Encryption リカバリ

Encryption v 10.0 / Data Guardian v2.0

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

Encryption v 10.0 / Data Guardian v2.0

2018 - 08

Rev. A01

目次

1

リカバリを開始する前に

本項には、リカバリ環境を作成するための必要事項詳細が記載されています。

- CD-R、DVD-R メディアまたはフォーマット済みの USB メディア
  - CD または DVD に書き込む場合は、「リカバリ環境 ISO の CD または DVD への書き込み」で詳細を確認してください。
  - USB メディアを使用する場合は、「リムーバブルメディアへのリカバリ環境の書き込み」で詳細を確認してください。
- 故障したデバイスのリカバリバンドル
  - リモート管理のクライアントでは、お使いの Dell Security Management Server からのリカバリバンドルの取得方法を説明する指示が後に記載されています。
  - ローカル管理のクライアントでは、リカバリバンドルパッケージはセットアップ中に共有ネットワークドライブまたは外部メディアのいずれかに作成されました。作業を進める前にこのパッケージを見つけてください。

Dell ProSupport へのお問い合わせ

デル製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 4310039）にご連絡ください。

さらに、デル製品のオンラインサポートも dell.com/support からご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の各国の電話番号を記載したページを参照してください。

2

Policy-Based 暗号化リカバリまたはファイル / フォルダ暗号化リカバリ

暗号化されたコンピュータでオペレーティングシステムを起動できない場合には、リカバリが必要です。この状況は、レジストリが間違って変更されたか、暗号化されたコンピュータでハードウェアの変更が行われた場合に発生します。

Policy-Based 暗号化リカバリまたはファイル / フォルダ暗号化（FFE）リカバリでは、以下に対するアクセスを復元できます。

- 起動せず、SDE リカバリを実行するためのプロンプトを表示するコンピュータ。
- コンピュータは、BSOD に 0x6f または 0x74 の STOP コードを表示します。
- 暗号化されたデータにアクセスできない、またはポリシーを編集できないコンピュータ。
- 前記条件のいずれかを満たす Dell Encryption が実行されているサーバ。
- Hardware Crypto Accelerator カードまたはマザーボード / TPM を交換しなければならないコンピュータ。

メモ: V8.9.3 以降、Hardware Crypto Accelerator はサポートされません。

リカバリプロセスの概要

メモ: リカバリには 32 ビットの環境が必要です。

障害が発生したシステムを回復するには、次の手順を実行します。

1 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 A - リカバリ環境の書き込み」を参照してください。
2 リカバリファイルを入手します。
3 リカバリを実行します。

Policy-Based 暗号化リカバリまたは FFE リカバリの実行

Policy-Based 暗号化リカバリまたは FFE リカバリを実行するには、以下の手順に従います。

リカバリファイルの入手 - ポリシーベース暗号化または FFE 暗号化クライアント

リカバリファイルをダウンロードするには、次の手順を実行します。

1 http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers から Dell Encryption インストールパッケージをダウンロードします。インストールパッケージの **AdminUtilities** フォルダに移動して、**CMGAd.exe** を開きます。
2 **デルサーバ** フィールドに、コンピュータがアクティブ化された Security Management Server / Security Management Server Virtual を入力します。
3 **デル管理者** フィールドに、フォレンジック管理者権限を持つユーザーアカウント名を入力します。
4 **パスワード** フィールドに、フォレンジック管理者のパスワードを入力します。
5 **MCID** フィールドに、リカバリするデバイスの FQDN を入力します。

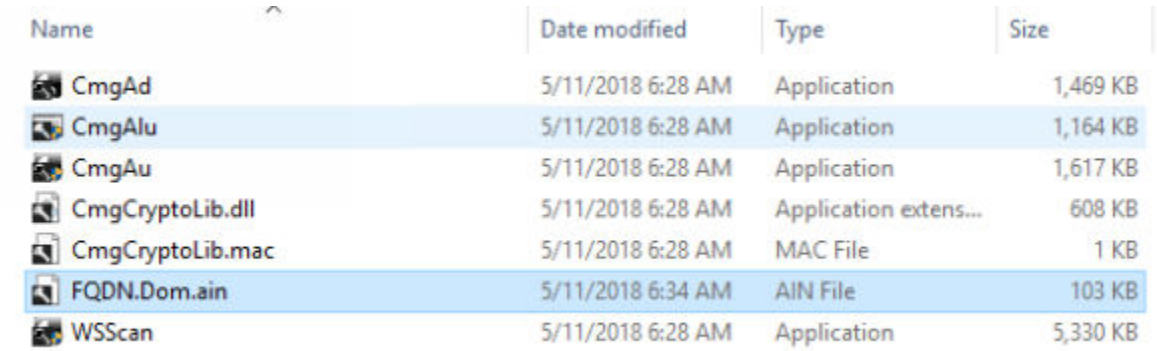
- **DCID** フィールドは、リカバリするデバイスのリカバリ ID です。

6 **次へ** を選択します。

7 リカバリファイルの **パスフレーズ** を定義して確認します。このパスフレーズはリカバリを実行する際に必要です。

8 **ダウンロード先：** フィールドにリカバリバンドルの保存先の場所を入力して、**次へ** を選択します。デフォルトでは、CMGAd.exe が実行されたディレクトリです。

9 **ダウンロード先：** で指定したフォルダに、リカバリバンドルがダウンロードされます。



10 WinPE の起動時にアクセスできる場所に、リカバリバンドルファイルをコピーします。

リカバリファイルの入手 - ローカル管理のコンピュータ

Encryption Personal リカバリファイルを入手するには、以下を行います。

1 **LSARecovery_<systemname> > .exe** という名前のリカバリファイルに移動します。このファイルは、Encryption Personal のインストール中にセットアップウィザードを実行したときにネットワークドライブまたはリムーバブルストレージに保存したものです。

2 対象コンピュータ (データを回復するコンピュータ) に **LSARecovery_<systemname> > .exe** をコピーします。

リカバリの実行

1 先ほど作成した起動可能なメディアを使用して、リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。WinPE 環境が開きます。

メモ: リカバリプロセスの前に SecureBoot を無効にします。終了したら、SecureBoot を再度有効にします。

2 **x** を入力して **Enter** を押し、コマンドプロンプトを表示します。

3 リカバリファイルに移動して起動します。

4 次の 1 つを選択します。

- システムが起動せず、SDE リカバリの実行を指示するメッセージを表示します。

  これにより OS へ起動する場合に、Encryption クライアントが実行するハードウェアチェックを再構築することができます。

- システムで暗号化データへのアクセスまたはポリシーの編集を実行できないか、再インストール中です。

  Hardware Crypto Accelerator カードまたはマザーボード / TPM を交換しなければならない場合はこれを使用してください。

5 バックアップおよびリカバリ情報 ダイアログで、回復するクライアントコンピュータの情報が正しいことを確認して **次へ** をクリックします。
デル以外のコンピュータを回復する場合は、SerialNumber および AssetTag フィールドは空白となります。

6 コンピュータのボリュームがリストされるダイアログで、該当するすべてのドライブを選択して **次へ** をクリックします。
複数のドライブをハイライトするには、Shift+ クリックまたは control+ クリックを行います。

選択されたドライブが Policy-Based 暗号化、または FFE 暗号化されていない場合、回復は失敗します。

7 リカバリパスワードを入力して、**次へ** をクリックします。
リモート管理クライアントでは、これは「リカバリファイルの入手 - リモート管理のコンピュータ」の手順 3 で指定したパスワードです。

Encryption Personal のパスワードは、キーがエスクローされたときにシステムに設定された、暗号化管理者パスワードです。

8 回復 ダイアログで、**回復** をクリックします。リカバリプロセスが開始されます。

9 リカバリが完了したら、**終了** をクリックします。

メモ:
コンピュータを起動するのに使用した USB、CD / DVD メディアを必ず取り外してください。取り外すのを忘れると再度リカバリ環境で起動してしまうことがあります。

10 コンピュータの再起動後、コンピュータは完全に機能した状態になります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

暗号化済みドライブのデータ回復

対象コンピュータが起動可能でなく、ハードウェア障害がない場合、データの回復は回復環境で起動されたコンピュータで実施することができます。対象コンピュータが起動可能でなく、ハードウェアに障害がある場合、または USB デバイスの場合、データの回復はスレーブに設定されたドライブで起動することで実施することができます。ドライブをスレーブに設定した場合、ファイルシステムを表示したり、ディレクトリを参照することができます。ただし、ファイルを開こうとすると、またはファイルをコピーしようとすると、アクセス拒否エラーが発生します。

暗号化されたドライブデータの回復

暗号化されたドライブデータを回復するには、以下を行います。

1 コンピュータから DCID / リカバリ ID を取得するには、以下のいずれかのオプションを選択します。

a 共有暗号化データが保存されているいずれかのフォルダで、WSScan を実行します。
「Common」の後に 8 桁の DCID / リカバリ ID が表示されます。

b リモート管理コンソールを開き、エンドポイントの **詳細とアクション** タブを選択します。

c エンドポイントの詳細画面のシールド詳細セクションにおいて、DCID / リカバリ ID を見つけます。

2 サーバからキーをダウンロードするには、Dell Administrative Unlock（**CMGAu**）ユーティリティに移動して実行します。
Dell Administrative Unlock ユーティリティは、Dell ProSupport から入手できます。

3 Dell Administrative Utility（CMGAu）ダイアログで、以下の情報（フィールドによっては予め入力されていることがあります）を入力して、**次へ** をクリックします。
サーバ：サーバの完全修飾ホスト名。たとえば、次のようなホスト名です。

デバイスサーバ（プレ 8.x クライアント）：**https://<server.organization.com>:8081/xapi**

セキュリティサーバ：**https://<server.organization.com>:8443/xapi/**

デル管理者：フォレンジック管理者のアカウント名（Security Management Server / Security Management Server Virtual で有効化されます）

デル管理者パスワード：フォレンジック管理者のアカウントパスワード（Security Management Server / Security Management Server Virtual で有効化されます）

MCID：MCID フィールドをクリアします

DCID：前の手順で取得した DCID / リカバリ ID

4 Dell Administrative Utility ダイアログで、**いいえ。サーバからのダウンロードを今すぐ実行します** を選択し、**次へ** をクリックします。

メモ:
Encryption クライアントがインストールされていない場合、アンロックが失敗したことを示すメッセージが表示されます。Encryption クライアントがインストールされているコンピュータに移動してください。

5 ダウンロードおよびロック解除が完了したら、ドライブから回復する必要のあるファイルをコピーします。すべてのファイルは読み出し可能です。**ファイルが回復されるまで、終了をクリックしないでください。**

6 ファイルの回復後、ファイルを再度ロックする準備ができたら、**終了** をクリックします。
終了 をクリックすると、暗号化済みファイルは使用不可となります。

3

Hardware Crypto Accelerator リカバリ

メモ: V8.9.3 以降、Hardware Crypto Accelerator はサポートされません。

Hardware Crypto Accelerator（HCA）リカバリでは、以下のアクセスを回復できます。

- HCA 暗号化ドライブ上のファイル - この方法では、提供されたキーを使用してドライブを復号化します。リカバリプロセス中に復号化する必要のある特定ドライブを選択することができます。
- ハードウェア交換後の HCA 暗号化ドライブ - この方法は、Hardware Crypto Accelerator カードまたはマザーボード / TPM の交換後に使用します。ドライブを復号化せずに暗号化されたデータへのアクセスを回復するため、リカバリを実行することができます。

