Dell Data Protection

Guida al ripristino v8.13/v1.7/v1.4/v1.2

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.

Guida al ripristino Dell Data Protection

2017 - 04

Rev. A01

Sommario

1

Guida introduttiva al ripristino

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
  - Per masterizzare un CD o un DVD, vedere Masterizzazione dell'ISO dell'ambiente di ripristino su CD\DVD per ulteriori dettagli.
  - Se si utilizzano supporti USB, vedere Masterizzazione dell'ambiente di ripristino su supporti rimovibili per ulteriori 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.

Contattare Dell ProSupport

Per assistenza telefonica sui prodotti Dell Data Protection, chiamare il numero +1-877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell Data Protection 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.

2

Ripristino della crittografia basato su regole o di file/cartelle

Con il ripristino della crittografia basato su regole o 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.

Panoramica del processo di ripristino

Per ripristinare un sistema in errore:

1 Masterizzare l'ambiente di ripristino su CD/DVD o creare un USB avviabile. Vedere Appendice A - Masterizzazione dell'ambiente di ripristino.
2 Ottenere il file di ripristino.
3 Effettuare il ripristino.

Eseguire il ripristino della crittografia basata su regole o FFE

Seguire questa procedura seguente per effettuare il ripristino della crittografia basata su regole o FFE.

Ottenere il file di ripristino - Computer gestito in remoto

Per scaricare il file **<nomemacchina_dominio.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 **<nomemacchina_dominio.com>** > **.exe** in una posizione accessibile quando avviato 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 **LSARecovery_<nomesistema> .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_<nomesistema> .exe** nel computer di destinazione (il computer da 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 il 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 crittografata in base a criteri o con FFE, non sarà possibile ripristinarla.

7 Immettere la password di ripristino e fare clic su **Avanti**.
Con un client gestito in remoto, questa è la password fornita nel passaggio 3 di 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 termine 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 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.
   L'ID di ripristino/DCID di otto caratteri viene visualizzato dopo "Comune".

   b Aprire la Console di gestione remota, quindi selezionare la scheda **Dettagli e azioni** dell'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**.
   Server: nome host completo del server, ad esempio:

   Device Server: **https://<server.organizzazione.com>:8081/xapi**

   Security Server: **https://<server.organizzazione.com>:8443/xapi/**

   Amministratore Dell: nome dell'account dell'amministratore Forensic (abilitato nel server)

   Password Amministratore Dell: password dell'account dell'amministratore Forensic (abilitato nel server)

   MCID: cancellare il campo MCID

   DCID: il DCID/ID di ripristino ottenuto in precedenza.

4 Nella finestra di dialogo dell'utilità amministrativa Dell, selezionare **No, eseguire il download da un server ora** e fare clic su **Avanti**.

> **N.B.:**
> Se il client di crittografia non è installato, viene visualizzato un messaggio indicante che l'operazione di sblocco non è riuscita. 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 fino a quando non sono stati ripristinati 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 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 dell'ambiente di ripristino
- Supporto CD\DVD o USB avviabile

Panoramica del processo di ripristino

Per ripristinare un sistema in errore:

1 Masterizzare l'ambiente di ripristino su CD/DVD o creare un USB avviabile. Vedere Appendice A - Masterizzazione dell'ambiente di ripristino.
2 Ottenere il file di ripristino.
3 Effettuare il ripristino.

