Encryption Recovery

Encryption v10.0 / Data Guardian v2.0

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2012-2018 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.Registered trademarks and trademarks used in the Dell Encryption, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox ℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App Store℠, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

Encryption v10.0 / Data Guardian v2.0

2018 - 08

Rev. A01

Contents

1 Getting Started with Recovery 5
Contact Dell ProSupport 5

2 Policy-Based or File/Folder Encryption Recovery 6
Overview of the Recovery Process 6
Perform Policy-Based Encryption or FFE Recovery 6
Obtain the Recovery File - Policy-Based Encryption or FFE Encryption Client 6
Obtain the Recovery File - Locally Managed Computer 8
Perform a Recovery 8
Encrypted Drive Data Recovery 12
Recover Encrypted Drive Data 12

3 Hardware Crypto Accelerator Recovery 17
Recovery Requirements 17
Overview of the Recovery Process 17
Perform HCA Recovery 17
Obtain the Recovery File - Remotely Managed Computer 17
Obtain the Recovery File - Locally Managed Computer 18
Perform a Recovery 19

4 Self-Encrypting Drive (SED) Recovery 25
Recovery Requirements 25
Overview of the Recovery Process 25
Perform SED Recovery 25
Obtain the Recovery File - Remotely Managed SED Client 25
Obtain the Recovery File - Locally Managed SED Client 26
Perform a Recovery 26
Challenge Recovery with SED 29

5 Full Disk Encryption Recovery 33
Recovery Requirements 33
Overview of the Recovery Process 33
Perform Full Disk Encryption Recovery 33
Obtain the Recovery File - Full Disk Encryption Client 33
Perform a Recovery 34
Challenge Recovery with Full Disk Encryption 36

6 Full Disk Encryption and Dell Encryption Recovery 40
Recovery Requirements 40
Overview of the Recovery Process 40
Perform Recovery of a Full Disk Encrypted and Dell Encrypted Disk 40
Obtain the Recovery File - Full Disk Encryption Client 40
Obtain the Recovery File - Policy-Based Encryption or FFE Encryption Client 41

Perform a Recovery....42
Challenge Recovery with Full Disk Encryption....45

7 PBA Device Control....49
Use PBA Device Control....49

8 General Purpose Key Recovery....50
Recover the GPK....50
Obtain the Recovery File....50
Perform a Recovery....51

9 BitLocker Manager Recovery....53
Recover Data....53

10 Password Recovery....55
Recovery Questions....55

11 Encryption External Media Password Recovery....58
Recover Access to Data....58
Self-Recovery....60

12 Dell Data Guardian Recovery....62
Prerequisites....62
Perform Data Guardian Recovery....62

13 Appendix A - Burning the Recovery Environment....67
Burning the Recovery Environment ISO to CD\DVD....67
Burning the Recovery Environment on Removable Media....67

1

Getting Started with Recovery

This section details what is needed to create the recovery environment.

- CD-R, DVD-R media, or formatted USB media
  - If burning a CD or DVD, review Burning the Recovery Environment ISO to CD\DVD for details.
  - If using USB media, review Burning the Recovery Environment on Removable Media for details.
- Recovery Bundle for failed device
  - For remotely managed clients, instructions that follow explain how to retrieve a recovery bundle from your Dell Security Management Server.
  - For locally managed clients, the recovery bundle package was created during setup on either a shared network drive or on external media. Please locate this package before proceeding.

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product.

Additionally, online support for Dell products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Tag or Express Service Code available when you call.

For phone numbers outside of the United States, see Dell ProSupport International Phone Numbers.

2

Policy-Based or File/Folder Encryption Recovery

Recovery is needed when the encrypted computer will not boot to the operating system. This occurs when the registry is incorrectly modified or hardware changes have occurred on an encrypted computer.

With Policy-Based Encryption or File/Folder Encryption (FFE) recovery, you can recover access to the following:

- A computer that does not boot and that displays a prompt to perform SDE Recovery.
- A computer displays BSOD with a STOP Code of 0x6f or 0x74.
- A computer on which you cannot access encrypted data or edit policies.
- A server running Dell Encryption that meets either of the preceding conditions.
- A computer on which the Hardware Crypto Accelerator card or the motherboard/TPM must be replaced.

NOTE: Hardware Crypto Accelerator is not supported, beginning with v8.9.3.

Overview of the Recovery Process

NOTE: Recovery requires a 32-bit environment.

To recover a failed system:

1 Burn the recovery environment onto a CD/DVD or create a bootable USB. See Appendix A - Burning the Recovery Environment.
2 Obtain the Recovery file.
3 Perform the recovery.

