Dell Data Protection

Wiederherstellungshandbuch v8.13/v1.7/v1.4/v1.2

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

Dell Data Protection, Wiederherstellungshandbuch

2017 - 04

Rev. A01

Inhaltsverzeichnis

Erste Schritte bei der Wiederherstellung

Dieser Abschnitt erläutert, was zum Erstellen der Wiederherstellungsumgebung benötigt wird.

- Laden Sie eine Kopie der Software der Wiederherstellungsumgebung herunter. Sie befindet sich im Ordner „Windows Recovery Kit“ auf dem Dell Data Protection Installationsmedium.
- CD-R-, DVD-R-Medien oder formatierten USB-Medien
  - Einzelheiten zum Brennen einer CD oder DVD finden Sie in Burning the Recovery Environment ISO to CD\DVD (Die Wiederherstellungsumgebung ISO auf CD/DVD brennen).
  - Einzelheiten zur Verwendung von USB-Medien finden Sie in Burning the Recovery Environment on Removable Media (Die Wiederherstellungsumgebung auf Wechseldatenträger brennen).
- Wiederherstellungspaket für fehlerhafte Gerät
  - Für im Remote-Zugriff verwaltete Clients erklären die folgenden Anweisungen wie Sie ein Wiederherstellungspaket von Ihrem Dell Data Protection Server abrufen.
  - Für lokal verwaltete Clients wurde das Wiederherstellungspaket während des Setups entweder auf einem freigegebenen Netzwerklaufwerk oder auf einem externen Datenträger erstellt. Suchen Sie dieses Paket, bevor Sie fortfahren.

Kontaktaufnahme mit dem Dell ProSupport

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

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

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

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

Richtlinienbasierte oder Datei-/Ordner-Verschlüsselungswiederherstellung

Mit der richtlinienbasierten Verschlüsselung oder FFE-Wiederherstellung (FFE steht für File Folder Encryption, Datei-/Ordnerverschlüsselung) können Sie den Zugriff auf Folgendes wiederherstellen:

- einen Computer, der nicht startet und eine Eingabeaufforderung zur Durchführung der SDE-Wiederherstellung anzeigt
- einen Computer, auf dem Sie nicht auf verschlüsselte Daten zugreifen und keine Richtlinien bearbeiten können
- einen Server, auf dem Dell Data Protection | Server Encryption ausgeführt wird, und auf den eine der oben genannten Bedingungen zutrifft
- einen Computer, auf dem die Hardware Crypto Accelerator-Karte oder die Hauptplatine/das TPM ersetzt werden müssen

Übersicht über den Wiederherstellungsprozess

So stellen Sie ein ausgefallenes System wieder her:

1 Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe Appendix A - Burning the Recovery Environment (Anhang A, Brennen der Wiederherstellungsumgebung).

2 Besorgen Sie sich die Wiederherstellungsdatei.

3 Führen Sie die Wiederherstellung durch.

Richtlinienbasierte Verschlüsselung oder FFE-Wiederherstellung (File Folder Encryption, Datei-/Ordnerverschlüsselung)

Führen Sie diese Schritte aus, um eine richtlinienbasierte Verschlüsselung oder FFE-Wiederherstellung auszuführen.

Wiederherstellungsdatei besorgen - Computer mit Remote-Verwaltung

So laden Sie die Datei **<machinename_domain.com>.exe** herunter:

1 Öffnen Sie die Remote Management Console und wählen Sie im linken Fensterbereich **Verwaltung** > **Endpunkt wiederherstellen** aus.

2 Geben Sie im Feld „Host-Name“ den vollständig qualifizierten Domänennamen (FQDN) des Endpunktes ein und klicken Sie auf **Suchen**.

3 Geben Sie im Fenster „Erweiterte Wiederherstellung“ ein Wiederherstellungspasswort ein und klicken Sie auf **Herunterladen**.

> **ANMERKUNG:**
> Sie müssen sich dieses Passwort für den Zugriff auf die Wiederherstellungsschlüssel merken.

4 Kopieren Sie die Datei **<machinename_domain.com** > **.exe** an einen Ort, wo auf sie zugegriffen werden kann, wenn WinPE gestartet wird.

Wiederherstellungsdatei besorgen - Computer mit lokaler Verwaltung

So erhalten Sie die Personal Edition-Wiederherstellungsdatei:

1 Suchen Sie die Wiederherstellungsdatei mit dem Namen **LSARecovery_<systemname> > .exe**. Diese Datei wurde beim Ausführen des Einrichtungsassistenten zur Installation von Personal Edition auf einem Netzwerklaufwerk oder Wechselspeichermedium gespeichert.

2 Kopieren Sie **LSARecovery_<systemname> > .exe** auf den Zielcomputer (den Computer, auf dem die Daten wiederhergestellt werden sollen).

Wiederherstellung durchführen

1 Starten Sie auf einem Wiederherstellungssystem oder auf dem Gerät mit dem Laufwerk, das Sie wiederzustellen versuchen den zuvor von Ihnen erstellten startfähigen Datenträger. Es wird eine WinPE-Umgebung geöffnet.

2 Geben Sie **x** ein und drücken Sie **Enter** (Eingabetaste), um eine Befehlseingabeaufforderung zu erhalten.

3 Navigieren Sie zur Wiederherstellungsdatei und starten Sie sie.

4 Wählen Sie eine Option aus:

- Mein System lässt sich nicht booten, und ich werde zur SDE-Wiederherstellung aufgefordert.

  Diese Option ermöglicht Ihnen die Neuerstellung der Hardwareüberprüfungen, die der Verschlüsselungs-Client beim Starten über das Betriebssystem durchführt.

- Mein System wird gerade neu installiert oder lässt mich keine verschlüsselten Daten anzeigen und Richtlinien bearbeiten.

  Verwenden Sie diese Option, falls die Hardware Crypto Accelerator-Karte oder die Hauptplatine/das TPM ersetzt werden müssen.

5 Bestätigen Sie im Dialogfeld mit den Sicherungs- und Wiederherstellungsinformationen, dass die Informationen zum wiederherzustellenden Client-Computer korrekt sind, und klicken Sie auf **Next** (Weiter).

Bei der Wiederherstellung von Computern, die nicht von Dell stammen, sind die Felder für die Seriennummer und die Systemkennnummer leer.

6 Wählen Sie in dem Dialogfeld mit der Liste der Volumes des Computers alle anwendbaren Laufwerke aus und klicken Sie auf **Next** (Weiter).