リカバリ要件

HCA リカバリには以下が必要です。

- リカバリ環境 ISO へのアクセス（リカバリには 32 ビット環境が必要）
- 起動可能な CD / DVD または USB メディア

リカバリプロセスの概要

メモ: リカバリには 32 ビットの環境が必要です。

障害が発生したシステムを回復するには、次の手順を実行します。

1 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 A - リカバリ環境の書き込み」を参照してください。
2 リカバリファイルを入手します。
3 リカバリを実行します。

HCA リカバリの実行

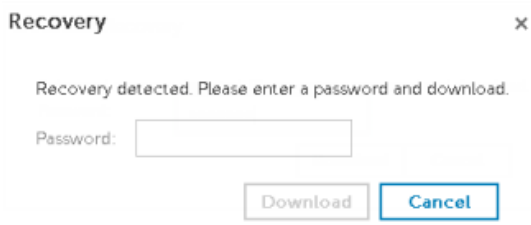
HCA リカバリを実行するには、以下の手順に従います。

リカバリファイルの入手 - リモート管理のコンピュータ

Dell Encryption のインストール時に生成された **<machinename_domain.com>.exe** ファイルをダウンロードするには、以下の手順に従います。

1 リモート管理コンソールを開き、左ペインから **管理** > **エンドポイントの回復** を選択します。
2 ホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。
3 リカバリウィンドウでリカバリパスワードを入力して、**ダウンロード** をクリックします。

メモ:
このパスワードは、リカバリキーへのアクセスのために覚えておかなければなりません。



リカバリファイルの入手 - ローカル管理のコンピュータ

Encryption Personal リカバリファイルを入手するには、以下を行います。

1 **LSARecovery_<systemname> > .exe** という名前のリカバリファイルに移動します。このファイルは、Encryption Personal のインストール中にセットアップウィザードを実行したときにネットワークドライブまたはリムーバブルストレージに保存したものです。

2 対象コンピュータ (データを回復するコンピュータ) に **LSARecovery_<systemname> > .exe** をコピーします。

リカバリの実行

1 先ほど作成した起動可能なメディアを使用して、リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。
WinPE 環境が開きます。

メモ: リカバリプロセスの前に SecureBoot を無効にします。終了したら、SecureBoot を有効にします。

2 **x** を入力して **Enter** を押し、コマンドプロンプトを表示します。

3 保存されたカバリファイルへ移動して起動します。

4 次の 1 つを選択します。
- HCA 暗号化済みドライブを復号化します。
- HCA 暗号化済みドライブへのアクセスを復元します。

5 バックアップおよびリカバリ情報 ダイアログで、サービスタグまたはアセット番号が正しいことを確認して、**次へ** をクリックします。

6 コンピュータのボリュームがリストされるダイアログで、該当するすべてのドライブを選択して **次へ** をクリックします。
複数のドライブをハイライトするには、Shift+ クリックまたは control+ クリックを行います。

選択されたドライブが HCA 暗号化されていない場合、回復は失敗します。

7 リカバリパスワードを入力して、**次へ** をクリックします。
リモート管理のコンピュータでは、これは「リカバリファイルの入手 - リモート管理のコンピュータ」の手順 3 で指定したパスワードです。

ローカル管理のコンピュータでは、このパスワードは、キーがエスクローされたときに、Personal Edition のステムに設定された、暗号化管理者パスワードです。

8 回復 ダイアログで、**回復** をクリックします。リカバリプロセスが開始されます。

9 プロンプトで指示された場合、保存されているリカバリファイルに移動して、**OK** をクリックします。
完全な復号化を実施する場合、以下のダイアログがステータスを表示します。このプロセスには時間がかかる場合があります。

10 リカバリが正しく完了したことを示すメッセージが表示されたら、**終了** をクリックします。コンピュータが再起動します。
コンピュータの再起動後、コンピュータは完全に機能した状態になります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

4

自己暗号化ドライブ（SED）リカバリ

SED リカバリでは、以下の方法を通して SED 上のファイルへのアクセスを回復することができます。

- ドライブの一回限りのアンロックを実施して、軌道前認証（PBA）を迂回します。
- アンロックして、ドライブから永続的に PBA を削除します。PBA が削除されると、シングルサインオンが機能しなくなります。
  - リモート管理 SED クライアントで、PBA を将来再度有効化できるようにして PBA を削除するには、リモート管理コンソールで製品を無効化する必要があります。
  - ローカル管理 SED クライアントで、PBA を将来再度有効化できるようにして PBA を削除するには、OS 内で製品を無効化する必要があります。

リカバリ要件

SED リカバリには、以下が必要です。

- リカバリ環境 ISO へのアクセス
- 起動可能な CD / DVD または USB メディア

リカバリプロセスの概要

メモ: リカバリを実行するには、BIOS 起動モードに応じて 64 ビットまたは 32 ビットのいずれかの環境が必要です。

障害が発生したシステムを回復するには、次の手順を実行します。

1 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 A - リカバリ環境の書き込み」を参照してください。
2 リカバリファイルを入手します。
3 リカバリを実行します。

SED リカバリの実行

SED リカバリを実行するには、以下の手順に従います。

リカバリファイルの入手 - リモート管理の SED クライアント

リカバリファイルを入手します。
リカバリファイルは、リモート管理コンソールからダウンロードすることができます。Dell Data Security のインストール時に生成された *<hostname>-sed-recovery.dat* ファイルをダウンロードするには、次の手順に従います。

a リモート管理コンソールを開き、左側のペインから、**管理、データの回復** の順に選択して **SED** タブを選択します。
b データの回復 画面のホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。
c SED フィールドでオプションを選択します。
d **リカバリファイルの作成** をクリックします。

<hostname>-sed-recovery.dat ファイルがダウンロードされます。

リカバリファイルの入手 - ローカル管理の SED クライアント

リカバリファイルを入手します。

ファイルが生成され、Advanced Authentication がコンピュータにインストールされたときに選択したバックアップロケーションからアクセスできます。ファイル名は *OpalSPkey<systemname>.dat* です。

リカバリの実行

1 先ほど作成した起動可能なメディアを使用して、リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。リカバリアプリケーションと共に WinPE 環境が開きます。

ⓘ **メモ: リカバリプロセスの前に SecureBoot を無効にします。終了したら、SecureBoot を有効にします。**

2 オプションを 1 つ選択して、**Enter** を押します。

3 **参照** を選択してリカバリファイルを確認し、**開く** をクリックします。

4 1 つのオプションを選択して、**OK** をクリックします。

- **ドライブを一回だけアンロックする**：この方法を選択すると、PBA がバイパスされます。
- **ドライブをアンロックして PBA を削除する**:この方法を選択すると、ドライブがアンロックされ、ドライブから PBA が永久的に削除されます。PBA を将来再度有効化できるようにして PBA を削除するには、リモート管理コンソール (リモート管理 SED クライアントの場合) から、または OS 内 (ローカル管理 SED クライアントの場合) で製品を無効化する必要があります。PBA が削除されると、シングルサインオンが機能しなくなります。

5 これでリカバリが完了しました。任意のキーを押してメニューに戻ります。

6 **r** を押して、コンピュータを再起動します。

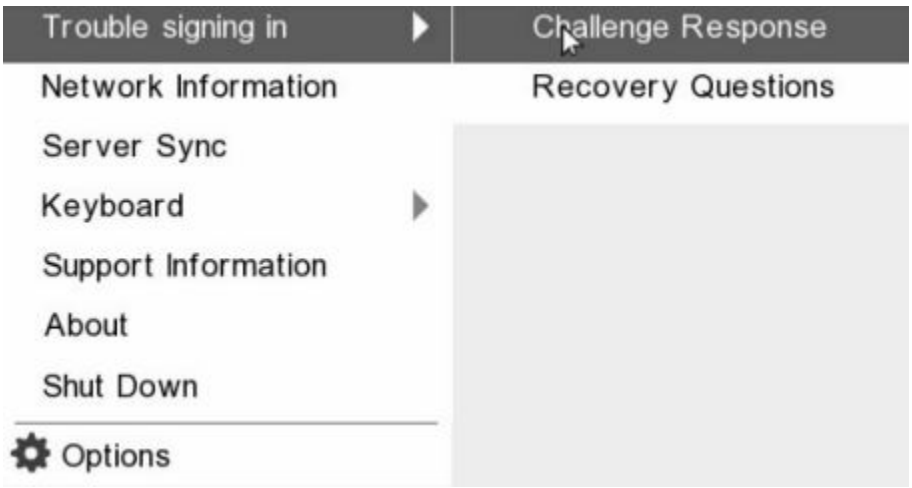
ⓘ **メモ:**
コンピュータを起動するのに使用した USB、CD / DVD メディアを必ず取り外してください。取り外すのを忘れると再度リカバリ環境で起動してしまうことがあります。

7 コンピュータの再起動後、コンピュータは完全に機能した状態になります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