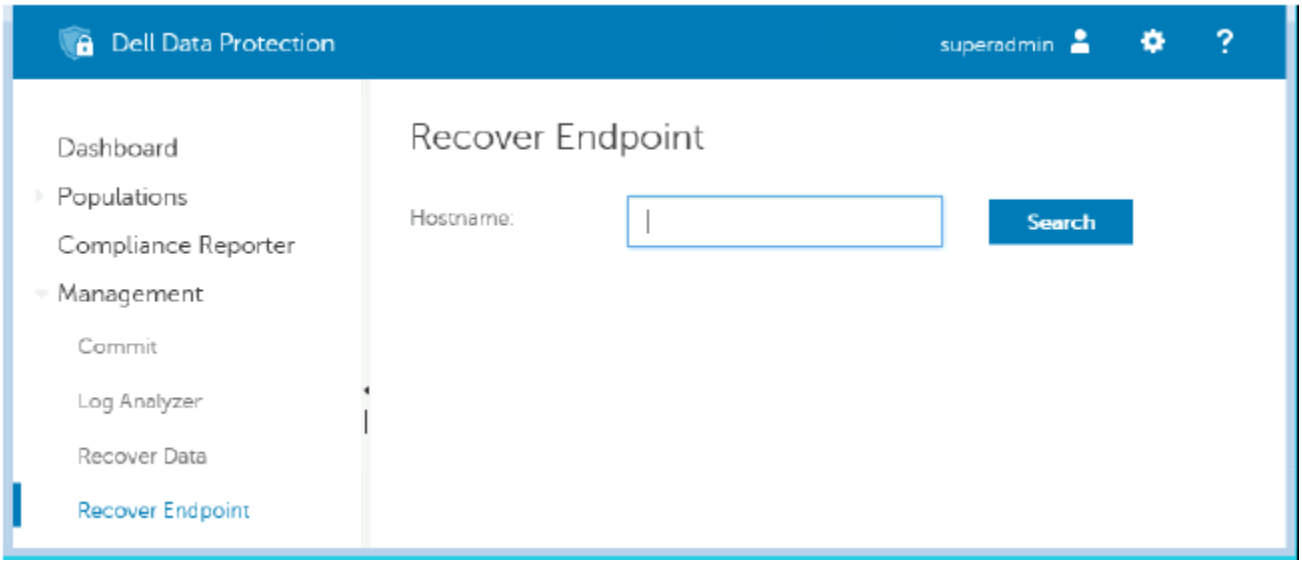
Effettuare il ripristino dell'HCA

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

Ottenere il file di ripristino - Computer gestito in remoto

Per scaricare il file **<nomemacchina_dominio.com>.exe** che è stato generato quando è stato installato Dell Data Protection:

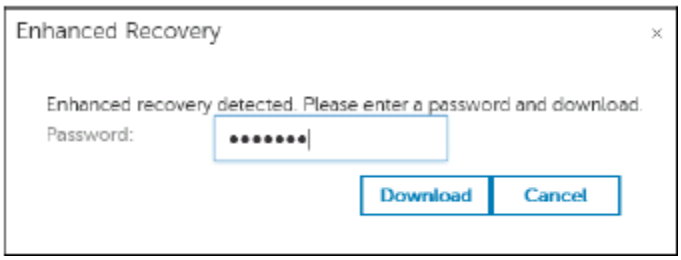
1 Aprire la Remote Management Console e, dal riquadro a sinistra, selezionare **Gestione** > **Ripristina endpoint**.



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.



Ottenere il file di ripristino - Computer gestito localmente

Per ottenere il file di ripristino di Personal Edition:

1 Individuare il file di ripristino **LSARecovery_<nomesistema> > .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_<nomesistema> > .exe** nel computer di destinazione (il computer da 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 aprire il 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**.

Con un computer gestito in remoto, questa è la password fornita nel passaggio 3 di 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 indicante 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 Masterizzare l'ambiente di ripristino su CD/DVD o creare un USB avviabile. Vedere Appendice A - Masterizzazione dell'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

Ottenere il file di ripristino.

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

a Aprire la console di gestione remota e, nel riquadro a sinistra, selezionare **Gestione > Ripristina dati** , quindi selezionare la scheda **SED**.

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 **<nomehost>-sed-recovery.dat**.

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

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 file è *OpalSPkey<nomesistema>.dat*.

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. Con l'applicazione di ripristino si apre un ambiente WinPE.