Klicken Sie bei gedrückter Umschalttaste oder Strg-Taste, um mehrere Laufwerke auszuwählen.

Falls das ausgewählte Laufwerk nicht über Richtlinien oder FFE verschlüsselt ist, kann es nicht wiederhergestellt werden.

7 Geben Sie Ihr Wiederherstellungspasswort ein und klicken Sie auf **Next** (Weiter).

Bei einem remote verwalteten Client handelt es sich um das in Step 3 (Schritt 3) in Obtain the Recovery File - Remotely Managed Computer (Wiederherstellungsdatei besorgen - Computer mit remote Verwaltung) eingegebene Passwort.

Bei der Personal Edition ist das Passwort das Encryption-Administrator-Passwort, das beim Hinterlegen der Schlüssel für das System festgelegt wurde.

8 Klicken Sie im Dialogfeld „Recover“ (Wiederherstellung) auf **Recover** (Wiederherstellen) Der Wiederherstellungsvorgang beginnt.

9 Wenn die Wiederherstellung abgeschlossen ist, klicken Sie auf **Finish** (Fertig stellen).

> **ANMERKUNG:**
> Stellen Sie sicher, dass sämtliche USB- oder CD-\DVD-Medien, die verwendet wurden, um den Computer zu starten, entfernt wurden. Ist das nicht der Fall, kann das zu einem Neustart in die Wiederherstellungsumgebung führen.

10 Nachdem der Computer neu gestartet wurde, sollte er voll funktionsfähig sein. Falls das Problem weiterhin besteht, kontaktieren Sie den Dell ProSupport.

Datenwiederherstellung auf einem verschlüsselten Laufwerk

Wenn der Zielcomputer nicht startfähig ist und kein Hardwarefehler vorliegt, kann die Datenwiederherstellung durchgeführt werden, indem der Computer in einer Wiederherstellungsumgebung gestartet wird. Wenn der Zielcomputer nicht startfähig ist und ein Hardwarefehler vorliegt, oder wenn es sich dabei um ein USB-Gerät handelt, kann die Datenwiederherstellung durchgeführt werden, indem der Computer über ein Slave-Laufwerk gestartet wird. Bei einem Slave-Laufwerk können Sie das Dateisystem sehen und die Verzeichnisse durchsuchen. Wenn Sie jedoch versuchen, eine Datei zu öffnen oder zu kopieren, tritt ein Fehler vom Typ *Access denied* (Zugriff verweigert) auf.

Daten auf verschlüsseltem Laufwerk wiederherstellen

So können Sie Daten auf einem verschlüsselten Laufwerk wiederherstellen:

1 Wählen Sie eine der folgenden Optionen aus, um die DCID/Wiederherstellungs-ID vom Computer zu erhalten:
   a Führen Sie WSScan auf einem beliebigen Ordner aus, in dem gemeinsame verschlüsselte Daten gespeichert sind.
   Die achtstellige DCID/Wiederherstellungs-ID wird nach dem Wort „Common“ (Gemeinsam) angezeigt.

   b Öffnen Sie die Remote-Verwaltungskonsole und wählen Sie die Registerkarte **Details & Actions** (Details und Aktionen) für den Endpunkt.
   c Suchen Sie im Abschnitt „Shield Detail“ (Shield-Detail) des Detailbildschirms für das Endgerät die DCID/Recovery-ID.

2 Um den Schlüssel vom Server herunterzuladen, wechseln Sie zum Dienstprogramm Dell Administrative Unlock (**CMGAu**)
Das Dienstprogramm Dell Administrative Unlock erhalten Sie über den Dell ProSupport.

3 Geben Sie im Dialogfeld des Dell Verwaltungsprogramms (CMGAu) die folgenden Informationen ein und klicken Sie auf **Next** (Weiter).
Server: Vollständig qualifizierter Hostname des Servers, zum Beispiel:

Geräteserver: **https://<server.organization.com>:8081/xapi**

Sicherheitsserver: **https://<server.organization.com>:8443/xapi/**

Dell Admin: Kontoname des forensischen Administrators (auf dem Server aktiviert)

Dell Admin Password: Kontopasswort für den forensischen Administrator (auf dem Server aktiviert)

MCID: Löschen Sie das MCID-Feld.

DCID: Die DCID/Wiederherstellungs-ID, die Sie vorhin ermittelt haben.

4 Wählen Sie im Dialogfeld des Dell Verwaltungsprogramms **No, perform a download from a server now** (Nein, Download von Server jetzt ausführen) und klicken Sie auf **Next** (Weiter).

> **ANMERKUNG:**
> Wenn der Verschlüsselungs-Client nicht installiert ist, wird die Meldung *Unlock failed* (Entsperren fehlgeschlagen) angezeigt. Wechseln Sie zu einem Computer, auf dem der Verschlüsselungs-Client installiert ist.

5 Wenn der Herunterladevorgang und die Entsperrung abgeschlossen sind, kopieren Sie die Dateien, die Sie für die Wiederherstellung über dieses Laufwerk benötigen. Alle Dateien sind lesbar. ***Klicken Sie nicht auf Finish (Fertig stellen), bevor Sie die Dateien wiederhergestellt haben***.

6 Wenn die Dateien wiederhergestellt sind und Sie bereit für die erneute Sperrung der Dateien sind, klicken Sie auf **Finish (Fertig stellen).**

Nachdem Sie auf Finish (Fertig stellen) geklickt haben, sind die verschlüsselten Dateien nicht mehr verfügbar.

3

HCA-Wiederherstellung (Hardware Crypto Accelerator)

Mit der Dell Data Protection Hardware Crypto Accelerator (HCA)-Wiederherstellung können Sie den Zugriff auf Folgendes wiederherstellen:

- Dateien auf einem HCA-verschlüsselten Laufwerk – Bei dieser Methode wird das Laufwerk mithilfe der bereitgestellten Schlüssel entschlüsselt. Sie können das konkrete Laufwerk, das Sie entschlüsseln möchten, während des Wiederherstellungsvorgangs auswählen.
- Ein HCA-verschlüsseltes Laufwerk nach dem Austausch von Hardeware – Diese Methode wird verwendet, wenn die Hardware Crypto Accelerator-Karte oder eine Hauptplatine/ein TPM ausgetauscht werden musste. Sie können eine Wiederherstellung ausführen, um wieder Zugriff auf die verschlüsselten Daten zu erhalten, ohne das Laufwerk zu entschlüsseln.

