# Encryption-Wiederherstellung

Encryption v10.0 / Data Guardian v2.0

## 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.**



**Encryption v10.0 / Data Guardian v2.0**

2018 - 08

Rev. A01

# Inhaltsverzeichnis

1

# Erste Schritte bei der Wiederherstellung

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

- CD-R-, DVD-R-Medien oder formatierten USB-Medien
  - Einzelheiten zum Brennen einer CD oder DVD finden Sie in Die Wiederherstellungsumgebung ISO auf CD/DVD brennen.
  - Einzelheiten zur Verwendung von USB-Medien finden Sie in 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 Security Management 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 Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell 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 Ihre Service-Tag-Nummer oder Ihren Express-Servicecode 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.

2

# Richtlinienbasierte oder Datei-/Ordner-Verschlüsselungswiederherstellung

Die Wiederherstellung wird benötigt, wenn der verschlüsselte Computer nicht mit dem Betriebssystem startet. Dieses Problem tritt auf, wenn die Registrierung falsch geändert wird oder Änderungen an der Hardware eines verschlüsselten Computers aufgetreten sind.

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
- Ein Computer zeigt BSOD mit einem Stoppcode 0x6f oder 0x74 an.
- einen Computer, auf dem Sie nicht auf verschlüsselte Daten zugreifen und keine Richtlinien bearbeiten können
- einen Server, auf dem Dell 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

**ANMERKUNG: Hardware Crypto Accelerator wird ab v8.9.3 nicht mehr unterstützt.**

## Übersicht über den Wiederherstellungsprozess

**ANMERKUNG: Für die Wiederherstellung ist eine 32-Bit-Umgebung erforderlich.**

So stellen Sie ein ausgefallenes System wieder her:

1 Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe 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 – Richtlinienbasierte Verschlüsselung oder FFE-Client für Verschlüsselungen

So laden Sie die Recovery-Datei herunter:

1 Laden Sie das Installationspaket Dell Encryption von http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers herunter. Navigieren Sie zum Ordner **AdminUtilities** im Installationspaket und öffnen Sie **CMGAd.exe**.

2 Geben Sie in das Feld **Dell Server** Security Management Server/Security Management Server Virtual ein, was auf dem Computer aktiviert wurde.

3 Geben Sie in das Feld **Dell Admin** den Namen des Benutzerkontos mit forensischen Administratorrechten ein.

4 Geben Sie in das Feld **Kennwort** das Kennwort für den forensischen Administrator ein.

5 Geben Sie im Feld **MCID** den FQDN des Geräts ein, das wiederhergestellt wird.

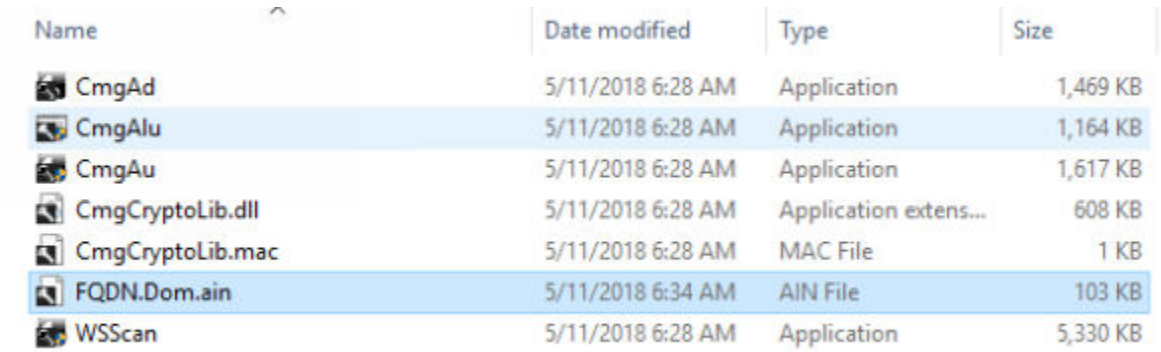
- Das Feld **DCID** ist die Wiederherstellungs-ID für das Gerät, das wiederhergestellt wird.

6 Klicken Sie auf **Weiter**.

7 Erstellen und bestätigen Sie eine **Passphrase** für die Wiederherstellungsdatei. Diese Passphrase ist erforderlich, um eine Wiederherstellung durchzuführen.

8 Geben Sie in das Feld **Herunterladen auf:** einen Zielspeicherort für das Wiederherstellungspaket ein und klicken Sie dann auf **Weiter**. Standardmäßig wird dies im Verzeichnis sein, von dem aus CMGAd.exe ausgeführt wurde.


9 Das Wiederherstellungspaket lädt sich auf die Datei herunter, die im Feld **Herunterladen auf:** festgelegt wurde.




10 Kopieren Sie die Wiederherstellungspaketdatei an einen Ort, wo auf sie zugegriffen werden kann, wenn WinPE gestartet wird.

# Wiederherstellungsdatei besorgen - Computer mit lokaler Verwaltung

So erhalten Sie die Encryption Personal-Wiederherstellungsdatei:

1 Suchen Sie die Wiederherstellungsdatei mit dem Namen **LSARecovery_<systemname> > .exe**. Diese Datei wurde beim Ausführen des Einrichtungsassistenten zur Installation von Encryption Personal 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.

**ANMERKUNG: Deaktivieren Sie vor dem Wiederherstellungsprozess SecureBoot. Wenn Sie fertig sind, können Sie SecureBoot wieder aktivieren.**

2 Geben Sie **x** ein und drücken Sie die **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 **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 **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 **Weiter**.

Bei einem remote verwalteten Client handelt es sich um das in Schritt 3 in Wiederherstellungsdatei besorgen - Computer mit Remote-Verwaltung eingegebene Passwort.

In Encryption Personal 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 **Wiederherstellen** Der Wiederherstellungsvorgang beginnt.

9 Wenn die Wiederherstellung abgeschlossen ist, klicken Sie auf **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 *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 „Gemeinsam“ angezeigt.

b Öffnen Sie die Remote-Verwaltungskonsole und wählen Sie die Registerkarte **Details und Aktionen** für den Endpunkt.

c Suchen Sie im Abschnitt „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 **Weiter**.
**Server**: Vollständig qualifizierter Hostname des Servers, zum Beispiel:

Geräteserver (Clients vor 8.x): **https://<server.organization.com>:8081/xapi**

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

**Dell Admin:** Kontoname des forensischen Administrators (aktiviert auf dem Security Management Server/Security Management Server Virtual)

**Dell Admin Password:** Kontopasswort für den forensischen Administrator (aktiviert auf dem Security Management Server/Security Management Server Virtual)

**MCID**: Löschen Sie das MCID-Feld.

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

4 Wählen Sie im Dialogfeld des Dell Verwaltungsprogramms **Nein, Download von Server jetzt ausführen** und klicken Sie auf **Weiter**.

**ANMERKUNG:**

Wenn der Verschlüsselungs-Client nicht installiert ist, wird die Meldung *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 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 **Fertig stellen**.

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

# HCA-Wiederherstellung (Hardware Crypto Accelerator)

**ANMERKUNG: Hardware Crypto Accelerator wird ab v8.9.3 nicht mehr unterstützt.**

Mit der 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 das Wiederherstellungsumgebung-ISO-Image (für die Wiederherstellung ist eine 32-Bit-Umgebung erforderlich)
- Startfähige CD\DVD oder USB-Medien

## Übersicht über den Wiederherstellungsprozess

**ANMERKUNG: Für die Wiederherstellung ist eine 32-Bit-Umgebung erforderlich.**

So stellen Sie ein ausgefallenes System wieder her:

1 Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe Anhang A, Brennen der Wiederherstellungsumgebung.
2 Besorgen Sie sich die Wiederherstellungsdatei.
3 Führen Sie die Wiederherstellung durch.

## HCA-Wiederherstellung durchführen

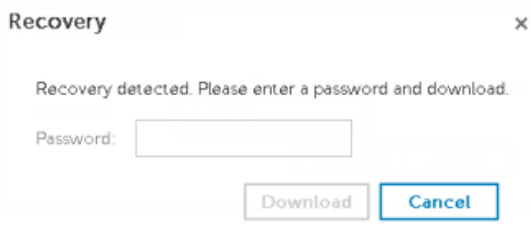
Führen Sie folgende Schritte aus, um eine HCA-Wiederherstellung durchzuführen.

### Wiederherstellungsdatei besorgen - Computer mit Remote-Verwaltung

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

1 Öffnen Sie die Remote Management-Konsole 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 "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 Encryption Personal-Wiederherstellungsdatei:

1 Suchen Sie die Wiederherstellungsdatei mit dem Namen **LSARecovery_<systemname> > .exe**. Diese Datei wurde beim Ausführen des Einrichtungsassistenten zur Installation von Encryption Personal 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.

**ANMERKUNG: Deaktivieren Sie vor dem Wiederherstellungsprozess SecureBoot. Wenn Sie fertig sind, aktivieren Sie SecureBoot wieder.**

2 Geben Sie **x** ein und drücken Sie die **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 **Weiter**.

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

Bei einem remote verwalteten Computer ist dies das in Schritt 3 in 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 „Wiederherstellung“ auf **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 **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.
- 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

**ANMERKUNG: Die Wiederherstellung erfordert eine 64-Bit- oder 32-Bit-Umgebung basierend auf dem BIOS-Startmodus.**

So stellen Sie ein ausgefallenes System wieder her:

1. Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe 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 Security installiert haben:

a Öffnen Sie die Remote-Verwaltungskonsole und wählen Sie im linken Fensterbereich **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 **Suchen**.

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

d Klicken Sie auf **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 Advanced Authentication auf Ihrem Computer generiert und ist an dem Speicherort der Sicherung zugreifbar, 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.

ⓘ **ANMERKUNG: Deaktivieren Sie vor dem Wiederherstellungsprozess SecureBoot. Wenn Sie fertig sind, aktivieren Sie SecureBoot wieder.**

2 Wählen Sie Option eins und drücken Sie die **Eingabetaste**.

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

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

- **Einmaliges Entsperren des Laufwerks** – Mit dieser Methode wird die PBA umgangen.
- **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.