2 Scegliere l'opzione uno e premere **Invio**.

3 Selezionare **Sfoglia**, individuare il file di ripristino, quindi fare clic su **Apri**.

4 Selezionare un'opzione e fare clic su **OK**.

- **Singolo sblocco dell'unità** - Questo metodo ignora e rimuove il 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).
- **Sblocco dell'unità e rimozione del PBA** - Questo metodo sblocca, quindi rimuove in modo permanente il 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 computer.

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.

5

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 **<nomemacchina_dominio.com>.exe** che è stato 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 **<nomemacchina_dominio.com>.exe**.

Effettuare il ripristino

1 Creare un supporto avviabile dell'ambiente di ripristino. Per istruzioni, vedere Appendice A - Masterizzazione dell'ambiente di ripristino.

2 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.

3 Immettere **x** e premere **Invio** per aprire il prompt dei comandi.

4 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.

5 Dal prompt dei comandi come amministratore, eseguire **<nomemacchina_dominio.com** > **.exe** > **-p <password** > **-gpk**
Questo restituisce il file GPKRCVR.txt per il computer.

6 Copiare il file **GPKRCVR.txt** nel percorso principale dell'unità del computer con il sistema operativo.

7 Riavviare il sistema.

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

8 Se richiesto, riavviare di nuovo il sistema.

6

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 console di gestione remota 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 di ripristino** ricevuto da BitLocker. Facoltativamente, immettendo il Nome host e il Volume, ID ripristino viene compilato.

Fare clic su **Ottieni password di ripristino** o su **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 su **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, vedere le istruzioni di Microsoft per il ripristino.

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.

7

Recupero password

Succede che gli utenti dimentichino la propria password. Per fortuna, in questo caso hanno vari modi di accedere nuovamente a un computer con autenticazione di preavvio.

- La funzione Domande di ripristino offre l'autenticazione basata su domanda e risposta.
- I codici Domanda/Risposta consentono agli utenti di collaborare con l'amministratore per riavere accesso al proprio computer. Questa funzione è disponibile solo per gli utenti i cui computer sono gestiti da un'organizzazione.

Domande di ripristino

La prima volta che un utente accede a un computer, deve rispondere a una serie standard di domande che l'amministratore ha configurato. Dopo che le risposte sono state registrate, verranno utilizzate nel momento in cui l'utente dimentica la propria password. Se risponderà correttamente alle domande, potrà riavere accesso a Windows.

Prerequisiti

- Le domande di ripristino devono essere impostate dall'amministratore.
- L'utente deve aver registrato le sue risposte alle domande.
- Prima di fare clic sull'opzione di menu **Problema d'accesso**, l'utente deve immettere un nome utente e un dominio validi.

Per accedere alle domande di ripristino dalla schermata di accesso PBA:

1 Immettere un nome dominio e un nome utente validi.
2 Nella parte inferiore sinistra della schermata, fare clic su **Opzioni** > **Problema d'accesso**.
3 Quando viene visualizzata la finestra di dialogo di domande e risposte, immettere le risposte fornite nelle Domande di ripristino al primo accesso.

Codici Domanda/Risposta

Il ripristino Domanda/Risposta può essere usato per l'autenticazione tramite PBA per accedere a Windows. Il metodo Domanda/Risposta può essere utilizzato nei seguenti scenari:

- Quando un utente non ricorda le risposte fornite al momento della registrazione delle domande di ripristino.
- Quando l'amministratore non ha abilitato la funzione Domande di ripristino.
- Quando un utente è in remoto senza la connettività di rete e non è in grado di ricevere un comando di sblocco da Security Server tramite Controllo dispositivo SED

Un utente può accedere alla schermata Domanda/Risposta facendo clic sull'opzione **Problema d'accesso** o inserendo password errate per un numero di volte oltre il limite, senza il cavo di rete collegato. Se la funzione Domande di ripristino è stata disattivata, l'opzione **Problema d'accesso** apre direttamente la schermata Domanda/Risposta.

Requisito

- Il ripristino Domanda/Risposta è disponibile solo per i computer di dominio gestiti in remoto dall'organizzazione o dall'azienda dell'utente.