Voraussetzungen für die Wiederherstellung

Für die HCA-Wiederherstellung benötigen Sie Folgendes:

- Zugriff auf die Wiederherstellungsumgebung ISO
- Startfähige CD\DVD oder USB-Medien

Übersicht über den Wiederherstellungsprozess

So stellen Sie ein ausgefallenes System wieder her:

1 Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe Appendix A - Burning the Recovery Environment (Anhang A, Brennen der Wiederherstellungsumgebung).
2 Besorgen Sie sich die Wiederherstellungsdatei.
3 Führen Sie die Wiederherstellung durch.

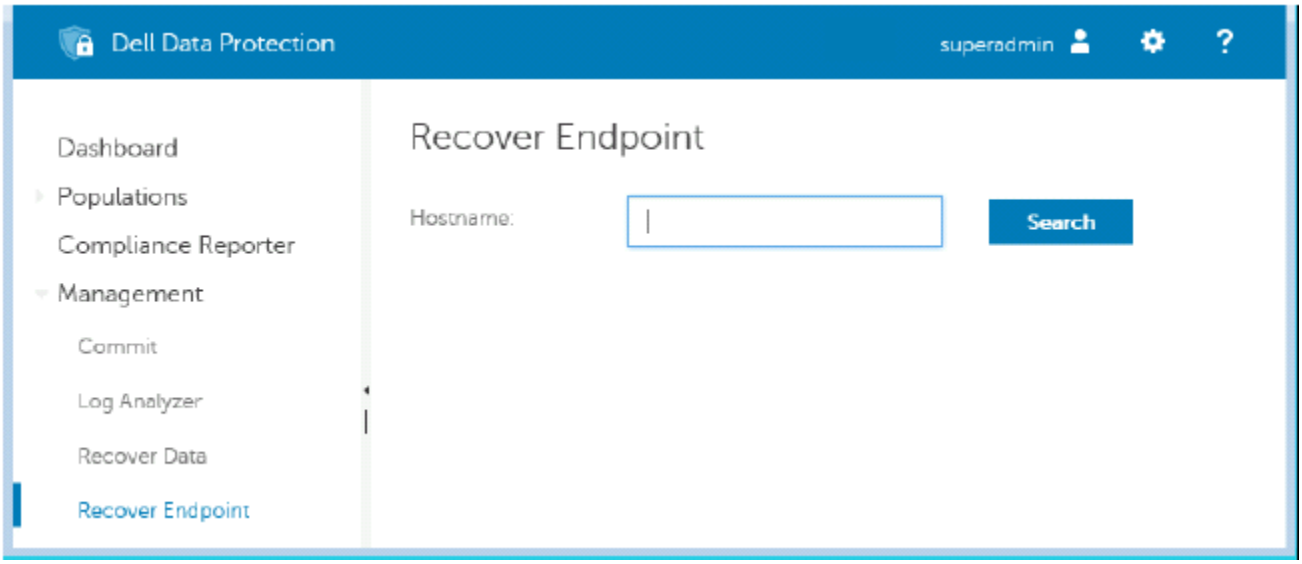
HCA-Wiederherstellung durchführen

Führen Sie folgende Schritte aus, um eine HCA-Wiederherstellung durchzuführen.

Wiederherstellungsdatei besorgen - Computer mit Remote-Verwaltung

So laden Sie die Datei **<machinename_domain.com>.exe** herunter, die bei der Installation von Dell Data Protection generiert wurde:

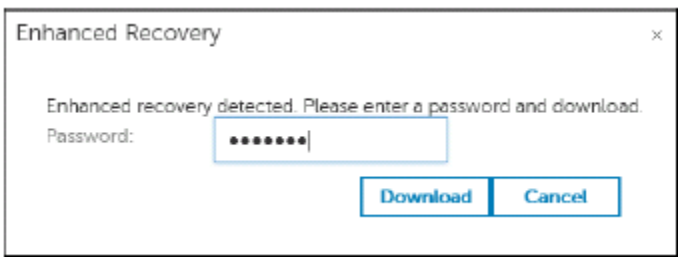
1 Öffnen Sie die Remote Management Console und wählen Sie im linken Fensterbereich **Verwaltung** > **Endpunkt wiederherstellen** aus.



2 Geben Sie im Feld „Host-Name“ den vollständig qualifizierten Domänennamen (FQDN) des Endpunktes ein und klicken Sie auf **Suchen**.

3 Geben Sie im Fenster „Erweiterte Wiederherstellung“ ein Wiederherstellungspasswort ein und klicken Sie auf **Herunterladen**.

ANMERKUNG:
Sie müssen sich dieses Passwort für den Zugriff auf die Wiederherstellungsschlüssel merken.



Wiederherstellungsdatei besorgen - Computer mit lokaler Verwaltung

So erhalten Sie die Personal Edition-Wiederherstellungsdatei:

1 Suchen Sie die Wiederherstellungsdatei mit dem Namen **LSARecovery_<systemname> > .exe**. Diese Datei wurde beim Ausführen des Einrichtungsassistenten zur Installation von Personal Edition auf einem Netzwerklaufwerk oder Wechselspeichermedium gespeichert.

2 Kopieren Sie **LSARecovery_<systemname> > .exe** auf den Zielcomputer (den Computer, auf dem die Daten wiederhergestellt werden sollen).

Wiederherstellung durchführen

1 Starten Sie auf einem Wiederherstellungssystem oder auf dem Gerät mit dem Laufwerk, das Sie wiederzustellen versuchen den zuvor von Ihnen erstellten startfähigen Datenträger.

Es wird eine WinPE-Umgebung geöffnet.

2 Geben Sie **x** ein und drücken Sie **Enter** (Eingabetaste), um eine Eingabeaufforderung zu erhalten.

3 Navigieren Sie zur gespeicherten Wiederherstellungsdatei, und starten Sie sie.

4 Wählen Sie eine Option aus:

- Ich möchte mein mit HCA verschlüsseltes Laufwerk entschlüsseln.
- Ich möchte den Zugriff auf mein mit HCA verschlüsseltes Laufwerk wiederherstellen.

5 Bestätigen Sie im Dialogfeld mit den Sicherungs- und Wiederherstellungsinformationen, dass die Service-Tag-Nummer bzw. die Systemkennnummer korrekt ist, und klicken Sie auf **Next** (Weiter).

6 Wählen Sie in dem Dialogfeld mit der Liste der Volumes des Computers alle anwendbaren Laufwerke aus und klicken Sie auf **Next** (Weiter).