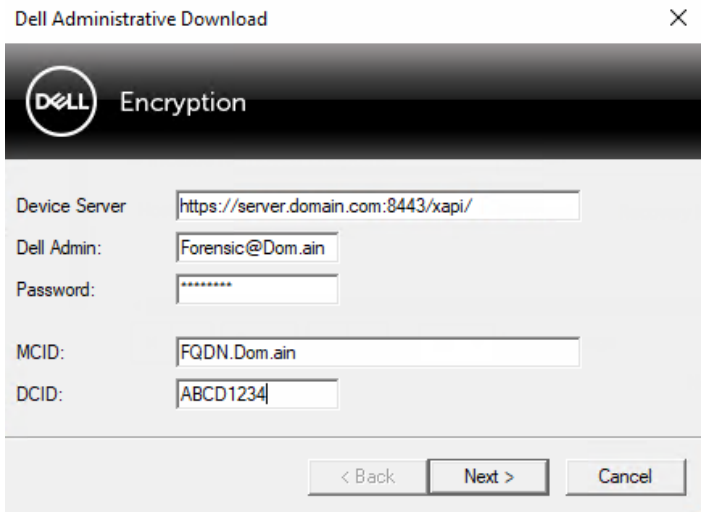
Perform Policy-Based Encryption or FFE Recovery

Follow these steps to perform Policy-Based Encryption or FFE recovery.

Obtain the Recovery File - Policy-Based Encryption or FFE Encryption Client

To download the recovery file:

1 Download the Dell Encryption installation package from http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Navigate to the **AdminUtilities** folder in the installation package and open **CMGAd.exe**.



2 In the **Dell Server** field, enter the Security Management Server/Security Management Server Virtual the computer was activated against.

3 In the **Dell Admin** field, enter a user account name with Forensic Administrator privileges.

4 In the **Password** field, enter the password for the Forensic Administrator.

5 In the **MCID** field, enter the FQDN of the device being recovered.

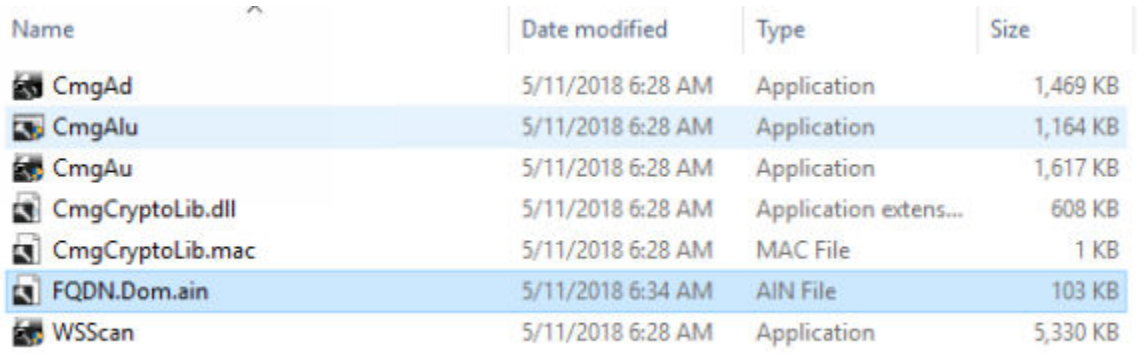
- The **DCID** field is the Recovery ID of the device being recovered.

6 Select **Next**.

7 Define and confirm a **Passphrase** for the recovery file. This Passphrase is needed to perform recovery.

8 In the **Download To:** field, enter a destination location for the recovery bundle then select **Next**. By default, this will be in the directory from which CMGAd.exe was run.

