` verrà utilizzato dal sistema operativo e rigenererà la GPK in tale computer.

**7** Se richiesto, riavviare di nuovo il sistema.

## Ripristino dei dati delle unità crittografate

Se il computer di destinazione non è avviabile e non esiste alcun guasto dell'hardware, il ripristino dei dati può essere effettuato nel computer avviato in un ambiente di ripristino. Se il computer di destinazione non è avviabile e ha un guasto all'hardware, oppure si tratta di un dispositivo USB, il ripristino dei dati può essere effettuato avviando da un'unità secondaria. Quando si imposta un'unità secondaria, è possibile visualizzare il file system e individuare le directory. Tuttavia, se si prova ad aprire o copiare un file, appare l'errore *Accesso negato*.

### Ripristinare i dati delle unità crittografate

Per ripristinare i dati delle unità crittografate:

- 1** Per ottenere il DCID/ID ripristino dal computer, scegliere un'opzione:
  - a** Eseguire WSScan in qualsiasi cartella in cui sono archiviati i dati crittografati comuni. Il DCID/ID ripristino di otto caratteri viene visualizzato dopo "Comune".
  - b** Aprire la Remote Management Console e selezionare la scheda **Dettagli e azioni** per l'endpoint.
  - c** Nella sezione Dettagli Shield della schermata Dettagli endpoint, individuare il DCID/ID ripristino.

- 2 Per scaricare la chiave dal server, individuare ed eseguire l'utilità di sblocco amministrativa Dell (CMGAu).  
È possibile ottenere l'utilità di sblocco amministrativa Dell da Dell ProSupport.
- 3 Nella finestra di dialogo dell'utilità amministrativa Dell (CMGAu), immettere le seguenti informazioni (alcuni campi potrebbero essere prepopolati) e fare clic su **Avanti**.
 

<b>Server:</b>	nome host completo del server, per esempio: Device Server: <a href="https://&lt;server.organizzazione.com&gt;:8081/xapi">https://&lt;server.organizzazione.com&gt;:8081/xapi</a> Security Server: <a href="https://&lt;server.organizzazione.com&gt;:8443/xapi">https://&lt;server.organizzazione.com&gt;:8443/xapi</a>
<b>Amministratore Dell:</b>	nome dell'account dell'amministratore Forensic (abilitato nel server)
<b>Password amministratore Dell:</b>	password dell'account dell'amministratore Forensic (abilitato nel server)
<b>MCID:</b>	cancellare il campo MCID
<b>DCID:</b>	il DCID/ID ripristino ottenuto in precedenza.
- 4 Nella finestra di dialogo dell'utilità amministrativa Dell, selezionare **No**, esegui il download da un server ora e fare clic su **Avanti**.
 

**N.B.** Se il Client B di crittografia non è installato, viene visualizzato il messaggio *Sblocco non riuscito*. Passare ad un computer con il Client di crittografia installato.
- 5 A completamento del download e dello sblocco, copiare i file che è necessario ripristinare da questa unità. Tutti i file sono leggibili. ***Non fare clic su Fine prima di aver ripristinato i file.***
- 6 Solo in seguito al ripristino dei file pronti da bloccare nuovamente, fare clic su **Fine**.  
*Una volta selezionato Fine, i file crittografati non saranno più disponibili.*

## Ripristino di BitLocker Manager

Per ripristinare i dati, è necessario ottenere un pacchetto chiavi o una password di ripristino dalla Remote Management Console, tramite i quali sarà possibile sbloccare i dati nel computer.

### Ripristinare i dati

- 1 Eseguire l'accesso alla Remote Management Console come amministratore Dell.
- 2 Nel riquadro sinistro, fare clic su **Gestione > Ripristina dati**.
- 3 Fare clic sulla scheda *Manager*.
- 4 Per *BitLocker*:

Immettere l'**ID ripristino** ricevuto da BitLocker. Facoltativamente, immettendo il Nome host e il Volume, ID ripristino viene compilato.

Fare clic su **Ottieni password di ripristino** o **Crea pacchetto chiavi**.

A seconda della modalità di ripristino dati desiderata, verrà utilizzata la password di ripristino o il pacchetto chiavi.

Per il *TPM*:

Immettere il **Nome host**.

Fare clic su **Ottieni password di ripristino** o **Crea pacchetto chiavi**.

A seconda della modalità di ripristino dati desiderata, verrà utilizzata la password di ripristino o il pacchetto chiavi.

- 5 Per completare il ripristino, consultare le [Istruzioni di ripristino Microsoft](#).
- N.B.** Se BitLocker Manager non è "proprietario" di TPM, il pacchetto chiavi e la password del TPM non sono disponibili nel database Dell. L'utente riceverà un messaggio di errore nel quale si informa che Dell non riesce a individuare la chiave (comportamento previsto).

Per ripristinare un TPM "di proprietà" il cui proprietario è un'entità diversa da BitLocker Manager, è necessario seguire il processo di ripristino del TPM da quel proprietario specifico oppure seguire il processo di ripristino del TPM esistente.



# A

## Appendice A - Masterizzare l'ambiente di ripristino

### Masterizzare l'ISO dell'ambiente di ripristino su CD\DVD

Il seguente collegamento rimanda alla procedura necessaria per usare Microsoft Windows 7/8/10 al fine di creare un CD o DVD avviabile per l'ambiente di ripristino.

<http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file>

### Masterizzare l'ambiente di ripristino su un supporto rimovibile

Per creare una USB avviabile, seguire le istruzioni in questo articolo di Microsoft:

[https://technet.microsoft.com/en-us/library/jj200124\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj200124(v=ws.11).aspx)









0XXXXXA0X