Klicken Sie bei gedrückter Umschalttaste oder Strg-Taste, um mehrere Laufwerke auszuwählen.

Falls das ausgewählte Laufwerk nicht HCA-verschlüsselt ist, kann es nicht wiederhergestellt werden.

7 Geben Sie Ihr Wiederherstellungspasswort ein und klicken Sie auf **Next** (Weiter).

Bei einem remote verwalteten Computer ist dies das in Schritt 3 in Obtain the Recovery File - Remotely Managed Computer (Wiederherstellungsdatei erhalten - Computer mit Remote-Verwaltung) angegebene Passwort.

Bei einem Computer mit lokaler Verwaltung ist dieses Passwort das Encryption-Administrator-Passwort, das für das System beim Hinterlegen der Schlüssel in Personal Edition festgelegt wurde.

8 Klicken Sie im Dialogfeld „Recover“ (Wiederherstellung) auf **Recover** (Wiederherstellen) Der Wiederherstellungsvorgang beginnt.

9 Navigieren Sie, wenn Sie dazu aufgefordert werden, zur gespeicherten Wiederherstellungsdatei, und klicken Sie auf **OK**.

Falls Sie eine vollständige Entschlüsselung durchführen, wird im nachfolgenden Dialogfeld der Status angezeigt. Dieser Vorgang kann etwas Zeit in Anspruch nehmen.

10 Wenn die Meldung mit dem Hinweis angezeigt wird, dass die Wiederherstellung erfolgreich abgeschlossen wurde, klicken Sie auf **Finish** (Fertig stellen). Der Computer wird neu gestartet.

Nachdem der Computer neu gestartet wurde, sollte er voll funktionsfähig sein. Falls das Problem weiterhin besteht, kontaktieren Sie den Dell ProSupport.

SED-Wiederherstellung (Self-Encrypting Drive)

Mithilfe der SED-Wiederherstellung (selbstverschlüsselndes Laufwerk) können Sie unter Verwendung der folgenden Methoden den Zugriff auf Dateien auf einem SED-Laufwerk wiederherstellen:

- Führen Sie eine einmalige Entsperrung des Laufwerks durch, um die Preboot-Authentifizierung (PBA) zu umgehen und zu entfernen.
  - Bei Verwendung eines SED-Clients mit Remote-Verwaltung kann PBA später über die Remote Management Console wieder aktiviert werden.
  - Bei Verwendung eines SED-Clients mit lokaler Verwaltung kann PBA über die Security Tools Administrator Console wieder aktiviert werden.
- Führen Sie die Entsperrung durch, und entfernen Sie anschließend die PBA dauerhaft vom Laufwerk. Single Sign-On funktioniert nicht, wenn die PBA entfernt wurde.
  - Bei Verwendung eines SED-Clients mit Remote-Verwaltung müssen Sie zum Entfernen der PBA das Produkt über die Remote Management Console deaktivieren, falls die PBA später wieder aktiviert werden soll.
  - Bei Verwendung eines SED-Clients mit lokaler Verwaltung müssen Sie zum Entfernen der PBA das Produkt innerhalb des Betriebssystems deaktivieren, falls die PBA später wieder aktiviert werden soll.

Voraussetzungen für die Wiederherstellung

Für die SED-Wiederherstellung benötigen Sie Folgendes:

- Zugriff auf die Wiederherstellungsumgebung ISO
- Startfähige CD\DVD oder USB-Medien

Übersicht über den Wiederherstellungsprozess

So stellen Sie ein ausgefallenes System wieder her:

1 Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe Appendix A - Burning the Recovery Environment (Anhang A, Brennen der Wiederherstellungsumgebung).
2 Besorgen Sie sich die Wiederherstellungsdatei.
3 Führen Sie die Wiederherstellung durch.

SED-Wiederherstellung durchführen

Führen Sie folgende Schritte aus, um eine SED-Wiederherstellung durchzuführen.

Wiederherstellungsdatei besorgen – SED-Client mit Remote-Verwaltung

Besorgen Sie sich die Wiederherstellungsdatei.

Die Wiederherstellungsdatei kann von der Remote Management Console heruntergeladen werden. So laden Sie die Datei *<hostname>-sed-recovery.dat* herunter, die erstellt wurde, als Sie Dell Data Protection installiert haben:

a Öffnen Sie die Remote-Verwaltungskonsole und wählen Sie im linken Fensterbereich **Management > Recover Data** (Verwaltung > Daten wiederherstellen), wählen Sie dann die Registerkarte **SED**.

b Geben Sie auf dem Bildschirm „Recover Data“ (Daten wiederherstellen) im Feld „Hostname“ den vollständig qualifizierten Domänennamen des Endpunktes ein und klicken Sie auf **Search** (Suchen).

c Wählen Sie im Feld „SED“ eine Option aus.

d Klicken Sie auf **Create Recovery File** (Wiederherstellungsdatei erstellen).

Die Datei **<hostname>-sed-recovery.dat** wird herunter geladen.

Wiederherstellungsdatei besorgen – SED-Client mit lokaler Verwaltung

Besorgen Sie sich die Wiederherstellungsdatei.

Die Datei wurde bei der Installation von Dell Data Protection | Security Tools auf Ihrem Computer generiert und ist an dem Speicherort der Sicherung verfügbar, den Sie bei der Installation ausgewählt haben. Der Dateiname ist *OpalSPkey<systemname>.dat*.

Wiederherstellung durchführen

1 Starten Sie auf einem Wiederherstellungssystem oder auf dem Gerät mit dem Laufwerk, das Sie wiederzustellen versuchen den zuvor von Ihnen erstellten startfähigen Datenträger. Es wird eine WinPE-Umgebung mit der Wiederherstellungsanwendung geöffnet.

2 Wählen Sie Option eins und drücken Sie **Enter** (Eingabetaste).

3 Wählen Sie **Browse** (Durchsuchen), suchen Sie die Wiederherstellungsdatei aus, und klicken Sie anschließend auf **Open** (Öffnen).