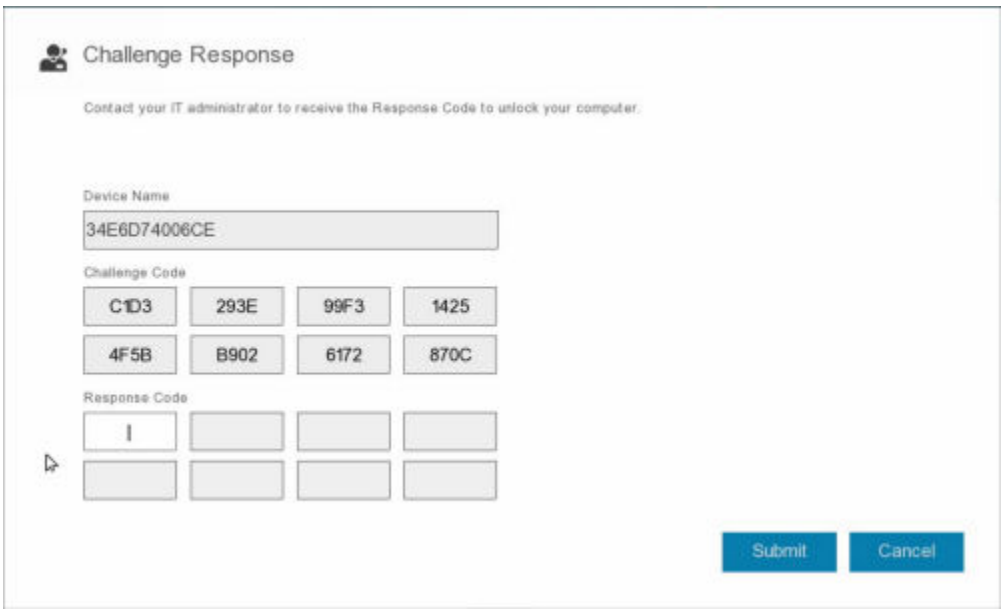
SED を使用したチャレンジリカバリ

起動前認証環境をバイパス

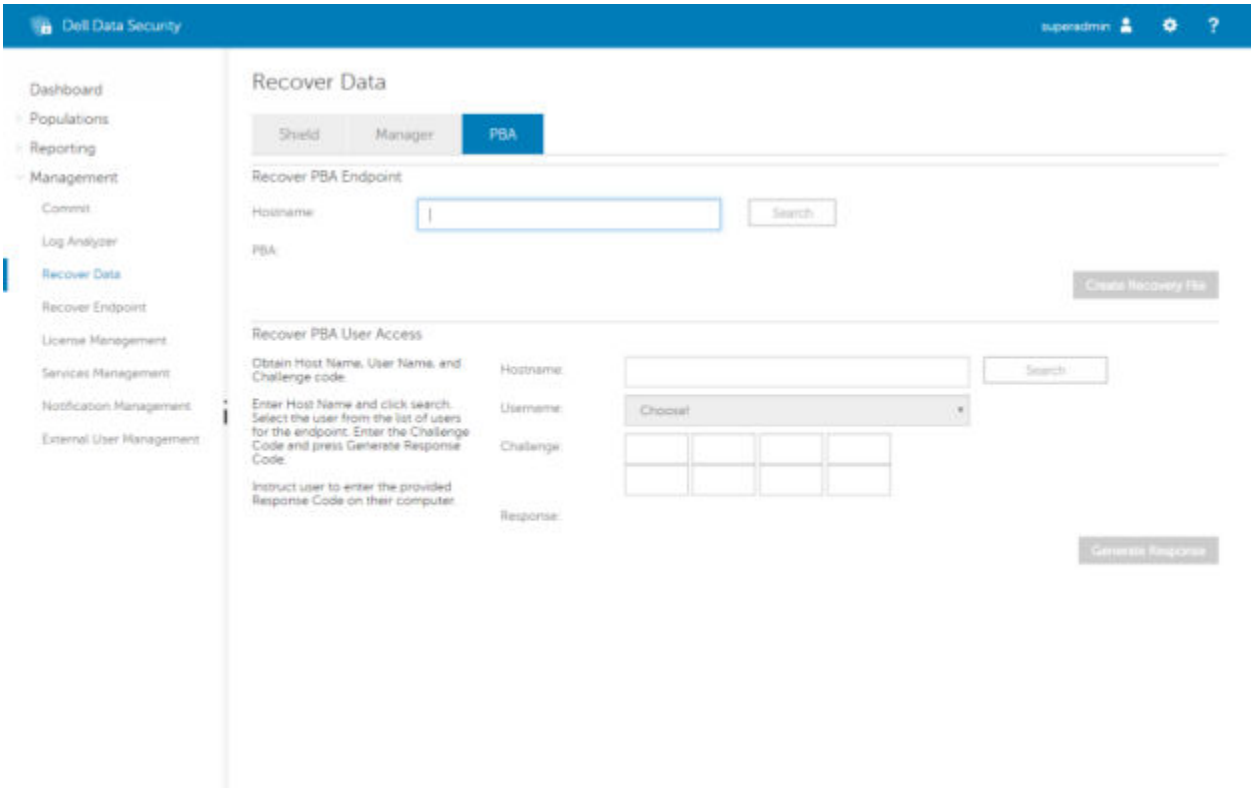
ユーザーがパスワードを忘れて、PBA 環境を通過する方法をヘルプデスクに電話で問い合わせてきました。デバイスに組み込まれているチャレンジ / 応答メカニズムを使用します。このメカニズムはユーザーごとに組み込まれており、交代式の英数字セットに基づいています。ユーザーは、**ユーザー名** フィールドに名前を入力し、**オプション > チャレンジ応答** の順に選択します。



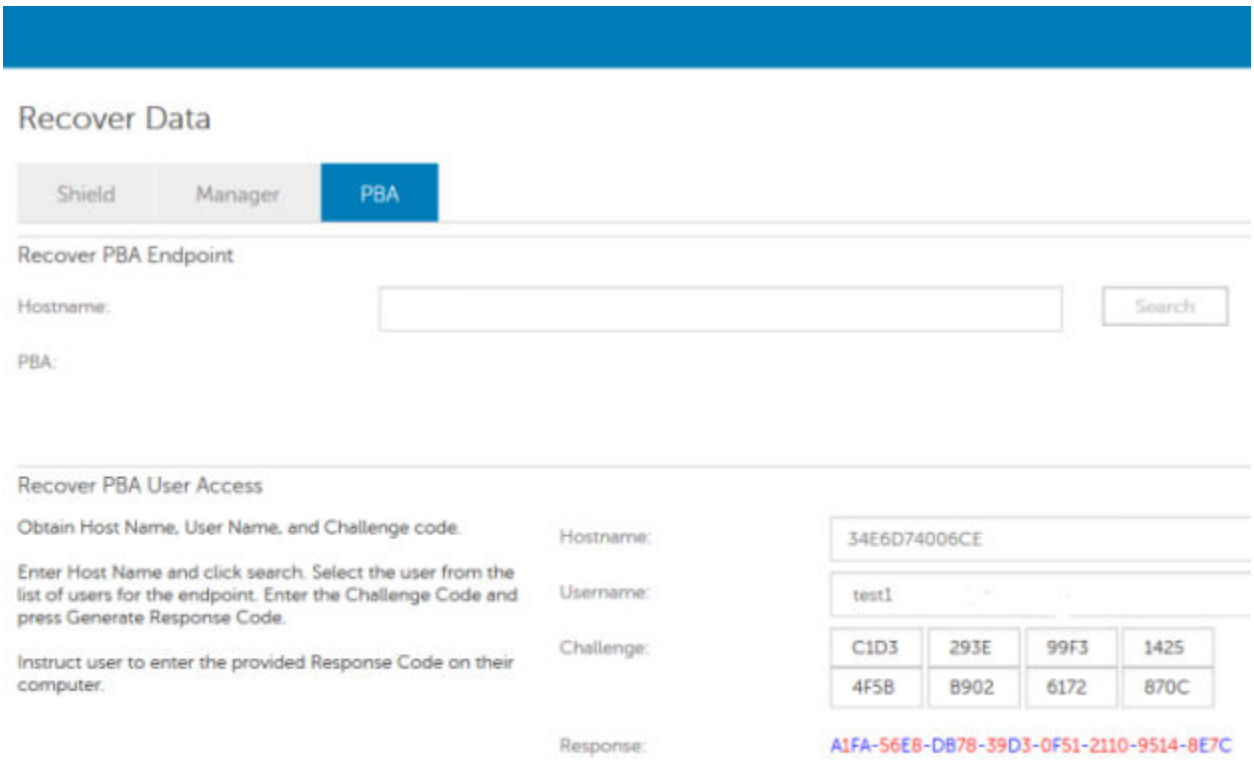
チャレンジ応答 を選択すると、次の情報が表示されます。



リモート管理コンソールの **デバイス名** フィールドは、ヘルプデスク技術者が適切なデバイスを見つけるために使用され、その後ユーザー名が選択されます。このフィールドは、**PBA** タブの **管理 > データのリカバリ** にあります。

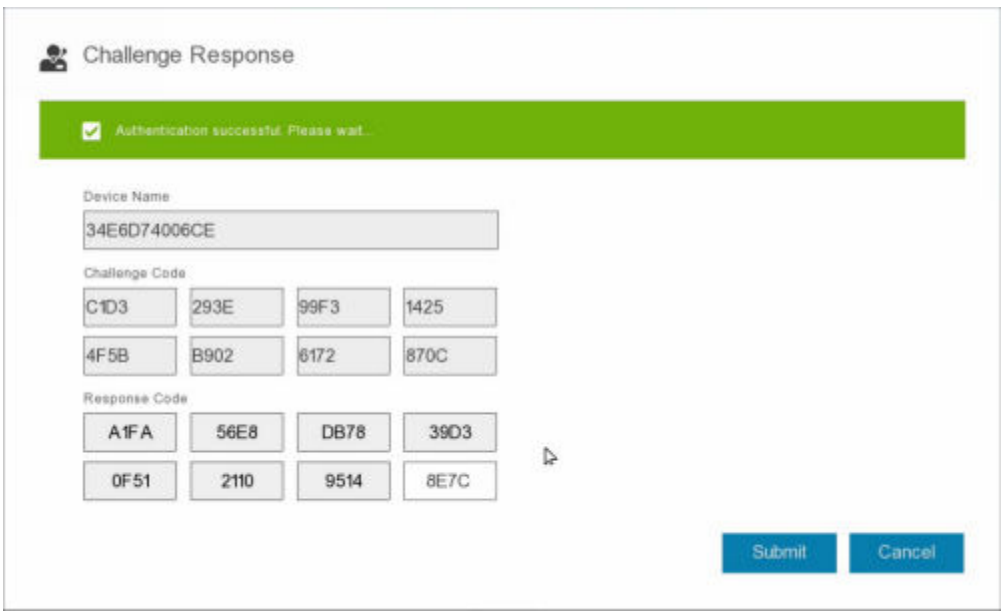


チャレンジコードはデータを入力するヘルプデスク技術者に渡されます。続いて **応答の生成** ボタンをクリックします。



この結果データは色分けされており、数字（赤）と英字（青色）を区別できるようになっています。エンドユーザーがこのデータを読み取り、PBA 環境に入力して **送信** ボタンをクリックすると、ユーザーは Windows に移動します。

認証に成功すると、次のメッセージが表示されます。



チャレンジリカバリが完了しました。

5

フルディスク暗号化リカバリ

リカバリを実行すると、フルディスク暗号化で暗号化されたドライブ上のファイルへのアクセスを回復することができます。

メモ: 復号化を中断しないでください。復号化を中断すると、データ損失が発生するおそれがあります。

リカバリ要件

フルディスク暗号化のリカバリには、以下が必要です。

- リカバリ環境 ISO へのアクセス
- 起動可能な CD / DVD または USB メディア

リカバリプロセスの概要

メモ: リカバリには 64 ビットの環境が必要です。

障害が発生したシステムを回復するには、次の手順を実行します。

1 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 A - リカバリ環境の書き込み」を参照してください。
2 リカバリファイルを入手します。
3 リカバリを実行します。

フルディスク暗号化リカバリの実行

フルディスク暗号化リカバリを実行するには、以下の手順に従います。

リカバリファイルの入手 - フルディスク暗号化クライアント

リカバリファイルを入手します。
リモート管理コンソールからリカバリファイルをダウンロードします。Dell Data Security のインストール時に生成された *<hostname>-sed-recovery.dat* ファイルをダウンロードするには、次の手順に従います。

a リモート管理コンソールを開き、左側のペインから、**管理 > データの回復** の順に選択して **PBA** タブを選択します。
b データの回復 画面のホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。
c SED フィールドでオプションを選択します。
d **リカバリファイルの作成** をクリックします。
<hostname>-sed-recovery.dat ファイルがダウンロードされます。

リカバリの実行

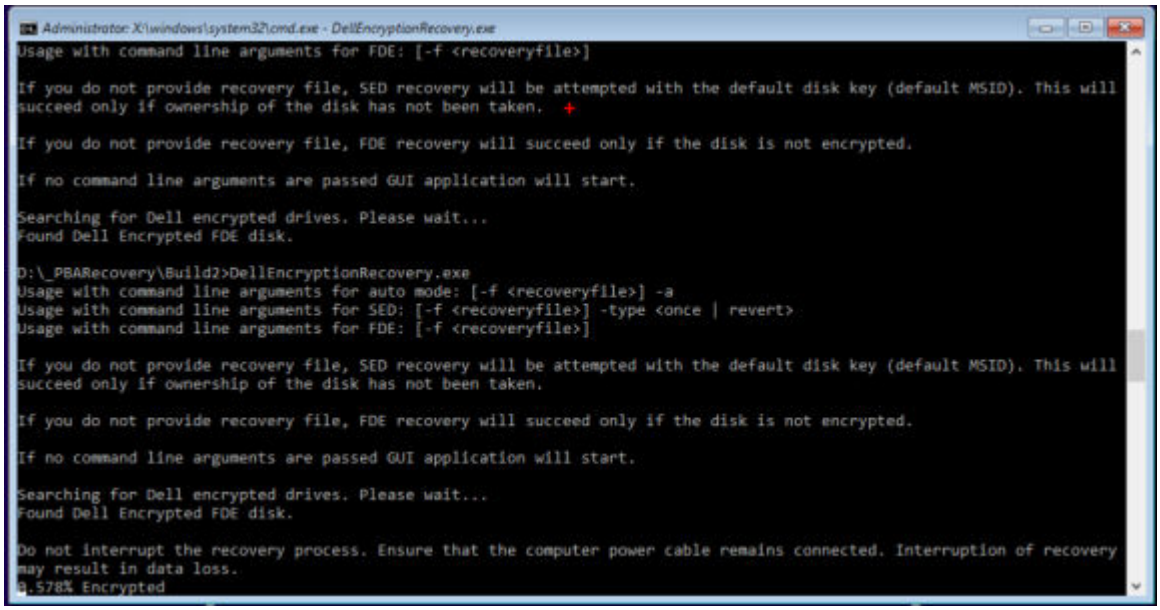
1 先ほど作成した起動可能なメディアを使用して、リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。リカバリアプリケーションと共に WinPE 環境が開きます。