9 The recovery bundle downloads to the folder specified in **Download To:**.

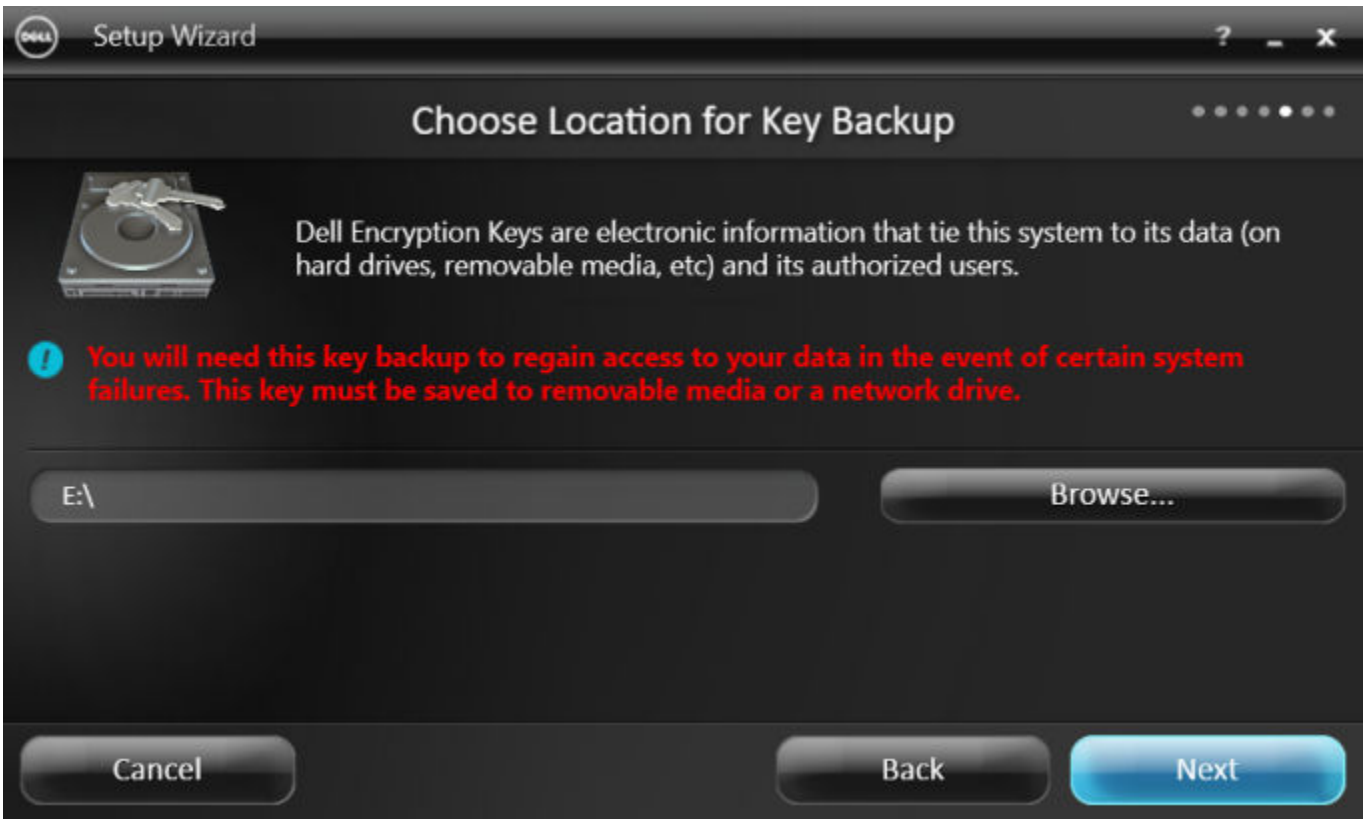


10 Copy the recovery bundle file to a location where it can be accessed when booted into WinPE.

Obtain the Recovery File - Locally Managed Computer

To obtain the Encryption Personal recovery file:

1 Locate the recovery file named **LSARecovery_<systemname** > **.exe** file. This file was stored on a network drive or removable storage when you went through Setup Wizard while installing Encryption Personal.



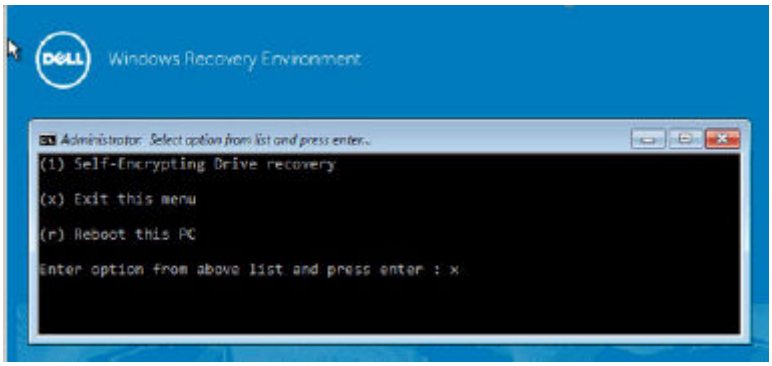
2 Copy **LSARecovery_<systemname** > **.exe** to the target computer (the computer to recover data).

Perform a Recovery

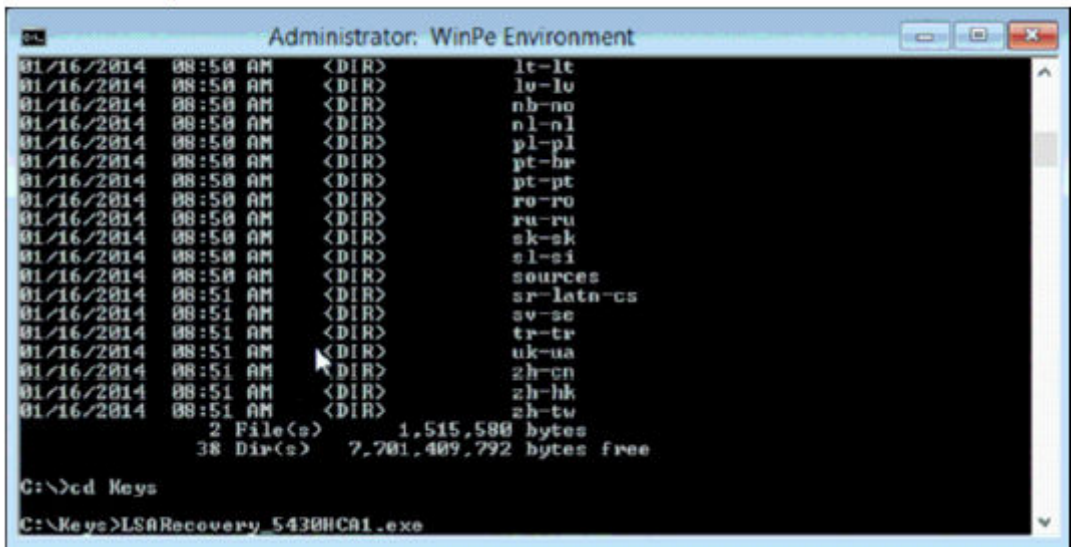
1 Using the bootable media created earlier, boot to that media on a recovery system or on the device with the drive you are attempting to recover. A WinPE Environment opens.