4 Wählen Sie eine Option aus, und klicken Sie auf **OK**.

- **Einmaliges Entsperren des Laufwerks** - Mit dieser Methode wird die PBA umgangen und entfernt. Sie kann später wieder aktiviert werden, und zwar über die Remote Management Console (bei Verwendung eines SED-Clients mit Remote-Verwaltung) bzw. über die Security Tools Administrator Console (bei Verwendung eines SED-Clients mit lokaler Verwaltung).
- **Laufwerk entsperren und PBA entfernen** - Durch diese Methode wird die PBA entsperrt und dauerhaft vom Laufwerk entfernt. Bei Verwendung eines SED-Clients mit Remote-Verwaltung müssen Sie zum Entfernen der PBA das Produkt über die Remote Management Console deaktivieren, falls die PBA später wieder aktiviert werden soll. Bei Verwendung eines SED-Clients mit lokaler Verwaltung müssen Sie zum Entfernen der PBA das Produkt innerhalb des Betriebssystems deaktivieren, falls die PBA später wieder aktiviert werden soll. Single Sign-On funktioniert nicht, wenn die PBA entfernt wurde.

5 Die Wiederherstellung ist jetzt abgeschlossen. Drücken Sie eine beliebige Taste, um zum Menü zurückzukehren.

6 Drücken Sie **r,** um den Computer neu zu starten.

> **ANMERKUNG:**
> Stellen Sie sicher, dass Sie sämtliche USB- oder CD-\DVD-Medien entfernt haben, die zum Starten des Computers verwendet wurden. Ist das nicht der Fall, kann das zu einem Neustart in die Wiederherstellungsumgebung führen.

7 Nachdem der Computer neu gestartet wurde, sollte er voll funktionsfähig sein. Falls das Problem weiterhin besteht, kontaktieren Sie den Dell ProSupport.

GPK-Wiederherstellung (General Purpose Key)

Der Allzweckschlüssel General Purpose Key (GPK) wird zum Verschlüsseln eines Teils der Registrierung für Domänenbenutzer verwendet. Während des Startvorgangs kann es jedoch in seltenen Fällen vorkommen, dass dieser Schlüssel beschädigt wird und sich nicht mehr öffnen lässt. In einem solchen Fall werden die folgenden Fehler in der Datei „CMGShield.log“ auf dem Client-Computer angezeigt:

```
[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
```

Falls der GPK nicht geöffnet werden kann, muss er durch Dekomprimieren des vom Server heruntergeladenen Wiederherstellungspakets wiederhergestellt werden.

GPK wiederherstellen

Wiederherstellungsdatei besorgen

So laden Sie die Datei **<machinename_domain.com>.exe** herunter, die bei der Installation von Dell Data Protection generiert wurde:

1 Öffnen Sie die Remote Management Console und wählen Sie im linken Fensterbereich **Verwaltung** > **Endpunkt wiederherstellen** aus.

2 Geben Sie im Feld „Host-Name“ den vollständig qualifizierten Domänennamen (FQDN) des Endpunktes ein und klicken Sie auf **Suchen**.

3 Geben Sie im Fenster „Enhanced Recovery“ (Erweiterte Wiederherstellung) ein Wiederherstellungspasswort ein und klicken Sie auf **Download**

> **ANMERKUNG:**
> Sie müssen sich dieses Passwort für den Zugriff auf die Wiederherstellungsschlüssel merken.

Die Datei **<machinename_domain.com>.exe** wird heruntergeladen.

Wiederherstellung durchführen

1 Erstellen Sie einen startfähigen Datenträger für die Wiederherstellungsumgebung. Anleitungen hierzu finden Sie in Appendix A - Burning the Recovery Environment (Anhang A - Brennen der Wiederherstellungsumgebung)

2 Starten Sie auf einem Wiederherstellungssystem oder auf dem Gerät mit dem Laufwerk, das Sie wiederherzustellen versuchen.
Es wird eine WinPE-Umgebung geöffnet.

3 Geben Sie **x** ein und drücken Sie **Enter**, um eine Eingabeaufforderung zu erhalten.

4 Navigieren Sie zur Wiederherstellungsdatei und starten Sie sie.
Es wird ein Verschlüsselungs-Client-Diagnosedialogfeld geöffnet, und die Wiederherstellungsdatei wird im Hintergrund generiert.

5 Führen Sie bei einer administrativen Befehlsaufforderung **<machinename_domain.com** > **.exe** > **-p <password** > **-gpk** aus
Durch diesen Befehl wird die Datei „GPKRCVR.txt“ für Ihren Computer ausgegeben.

6 Kopieren Sie die Datei **GPKRCVR.txt** in das Root-Verzeichnis des BS-Laufwerks des Computers.

7 Starten Sie den Computer neu.

Das Betriebssystem verwendet die Datei „GPKRCVR.txt“, um den GPK erneut auf dem Computer zu generieren.

8 Führen Sie bei entsprechender Aufforderung einen weiteren Neustart durch.

6

BitLocker Manager-Wiederherstellung

Zur Datenwiederherstellung erhalten Sie ein Passwort oder ein Schlüsselpaket für die Wiederherstellung von der Remote Management Console, mit dem Sie dann die Daten auf dem Computer entsperren können.

Daten wiederherstellen

1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.

2 Klicken Sie im linken Bereich auf **Management** (Verwaltung) > **Recover Data** (Daten wiederherstellen).

3 Klicken Sie auf die Registerkarte **Manager**.

4 Für *BitLocker*

Geben Sie die **Revocery ID** (Wiederherstellungs-ID) ein, die Sie von BitLocker erhalten haben. Wenn Sie den Hostnamen und das Volume eingeben, wird optional die Wiederherstellungs-ID bestückt.

Klicken Sie auf **Get Recovery Password** (Wiederherstellungspasswort erhalten) oder **Create Key Package** (Schlüsselpaket) erstellen.

Je nach der gewünschten Art der Wiederherstellung verwenden Sie dieses Passwort oder dieses Schlüsselpaket für die Wiederherstellung.

Für das *TPM*:

Geben Sie den **Hostname** (Hostnamen) ein.

Klicken Sie auf **Get Recovery Password** (Wiederherstellungspasswort erhalten) oder **Create Key Package** (Schlüsselpaket) erstellen.

Je nach der gewünschten Art der Wiederherstellung verwenden Sie dieses Passwort oder dieses Schlüsselpaket für die Wiederherstellung.

5 Anweisungen zum Abschluss der Wiederherstellung finden Sie in der Anleitung zur Wiederherstellung von Microsoft.

ANMERKUNG:

Falls das TMP nicht BitLocker Manager zugewiesen ist, sind das TPM-Passwort und das Schlüsselpaket in der Dell Datenbank nicht verfügbar. Sie erhalten in diesem Fall erwartungsgemäß die Fehlermeldung, dass Dell den Schlüssel nicht finden kann.