メモ: リカバリプロセスの前に SecureBoot を無効にします。終了したら、SecureBoot を再度有効にします。

2 オプションを 1 つ選択して、**Enter** を押します。

3 **参照** を選択してリカバリファイルを確認し、**開く** をクリックします。

4 **OK** をクリックします。



5 これでリカバリが完了しました。任意のキーを押してメニューに戻ります。

6 **r** を押して、コンピュータを再起動します。

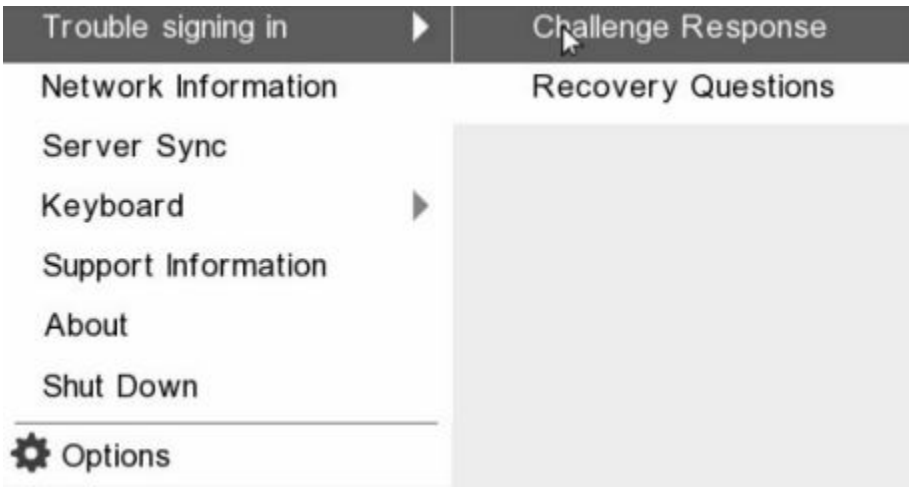
メモ:
コンピュータを起動するのに使用した USB、CD / DVD メディアを必ず取り外してください。取り外すのを忘れると再度リカバリ環境で起動してしまうことがあります。

7 コンピュータの再起動後、コンピュータは完全に機能した状態になります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

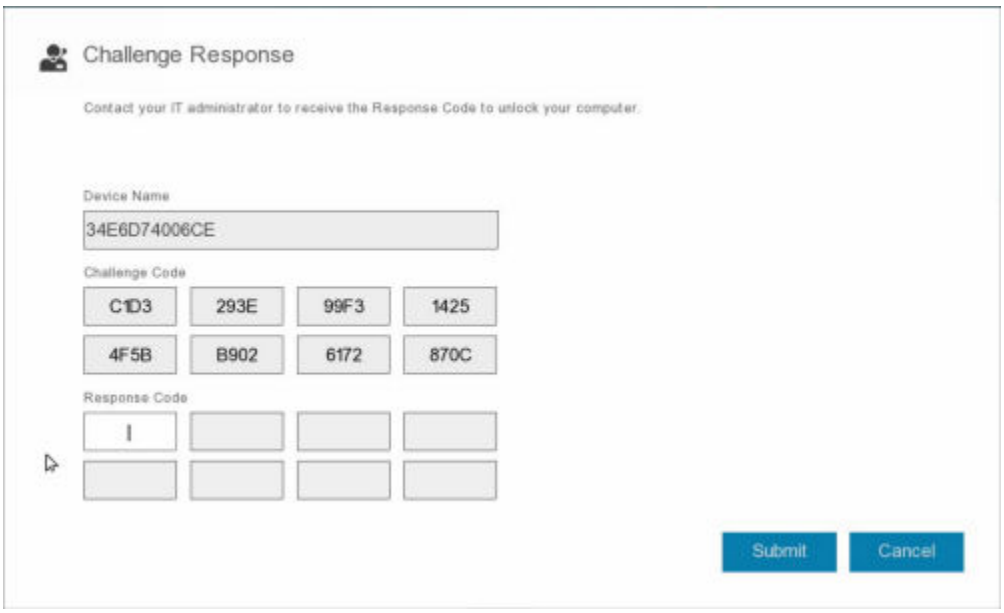
フルディスク暗号化を使用したチャレンジリカバリ

起動前認証環境をバイパス

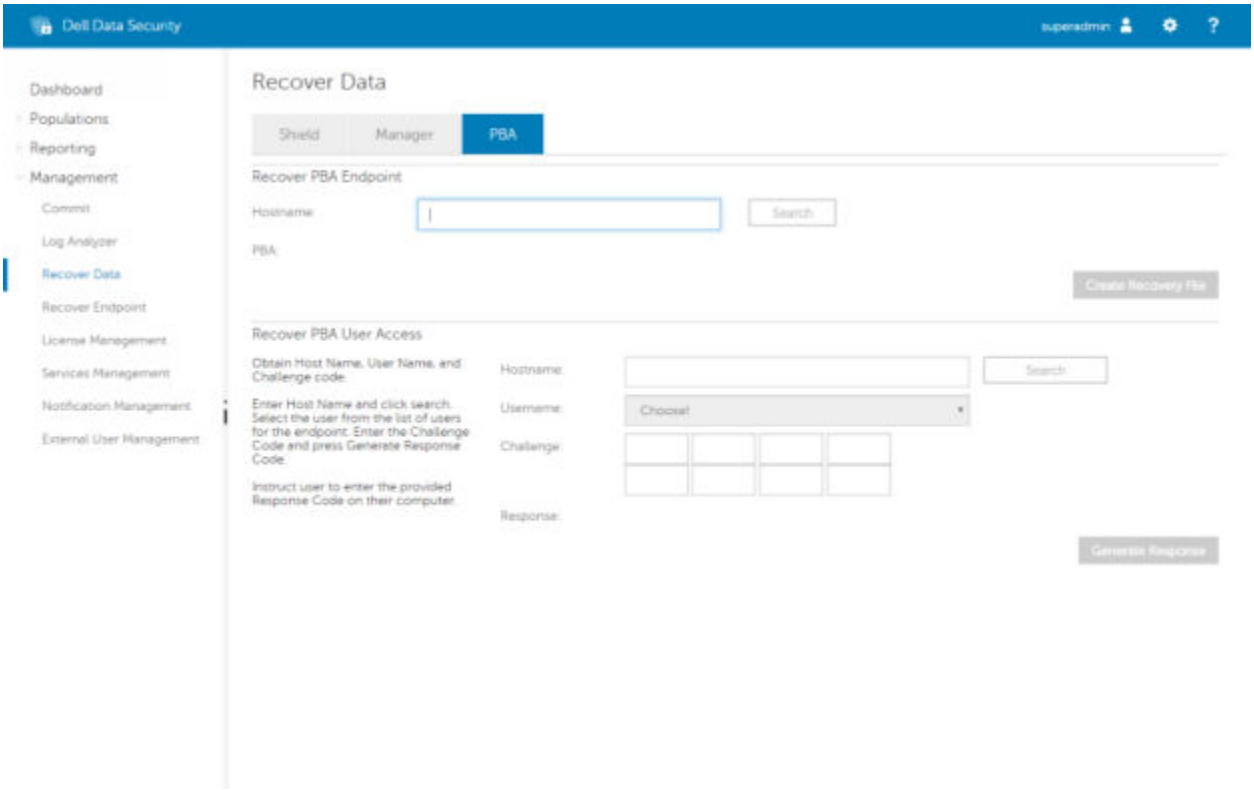
ユーザーがパスワードを忘れて、PBA 環境を通過する方法をヘルプデスクに電話で問い合わせてきました。デバイスに組み込まれているチャレンジ / 応答メカニズムを使用します。このメカニズムはユーザーごとに組み込まれており、交代式の英数字セットに基づいています。ユーザーは、**ユーザー名** フィールドに名前を入力し、**オプション > チャレンジ応答** の順に選択します。



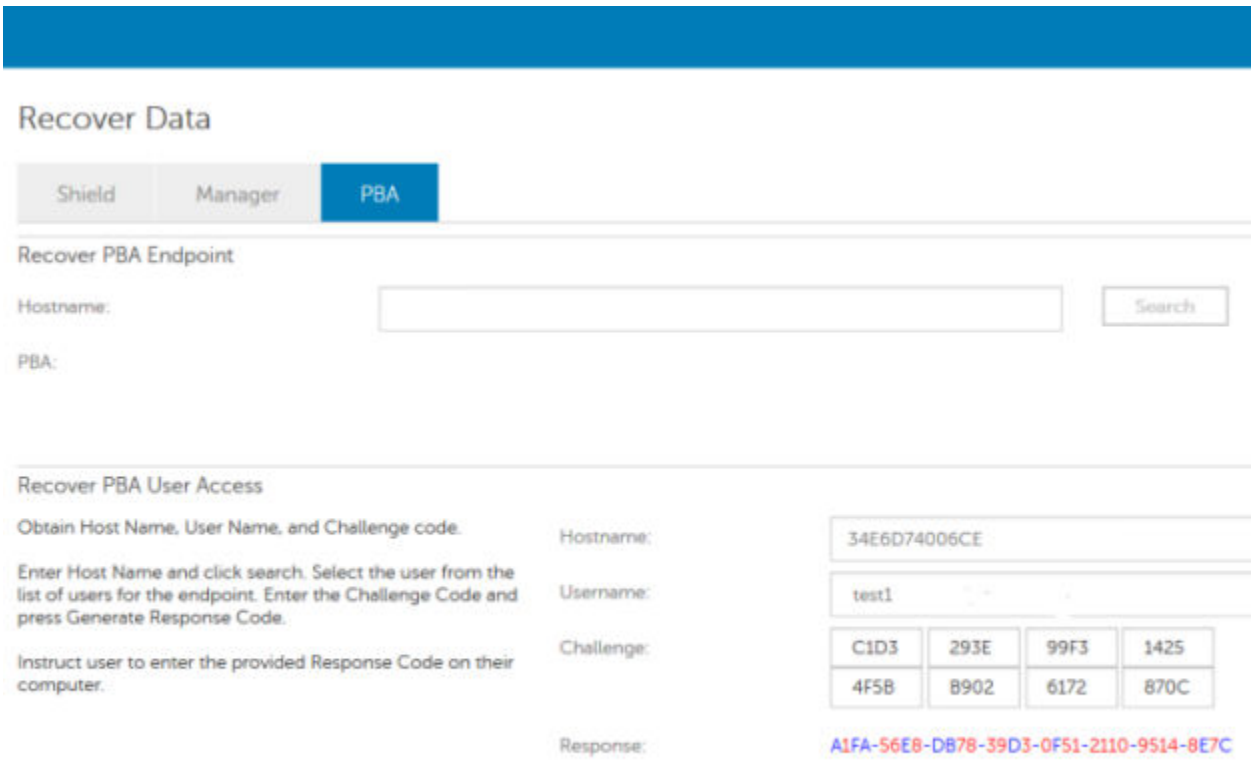
チャレンジ応答 を選択すると、次の情報が表示されます。



リモート管理コンソールの **デバイス名** フィールドは、ヘルプデスク技術者が適切なデバイスを見つけるために使用され、その後ユーザー名が選択されます。このフィールドは、**PBA** タブの **管理 > データのリカバリ** にあります。