Prerequisiti

- Scollegare il computer dalla rete prima di rispondere alle Domande di ripristino o prima di inserire i codici Domanda/Risposta.
- Prima di fare clic sull'opzione Problema d'accesso, immettere un nome utente e un dominio validi.

Per utilizzare il ripristino Domanda/Risposta

1 L'utente fa clic sul collegamento **Opzioni** per visualizzare il menu.

2 L'utente fa clic su **Problema d'accesso** > **Domanda/Risposta**.

> **N.B.:**
> L'opzione Domanda/Risposta è disponibile solo sui computer gestiti da un'azienda. Se il computer non fa parte di un dominio, l'opzione Domanda/Risposta non viene visualizzata nel menu.

3 Quando richiesto, l'utente contatta l'help desk e fornisce all'amministratore il nome dispositivo (nome host) e il codice domanda.

4 L'amministratore apre la console di gestione remota, fa clic su **Gestione** > **Ripristina dati**, quindi fa clic su **SED** dal menu principale.

5 Sotto Ripristina accesso utente SED, l'amministratore inserisce il **Nome host** ricevuto dall'utente e fa clic su **Cerca**.

6 L'amministratore seleziona il nome dell'utente che chiede assistenza:

7 Immette il codice ricevuto dall'utente nel campo **Domanda** e fa clic su **Genera risposta**.

8 Fornisce all'utente il codice risposta generato.

> **N.B.:**
> Questi codici non distinguono maiuscole e minuscole. I numeri sono visualizzati in rosso e le lettere in blu.

9 L'utente immette il codice di risposta nei campi **Codice di risposta** della schermata di accesso PBA. Esempio di codice di risposta immesso dall'utente:

10 L'utente fa clic sulla freccia destra per continuare e per eseguire l'autenticazione dopo la schermata PBA.

11 Fare clic su **Invia**.

L'utente può eseguire l'autenticazione dopo il PBA utilizzando la funzione di Domanda/Risposta una sola volta. Dopo il riavvio del computer, il livello PBA riprende la protezione del computer e chiede di nuovo all'utente di eseguire l'accesso nella schermata PBA.

> **N.B.:**
> Dopo che l'utente ha visualizzato la finestra di dialogo Domanda/Risposta, deve completare la sequenza Domanda/Risposta per poter avere di nuovo accesso al sistema. Se l'utente spegne il computer e tenta di effettuare nuovamente l'accesso, anche con la password corretta, il PBA ripete la richiesta all'utente con la finestra di dialogo Domanda/Risposta.

8

Ripristino della password con External Media Shield

External Media Shield (EMS) offre la possibilità di proteggere dispositivi di archiviazione rimovibili sia all'interno che all'esterno dell'organizzazione, consentendo agli utenti di crittografare le unità flash USB e altri supporti di archiviazione rimovibili. L'utente assegna una password a ciascun supporto rimovibile da proteggere. In questa sezione viene descritto il processo di ripristino dell'accesso a un dispositivo USB di archiviazione crittografato quando un utente dimentica la password dello stesso.

Ripristino dell'accesso ai dati

Quando un utente sbaglia la password per un numero di volte che supera i tentativi consentiti, il dispositivo USB passa in modalità di autenticazione manuale.

Quello di **autenticazione manuale** è il processo di erogazione dei codici dal cliente a un amministratore che è collegato al server.

Quando è in modalità di autenticazione manuale, l'utente dispone di due opzioni per reimpostare la propria password e ripristinare l'accesso ai dati.

L'amministratore fornisce un codice di accesso per il client, consentendo all'utente di reimpostare la propria password e avere di nuovo accesso ai propri dati crittografati.

1 Quando viene richiesta la password, fare clic sul pulsante **Password dimenticata**.

   Viene visualizzata la finestra di dialogo di conferma.