Zur Wiederherstellung eines TPM, das einer anderen Einheit als BitLocker Manager zugewiesen ist, befolgen Sie das inhaberspezifische oder das bei Ihnen geltende Verfahren zur Wiederherstellung eines TPM.

Passwort-Wiederherstellung

Benutzer vergessen oft ihr Passwort. Glücklicherweise gibt es in diesem Fall mehrere Möglichkeiten für Benutzer, mit Preboot-Authentifizierung wieder Zugang zu einem Computer zu erlangen.

- Die Funktion der Wiederherstellungsfragen bietet eine auf Frage und Antwort basierende Authentifizierung.
- Anfrage-/Antwort-Codes ermöglichen Benutzern, gemeinsam mit ihrem Administrator Zugriff auf den Computer zu erlangen. Diese Funktion steht nur Benutzern zur Verfügung, die Computer besitzen, die von ihrem Unternehmen verwaltet werden.

Wiederherstellungsfragen

Meldet sich ein Benutzer erstmalig bei einem Computer an, wird er dazu aufgefordert, einen Standardsatz von Fragen zu beantworten, die der Administrator konfiguriert hat. Hat er seine Antworten auf diese Fragen gegeben, wird er, wenn er das nächste Mal sein Passwort vergisst, aufgefordert, die Antworten anzugeben. Vorausgesetzt er hat die Fragen korrekt beantwortet, kann er sich anmelden und so erneut auf Windows zugreifen.

Voraussetzungen

- Wiederherstellungsfragen müssen durch den Administrator eingerichtet werden.
- Der Benutzer muss seine Antworten auf die Fragen gegeben haben.
- Bevor er auf die Menüoption **Trouble Signing In** (Probleme bei der Anmeldung) klickt, muss der Benutzer einen gültigen Benutzernamen und Domäne eingeben.

So greifen Sie vom PBA-Anmeldebildschirm auf die Fragen zu:

1 Geben Sie einen gültigen Domänennamen und Benutzernamen ein.
2 Klicken Sie im Bildschirm unten links auf **Options** (Optionen) > **Trouble Signing In** (Probleme bei der Anmeldung).
3 Wird der Frage-und-Antwort-Dialog angezeigt, geben Sie die Antworten ein, die Sie auf Wiederherstellungsfragen bei der ersten Anmeldung eingegeben haben.

Anfrage-/Antwortcodes

Die Anfrage-/Antwortwiederherstellung kann verwendet werden, um mit der Authentifizierung über PBA auf Windows zuzugreifen. Anfrage/Antwort kann in den folgenden Szenarien verwendet werden:

- Wenn ein Benutzer sich nicht an die Antworten erinnert, die er bei der Wiederherstellungsfrage zur Anmeldung gegeben hat.
- Wenn der Administrator die Funktion der Wiederherstellungsfragen nicht aktiviert hat.
- Wenn der Benutzer kein lokaler Benutzer ist, nicht über eine Netzwerkverbindung verfügt und keinen Entsperrbefehl über den Sicherheitsserver durch die SED-Gerätesteuerung empfangen kann

Wenn ein Benutzer zum Bildschirm „Challenge/Response“ (Anfrage/Antwort) gelangt, weil er auf die Option **Trouble Signing In** (Probleme bei der Anmeldung) klickt oder sein Passwort falsch eingibt und die Grenze zur Fehleingabe des Passwortes überschreitet, ohne dass das Netzwerkkabel angeschlossen ist. Wenn Wiederherstellungsfragen deaktiviert sind, öffnet die Option **Trouble Signing In** (Probleme bei der Anmeldung) den Bildschirm „Challenge/Response“ (Anfrage/Antwort) direkt.

Anforderung

- Die Wiederherstellung über Anfrage/Antwort steht nur auf Domain-Computern, die remote von Ihrer Organisation oder Ihrem Unternehmen verwaltet werden, zur Verfügung.

Voraussetzungen

- Trennen Sie den Computer vom Netzwerk, bevor Sie Wiederherstellungsfragen beantworten oder Anfrage-/Antwortcodes eingeben.
- Geben Sie einen gültigen Benutzernamen und eine Domäne an, bevor Sie auf „Trouble Signing In“ (Probleme bei der Anmeldung) klicken.

So verwenden Sie Wiederherstellung durch Anfrage/Antwort:

1 Der Benutzer klickt auf den Link **Options** (Optionen), um das Menü anzuzeigen.

2 Der Benutzer klickt auf **Trouble Signing In** > **Challenge/Response** (Probleme bei der Anmeldung > Anfrage/Antwort).

> **ANMERKUNG:**
> Die Option „Challenge/ Response“ (Anfrage/Antwort) ist nur verfügbar auf Computern, die von einem Unternehmen verwaltet werden. Wenn der Computer keine Domäne ist, wird die Option „Challenge/ Response“ (Anfrage/Antwort) nicht im Menü angezeigt.

3 Bei Aufforderung wendet sich der Benutzer an den Helpdesk und gibt dem Administrator den Gerätenamen (Hostnamen) und den Anfragecode.

4 Der Administrator öffnet die Remote Management Console, klickt auf **Management** > **Recover Data**(Verwaltung > Daten wiederherstellen) und klickt dann auf **SED** im Menü oben.

5 Unter „Recover SED User Access“ (SED-Benutzerzugriff wiederherstellen) gibt der Administrator den **Hostnamen** ein, den er vom Benutzer erhalten hat, und klickt auf **Search** (Suchen).

6 Der Administrator wählt den Namen des Benutzers aus, der um Hilfe bittet:

7 Geben Sie den vom Benutzer erhaltenen Gerätecode in das Feld **Challenge** (Anfrage) ein und klicken Sie auf **Generate Response** (Antwort erstellen).

8 Geben Sie den generierten Antwortcode dem Benutzer.

> **ANMERKUNG:**
> Bei diesen Codes wird keine Groß- und Kleinschreibung beachtet. Die Zahlen werden in Rot angezeigt, die Buchstaben in Blau.

9 Der Benutzer gibt den Antwortcode in die Felder **Response code** (Antwortcode) auf dem PBA-Anmeldebildschirm ein. Dies ist ein Beispiel für einen vom Benutzer eingegebenen Antwortcode:

10 Klicken Sie auf den Rechtspfeil, um fortzufahren, und um den letzten PBA-Bildschirm zu authentifizieren.

11 Klicken Sie auf **Senden**.

Ein Benutzer kann den letzten PBA nur einmalig mithilfe der Funktion „Challenge/Response“ (Anfrage/Antwort) authentifizieren. Nach einem Neustart des Computers übernimmt die PBA-Ebene den Schutz des Computers erneut und fordert den Benutzer wieder auf, sich auf dem PBA-Bildschirm anzumelden.