NOTE: Disable SecureBoot before the recovery process. When finished, re-enable SecureBoot.

2 Enter **x** and press **Enter** to get a command prompt.



3 Navigate to the recovery file and launch it.



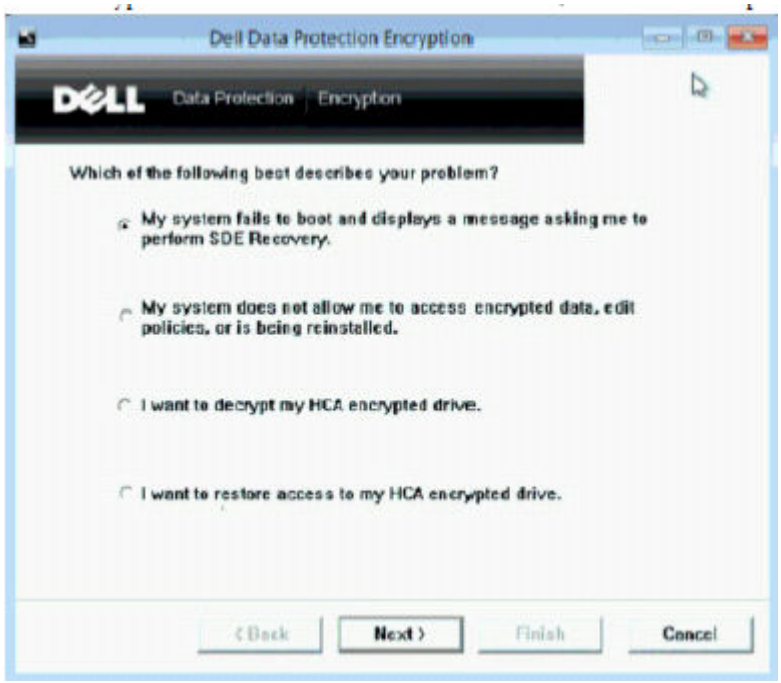
4 Select one option:

- My system fails to boot and displays a message asking me to perform SDE Recovery.

  This will allow you to rebuild the hardware checks that the Encryption client performs when you boot into the OS.

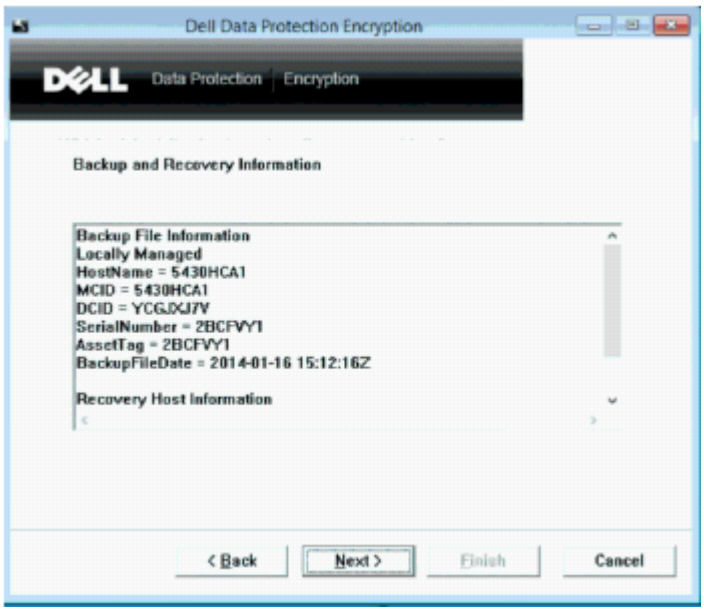
- My system does not allow me to access encrypted data, edit policies, or is being reinstalled.

  Use this if the Hardware Crypto Accelerator card or the motherboard/TPM must be replaced.



5 In the Backup and Recovery Information dialog, confirm that the information about the client computer to be recovered is correct and click **Next**.