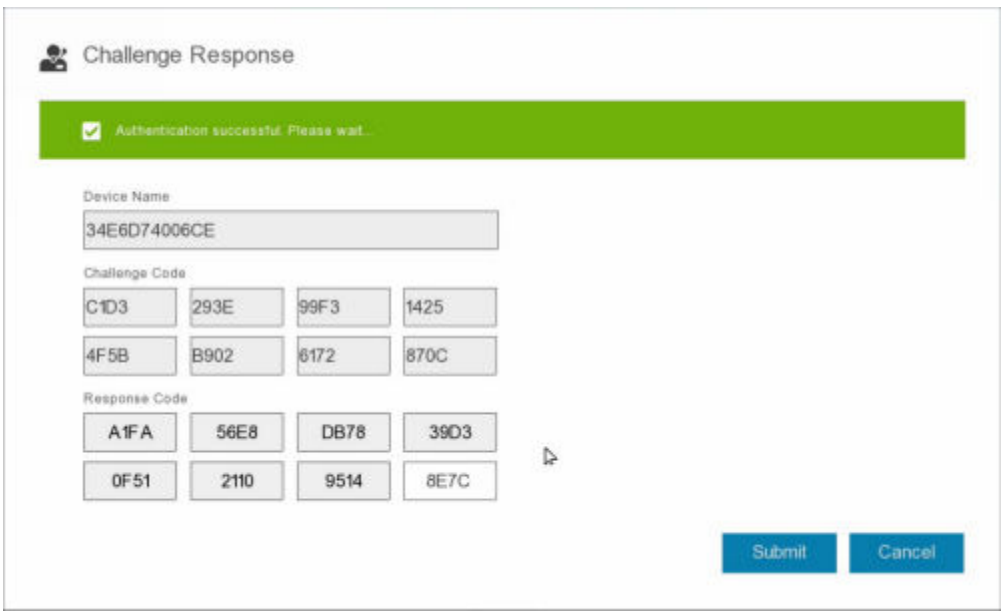


チャレンジコードはデータを入力するヘルプデスク技術者に渡されます。続いて **応答の生成** ボタンをクリックします。



この結果データは色分けされており、数字（赤）と英字（青色）を区別できるようになっています。エンドユーザーがこのデータを読み取り、PBA 環境に入力して **送信** ボタンをクリックすると、ユーザーは Windows に移動します。

認証に成功すると、次のメッセージが表示されます。



チャレンジリカバリが完了しました。

6

フルディスク暗号化と Dell Encryption のリカバリ

この章では、フルディスク暗号化で保護されたディスク上にある Dell Encryption で保護されたファイルへのアクセスをリカバリする際に必要なリカバリ手順の詳細を説明します。

メモ: 復号化を中断しないでください。復号化を中断すると、データ損失が発生するおそれがあります。

リカバリ要件

フルディスク暗号化と Dell Encryption のリカバリには、以下が必要です。

- リカバリ環境 ISO へのアクセス
- 起動可能な CD / DVD または USB メディア

リカバリプロセスの概要

メモ: リカバリには 64 ビットの環境が必要です。

障害が発生したシステムを回復するには、次の手順を実行します。

1 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 A - リカバリ環境の書き込み」を参照してください。
2 Dell Encryption およびフルディスク暗号化のためのリカバリファイルを入手します。
3 リカバリを実行します。

フルディスク暗号化および Dell Encryption により暗号化されたディスクのリカバリの実行

フルディスク暗号化および Dell Encryption により暗号化されたディスクをリカバリするには、次の手順を実行します。

リカバリファイルの入手 - フルディスク暗号化クライアント

リカバリファイルを入手します。
リモート管理コンソールからリカバリファイルをダウンロードします。Dell Data Security のインストール時に生成された *<hostname>-sed-recovery.dat* ファイルをダウンロードするには、次の手順に従います。

a リモート管理コンソールを開き、左側のペインから、**管理 > データの回復** の順に選択して **PBA** タブを選択します。
b データの回復 画面のホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。
c SED フィールドでオプションを選択します。
d **リカバリファイルの作成** をクリックします。
<hostname>-sed-recovery.dat ファイルがダウンロードされます。

リカバリファイルの入手 - ポリシーベース暗号化または FFE 暗号化クライアント

リカバリファイルをダウンロードするには、次の手順を実行します。

1 http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers から Dell Encryption インストールパッケージをダウンロードします。インストールパッケージの **AdminUtilities** フォルダに移動して、**CMGAd.exe** を開きます。

2 **デルサーバ** フィールドに、コンピュータがアクティブ化された Security Management Server / Security Management Server Virtual を入力します。

3 **デル管理者** フィールドに、フォレンジック管理者権限を持つユーザーアカウント名を入力します。

4 **パスワード** フィールドに、フォレンジック管理者のパスワードを入力します。

5 **MCID** フィールドに、リカバリするデバイスの FQDN を入力します。

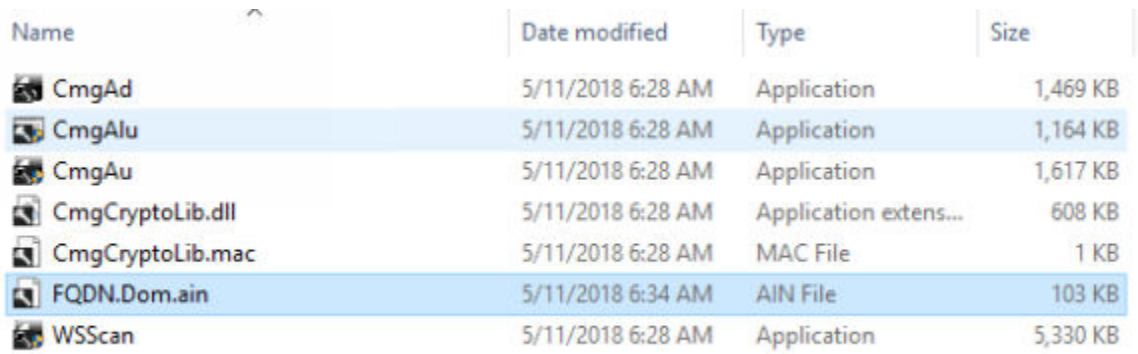
- **DCID** フィールドは、リカバリするデバイスのリカバリ ID です。

6 **次へ** を選択します。

7 リカバリファイルの **パスフレーズ** を定義して確認します。このパスフレーズはリカバリを実行する際に必要です。

8 **ダウンロード先：** フィールドにリカバリバンドルの保存先の場所を入力して、**次へ** を選択します。デフォルトでは、CMGAd.exe が実行されたディレクトリです。

9 **ダウンロード先：** で指定したフォルダに、リカバリバンドルがダウンロードされます。

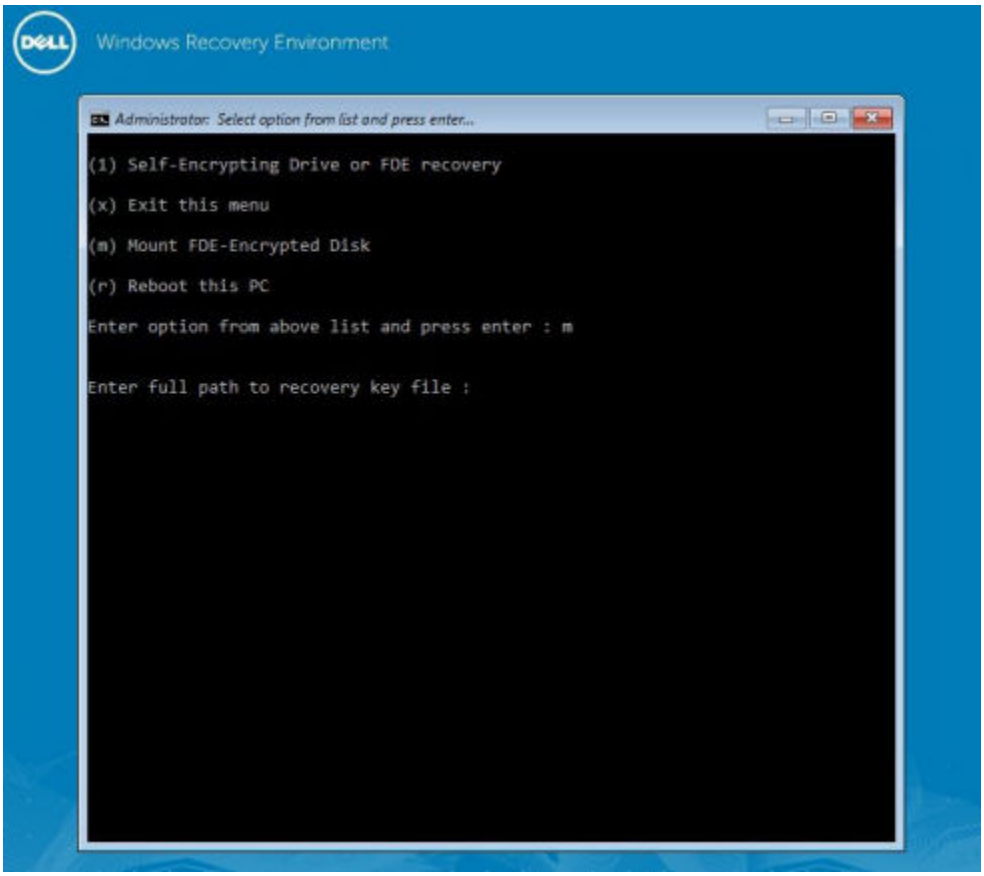


10 WinPE の起動時にアクセスできる場所に、リカバリバンドルファイルをコピーします。

リカバリの実行

1 先ほど作成した起動可能なメディアを使用して、リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。リカバリアプリケーションと共に WinPE 環境が開きます。