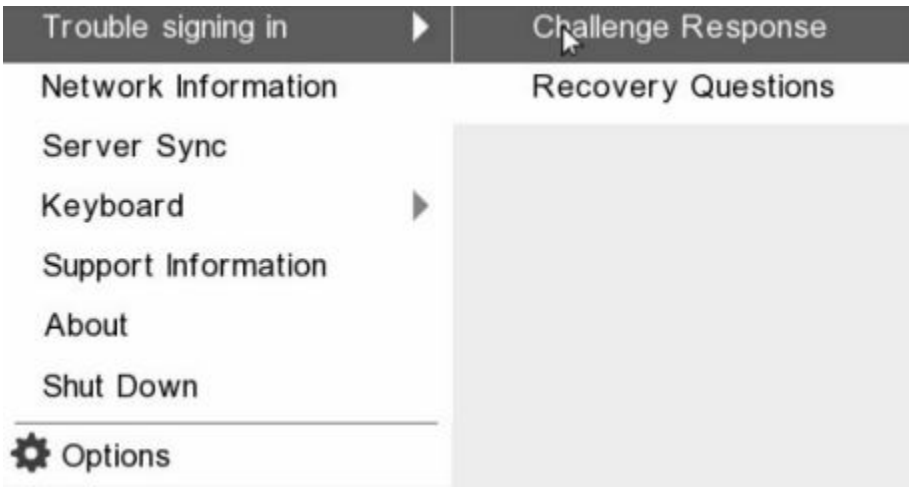
ⓘ **ANMERKUNG:**
Stellen Sie sicher, dass Sie sämtliche USB- oder CD-\DVD-Medien entfernt haben, die zum Starten des Computers verwendet wurden. Ist das nicht der Fall, kann das zu einem Neustart in die Wiederherstellungsumgebung führen.

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

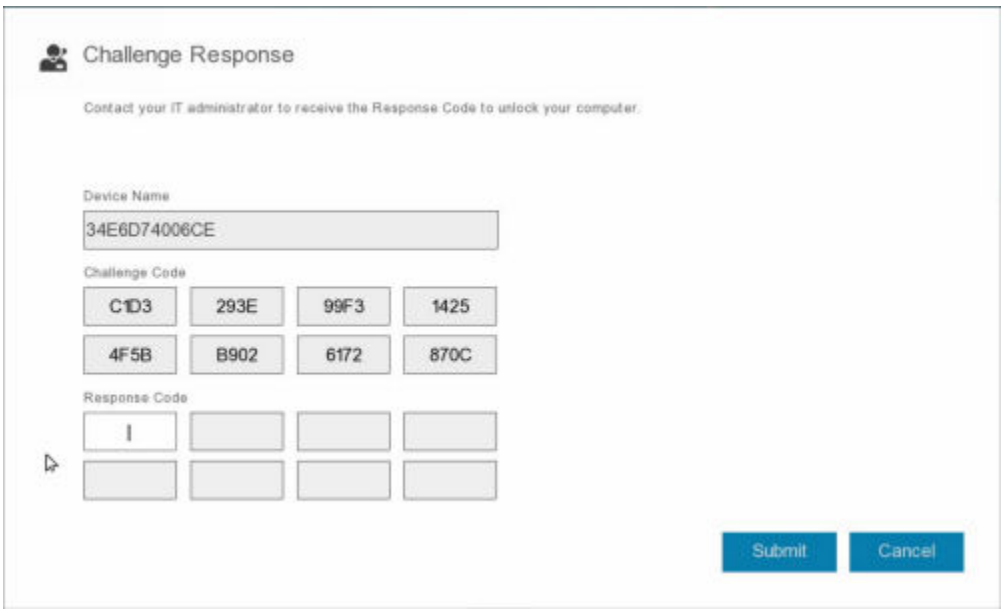
# Abfragewiederherstellung mit SED

**Umgehen der Preboot-Authentifizierungsumgebung**

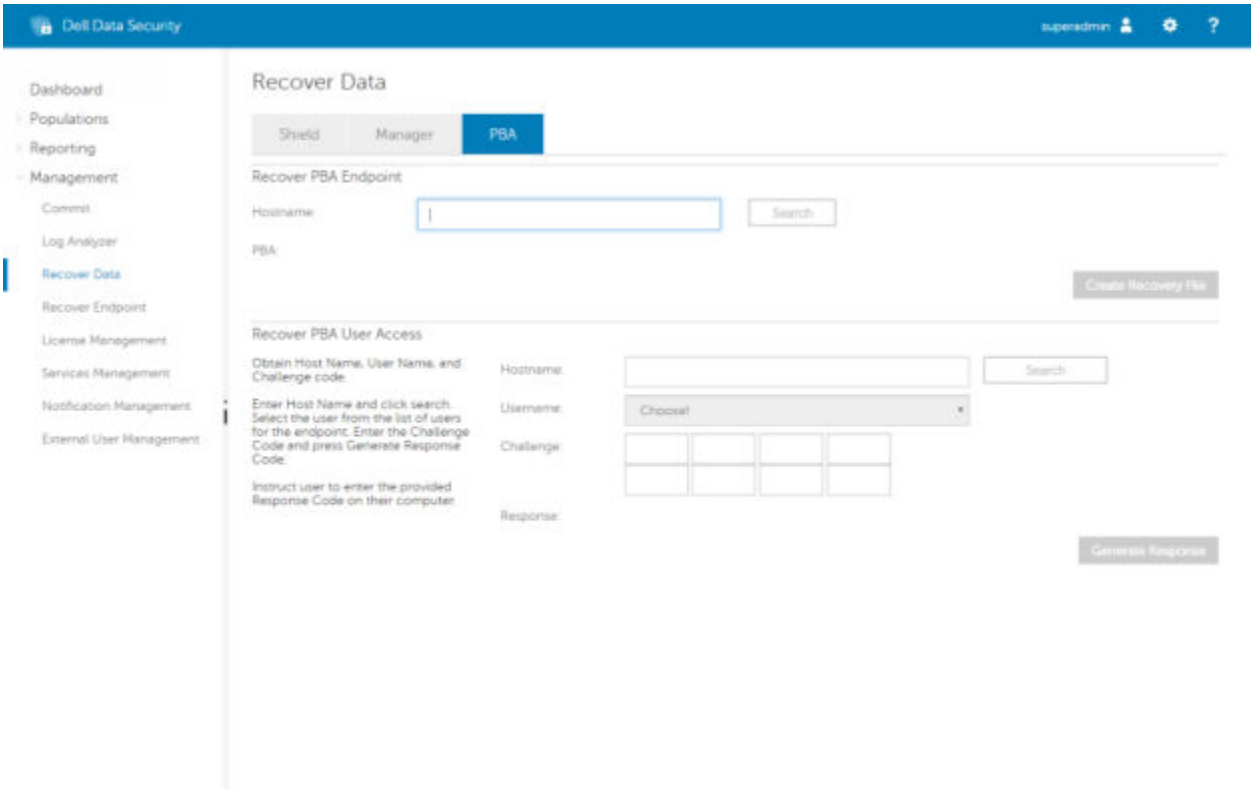
Benutzer vergessen ihre Kennwörter und rufen beim Helpdesk an, um sich zu erkundigen, wie sie die PBA-Umgebung überwinden können. Verwenden Sie den Abfrage-/Antwort-Mechanismus, der in das Gerät integriert ist. Dieser gilt pro Benutzer und basiert auf einem rotierenden Satz von alphanumerischen Zeichen. Der Benutzer muss seinen Namen in das Feld **Benutzername** eingeben und anschließend **Optionen > Abfrageantwort** auswählen.



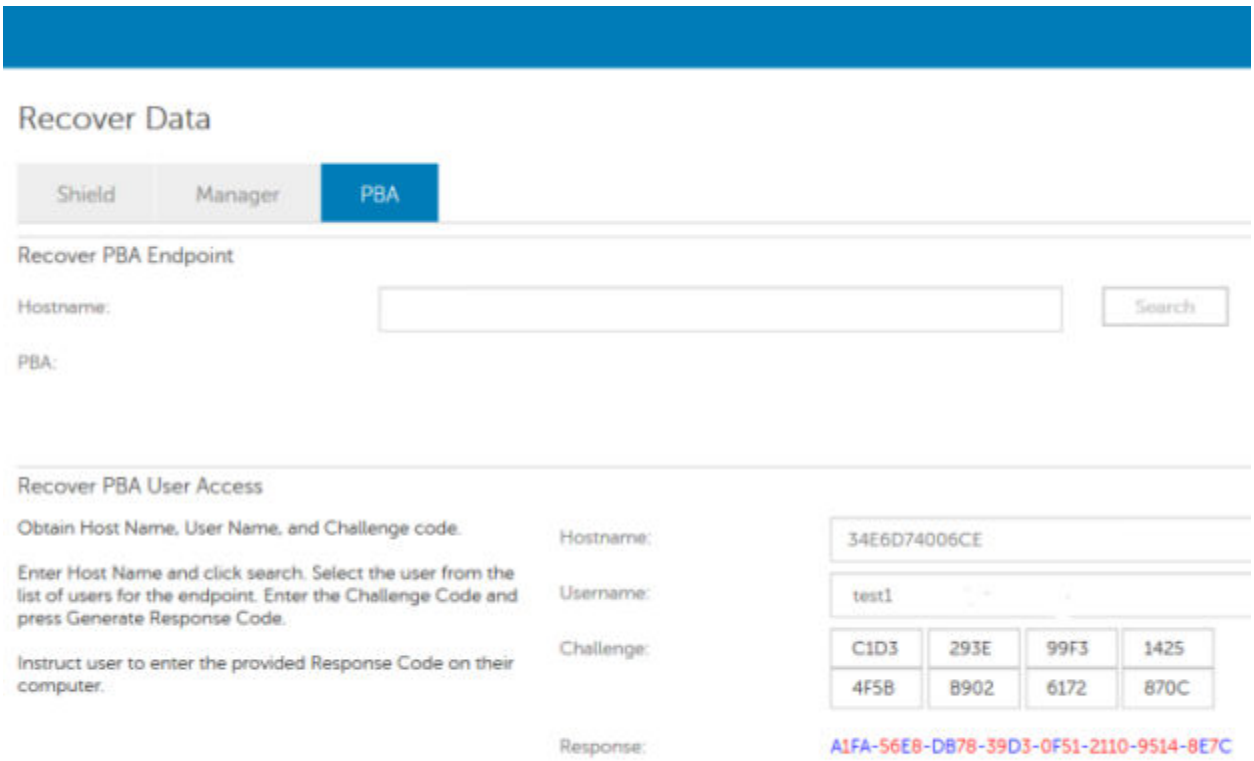

Die folgenden Informationen werden nach der Auswahl von **Abfrageantwort** angezeigt.