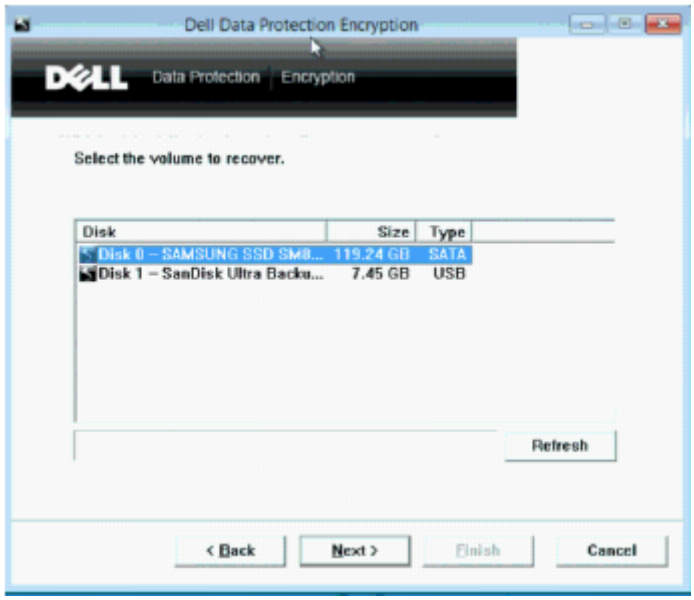
When recovering non-Dell computers, the SerialNumber and AssetTag fields will be blank.



6 In the dialog that lists the computer's volumes, select all applicable drives and click **Next**.

Shift-click or control-click to highlight multiple drives.

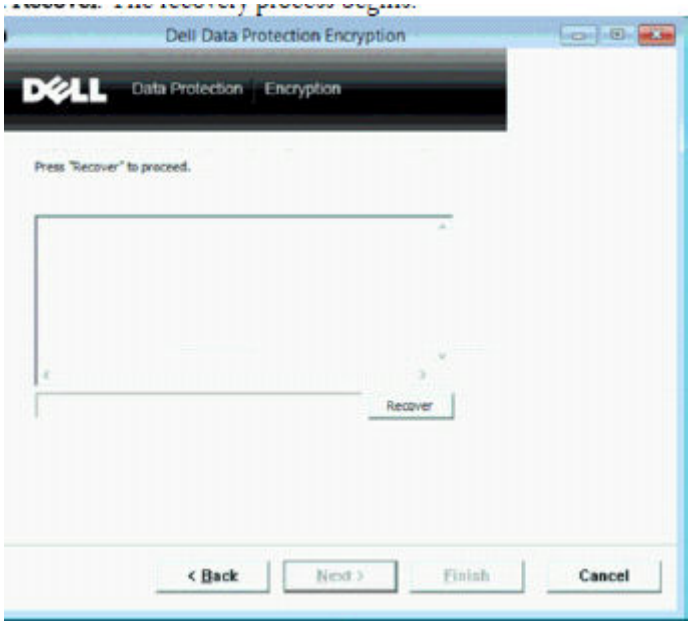
If the selected drive is not Policy-Based or FFE-encrypted, it will fail to recover.



7 Enter your recovery password and click **Next**.
With a remotely managed client, this is the password provided in step 3 in Obtain the Recovery File - Remotely Managed Computer.

In Encryption Personal, the password is the Encryption Administrator Password set for the system at the time the keys were escrowed.

8 In the Recover dialog, click **Recover**. The recovery process begins.



9 When recovery is complete, click **Finish**.

NOTE:
Be sure to remove any USB or CD\DVD media that was used to boot the machine. Failure to do this may result in booting back into the recovery environment.

10 After the computer reboots, you should have a fully functioning computer. If problems persist, contact Dell ProSupport.