> **ANMERKUNG:**
> Wenn der Benutzer den Dialog „Challenge/Response“ (Anfrage/Antwort) angezeigt hat, muss er die Sequenz Anfrage/Antwort abschließen, um erneut Zugriff auf das System zu erhalten. Wenn der Benutzer den Computer ausschaltet und versucht, sich erneut anzumelden - auch durch Eingabe des richtigen Passwortes - fordert PBA den Benutzer erneut zur Authentifizierung mit dem Dialog Anfrage/Antwort auf.

Passwort für External Media Shield-Wiederherstellung (Externes Medien-Shield, EMS)

Das externe Medien-Shield, EMS, bietet Ihnen die Möglichkeit, Wechselspeichermedien innerhalb und außerhalb Ihrer Organisation zu schützen, indem Sie Benutzern ermöglichen, USB-Speichersticks und andere Wechselspeichermedien zu verschlüsseln. Der Benutzer weist jedem Wechselspeichergerät, das er schützen möchte, ein Passwort zu. Dieser Abschnitt beschreibt das Verfahren für die Wiederherstellung des Zugriffs auf verschlüsselte USB-Speichergeräte, wenn ein Benutzer das Gerätepasswort vergisst.

Wiederherstellen des Datenzugriffs

Gibt ein Benutzer sein Passwort so oft falsch ein, dass er die zulässige Anzahl von Passworteingabeversuchen überschreitet, wird das USB-Gerät in den manuellen Authentifizierungsmodus versetzt.

Bei der **manuellen Authentifizierung** liefert der Client Codes an einen Administrator, der beim Server angemeldet ist.

Im manuellen Authentifizierungsmodus hat der Benutzer zwei Optionen zum Zurücksetzen seines Passworts und Wiederherstellen des Zugriffs auf seine Daten.

Der Administrator liefert dem Client einen Zugriffscode, der es dem Benutzer erlaubt, sein Passwort zurückzusetzen und erneuten Zugriff auf seine verschlüsselten Daten zu erhalten.

1 Wenn Sie dazu aufgefordert werden, Ihr Passwort einzugeben, klicken Sie auf die Schaltfläche **I Forgot** (Passwort vergessen).

   Das Dialogfeld zum Bestätigen wird angezeigt.

2 Klicken Sie zum Bestätigen auf **Yes** (Ja). Nach der Bestätigung wechselt das Gerät in den manuellen Authentifizierungsmodus.

3 Wenden Sie sich an den Helpdesk-Administrator und geben Sie ihm die Codes, die im Dialogfeld angezeigt werden.

4 Melden Sie sich als Helpdesk-Administrator bei der Remote-Verwaltungskonsole an. Das Konto des Helpdesk-Administrators muss über Helpdesk-Berechtigungen verfügen.

5 Navigieren Sie zur Menüoption **Recover Data** (Daten wiederherstellen) im linken Fenster.

6 Geben Sie die vom Endbenutzer gelieferten Codes ein.

7 Klicken Sie auf die Schaltfläche **Generate Response** (Antwort erzeugen) in der unteren rechten Ecke des Bildschirms.

8 Geben Sie dem Benutzer den Zugriffscode.

> **ANMERKUNG:**
> Achten Sie darauf, den Benutzer manuell zu authentifizieren bevor Sie einen Zugriffscode liefern. Bitten Sie beispielsweise den Benutzer eine Reihe von Fragen, die nur diese Person beantworten kann, telefonisch zu beantworten, wie z. B. „Nennen Sie Ihre Mitarbeiter-ID?“ Ein weiteres Beispiel: Fordern Sie den Benutzer auf, zum Helpdesk zu kommen, und sich zu identifizieren, um sicherzugehen, dass er der Besitzer der Medien ist. Erfolgt vor der Vergabe eines Zugriffscodes über das Telefon keine Authentifizierung, kann ein Angreifer Zugriff auf verschlüsselte tragbare Medien erhalten.

9 Setzen Sie Ihr Passwort für den verschlüsselten Datenträger zurück.

   Der Benutzer wird aufgefordert, sein Passwort für den verschlüsselten Datenträger zurückzusetzen.

Selbstwiederherstellung

Selbstwiederherstellung ist der Prozess, wenn das Passwort für ein verschlüsseltes Wechselspeichergerät durch Einsetzen des Laufwerks in einen geschützten Rechner, bei dem der Eigentümer des Datenträger angemeldet ist, zurückgesetzt wird. Solange der Besitzer des Datenträgers auf dem geschützten Mac oder PC authentifiziert ist, erkennt der Client den Verlust von Schlüsselmaterial und fordert den Benutzer auf, das Gerät erneut zu initialisieren. Zu diesem Zeitpunkt kann der Benutzer das Passwort zurücksetzen und sofortigen Zugriff auf seine verschlüsselten Daten erlangen.

1 Melden Sie sich bei einer mit Dell Data Protection verschlüsselten Workstation als Datenträgerbesitzer an.
2 Schließen Sie das verschlüsselte Wechselspeichermedium an.
3 Wenn Sie dazu aufgefordert werden, geben Sie ein neues Passwort ein, um den Wechseldatenträger erneut zu initialisieren.

   War der Vorgang erfolgreich wird eine kurze Meldung angezeigt, dass das Passwort akzeptiert wurde.
4 Navigieren Sie zum Speichergerät und bestätigen Sie den Zugriff auf die Daten.

Dell Data Guardian Wiederherstellung

Das Wiederherstellungstool ermöglicht:

- Entschlüsselung geschützter Office-Dateien

  Dazu gehören Dateien mit bis zu dreifacher Verschlüsselung - Bei mehr als einer Art und Weise zur Verschlüsselung von Dateien ist gelegentlich eine Datei doppelt oder dreifach verschlüsselt. Wenn der Benutzer die Datei öffnet, weist eine Fehlermeldung daraufhin, sich für eine Wiederherstellung an den Administrator zu wenden.
- Hinterlegen von Schlüsseldaten
- Möglichkeit, nach manipulierten Dateien zu suchen
- Die Möglichkeit, eine Entschlüsselung der geschützten Office-Dokumente zu erzwingen, bei welchen der Wrapper der Datei manipuliert wurde, z. B. das Deckblatt der geschützten Office-Datei in der Cloud oder auf einem Gerät ohne Data Guardian.