2 Fare clic su **Sì** per confermare. Dopo la conferma, il dispositivo passa in modalità di autenticazione manuale.

3 Contattare l'amministratore dell'Help desk e fornirgli i codici visualizzati nella finestra di dialogo.

4 Accedere alla Console di gestione remota come amministratore dell'Help desk amministratore; l'amministratore dell'Help desk deve disporre dei privilegi Help desk.

5 Andare all'opzione di menu **Ripristina dati** nel riquadro di sinistra.

6 Immettere i codici forniti dall'utente finale.

7 Fare clic sul pulsante **Genera risposta** nell'angolo in basso a destra della schermata.

8 Fornire all'utente il codice di accesso.

> **N.B.:**
>
> Assicurarsi di eseguire manualmente l'autenticazione dell'utente prima di fornire il codice di accesso. Ad esempio, al telefono porre all'utente una serie di domande di cui dovrebbe essere l'unico a conoscere le risposte, ad esempio "Qual è il suo numero di ID dipendente?" Un altro esempio: richiedere all'utente di passare all'Help desk con i documenti per accertarsi che sia il proprietario dei supporti. La mancata autenticazione di un utente prima di fornire il codice di accesso al telefono potrebbe consentire a un malintenzionato di accedere a supporti rimovibili crittografati.

9 Reimpostare la password dei supporti crittografati.

   All'utente viene richiesto di reimpostare la propria password per i supporti crittografati.

Ripristino autonomo

Ripristino autonomo è il processo di reimpostazione della password di un dispositivo rimovibile cifrato tramite il reinserimento dell'unità in una macchina protetta, una volta che il proprietario del supporto ha effettuato l'accesso. Se il proprietario del supporto ha eseguito l'autenticazioen del Mac o del PC protetto, il client rileva la perdita di materiale chiave e richiede all'utente di inizializzare nuovamente il dispositivo. In quel momento, l'utente può reimpostare la propria password e avere nuovamente accesso ai dati crittografati.

1 Accedere a una workstation crittografata con Dell Data Protection come proprietario del supporto.
2 Inserire il dispositivo di archiviazione rimovibile crittografato.
3 Quando richiesto, immettere una nuova password per inizializzare nuovamente il dispositivo di archiviazione rimovibile.

   Se l'operazione è stata completata correttamente, viene visualizzata una piccola notifica indicante che la password è stata accettata.
4 Accedere al dispositivo di archiviazione e verificare l'accesso ai dati.

9

Ripristino di Dell Data Guardian

Lo strumento di ripristino consente:

- Decrittazione di file di Office protetti

  Sono inclusi i file fino alla tripla crittografia: con più metodi di crittografia, può accadere che a un file ne vengano applicati due o tre. Se l'utente apre il file, un messaggio di errore indica di contattare l'amministratore per ripristinarlo.
- Deposito di materiale chiave
- Possibilità di verificare i file manomessi
- Possibilità di forzare la decrittografia dei documenti di Office protetti con wrapper manomesso, ad esempio il frontespizio di un file Office protetto nel cloud o su un dispositivo che non dispone di Data Guardian

Requisiti per il ripristino

I requisiti comprendono:

- Microsoft .NET Framework 4.5.2 in esecuzione sull'endpoint da ripristinare.
- Il ruolo di Amministratore Forensic deve essere assegnato nella Console di gestione remota per l'amministratore che esegue il ripristino.

Eseguire il ripristino di Data Guardian

Attenersi a questi passaggi per eseguire il ripristino dei documenti Office protetti di Data Guardian.

Eseguire il ripristino da Windows, da un'unità flash USB o da un'unità di rete

Per eseguire il ripristino:

1 Dal supporto di installazione Dell, copiare **RecoveryTools.exe** su una delle seguenti destinazioni:

   - Computer - Copiare il file .exe sul computer su cui verranno ripristinati i documenti Office.
   - USB - Copiare il file .exe sull'unità flash USB ed eseguirlo dalla stessa.
   - Unità di rete

2 Fare doppio clic su **RecoveryTools.exe** per avviare il programma di installazione.

3 Nella finestra di Data Guardian, immettere l'URL del server Dell in questo formato:

   https://<server.dominio.com>:8443/cloud

   N.B.:
   Sostituire <server.dominio.com> con il nome host completo del server Dell che gestisce Data Guardian su tale endpoint. Per individuare l'URL del server Dell, fare clic sull'icona Data Guardian nella barra delle applicazioni, quindi su **Dettagli**. Nell'angolo superiore sinistro della schermata Dettagli viene visualizzato l'URL del server.