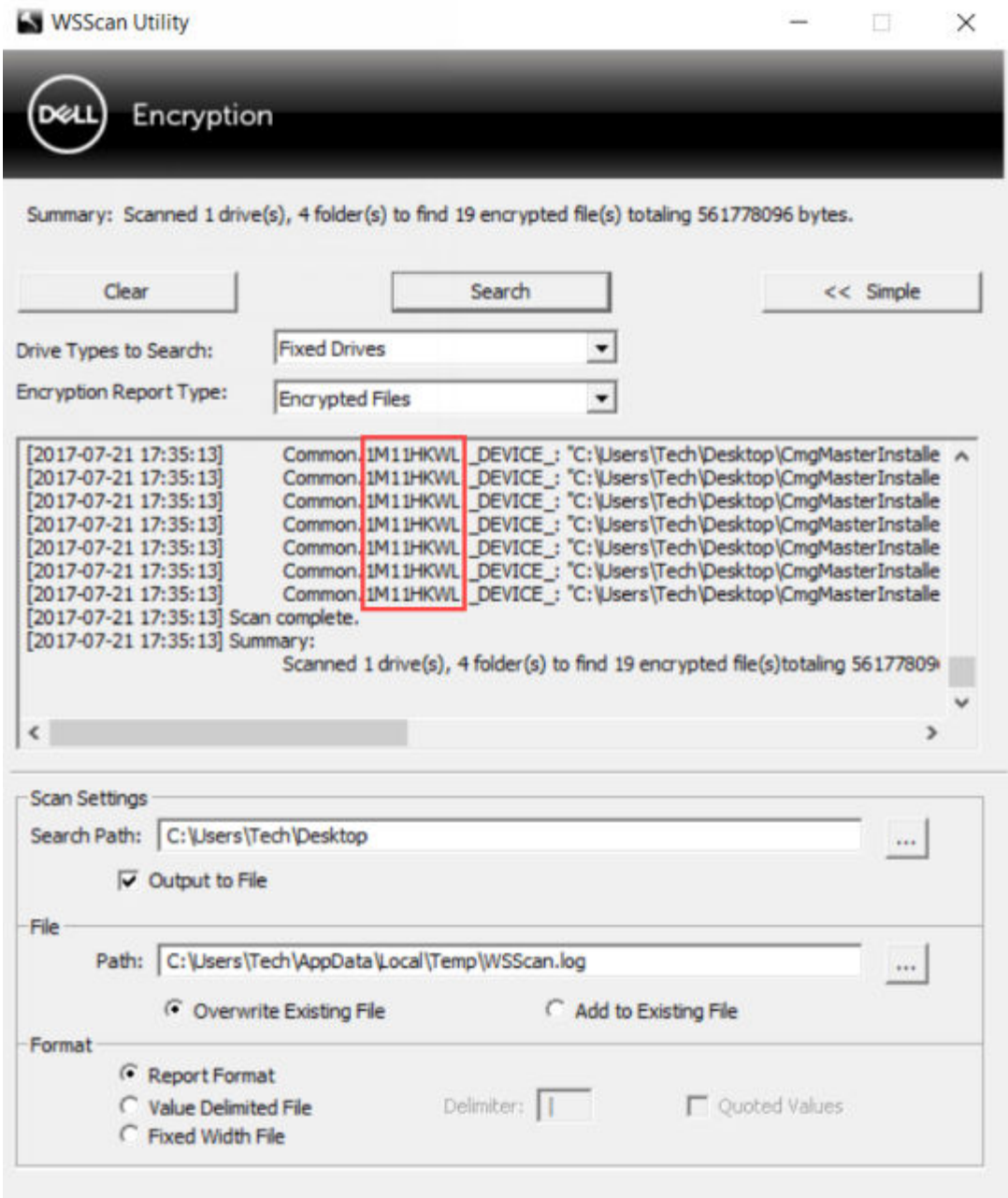
Encrypted Drive Data Recovery

If the target computer is not bootable and no hardware failure exists, data recovery can be accomplished on the computer booted into a recovery environment. If the target computer is not bootable and has failed hardware or is a USB device, data recovery can be accomplished by booting into a slaved drive. When you slave a drive, you can see the file system and browse the directories. However, if you try to open or copy a file, an *Access denied* error occurs.