メモ: リカバリプロセスの前に SecureBoot を無効にします。終了したら、SecureBoot を再度有効にします。



2 3 番目のオプションを選択して、**Enter** を押します。

3 プロンプトが表示されたら、リカバリファイルの名前と場所を入力します。

4 リカバリキーを使用して、フルディスク暗号化ディスクがマウントされます。

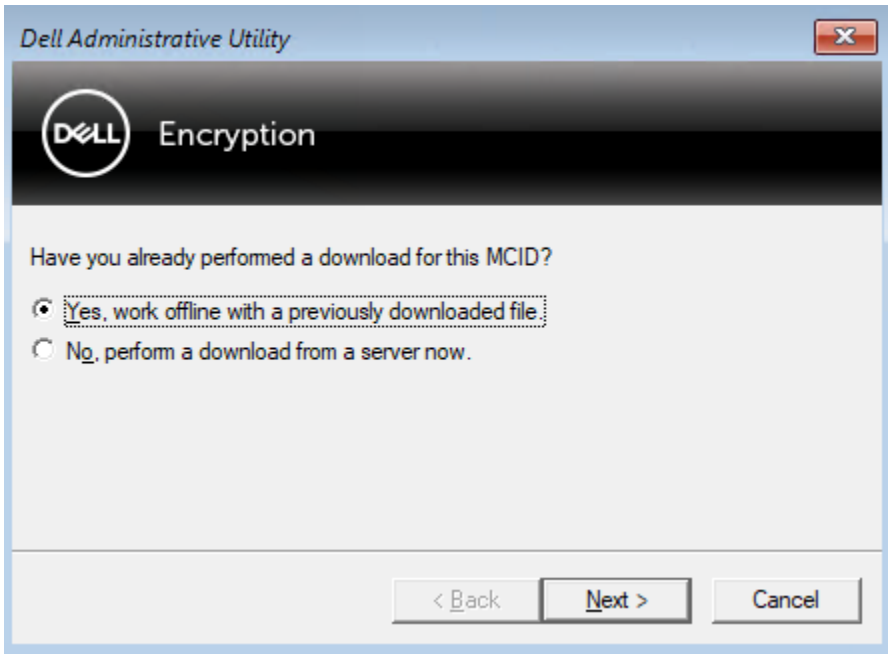
```
Enter option from above list and press enter : m


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 次のコマンドにより、CMGAu.exe ユーティリティに移動します。`cd DDPEAdminUtilities\`

6 次のコマンドにより、CMGAu.exe を起動します。`\DDPEAdminUtilities>CmgAu.exe`
はい、以前にダウンロードしたファイルを使ってオフラインで作業をします。 を選択します。



7 **ダウンロードしたファイル：** フィールドに**リカバリバンドル**の場所を入力し、続けてフォレンジック管理者のパスフレーズを **パスフレーズ** に入力して、**次へ** を選択します。

リカバリが完了したら、**終了** をクリックします。

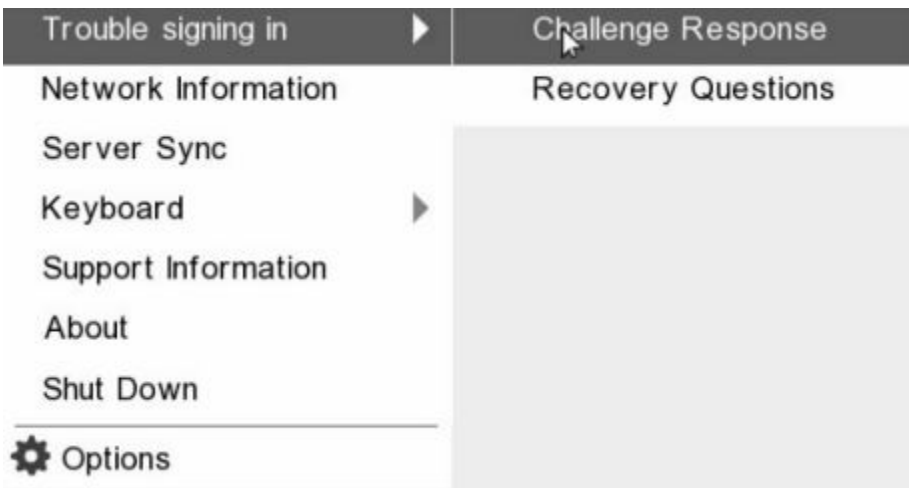
メモ:
コンピュータを起動するのに使用した USB、CD / DVD メディアを必ず取り外してください。取り外すのを忘れると再度リカバリ環境で起動してしまうことがあります。

8 コンピュータを再起動すると、暗号化ファイルにアクセスできるようになります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

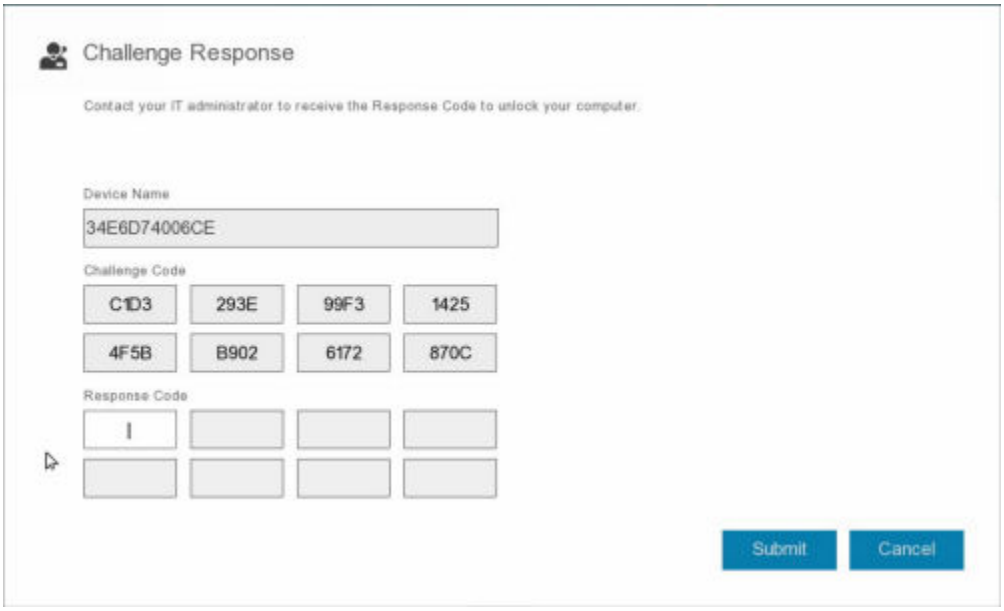
フルディスク暗号化を使用したチャレンジリカバリ

起動前認証環境をバイパス

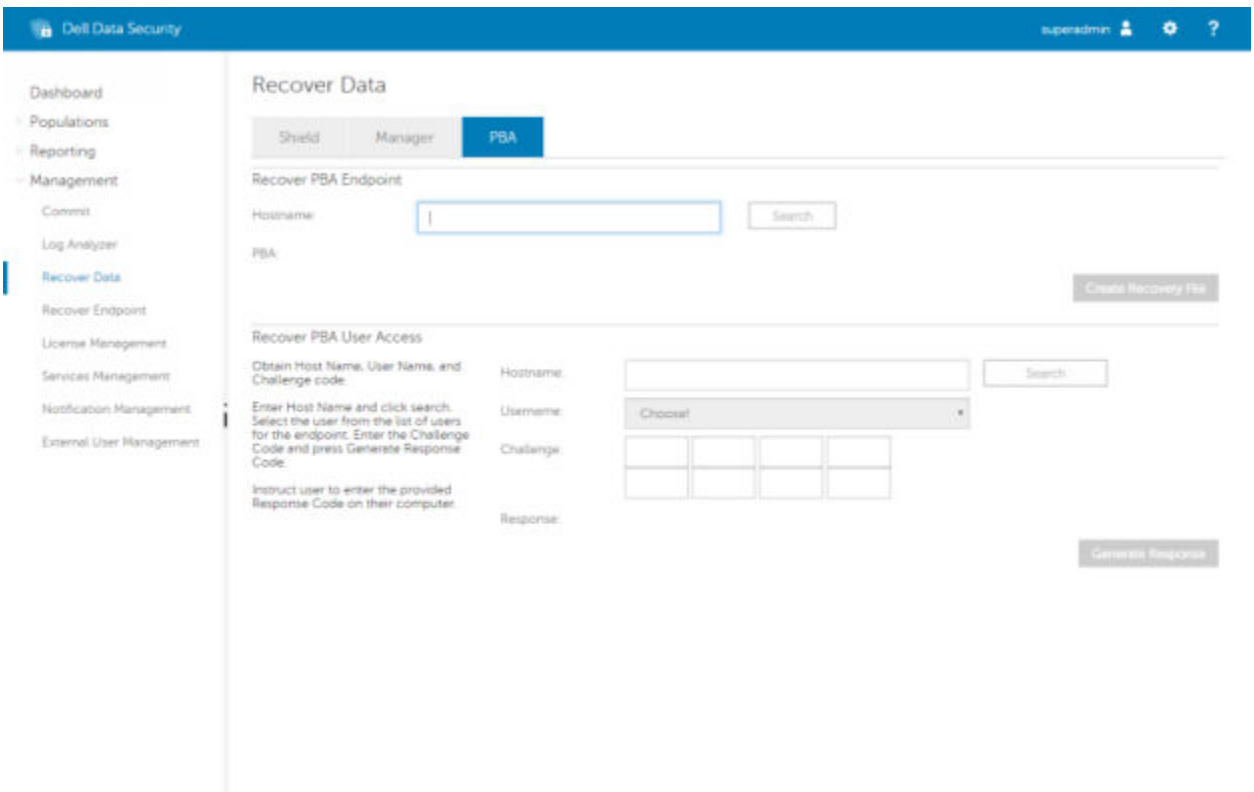
ユーザーがパスワードを忘れて、PBA 環境を通過する方法をヘルプデスクに電話で問い合わせてきました。デバイスに組み込まれているチャレンジ / 応答メカニズムを使用します。このメカニズムはユーザーごとに組み込まれており、交代式の英数字セットに基づいています。ユーザーは、**ユーザー名** フィールドに名前を入力し、**オプション > チャレンジ応答** の順に選択します。



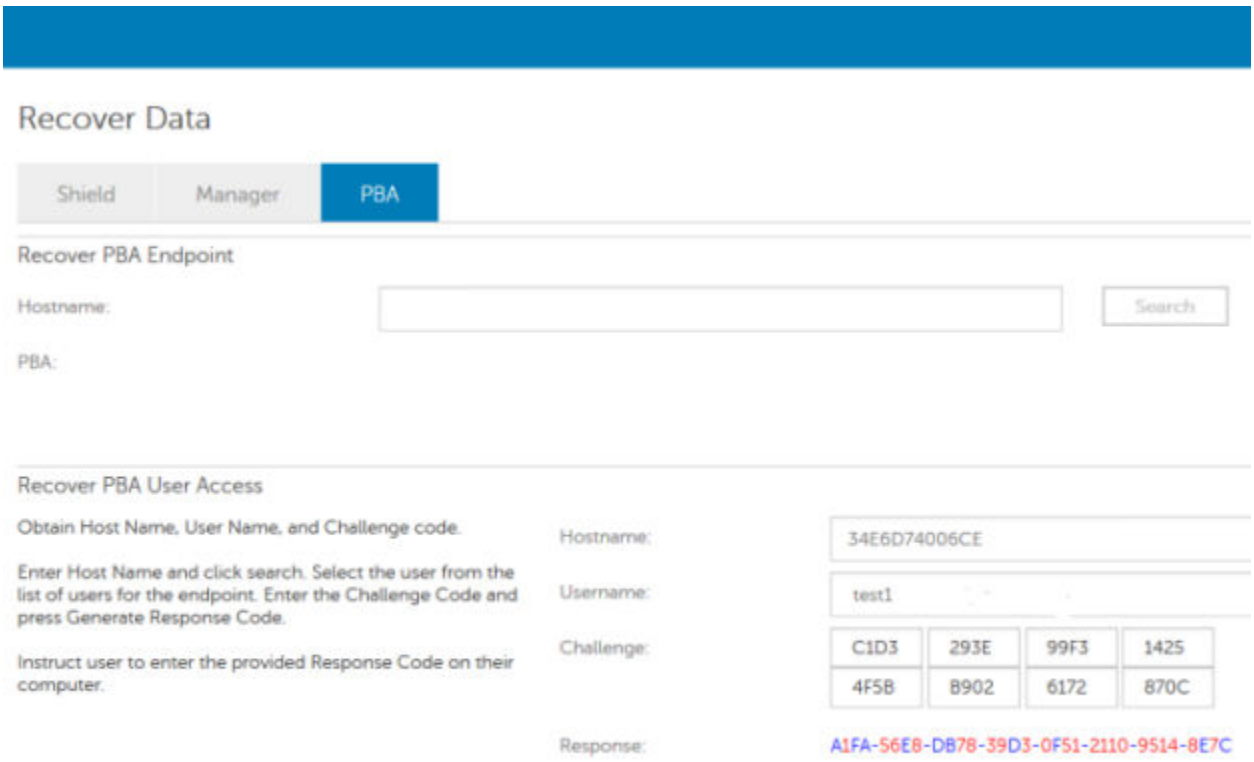
チャレンジ応答 を選択すると、次の情報が表示されます。



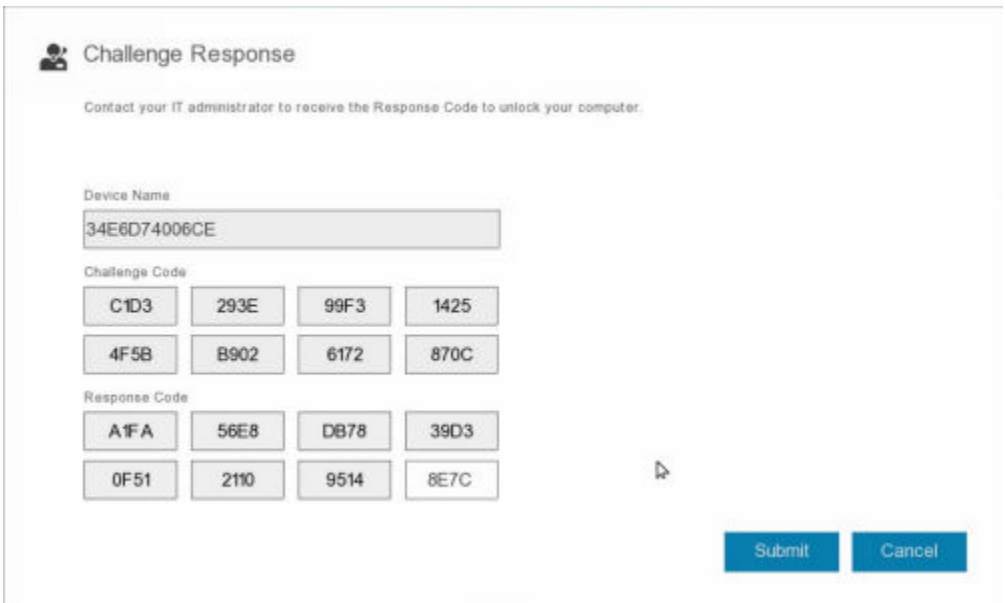
リモート管理コンソールの **デバイス名** フィールドは、ヘルプデスク技術者が適切なデバイスを見つけるために使用され、その後ユーザー名が選択されます。このフィールドは、**PBA** タブの **管理 > データのリカバリ** にあります。