4 Immettere nome utente e password, quindi fare clic su **Effettuare l'accesso**.

N.B.:
Non deselezionare la casella di controllo di attivazione del certificato di attendibilità SSL, a meno che l'amministratore non lo richieda.

N.B.:
Se non si è Amministratore Forensic e si immettono le credenziali, viene visualizzato un messaggio indicante che non si dispone dei diritti di accesso.

Se si è Amministratore Forensic, lo strumento di ripristino si apre.

5 Selezionare **Origine**.

N.B.:
È necessario selezionare un'origine e una destinazione, ma è possibile selezionarle in entrambi gli ordini.

6 Fare clic su **Sfoglia** per selezionare la cartella o unità da ripristinare.

7 Fare clic su **OK**.

8 Fare clic su **Destinazione**

9 Fare clic su **Sfoglia** per selezionare una destinazione, come ad esempio un dispositivo esterno, un percorso di directory o il desktop.

10 Fare clic su **OK**.

11 Selezionare una o più caselle di controllo in base a ciò che si desidera ripristinare.

Opzioni	Descrizione
Deposito	• Ripristina chiavi generate offline, che potrebbero non essere depositate sul server Dell. • Se l'unità disco rigido non funziona mentre l'utente è offline dalla rete, utilizzare l'unità collegata in modalità Slave per ripristinare i dati e le chiavi depositate dal computer.
Decrittografato	Puntare lo strumento di ripristino su una directory contenente i documenti Office protetti per decrittografarli. In alternativa, se si sono verificate manomissioni, selezionare una o entrambe queste opzioni (vedere i dettagli riportati di seguito): • **Verifica manomissione** - verifica la disponibilità di file manomessi ma non li decrittografa. • **Verifica manomissione** e **Forza decrittografia anche se manomesso** - verifica la presenza di file manomessi e se il wrapper di un documento Office protetto è stato manomesso, Data Guardian ripara il wrapper e decrittografa il documento Office.
Verifica manomissione	Rileva i file che sono stati manomessi e li registra o invia una notifica all'utente. Registra l'autore della manomissione del file. Non decrittografa i file.
Forza decrittografia anche se manomesso	Per selezionare tale opzione, è necessario selezionare anche **Verifica manomissione**. Se un utente non autorizzato ha manomesso il wrapper di un documento Office protetto, ad esempio il frontespizio, sia nel cloud sia su un dispositivo che non dispone di Data Guardian, selezionare questa opzione per riparare il wrapper e per forzare la decrittografia del file Office protetto. **N. B.:** se il file .xen nel wrapper del file di Office crittografato è stato manomesso, il file non può essere ripristinato.

Ciascun documento protetto di Office ha una filigrana nascosta che contiene la cronologia utenti, il nome del computer originale e gli altri nomi di computer che hanno modificato il file. Per impostazione predefinita, lo strumento di ripristino controlla le filigrane nascoste e registra le informazioni.

12 Al termine delle selezioni, fare clic su **Scansione**.

L'area Registro visualizza:

- Cartelle trovate e sottoposto a scansione nell'origine selezionata
- Riuscita o meno della decrittografia

Lo strumento di ripristino aggiunge i file ripristinati alla destinazione selezionata. È possibile aprire e visualizzare i file

Appendice A - Masterizzazione dell'ambiente di ripristino

È possibile scaricare Master Installer.

Masterizzazione dell'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

Masterizzazione dell'ambiente di ripristino su supporti rimovibili

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

https://technet.microsoft.com/it-it/library/jj200124(v=ws.11).aspx