Recover Encrypted Drive Data

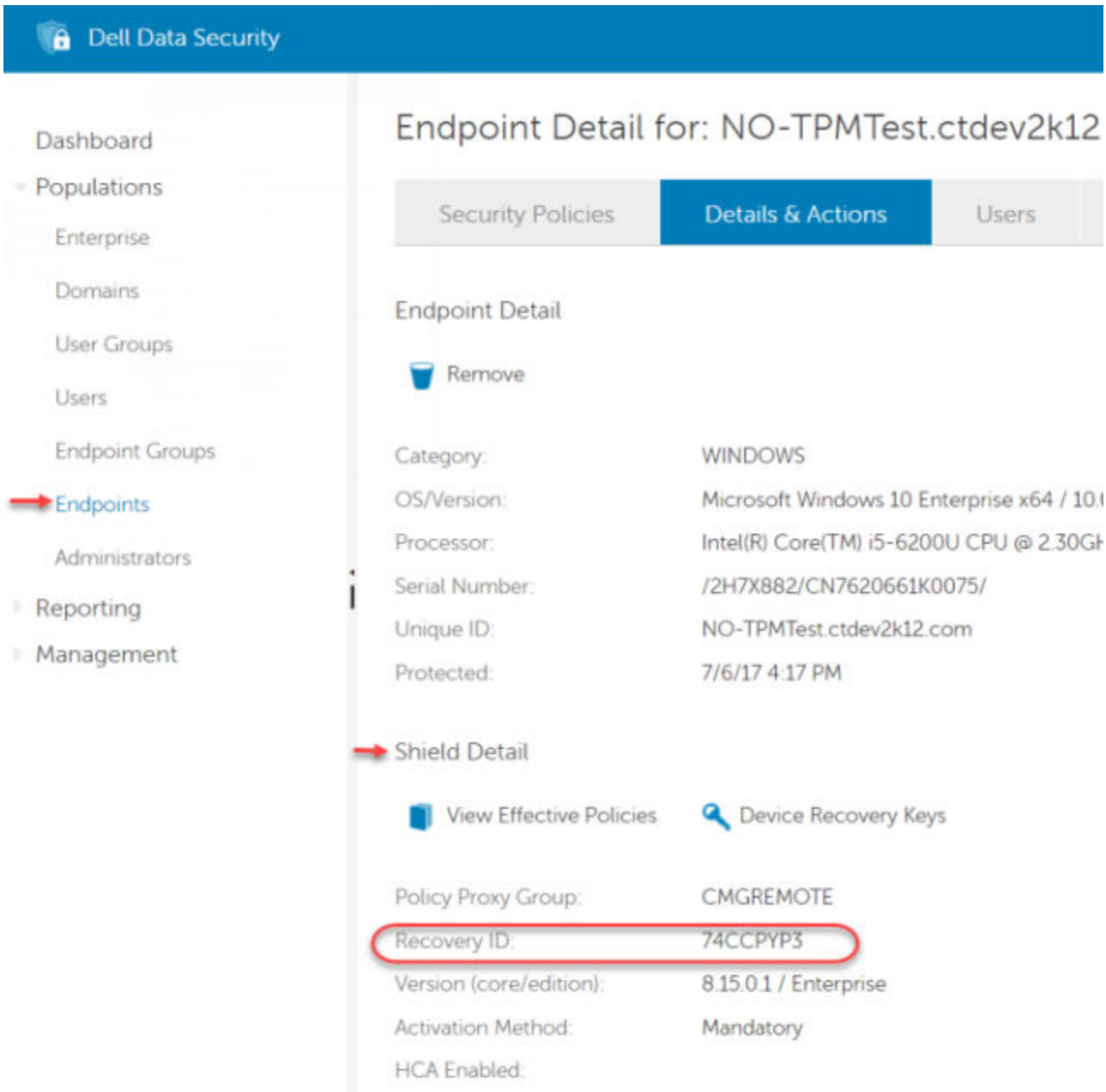
To recover encrypted drive data:

1 To obtain the DCID/Recovery ID from the computer, choose one option:
   a Run WSScan on any folder where Common encrypted data is stored.
   The eight-character DCID/Recovery ID displays after "Common."

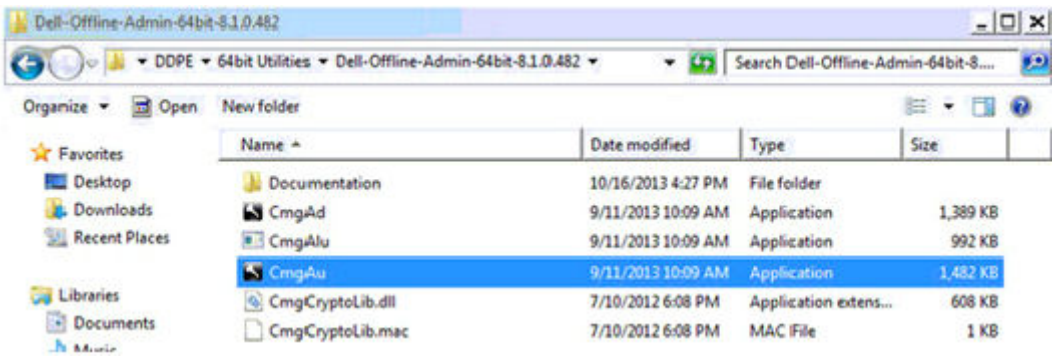


b Open the Remote Management Console, and select the **Details & Actions** tab for the endpoint.

c In the Shield Detail section of the Endpoint Detail screen, locate the DCID/Recovery ID.



2 To download the key from the Server, navigate to and run the Dell Administrative Unlock (**CMGAu**) utility.
The Dell Administrative Unlock utility can be obtained from Dell ProSupport.



3 In the Dell Administrative Utility (CMGAu) dialog, enter the following information (some fields may be prepopulated) and click **Next**.

Server: Fully Qualified Hostname of the Server, for example:

Device Server (Pre 8.x clients): **https://<server.organization.com>:8081/xapi**

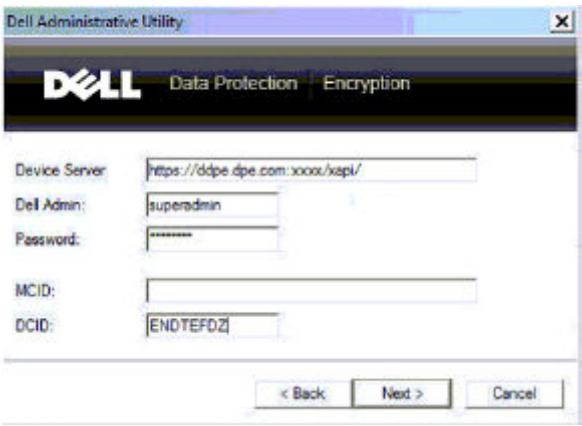
Security Server: **https://<server.organization.com>:8443/xapi/**