チャレンジコードはデータを入力するヘルプデスク技術者に渡されます。続いて **応答の生成** ボタンをクリックします。



この結果データは色分けされており、数字（赤）と英字（青色）を区別できるようになっています。エンドユーザーがこのデータを読み取り、PBA 環境に入力して **送信** ボタンをクリックすると、ユーザーは Windows に移動します。



認証に成功すると、次のメッセージが表示されます。

チャレンジリカバリが完了しました。

7

PBA デバイスコントロール

PBA デバイスコントロールは SED またはフルディスク暗号化で暗号化されたエンドポイントに適用されます。

PBA デバイスコントロールの使用

各エンドポイントに対する PBA コマンドは、PBA デバイスコントロールエリアで実行します。各コマンドには、優先度ランランキングがあります。実施キューにおいて、優先度が高いランクのコマンドが優先度の低いコマンドをキャンセルします。コマンドの優先度ランキングのリストについては、リモート管理コンソールで ? をクリックすると表示される *AdminHelp* を参照してください。PBA デバイスコントロールは、リモート管理コンソールの [エンドポイントの詳細] ページで使用できます。

次のコマンドは、PBA デバイスコントロールで使用できます。

- **ロック** - PBA 画面をロックして、コンピュータへのユーザーのログインを防止します。
- **ロック解除** - ロックコマンドを送信するか、ポリシーで許可された最大認証試行回数を超過すると、このエンドポイントにロックされた PBA 画面のロックが解除されます。
- **ユーザーを削除** - PBA からすべてのユーザーを削除します。
- **ログインのバイパス** - PBA 画面を 1 回バイパスして、認証を実行しなくても、ユーザーがコンピューターにログインすることを許可します。PBA がバイパスされても、ユーザーは引き続き Windows にログインする必要があります。
- **ワイプ** - ワイプコマンドを暗号化済みドライブに対して実行すると、「工場出荷時の状態に復元」されます。ワイプコマンドを使用すると、コンピュータを別の目的で使用したり、緊急時にコンピュータを消去して、データを永続的に復元不能にすることができます。このコマンドを起動する前に、その実行が必要であることを確認してください。フルディスク暗号化の場合、ワイプコマンドはドライブの暗号的消去を実行し、PBA が削除されます。SED の場合、ワイプコマンドはドライブの暗号的消去を実行し、PBA に「デバイスがロックされています」と表示されます。SED を別の目的で使用するには、SED リカバリアプリを使用して PBA を削除します。

8

General Purpose Key のリカバリ

General Purpose Key (GPK) は、ドメインユーザーのレジストリの一部を暗号化するために使用されます。ただし、起動プロセス中、まれに、破損され復号化に失敗することがあります。その場合、クライアントコンピュータの CMGShield.log ファイルに以下のエラーが表示されます。