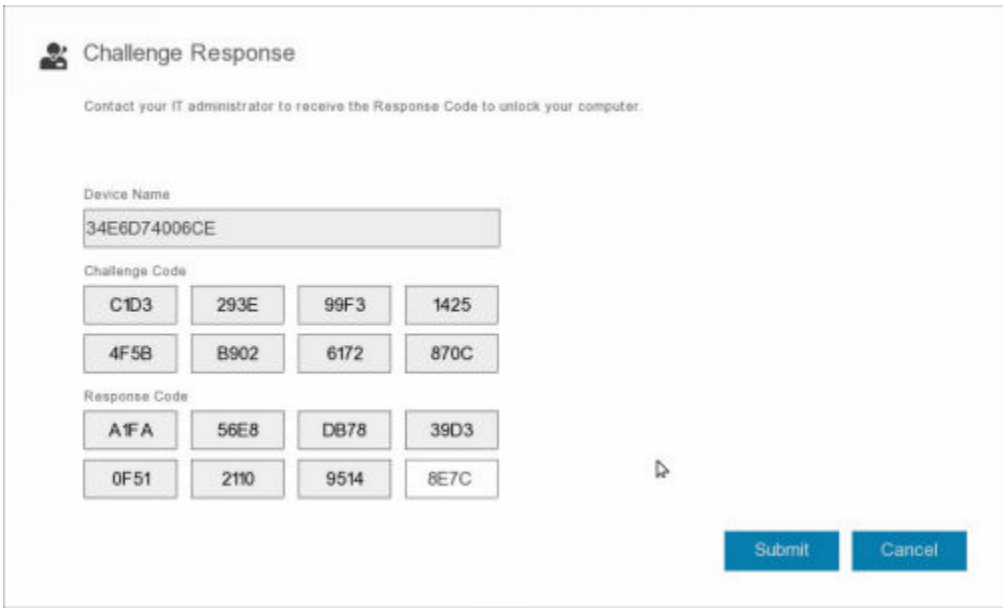

Das Feld **Gerätename** wird vom Helpdesk-Techniker innerhalb der Remote Management-Konsole verwendet, um das richtige Gerät zu finden, dann wird ein Benutzername ausgewählt. Dieser befindet sich in **Management > Daten wiederherstellen** unter der Registerkarte **PBA**.



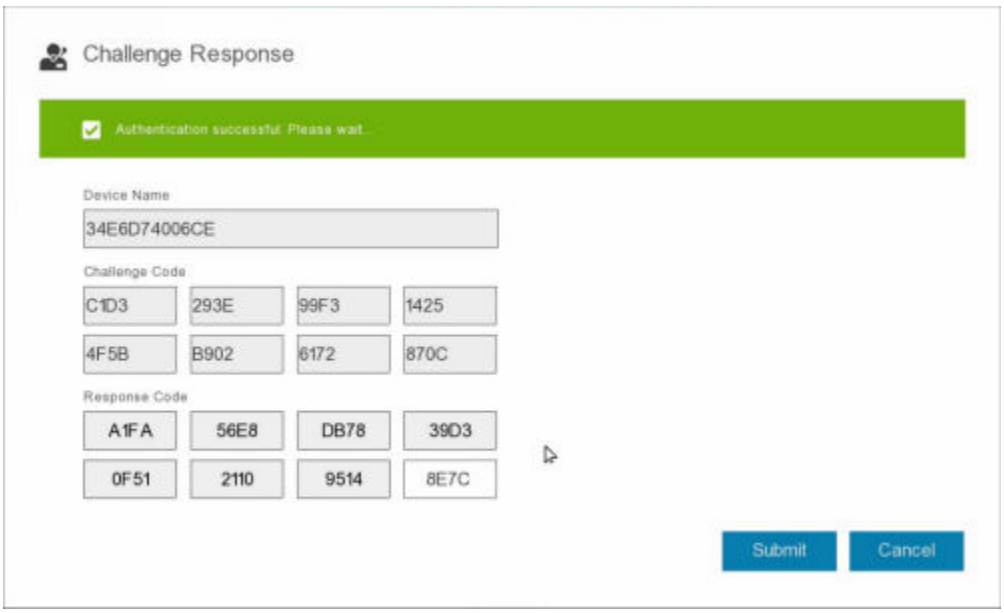

Der Abfragecode wird dem Helpdesk-Techniker zur Verfügung gestellt, der die Daten eingibt und dann auf die Schaltfläche **Antwort erzeugen** klickt.



Die ausgegebenen Daten sind farbcodiert, um bei der Unterscheidung zwischen Ziffern (rot) und Buchstaben (blau) zu helfen. Diese Daten werden dem Endanwender vorgelesen, der sie in die PBA-Umgebung eingibt und dann auf die Schaltfläche **Senden** klickt, wodurch der Benutzer unter Windows gelangt.




Nach der erfolgreichen Authentifizierung wird die folgende Meldung angezeigt:




Die Abfragewiederherstellung ist abgeschlossen.

5

# Wiederherstellung bei voller Datenträgerverschlüsselung

Die Wiederherstellung ermöglicht es Ihnen, wieder Zugriff auf Dateien auf einem mit vollständiger Datenträgerverschlüsselung verschlüsselten Datenträger zu erlangen.

**ANMERKUNG: Die Entschlüsselung sollte nicht unterbrochen werden. Wenn die Entschlüsselung unterbrochen wird, kann es zu Datenverlust kommen.**

## Voraussetzungen für die Wiederherstellung

Für die Wiederherstellung bei vollständiger Datenträgerverschlüsselung benötigen Sie Folgendes:

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

## Übersicht über den Wiederherstellungsprozess

**ANMERKUNG: Für die Wiederherstellung ist eine 64-Bit-Umgebung erforderlich.**

So stellen Sie ein ausgefallenes System wieder her:

1 Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe Anhang A, Brennen der Wiederherstellungsumgebung.
2 Besorgen Sie sich die Wiederherstellungsdatei.
3 Führen Sie die Wiederherstellung durch.

## Durchführen einer Wiederherstellung bei vollständiger Datenträgerverschlüsselung

Führen Sie folgende Schritte aus, um eine Wiederherstellung bei vollständiger Datenträgerverschlüsselung durchzuführen.

### Wiederherstellungsdatei besorgen – Client für volle Datenträgerverschlüsselung

Besorgen Sie sich die Wiederherstellungsdatei.

Laden Sie die Wiederherstellungsdatei von der Remote Management-Konsole herunter. So laden Sie die Datei *<hostname>-sed-recovery.dat* herunter, die erstellt wurde, als Sie Dell Data Security installiert haben:

a Öffnen Sie die Remote-Verwaltungskonsole und wählen Sie im linken Fensterbereich **Verwaltung > Daten wiederherstellen**, wählen Sie dann die Registerkarte **PBA**.
b Geben Sie auf dem Bildschirm „Daten wiederherstellen“ im Feld „Hostname“ den vollständig qualifizierten Domänennamen des Endpunktes ein und klicken Sie auf **Suchen**.

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

d Klicken Sie auf **Wiederherstellungsdatei erstellen**.

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

# 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.

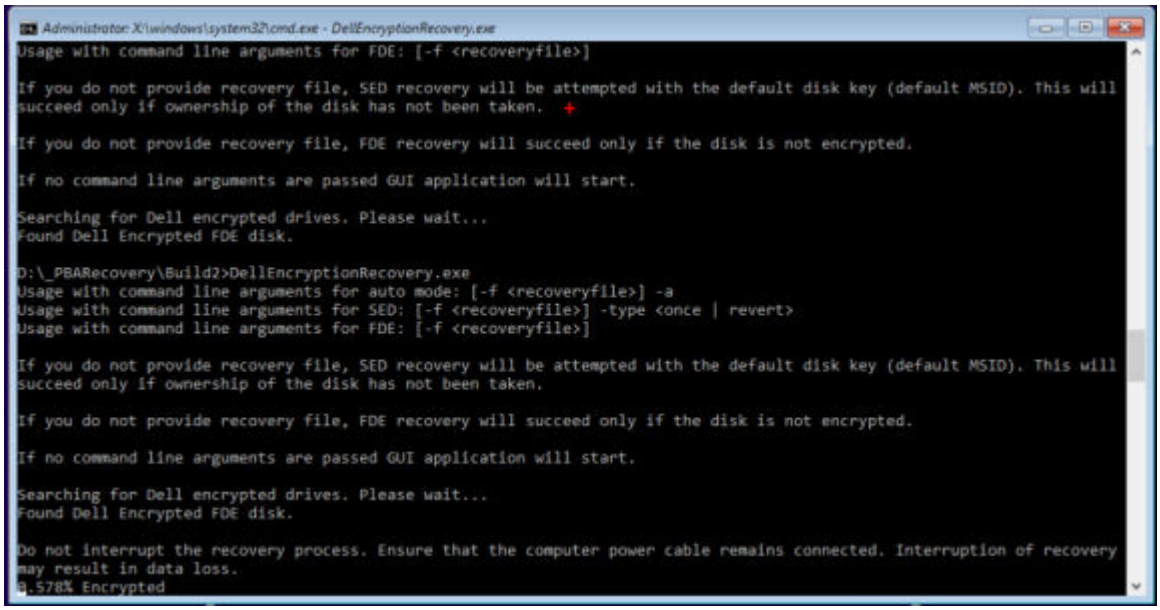
**ANMERKUNG: Deaktivieren Sie vor dem Wiederherstellungsprozess SecureBoot. Wenn Sie fertig sind, können Sie SecureBoot wieder aktivieren.**

2 Wählen Sie Option eins und drücken Sie die **Eingabetaste**.

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

4 Klicken Sie auf **OK**.

.




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.

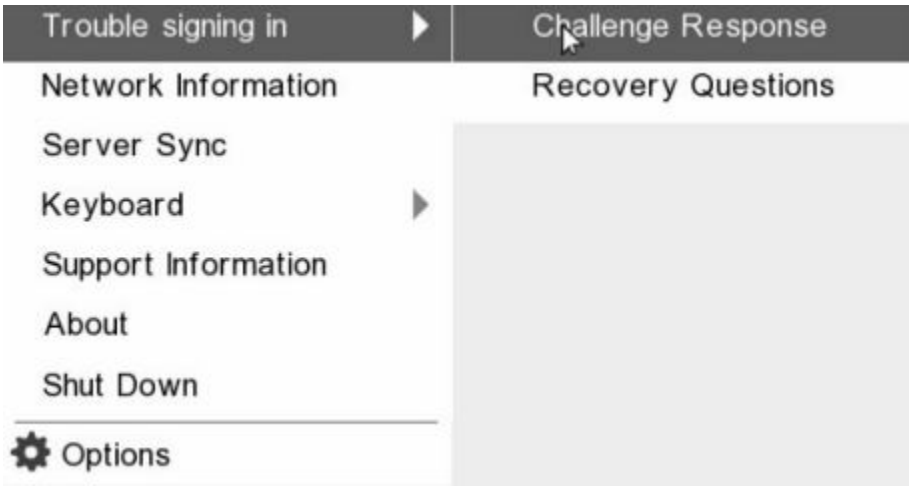
7 Nachdem der Computer neu gestartet wurde, sollte er voll funktionsfähig sein. Falls das Problem weiterhin besteht, kontaktieren Sie den Dell ProSupport.