Voraussetzungen für die Wiederherstellung

Die Voraussetzungen umfassen:

- Microsoft .Net Framework 4.5.2 muss auf dem wiederherzustellenden Endgerät laufen.
- Die forensische Administratorrolle muss in der Remote-Verwaltungskonsole für den Administrator, der die Wiederherstellung ausführt, zugewiesen werden.

Wiederherstellung von Data Guardian durchführen

Führen Sie die folgenden Schritte aus, um eine Wiederherstellung der geschützten Office-Dokumente von Data Guardian auszuführen.

Führen Sie eine Wiederherstellung von Windows, einem USB-Flashlaufwerk oder Netzlaufwerk aus durch

So führen Sie eine Wiederherstellung durch:

1 Kopieren Sie vom Dell Installationsmedium **RecoveryTools.exe** auf einen der folgenden:

   - Computer - Kopieren Sie die .exe auf den Computer, auf dem Office-Dokumente wiederhergestellt werden.
   - USB - Kopieren Sie die .exe in das USB-Flashlaufwerk und führen Sie es vom USB-Flash-Laufwerk aus.
   - Netzlaufwerk

2 Doppelklicken Sie auf **RecoveryTools.exe**, um das Wiederherstellungstool aufzurufen.

3 Geben Sie im Fenster Data Guardian die DDP-Server-URL in diesem Format ein:

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

   ANMERKUNG:
   Ersetzen Sie <server.domain.com> mit den voll qualifizierten Hostnamen des DDP-Servers, der Data Guardian auf dem Endgerät verwaltet. Um die DDP-Server-URL zu ermitteln, klicken Sie auf das Symbol Data Guardian in der Taskleiste und auf **Details**. Oben links auf dem Bildschirm „Details“ wird die Server-URL angezeigt.

4 Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Anmelden**.

ANMERKUNG:
Deaktivieren Sie das Kontrollkästchen *SSL Trust aktivieren* nicht, es sei denn, Ihr Administrator fordert Sie dazu auf.

ANMERKUNG:
Wenn Sie kein forensischer Administrator sind und Anmeldeinformationen eingeben, wird eine Meldung angezeigt, dass Sie keine Anmeldungsrechte haben.

Wenn Sie ein forensischer Administrator sind, wird das Wiederherstellungstool geöffnet.

5 Wählen Sie **Quelle**.

ANMERKUNG:
Sie müssen zu einer Quelle und einem Ziel navigieren, aber Sie können diese in beliebiger Reihenfolge auswählen.

6 Klicken Sie auf **Durchsuchen**, um den Ordner oder ein Laufwerk zur Wiederherstellung auszuwählen.

7 Klicken Sie auf **OK**.

8 Klicken Sie auf **Ziel**.

9 Klicken Sie auf **Durchsuchen**, um ein Ziel auszuwählen, wie z. B. ein externes Gerät, ein Verzeichnis oder den Desktop.

10 Klicken Sie auf **OK**.

11 Aktivieren Sie ein oder mehrere Kontrollkästchen, je nach dem, was Sie wiederherstellen möchten.

Optionen	Beschreibung
Hinterlegung	• Stellen Sie offline generierte Schlüssel, die nicht beim Dell Server hinterlegt werden konnten, wieder her. • Fällt ein Laufwerk aus, wenn der Benutzer offline ist, verwenden Sie das Slave-Laufwerk für die Wiederherstellung von Daten und nicht hinterlegten Schlüssel vom Computer.
Entschlüsselt	Verweisen Sie mit dem Wiederherstellungstool auf ein Verzeichnis, das geschützte Office-Dokumente enthält, um diese zu entschlüsseln. Falls Manipulationen aufgetreten sind, wählen Sie optional eine oder beide dieser Optionen (Details siehe unten): • **Überprüfung auf Manipulation** – sucht nach manipulierten Dateien, aber entschlüsselt diese nicht. • **Überprüfung auf Manipulation** und **Entschlüsselung auch bei Manipulation erzwingen** – Data Guardian sucht nach manipulierten Dateien, wenn der Wrapper des geschützten Office-Dokuments verändert wurde. Danach wird das Office-Dokument repariert und erneut verschlüsselt.
Überprüfung auf Manipulation	Erkennt Dateien, die manipuliert wurden, und protokolliert diese oder informiert Sie darüber. Protokolliert den Autor, der die Datei manipuliert hat. Es kann jedoch die Dateien nicht entschlüsseln.
Entschlüsselung auch bei Manipulation erzwingen	Um diese Option auszuwählen, müssen Sie auch die Option **Überprüfung auf Manipulation** wählen. Wenn eine nicht befugte Person den Wrapper eines geschützten Office-Dokuments, wie z. B. das Deckblatt, in der Cloud oder auf einem Gerät ohne Data Guardian manipuliert hat, wählen Sie diese Option zur Reparatur des Wrappers und erzwingen die Entschlüsselung der geschützten Office-Datei. **Hinweis:** Wenn jemand die verschlüsselte Office-Datei .xen im Wrapper manipuliert hat, kann die Datei nicht wiederhergestellt werden.

Jedes geschützte Office-Dokument hat ein verstecktes Wasserzeichen, es enthält den Verlauf des ursprünglichen Benutzers und den Computername sowie alle anderen Computernamen, die die Datei manipuliert haben. Standardmäßig überprüft das Wiederherstellungstool die verborgenen Wasserzeichen und protokolliert die Daten.

12 Ist die Auswahl abgeschlossen, klicken Sie auf **Scan** (Scannen).

Der Protokollbereich zeigt Folgendes an:

- Innerhalb der ausgewählten Quelle gefundene und gescannte Ordner
- Ob die Entschlüsselung erfolgreich war oder fehlgeschlagen ist

Das Wiederherstellungstool fügt die wiederhergestellten Dateien dem ausgewählten Ziel hinzu. Sie können die Dateien öffnen und anzeigen

Anhang A - Brennen der Wiederherstellungsumgebung

Sie können das Master-Installationsprogramm herunterladen.

Brennen der Wiederherstellungsumgebung ISO auf CD \DVD

Der folgende Link enthält das Verfahren zur Verwendung von Microsoft Windows 7, Windows 8 oder Windows 10, um eine startfähige CD oder DVD für die Wiederherstellungsumgebung zu erstellen.

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

Brennen der Wiederherstellungsumgebung auf Wechselmedien

Befolgen Sie zum Erstellen eines startfähigen USB-Laufwerks die Anweisungen in diesem Microsoft-Artikel:

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