```
[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
```

GPK が復号化に失敗した場合、Dell Server からダウンロードされたリカバリバンドルから GPK を解凍することで回復する必要があります。

GPK の回復

リカバリファイルの入手

Dell Data Security のインストール時に生成された **<machinename_domain.com>.exe** ファイルをダウンロードするには、以下の手順に従います。

1 リモート管理コンソールを開き、左ペインから **管理** > **エンドポイントの回復** を選択します。

2 ホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。

3 リカバリウィンドウでリカバリパスワードを入力し、**ダウンロード** をクリックします

> **メモ:**
> このパスワードは、リカバリキーへのアクセスのために覚えておかなければなりません。

<machinename_domain.com>.exe ファイルがダウンロードされます。

リカバリの実行

1 リカバリ環境の起動可能なメディアを作成します。手順については、「付録 A - リカバリ環境の書き込み」を参照してください。

> **メモ: リカバリプロセスの前に SecureBoot を無効にします。終了したら、SecureBoot を有効にします。**

2 リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。
WinPE 環境が開きます。

3 **x** を入力して **Enter** を押し、コマンドプロンプトを表示します。

4 リカバリファイルに移動して起動します。
Encryption クライアント診断ダイアログが開き、リカバリファイルはバックグラウンドで生成されています。

5 管理者のコマンドプロンプトで、**<machinename_domain.com>** > **.exe** > **-p <password>** > **-gpk** を実行します。
GPKRCVR.txt をコンピュータに返します。

6 **GPKRCVR.txt** ファイルをコンピュータの OS ドライブのルートにコピーします。

7 コンピュータを再起動します。
GPKRCVR.txt ファイルはオペレーティングシステムに消費され、コンピュータに GPK が再生成されます。
8 プロンプトで指示された場合、再起動します。

9

BitLocker Manager リカバリ

データを回復するには、リモート管理コンソールからリカバリパスワードまたはキーパッケージを取得します。これにより、コンピュータのデータのロックを解除できるようになります。

データの回復

1 リモート管理コンソールに Dell 管理者としてログインします。
2 左のペインで、**管理**、**データの回復** の順にクリックします。
3 **管理者** タブをクリックします。
4 *BitLocker* の場合：
BitLocker から受け取った**リカバリ ID** を入力します。オプションとしてホスト名とボリュームを入力すると、リカバリ ID が自動入力されます。

リカバリパスワードの取得 または **キーパッケージの作成** をクリックします。

希望するリカバリ方法に応じて、データの回復にこのリカバリパスワードまたはキーパッケージを使用します。

TPM の場合：

ホスト名を入力します。

リカバリパスワードの取得 または **キーパッケージの作成** をクリックします。

希望するリカバリ方法に応じて、データの回復にこのリカバリパスワードまたはキーパッケージを使用します。
5 リカバリを完了するには、Microsoft によるリカバリ手順を参照してください。

メモ:
BitLocker Manager が TPM を「所有」していない場合、TPM パスワードおよびキーパッケージをデルデータベースで使用することはできません。その場合は、キーが見つからないというエラーメッセージが表示されます。この動作は予期されたものです。

BitLocker Manager 以外のエンティティによって「所有」されている TPM を回復するには、その特定の所有者から TPM を回復するプロセスに従うか、TPM リカバリのための既存プロセスに従う必要があります。

10

パスワードリカバリ

ユーザーは自分のパスワードをよく忘れます。その場合、幸いにも、プリブート認証によりコンピュータへのアクセス権を取り戻す方法がいくつかあります。

- リカバリ質問機能は、質問と回答によって認証する機能です。
- チャレンジ / 応答コードにより、管理者の手を借りてコンピュータへのアクセス権を取り戻すことができます。この機能は、組織によって管理されているコンピュータを持つユーザーのみが使用できます。

リカバリ質問

ユーザーが初めてコンピュータにサインインすると、管理者が設定した標準質問セットに回答するように求められます。これらの質問への回答を登録すると、次回パスワードを忘れたとき、ユーザーはその回答を要求されます。質問に正しく回答すると、サインインできるようになり Windows へのアクセス権を取り戻すことができます。

前提条件

- リカバリ質問は、管理者によってセットアップされている必要があります。
- ユーザーは、質問への回答を登録しておく必要があります。
- **サインインできない場合** メニューオプションをクリックする前に、ユーザーは有効なユーザー名とドメインを入力しておく必要があります。

PBA サインイン画面からリカバリ質問にアクセスするには、次の手順に従います。

1 有効なドメイン名およびユーザー名を入力します。
2 画面の左下隅で **オプション**、**サインインできない場合** の順にクリックします。
3 Q&A ダイアログが表示されたら、初回サインイン時にリカバリ質問に登録したときに提供した回答を入力します。

11

Encryption External Media パスワードリカバリ

Encryption External Media を使用すると、ユーザーにユニバーサルシリアルバス (USB) フラッシュドライブや他のリムーバブルストレージメディアの暗号化を許可すると、組織内部と外部の両方のリムーバブルストレージメディアを保護することができます。ユーザーは、保護する各リムーバブルメディアデバイスにパスワードを割り当てます。このセクションでは、ユーザーがデバイスのパスワードを忘れたときに、暗号化された USB ストレージデバイスへのアクセスを復元するプロセスについて説明します。

データへのアクセスの回復

ユーザーがパスワードの試行許可回数を超えて自分のパスワードが何回も間違って入力すると、USB デバイスは手動認証モードになります。

手動認証 は、Dell Server にログインしている管理者に、クライアントからコードを提供するプロセスです。

手動認証モードでは、ユーザーがパスワードをリセットして自分のデータへのアクセス権を取り戻すための 2 つのオプションがあります。

管理者がアクセスコードをクライアントに提供し、ユーザーが自分のパスワードをリセットして自分の暗号化データへのアクセスを取り戻すことを許可します。

1 パスワードの入力を求められたら、**忘れた場合** ボタンをクリックします。

確認のダイアログが表示されます。

2 **はい** をクリックして確定します。確定後に、デバイスは手動認証モードになります。
3 ヘルプデスク管理者に連絡し、ダイアログに表示されるコードを伝えます。
4 ヘルプデスク管理者として、リモート管理コンソールへログインします。ヘルプデスク管理者のアカウントにはヘルプデスク権限がついていることが必要です。
5 左ペインの **データの回復** メニューオプションに進みます。
6 エンドユーザーから提供されたコードを入力します。
7 画面の右下隅にある **応答を生成** ボタンをクリックします。
8 ユーザーにアクセスコードを与えます。

> **メモ:**
> アクセスコードを提供する前に手動でユーザーを認証するようにします。たとえば、ユーザーに対して「従業員 ID 番号を教えてください」など、本人しかわからない質問をいくつかします。またはユーザーをヘルプデスクに来て ID を見せるように要請し、メディアのオーナーであることを確認します。電話でのユーザー認証に失敗したにもかかわらず、アクセスコードを提供すると、暗号化されたリムーバブルメディアへのアクセス権を攻撃者に与えてしまう可能性があります。

9 暗号化されたメディアのパスワードをリセットします。

暗号化されたメディアのパスワードをリセットするように求められます。

自己復元

自己復元を機能させるには、最初にドライブを暗号化したマシンに、ドライブを元通りに挿入する必要があります。メディアの所有者が、保護された Mac または PC に認証されている限り、クライアントはキーマテリアルの消失を検知し、ユーザーにデバイスを再初期化するよう求めます。その時点で、ユーザー

はパスワードをリセットし、暗号化されたデータへのアクセスを取り戻すことができます。部分的に破損しているメディアの問題が、このプロセスによって解決できる場合があります。

1 メディアの所有者として Dell Data Security の暗号化されたワークステーションにサインインします。
2 暗号化されたリムーバブルストレージデバイスを挿入します。
3 プロンプトが表示されたら、新しいパスワードを入力し、リムーバブルストレージデバイスを再初期化します。
成功した場合、パスワードが受け入れられたことを示す小さな通知が表示されます。
4 ストレージデバイスに移動し、データにアクセスできるかを確認します。

12

Dell Data Guardian のリカバリ

リカバリツールでは、以下を実施できます。

- 復号化：
  - サポートされるあらゆる形式の保護対象 Office ファイル - Data Guardian の保護対象 Office ドキュメント暗号化とそのクラウドサービスプロバイダ保護の両方で保護されているファイルをリカバリ可能。
  - 基本ファイル保護ポリシー（有効な場合）に記載されているファイル形式。
- キーマテリアルの手動エスクロー
- 改ざんされたファイルをチェックする機能
- 保護された Office ドキュメント（たとえばクラウドまたは Data Guardian のないデバイス上で、保護されている Office ファイルのカバーページ）のラッパーが改ざんされた場合に、そのファイルを強制的に復号化する機能

メモ:
Windows リカバリツールは、Mac、モバイル、Web ポータルのプラットフォームで作成されたファイルに使用することができます。

前提条件

前提条件は次のとおりです

- リカバリするエンドポイントで Microsoft .Net Framework 4.5.2 が実行されていること。
- 管理コンソールにおいて、リカバリを実行する管理者に、フォレンジック管理者役割が与えられていること。

Data Guardian のリカバリの実行

Data Guardian の保護された Office ドキュメントのリカバリを実行するには、次の手順を実行します。一度にリカバリできるコンピュータは 1 台だけです。

重要:
ファイルが破損した場合にその内容が失われないようにするため、元のファイルではなくコピーを復号化してください。

Windows、USB フラッシュドライブ、またはネットワークドライブからリカバリを実行

リカバリを実行するには、次の手順に従います。

1 デルのインストールメディアから、**RecoveryTools.exe** を、次のいずれかにコピーします。

- コンピュータ - Office ドキュメントをリカバリするコンピュータに.exe をコピーします。
- USB - USB フラッシュドライブに.exe をコピーし、USB フラッシュドライブから.exe を実行します。
- ネットワークドライブ

重要:
管理者はインストーラではなく、**RecoveryTools.exe** のみをコピーしてください。**RecoveryTools.exe** は、スイープまたは復号化が実行中でない場合、より適切に処理します。

2 **RecoveryTools.exe** をダブルクリックしてリカバリツールを起動します。

3 Data Guardian リカバリツールウィンドウで、**ドメインログイン** を選択します。

メモ:
ホストされているソリューションの SaaS ログインオプションは、将来のリリース用です。

4 このフォーマットに、Dell Server FQDN を入力します。
server.domain.com

メモ:
プレフィックスとサフィックスは自動的に FQDN に追加されます。

5 ユーザー名とパスワードを入力して **ログイン** をクリックします。

メモ:
管理者に指示されない限り、*SSL* トラストを有効にする チェックボックスをクリアしないでください。

メモ:
フォレンジック管理者でない者が資格情報を入力すると、ログイン権限を持っていないことを示すメッセージが表示されます。

6 フォレンジック管理者である場合は、リカバリツールが開きます。

7 **ソース** を選択します。

メモ:
ソースおよび宛先に移動する必要がありますが、どちらを先に選択してもかまいません。

8 **参照** をクリックして、リカバリするフォルダまたはドライブを選択します。

9 **OK** をクリックします。

10 **宛先** をクリックします (復号化またはリカバリしたファイル用の空のフォルダ)。

11 **参照** をクリックして、外付けデバイス、ディレクトリの場所、デスクトップなど、宛先を選択します。

12 **OK** をクリックします。

13 リカバリする内容に基づいて、1 つ以上のチェックボックスを選択します。

オプション	説明
エスクロー	• Dell サーバにエスクローできなかったオフライン生成キーをリカバリします。 • ネットワークに接続されていないときにハードドライブが故障した場合は、スレーブドライブを使用して、データおよび非エスクローキーをコンピュータからリカバリしてください。
復合化	リカバリツールを保護された Office ドキュメントを含むディレクトリに向け、復号化します。 **メモ:** ファイルが破損するおそれがあるため、復号化はファイルのオリジナルではなくコピーを使用して実行することをお勧めします。 改ざんが発生した場合は、オプションとして、次のいずれか、または両方のオプションを選択します (詳細は下記参照)。 • **改ざんチェック** - 改ざんファイルがあるかどうかを確認しますが復号化しません。 • **改ざんチェック** および **改ざんされていても強制的に復号化する** - 改ざんファイルがあるかどうかを確認し、保護された Office ドキュメントのラッ

オプション	説明
	パーが改ざんされている場合、Data Guardian はラッパーを修復し Office ドキュメントを復号化します。
改ざんチェック	改ざんされたファイルを検知して、ログに記録するか管理者に通知します。ファイルを改ざんした作成者をログに記録します。ファイルは復号化されません。
改ざんされていても強制的に復号化する	このオプションを選択するには、**改ざんチェック** も選択する必要があります。 クラウドまたは Data Guardian のないデバイス上で、未承認者が保護された Office ドキュメント（カバーページなど）を改ざんした場合は、このオプションを選択してラッパーを修復し、保護された Office ファイルを強制的に復号化します。 **メモ:** メモ：ラッパー内の暗号化された Office .xen ファイルが改ざんされた場合、そのファイルはリカバリできません。

保護されている各 Office ドキュメントには、オリジナルのユーザーとコンピュータ名、およびファイルを変更した他のコンピュータ名の履歴を含む隠し情報があります。デフォルトでは、リカバリツールは、非表示のウォーターマークをチェックし、すべての作成者の一覧が含まれたテキストファイルが、ログ内の *HiddenWatermark* フォルダに追加されます。

14 選択を完了したら、**スキャン** をクリックします。

ログ領域には以下が表示されます。

- 選択したソース内で見つかり、スキャンされたフォルダ
- ファイルごとに復号化が成功したか失敗したかどうか
- ファイルの最終作成者の名前

リカバリツールにより、リカバリされたファイルが選択した宛先に追加されます。ファイルを開いて表示することができます。

非表示の監査記録のデータを表示します。

Windows では、保護対象 Office 文書の 非表示監査記録ポリシーが有効になっている場合、ユーザー情報はファイルメタデータにキャプチャされます。このデータを表示するには、次のようにリカバリツールを使用します。

1 リカバリツールを起動します。
   - **ソース** の場合は、非表示監査データのある保護対象 Office 文書のあるフォルダを参照します。リカバリツールがフォルダおよびサブフォルダ構造をコピーして、非表示監査データのある保護対象の任意の Office 文書を復号化します。
   - **宛先** を参照する前に、復号化ファイルのフォルダを作成し、参照することができます。
2 **復号化** を選択します。
3 選択を完了したら、**スキャン** をクリックします。
   宛先として選択したフォルダには、次のファイルが入った日付つきの リカバリ済みファイル フォルダがあります。
   - 復号化された保護対象 Office ファイル
   - リカバリツールによって作成された 監査記録 フォルダ（復号化された各ファイルの .txt ファイルが入っている）。各 .txt ファイルには、作成者、最終更新者、タイムスタンプなど、復号化されたファイルの情報を表示するログが含まれます。

付録 A - リカバリ環境の書き込み

マスターインストーラをダウンロードできます。

リカバリ環境 ISO の CD または DVD への書き込み

次のリンクには、Microsoft Window 7、Windows 8、または Windows 10 でリカバリ環境のための起動可能 CD または DVD を作成するのに必要なプロセスが記載されています。

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

リムーバブルメディアへのリカバリ環境の書き込み

起動可能 USB を作成するには、次の手順にしたがってください。

レガシー起動：

1 USB ドライブをシステムに接続します。
2 管理者のコマンドプロンプトを開きます。
3 **Diskpart** と入力して Diskpart ユーティリティを起動します。
4 **list disk** と入力して、変更するターゲットディスクを検索します。ディスクは番号で指定します。
5 コマンド **select disk #** を使用して適切なディスクを選択します。# は、前の手順で示された対応するドライブのディスク番号です。
6 **clean** コマンドでディスクを消去します。この結果、ファイルテーブルが消去されるため、データのドライブはパージされます。
7 起動イメージを格納するパーティションを作成します。
   a **create partition primary** コマンドは、ドライブ上にプライマリパーティションを生成します。
   b **select partition 1** コマンドは新しいパーティションを選択します。
   c NTFS ファイルシステムを使用してドライブをクイックフォーマットするには、次のコマンドを使用します：**format FS=NTFS quick**。
8 ドライブは起動可能ドライブとしてマークされている必要があります。**active** コマンドを使用して、ドライブを起動可能としてマークします。
9 ファイルをドライブに直接移動するには、**assign** コマンドを使用してドライブに使用可能な文字を割り当てます。
10 ドライブは自動的にマウントされて、ISO ファイルの内容をドライブのルートにコピーできるようになります。

ISO の内容を完全にコピーしたら、ドライブが起動可能になり、リカバリのために使用できるようになります。

EUFI 起動：

1 USB ドライブをシステムに接続します。
2 管理者のコマンドプロンプトを開きます。
3 **Diskpart** と入力して Diskpart ユーティリティを起動します。
4 **list disk** と入力して、変更するターゲットディスクを検索します。ディスクは番号で指定します。
5 コマンド **select disk #** を使用して適切なディスクを選択します。# は、前の手順で示された対応するドライブのディスク番号です。
6 **clean** コマンドでディスクを消去します。この結果、ファイルテーブルが消去されるため、データのドライブはパージされます。
7 起動イメージを格納するパーティションを作成します。
   a **create partition primary** コマンドは、ドライブ上にプライマリパーティションを生成します。

b **select partition 1** コマンドは新しいパーティションを選択します。

c FAT32 ファイルシステムを使用してドライブをクイックフォーマットするには、次のコマンドを使用します。**format FS=FAT32 quick**

8 ドライブは起動可能ドライブとしてマークされている必要があります。**active** コマンドを使用して、ドライブを起動可能としてマークします。

9 ファイルをドライブに直接移動するには、**assign** コマンドを使用してドライブに使用可能な文字を割り当てます。

10 ドライブは自動的にマウントされて、ISO ファイルの内容をドライブのルートにコピーできるようになります。

ISO の内容を完全にコピーしたら、ドライブが起動可能になり、リカバリのために使用できるようになります。