# Abfragewiederherstellung mit vollständiger Datenträgerverschlüsselung

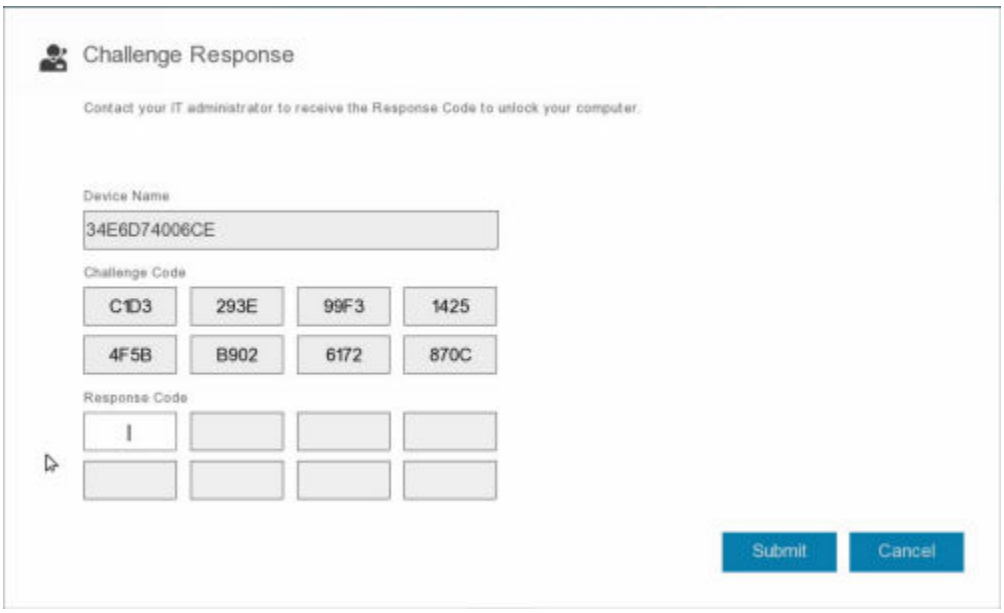
### Umgehen der Preboot-Authentifizierungsumgebung

Benutzer vergessen ihre Kennwörter und rufen beim Helpdesk an, um sich zu erkundigen, wie sie die PBA-Umgebung überwinden können. Verwenden Sie den Abfrage-/Antwort-Mechanismus, der in das Gerät integriert ist. Dieser gilt pro Benutzer und basiert auf einem

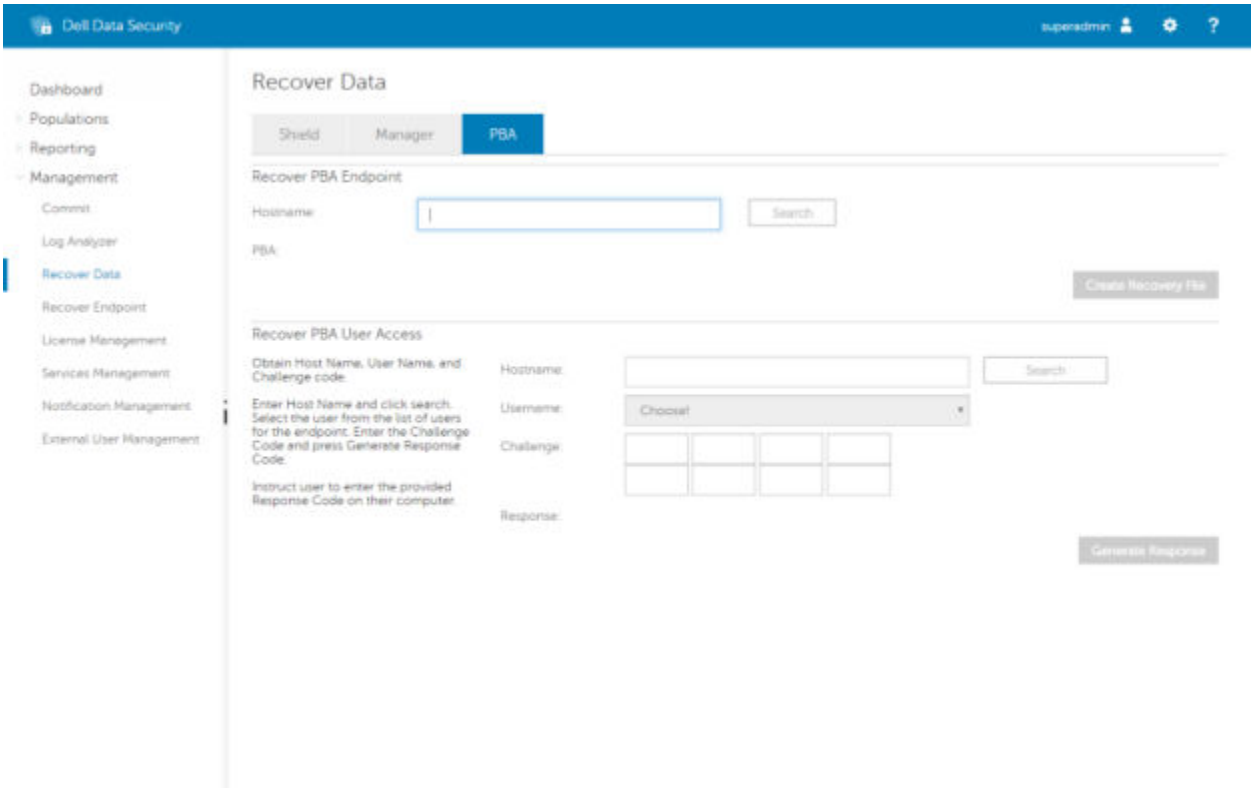
rotierenden Satz von alphanumerischen Zeichen. Der Benutzer muss seinen Namen in das Feld **Benutzername** eingeben und anschließend **Optionen > Abfrageantwort** auswählen.



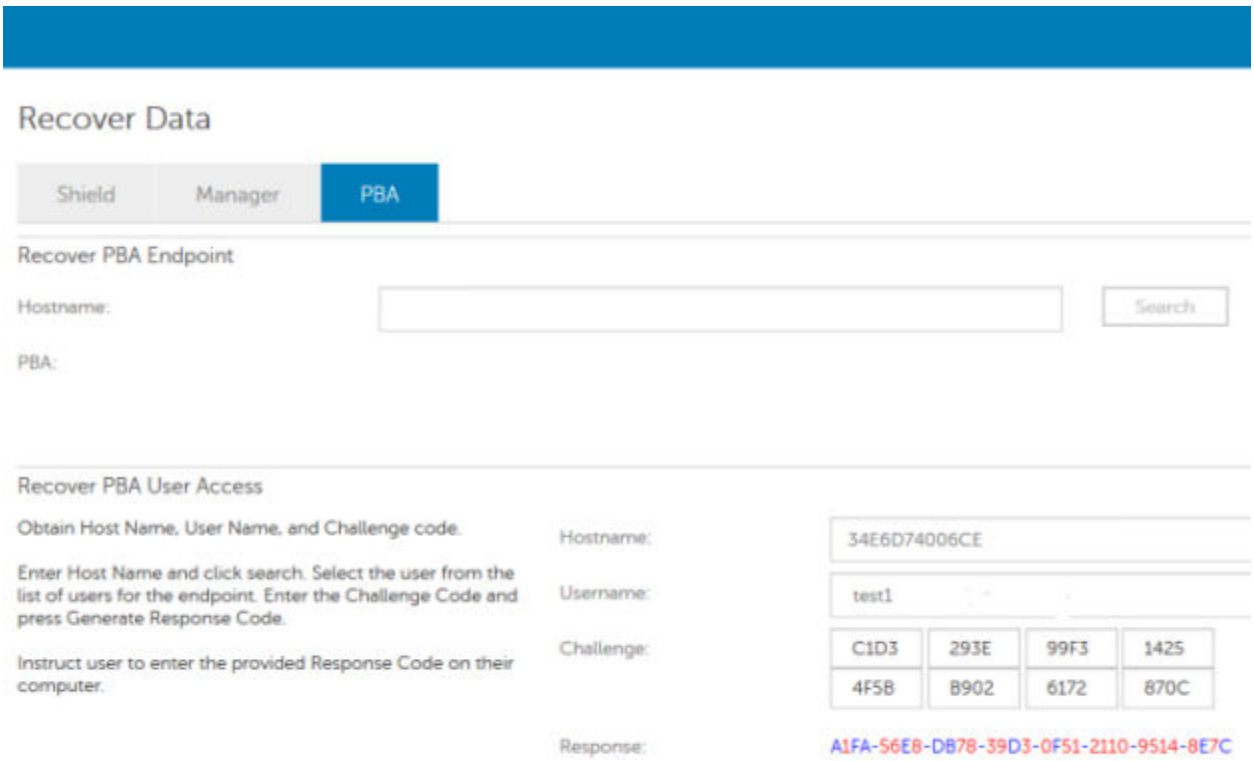

Die folgenden Informationen werden nach der Auswahl von **Abfrageantwort** angezeigt.



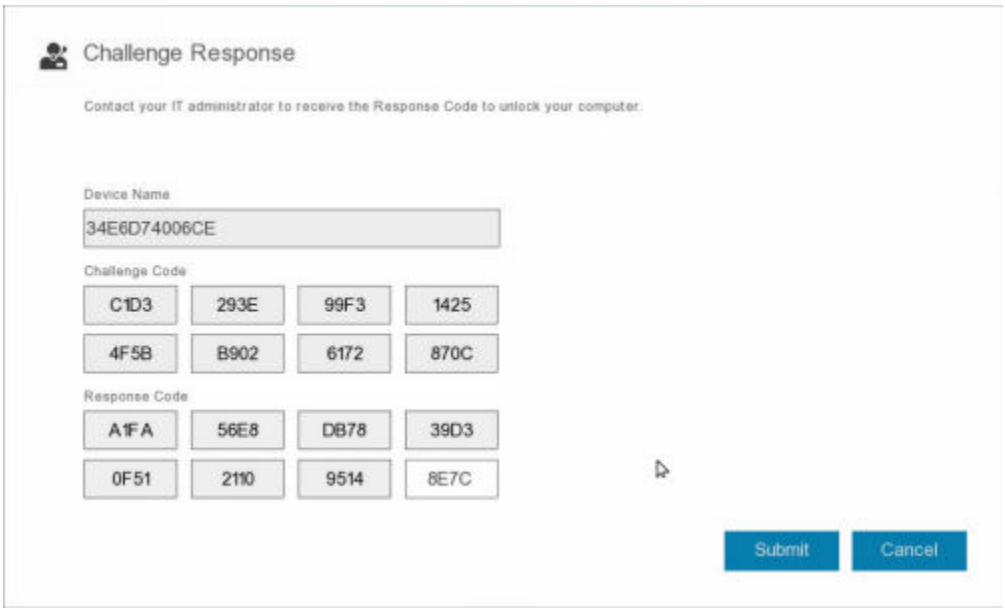

Das Feld **Gerätename** wird vom Helpdesk-Techniker innerhalb der Remote Management-Konsole verwendet, um das richtige Gerät zu finden, dann wird ein Benutzername ausgewählt. Dieser befindet sich in **Management > Daten wiederherstellen** unter der Registerkarte **PBA**.



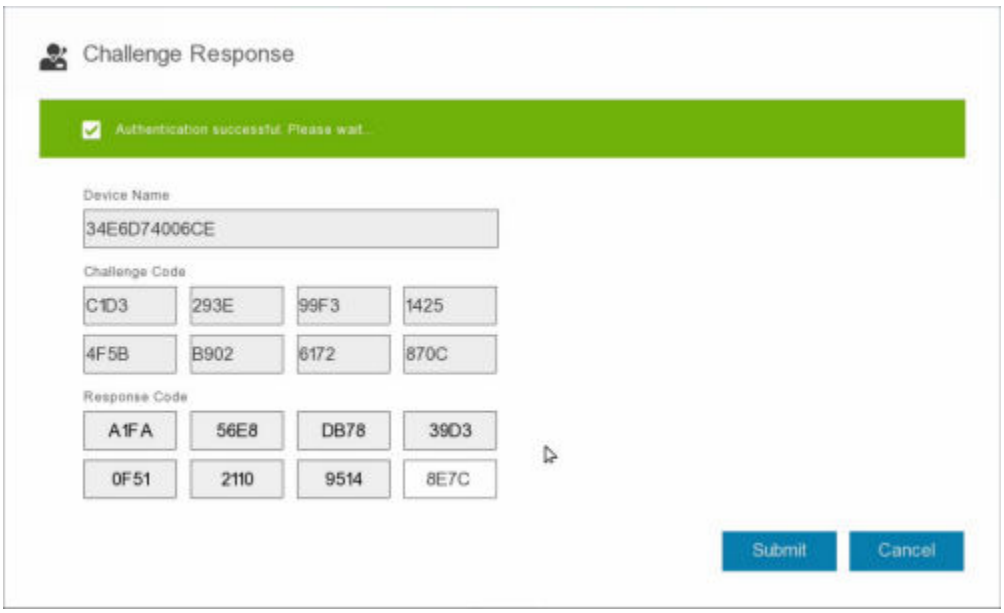

Der Abfragecode wird dem Helpdesk-Techniker zur Verfügung gestellt, der die Daten eingibt und dann auf die Schaltfläche **Antwort erzeugen** klickt.



Die ausgegebenen Daten sind farbcodiert, um bei der Unterscheidung zwischen Ziffern (rot) und Buchstaben (blau) zu helfen. Diese Daten werden dem Endanwender vorgelesen, der sie in die PBA-Umgebung eingibt und dann auf die Schaltfläche **Senden** klickt, wodurch der Benutzer unter Windows gelangt.




Nach der erfolgreichen Authentifizierung wird die folgende Meldung angezeigt:




Die Abfragewiederherstellung ist abgeschlossen.

6

# Wiederherstellung bei voller Datenträgerverschlüsselung und Dell Encryption

Dieses Kapitel erläutert die Wiederherstellungsschritte, um den Zugriff auf von Dell Encryption geschützte Dateien wiederherzustellen, die sich auf einem Datenträger befinden, der durch vollständige Datenträgerverschlüsselung geschützt wird.

**ANMERKUNG: Die Entschlüsselung sollte nicht unterbrochen werden. Wenn die Entschlüsselung unterbrochen wird, kann es zu Datenverlust kommen.**

## Voraussetzungen für die Wiederherstellung

Für die Wiederherstellung bei vollständiger Datenträgerverschlüsselung und Dell Encryption benötigen Sie Folgendes:

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

## Übersicht über den Wiederherstellungsprozess

**ANMERKUNG: Für die Wiederherstellung ist eine 64-Bit-Umgebung erforderlich.**

So stellen Sie ein ausgefallenes System wieder her:

1 Brennen Sie die Wiederherstellungsumgebung auf eine CD/DVD oder erstellen Sie einen startfähigen USB. Siehe Anhang A, Brennen der Wiederherstellungsumgebung.
2 Besorgen Sie sich die Wiederherstellungsdatei für Dell Encryption und die vollständige Datenträgerverschlüsselung.
3 Führen Sie die Wiederherstellung durch.

## Wiederherstellung von einer vollen Datenträgerverschlüsselung und einem verschlüsselten Datenträger von Dell durchführen

Führen Sie die folgenden Schritte durch, um eine Wiederherstellung von einer vollen Datenträgerverschlüsselung und einem verschlüsselten Datenträger von Dell durchzuführen.

### Wiederherstellungsdatei besorgen – Client für volle Datenträgerverschlüsselung

Besorgen Sie sich die Wiederherstellungsdatei.

Laden Sie die Wiederherstellungsdatei von der Remote Management-Konsole herunter. So laden Sie die Datei *<hostname>-sed-recovery.dat* herunter, die erstellt wurde, als Sie Dell Data Security installiert haben:

a Öffnen Sie die Remote-Verwaltungskonsole und wählen Sie im linken Fensterbereich **Verwaltung > Daten wiederherstellen**, wählen Sie dann die Registerkarte **PBA**.

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

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

d Klicken Sie auf **Wiederherstellungsdatei erstellen**.

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

# Wiederherstellungsdatei besorgen – Richtlinienbasierte Verschlüsselung oder FFE-Client für Verschlüsselungen

So laden Sie die Recovery-Datei herunter:

1 Laden Sie das Installationspaket Dell Encryption von http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers herunter. Navigieren Sie zum Ordner **AdminUtilities** im Installationspaket und öffnen Sie **CMGAd.exe**.

2 Geben Sie in das Feld **Dell Server** Security Management Server/Security Management Server Virtual ein, was auf dem Computer aktiviert wurde.

3 Geben Sie in das Feld **Dell Admin** den Namen des Benutzerkontos mit forensischen Administratorrechten ein.

4 Geben Sie in das Feld **Kennwort** das Kennwort für den forensischen Administrator ein.

5 Geben Sie im Feld **MCID** den FQDN des Geräts ein, das wiederhergestellt wird.

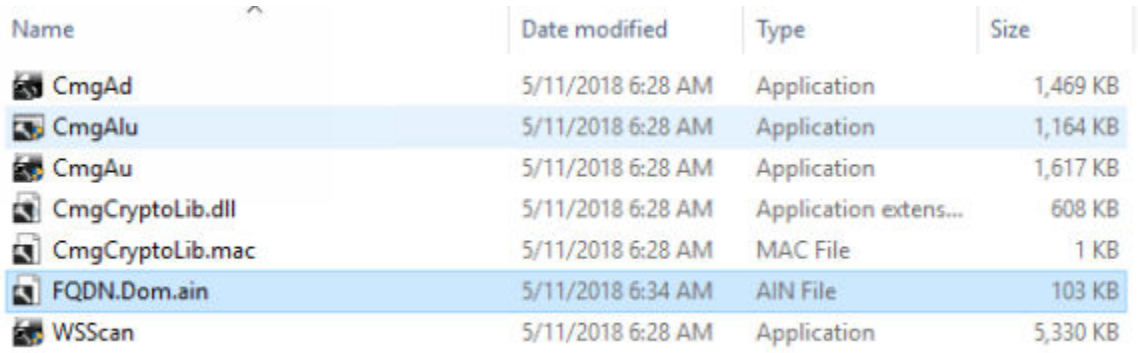
- Das Feld **DCID** ist die Wiederherstellungs-ID für das Gerät, das wiederhergestellt wird.

6 Klicken Sie auf **Weiter**.

7 Erstellen und bestätigen Sie eine **Passphrase** für die Wiederherstellungsdatei. Diese Passphrase ist erforderlich, um eine Wiederherstellung durchzuführen.

8 Geben Sie in das Feld **Herunterladen auf:** einen Zielspeicherort für das Wiederherstellungspaket ein und klicken Sie dann auf **Weiter**. Standardmäßig wird dies im Verzeichnis sein, von dem aus CMGAd.exe ausgeführt wurde.


9 Das Wiederherstellungspaket lädt sich auf die Datei herunter, die im Feld **Herunterladen auf:** festgelegt wurde.

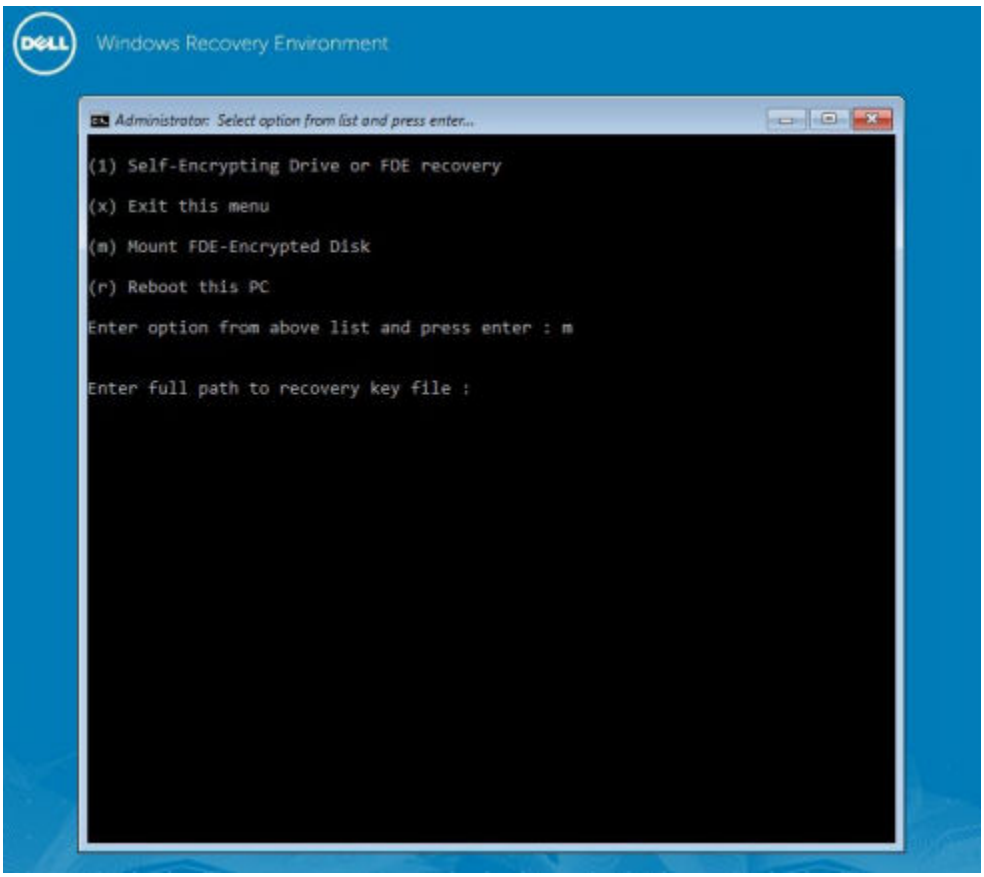



10 Kopieren Sie die Wiederherstellungspaketdatei an einen Ort, wo auf sie zugegriffen werden kann, wenn WinPE gestartet wird.

# 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.

ANMERKUNG: **Deaktivieren Sie vor dem Wiederherstellungsprozess SecureBoot. Wenn Sie fertig sind, können Sie SecureBoot wieder aktivieren.**




2 Wählen Sie Option drei und drücken Sie die **Eingabetaste**.

3 Wenn Sie dazu aufgefordert werden, geben Sie den Namen und Speicherort der Wiederherstellung ein.

4 Unter Verwendung des Wiederherstellungsschlüssels wird die Datei für die vollständige Datenträgerverschlüsselung installiert.

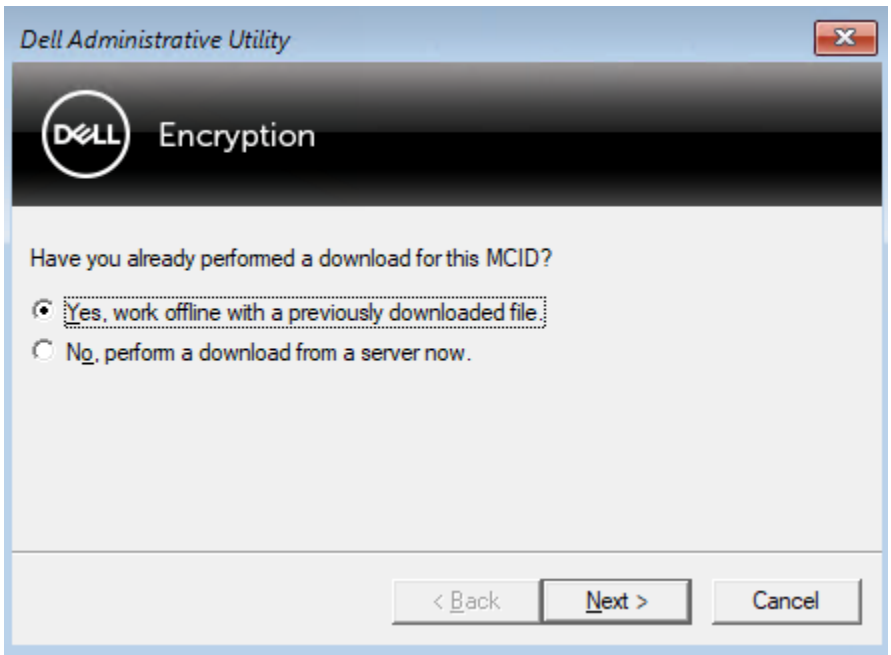
```
Enter option from above list and press enter : m

Enter the full path to the recovery key file: c:\recovery\opalSPKey.DESKTOP-XXYYZZ.recovery.dat

Recoveryfile loaded
====================   Disk 0   ====================
     Cylinders       = 15566
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 128035676160 (Bytes)
                     = 119.24 GB
---> Disk 0, returned status...........: EDriverStatus_Success
====================   Disk 1   ====================
     Cylinders       = 973
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 8004304896 (Bytes)
                     = 7.45 GB
---> Disk 0, returned status...........: EDriverStatus_DriveNotEncrypted
```

.

5 Navigieren Sie zur Datei CMGAu.exe mithilfe des folgenden Befehls: `cd DDPEAdminUtilities\`

6 Starten Sie CMGAu.exe mit dem folgenden Befehl: `\DDPEAdminUtilities>CmgAu.exe`

Wählen Sie **Ja, mit bereits heruntergeladener Datei offline arbeiten** aus.




7 Geben Sie in das Feld **Heruntergeladene Datei:** den Ort des **Wiederherstellungspakets** ein, geben Sie dann die **Passphrase** des forensischen Administrators ein und klicken Sie auf **Weiter**.


Wenn die Wiederherstellung abgeschlossen ist, klicken Sie auf **Fertig stellen**.

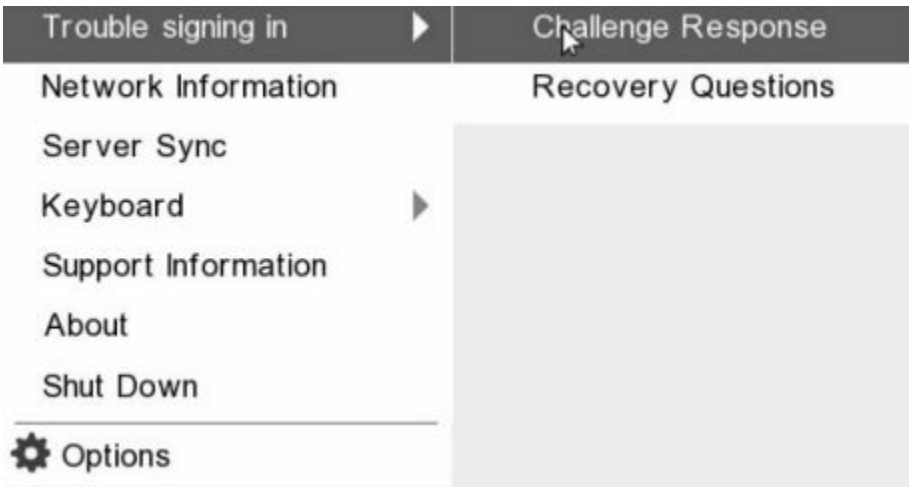
**ANMERKUNG:**
Stellen Sie sicher, dass Sie sämtliche USB- oder CD-\DVD-Medien entfernt haben, die zum Starten des Computers verwendet wurden. Ist das nicht der Fall, kann das zu einem Neustart in die Wiederherstellungsumgebung führen.

8 Nachdem der Computer neu gestartet wurde, sollten Sie Zugriff auf die verschlüsselten Dateien haben. Falls das Problem weiterhin besteht, kontaktieren Sie den Dell ProSupport.

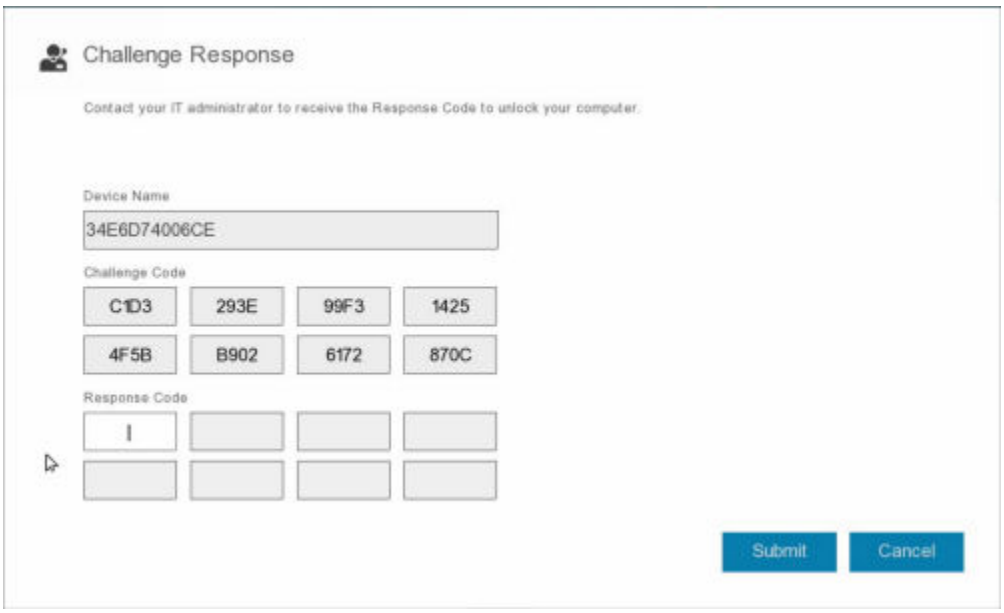
# Abfragewiederherstellung mit vollständiger Datenträgerverschlüsselung

**Umgehen der Preboot-Authentifizierungsumgebung**

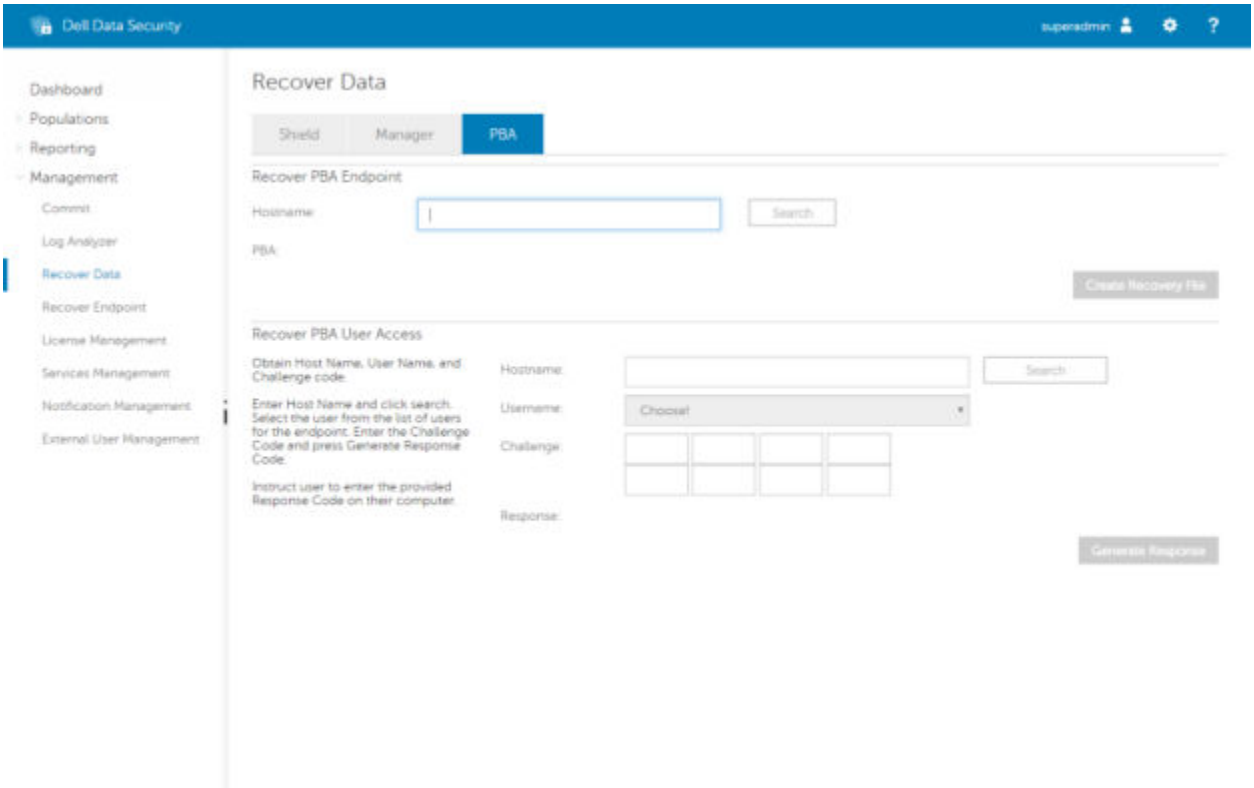
Benutzer vergessen ihre Kennwörter und rufen beim Helpdesk an, um sich zu erkundigen, wie sie die PBA-Umgebung überwinden können. Verwenden Sie den Abfrage-/Antwort-Mechanismus, der in das Gerät integriert ist. Dieser gilt pro Benutzer und basiert auf einem rotierenden Satz von alphanumerischen Zeichen. Der Benutzer muss seinen Namen in das Feld **Benutzername** eingeben und anschließend **Optionen > Abfrageantwort** auswählen.



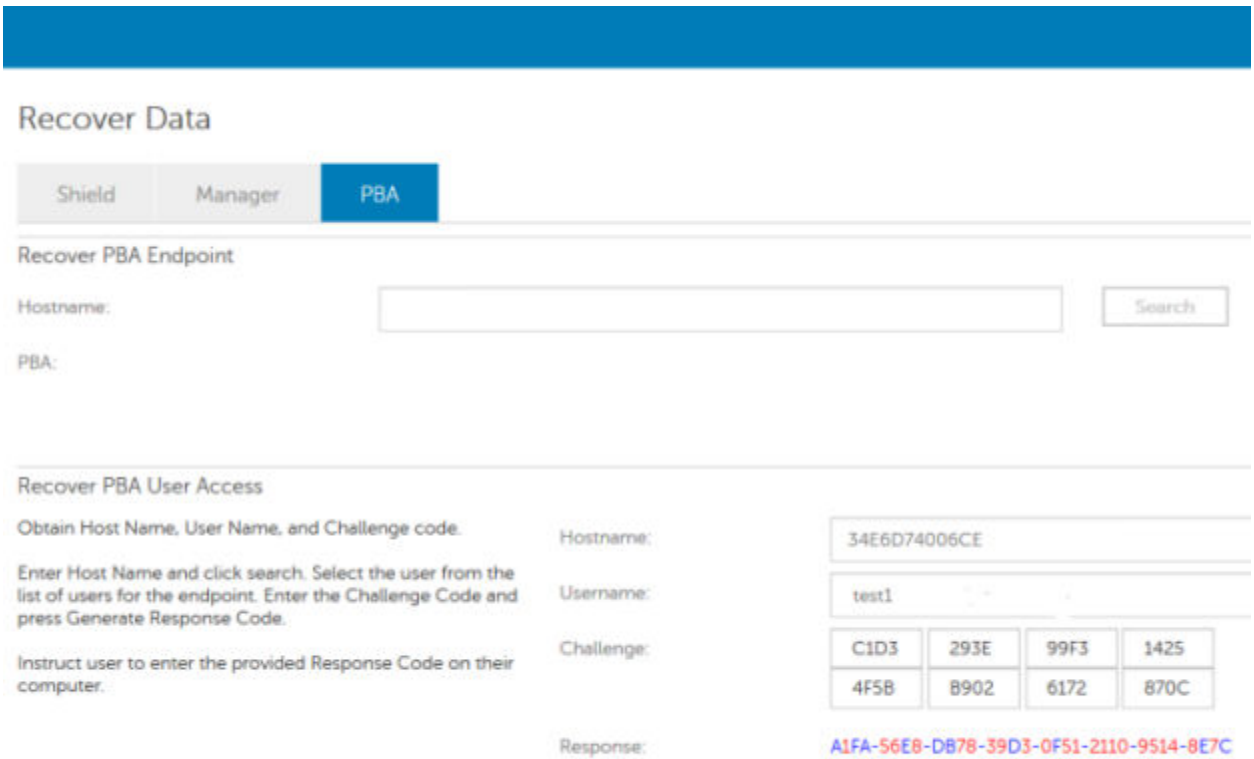

Die folgenden Informationen werden nach der Auswahl von **Abfrageantwort** angezeigt.



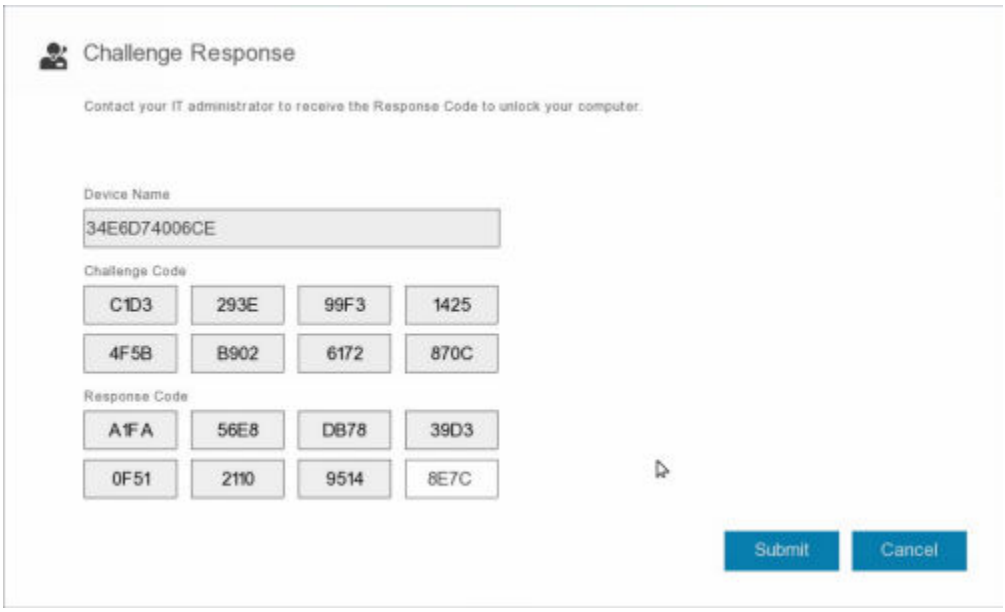

Das Feld **Gerätename** wird vom Helpdesk-Techniker innerhalb der Remote Management-Konsole verwendet, um das richtige Gerät zu finden, dann wird ein Benutzername ausgewählt. Dieser befindet sich in **Management > Daten wiederherstellen** unter der Registerkarte **PBA**.



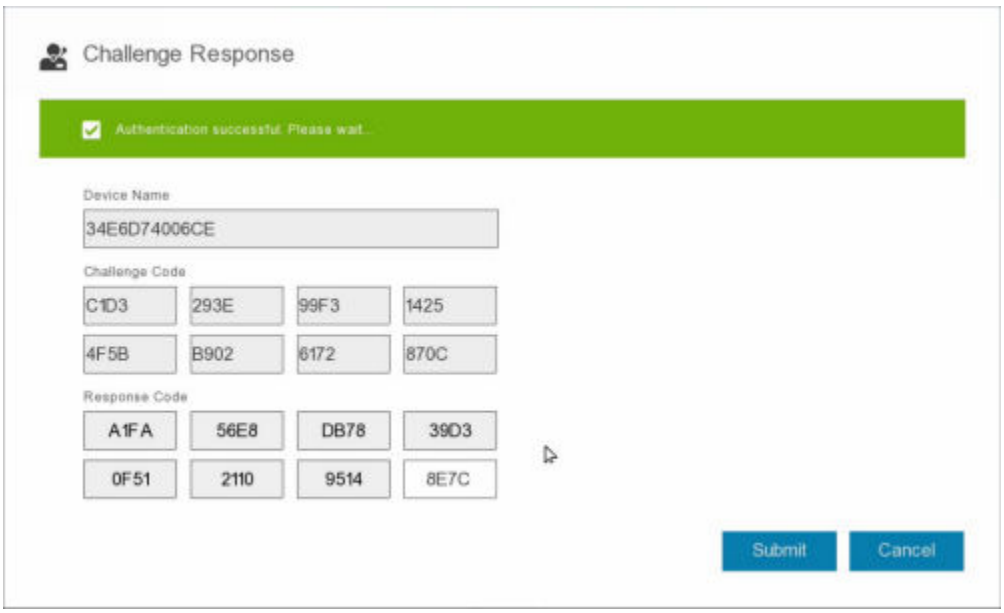

Der Abfragecode wird dem Helpdesk-Techniker zur Verfügung gestellt, der die Daten eingibt und dann auf die Schaltfläche **Antwort erzeugen** klickt.



Die ausgegebenen Daten sind farbcodiert, um bei der Unterscheidung zwischen Ziffern (rot) und Buchstaben (blau) zu helfen. Diese Daten werden dem Endanwender vorgelesen, der sie in die PBA-Umgebung eingibt und dann auf die Schaltfläche **Senden** klickt, wodurch der Benutzer unter Windows gelangt.




Nach der erfolgreichen Authentifizierung wird die folgende Meldung angezeigt:




Die Abfragewiederherstellung ist abgeschlossen.

7

# PBA-Gerätesteuerung

Die PBA-Gerätesteuerung gilt für Endpunkte, die mit SED oder vollständiger Datenträgerverschlüsselung verschlüsselt sind.

## PBA-Gerätesteuerung verwenden

Befehle von der PBA für einen bestimmten Endpunkt werden im Bereich „PBA-Gerätesteuerung“ ausgeführt. Jeder Befehl verfügt über eine bestimmte Priorität. In der Warteschlange für die Durchsetzung setzen Befehle mit höherer Priorität die Befehle mit niedrigerer Priorität außer Kraft. Eine Liste der Prioritätenreihung von Befehlen finden Sie unter *AdminHelp*, indem Sie auf das ? in der Remote Management-Konsole klicken. Die PBA-Gerätesteuerung ist auf der Seite „Endpunkt-Details“ der Remote Management-Konsole verfügbar.

Die folgenden Befehle stehen in der PBA-Gerätesteuerung zur Verfügung:

- **Sperren**: Sperrt den PBA-Bildschirm und verhindert, dass Benutzer sich beim Computer anmelden können.
- **Entsperren**: Sie können die Sperrung eines PBA-Bildschirms aufheben, der entweder durch das Senden eines Befehls zum Sperren oder durch Überschreitung der nach der Richtlinie maximal zulässigen Authentifizierungsversuche gesperrt wurde.
- **Benutzer entfernen**: Alle Benutzer werden aus der PBA entfernt.
- **Anmeldung umgehen**: Umgeht den PBA-Bildschirm ein Mal, um eine Benutzeranmeldung ohne Authentifizierung zuzulassen. Der Benutzer muss sich nach der Umgehung von PBA bei Windows anmelden.
- **Löschen**: Der Löschbefehl bewirkt, dass das verschlüsselte Laufwerk auf die Werkseinstellungen zurückgesetzt wird. Der Befehl zum Löschen ermöglicht die Wiederverwendung des Computers und kann im Notfall zur Löschung der Daten verwendet werden, um den unbefugten Zugriff zu unterbinden. Verwenden Sie diesen Befehl daher nur, wenn dies das gewünschte Ergebnis ist. Für die vollständige Datenträgerverschlüsselung löscht der Befehl Wipe kryptografisch das Laufwerk und die PBA wird entfernt. Für SED löscht der Befehl Wipe kryptografisch das Laufwerk, und die PBA zeigt "Gerät gesperrt" an. Zum Wiederverwenden des SED entfernen Sie die PBA mit der App SED Recovery.

# 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 Dell 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 Security generiert wurde:

1 Öffnen Sie die Remote Management-Konsole 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 "Wiederherstellung" ein Wiederherstellungspasswort ein und klicken Sie auf **Herunterladen**.

> **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)

> **ANMERKUNG: Deaktivieren Sie vor dem Wiederherstellungsprozess SecureBoot. Wenn Sie fertig sind, aktivieren Sie SecureBoot wieder.**

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 die **Eingabetaste**, 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.

# 9

# 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.

10

# 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.

# Wiederherstellung des Encryption External Media-Kennworts

Encryption External Media 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 Dell 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

Das Laufwerk muss zurück in den Rechner eingesetzt werden, der es ursprünglich verschlüsselt hat, damit die Selbstwiederherstellung funktioniert. 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. Dieser Vorgang kann das Problem mit teilweise beschädigtem Datenträger lösen.

1 Melden Sie sich bei einer mit Dell Data Security 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 von:
  - Geschützte Office-Dateien in jedem unterstützten Format – Dateien, die sowohl mit Protected Office Dokument-Verschlüsselung von Data Guardian als auch mit dessen Cloud Service Provider-Schutz geschützt sind, können wiederhergestellt werden.
  - Dateienformate, die in der einfachen Dateischutzrichtlinie aufgelistet sind, wenn sie aktiviert sind.
- Manuelles 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.

**ANMERKUNG:**
Sie können das Windows-Wiederherstellungtool mit den Dateien verwenden, die auf einem Mac, einer Mobile-Version oder in einem Webportal erstellt wurden.

## Voraussetzungen

Die Voraussetzungen sind:

- Microsoft .Net Framework 4.5.2 muss auf dem wiederherzustellenden Endgerät laufen.
- Die forensische Administratorrolle muss in der 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. Sie können einen Computer auf einmal wiederherstellen.

**WICHTIG:**
Verschlüsseln Sie Kopien der Dateien (nicht die Originaldateien), um zu verhindern, dass Inhalte im Fall einer Beschädigung verloren gehen.

**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

**WICHTIG:**

Achten Sie als Administrator darauf, dass Sie nur die Datei **RecoveryTools.exe** und nicht das Installationsprogramm kopieren. **RecoveryTools.exe** funktioniert besser, wenn keine Such- oder Enschlüsselungsvorgänge ausgeführt werden.

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

3 Wählen Sie im Fenster „Data Guardian Wiederherstellungstool“ **Domain-Anmeldung** aus.

**ANMERKUNG:**

Die SaaS-Anmeldeoption für eine gehostete Lösung ist für eine zukünftige Version vorgesehen.

4 Geben Sie den Dell Server FQDN in diesem Format ein:
server.domain.com

**ANMERKUNG:**

Ein Präfix und Suffix werden dem vollständig qualifizierten Domänennamen (FQDN) automatisch hinzugefügt.

5 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 Anmelderechte haben.

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

7 Wählen Sie **Quelle**.

**ANMERKUNG:**

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

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

9 Klicken Sie auf **OK**.

10 Klicken Sie auf **Ziel** und geben Sie einen leeren Ordner für die entschlüsselte oder wiederhergestellten Dateien an.

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

12 Klicken Sie auf **OK**.

13 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.<br>• 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. |
| Entschlüsseln | Verweisen Sie mit dem Wiederherstellungstool auf ein Verzeichnis, das geschützte Office-Dokumente enthält, um diese zu entschlüsseln. |

| Optionen | Beschreibung |
| --- | --- |
| | **ANMERKUNG:** Die bewährte Methode ist es, Kopien der Dateien zu entschlüsseln und nicht die Originaldateien, falls es zu einer Beschädigung kommt.<br><br>Falls Manipulationen aufgetreten sind, wählen Sie optional eine oder beide dieser Optionen (Details siehe unten):<br><br>· **Überprüfung auf Manipulation** – sucht nach manipulierten Dateien, aber entschlüsselt diese nicht.<br>· **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.<br><br>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.<br><br>**ANMERKUNG:** 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. Das Wiederherstellungs-Tool überprüft standardmäßig die verborgenen Wasserzeichen und fügt eine Textdatei mit einer Liste aller Autoren zu einem Ordner namens *HiddenWatermark* in den Protokollen hinzu.

14 Ist die Auswahl abgeschlossen, klicken Sie auf **Scannen**.

Der Protokollbereich zeigt Folgendes an:

- Innerhalb der ausgewählten Quelle gefundene und gescannte Ordner
- Ob die Entschlüsselung einer Datei erfolgreich war oder fehlgeschlagen ist
- Der Name des letzten Autors einer Datei

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

### Anzeigen von Daten von einem versteckten Überwachungspfad

Wenn unter Windows die Richtlinie für den verborgenen Überwachungspfad für geschützte Office-Dokumente aktiviert ist, werden Benutzerinformationen in den Metadaten der Datei erfasst. Zum Anzeigen dieser Daten verwenden Sie das Recovery Tool:

1 Starten Sie das Recovery Tool.

- Für die **Quelle** navigieren Sie zu einem Ordner, der geschützte Office-Dokumente mit versteckten Prüfdaten enthält. Das Wiederherstellungstool kopiert den Ordner und die Unterordnerstruktur und entschlüsselt geschützte Office-Dokumente, die versteckte Prüfdaten enthalten.

- Vor dem Navigieren zu einem **Ziel** können Sie einen neuen Ordner für entschlüsselte Dateien erstellen und anschließend dorthin navigieren.

2 Wählen Sie **Entschlüsseln**.

3 Ist die Auswahl abgeschlossen, klicken Sie auf **Scannen**.

Der als Ziel ausgewählte Ordner enthält einen datierten Ordner mit *wiederhergestellten Dateien* mit Folgendem:

- Entschlüsselte, geschützte Office-Dateien
- *Überwachungspfad*-Ordner, vom Recovery Tool erstellt, mit einer .txt-Datei für jede entschlüsselte Datei. Jede .txt-Datei enthält ein Protokoll mit Informationen über die entschlüsselte Datei wie z. B. Ersteller, letzter Ersteller, Zeitstempel.

13

# 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

So erstellen Sie ein startfähiges USB-Laufwerk:

Legacy-Start:

1 Schließen Sie ein USB-Laufwerk an das System an.
2 Öffnen Sie mit Administratorrechten eine Eingabeaufforderung.
3 Rufen Sie das Dienstprogramm Diskpart auf, indem Sie **diskpart** eingeben.
4 Suchen Sie das Ziellaufwerk, indem Sie **list disk** eingeben. Datenträger werden nach Nummer benannt.
5 Wählen Sie den entsprechenden Datenträger mit dem Befehl **select disk #**, wobei # für die im vorherigen Schritt angegebene Laufwerksnummer steht.
6 Löschen Sie den Datenträger, indem Sie den Befehl **clean** erteilen. Dadurch wird der Datenträger von Daten gesäubert, indem die Dateitabelle gelöscht wird.
7 Erstellen Sie eine Partition für das Startabbild.
   a Der Befehl **create partition primary** generiert auf dem Datenträger eine Primärpartition.
   b Der Befehl **select partition 1** wählt die neue Partition aus.
   c Verwenden Sie den folgenden Befehl für die Schnellformatierung mit dem NTFS-Dateisystem: **Format FS=NTFS quick**.
8 Der Datenträger muss als startfähiges Laufwerk gekennzeichnet werden. Verwenden Sie den Befehl **active**, um den Datenträger als startfähig zu kennzeichnen.
9 Um Dateien direkt auf den Datenträger zu verschieben, weisen Sie dem Datenträger mit dem Befehl **assign** einen Laufwerksbuchstaben zu.
10 Der Datenträger wird automatisch bereitgestellt und der Inhalt der ISO-Datei kann in das Stammverzeichnis des Datenträgers kopiert werden.

Nachdem der ISO-Inhalt vollständig kopiert ist, ist das Laufwerk startfähig und kann zur Wiederherstellung verwendet werden.

EUFI-Boot:

1 Schließen Sie ein USB-Laufwerk an das System an.

2 Öffnen Sie mit Administratorrechten eine Eingabeaufforderung.

3 Rufen Sie das Dienstprogramm Diskpart auf, indem Sie **diskpart** eingeben.

4 Suchen Sie das Ziellaufwerk, indem Sie **list disk** eingeben. Datenträger werden nach Nummer benannt.

5 Wählen Sie den entsprechenden Datenträger mit dem Befehl **select disk #**, wobei # für die im vorherigen Schritt angegebene Laufwerksnummer steht.

6 Löschen Sie den Datenträger, indem Sie den Befehl **clean** erteilen. Dadurch wird der Datenträger von Daten gesäubert, indem die Dateitabelle gelöscht wird.

7 Erstellen Sie eine Partition für das Startabbild.

   a Der Befehl **create partition primary** generiert auf dem Datenträger eine Primärpartition.

   b Der Befehl **select partition 1** wählt die neue Partition aus.

   c Verwenden Sie den folgenden Befehl für die Schnellformatierung des Datenträgers mit dem FAT32-Dateisystem: **format FS=FAT32 quick**.

8 Der Datenträger muss als startfähiges Laufwerk gekennzeichnet werden. Verwenden Sie den Befehl **active**, um den Datenträger als startfähig zu kennzeichnen.

9 Um Dateien direkt auf den Datenträger zu verschieben, weisen Sie dem Datenträger mit dem Befehl **assign** einen Laufwerksbuchstaben zu.

10 Der Datenträger wird automatisch bereitgestellt und der Inhalt der ISO-Datei kann in das Stammverzeichnis des Datenträgers kopiert werden.

Nachdem der ISO-Inhalt vollständig kopiert ist, ist das Laufwerk startfähig und kann zur Wiederherstellung verwendet werden.