Dell Admin: The account name for the Forensic Administrator (enabled in the Security Management Server/Security Management Server Virtual)

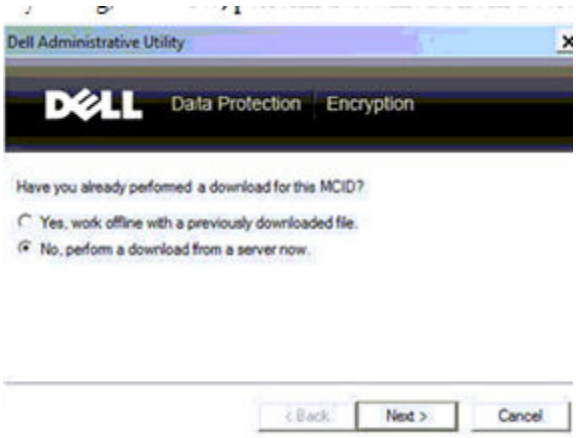
Dell Admin Password: The account password for the Forensic Administrator (enabled in the Security Management Server/Security Management Server Virtual)

MCID: Clear the MCID field

DCID: The DCID/Recovery ID that you obtained earlier.



4 In the Dell Administrative Utility dialog, select **No, perform a download from a server now** and click **Next**.



NOTE:

If the Encryption client is not installed, a message displays that *Unlock failed*. Move to a computer with the Encryption client installed.

5 When download and unlock are complete, copy files you need to recover from this drive. All files are readable. ***Do not click Finish until you have recovered the files***.

6 After you recover the files and are ready to re-lock the files, click **Finish**.
After you click Finish, the encrypted files are no longer available.

Hardware Crypto Accelerator Recovery

NOTE: Hardware Crypto Accelerator is not supported, beginning with v8.9.3.

With Hardware Crypto Accelerator (HCA) Recovery, you can recover access to the following:

- Files on an HCA encrypted drive - This method decrypts the drive using the keys provided. You can select the specific drive that you need to decrypt during the recovery process.
- An HCA encrypted drive after a hardware replacement - This method is used after you must replace the Hardware Crypto Accelerator card or a motherboard/TPM. You can run a recovery to regain access to the encrypted data without decrypting the drive.

Recovery Requirements

For HCA recovery, you need the following:

- Access to the recovery environment ISO (Recovery requires a 32-bit environment)
- Bootable CD\DVD or USB media

Overview of the Recovery Process

NOTE: Recovery requires a 32-bit environment.

To recover a failed system:

1 Burn the recovery environment onto a CD/DVD or create a bootable USB. See Appendix A - Burning the Recovery Environment.
2 Obtain the Recovery file.
3 Perform the recovery.

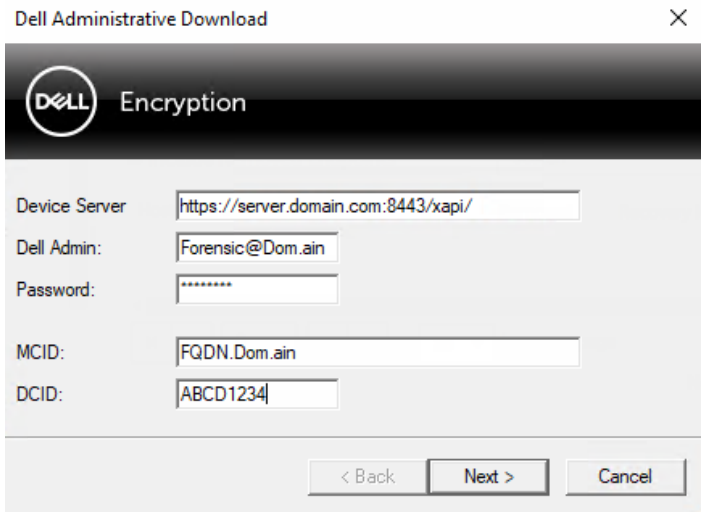
Perform HCA Recovery

Follow these steps to perform an HCA recovery.

Obtain the Recovery File - Remotely Managed Computer

To download the **<machinename_domain.com>.exe** file that was generated when you installed Dell Encryption:

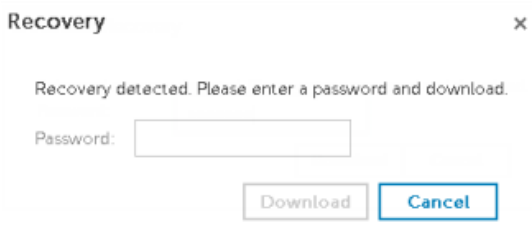
1 Open the Remote Management Console and, from the left pane, select **Management** > **Recover Endpoint**.



2 In the Hostname field, enter the fully qualified domain name of the endpoint and click **Search**.

3 In the Recovery window, enter a recovery Password and click **Download**.

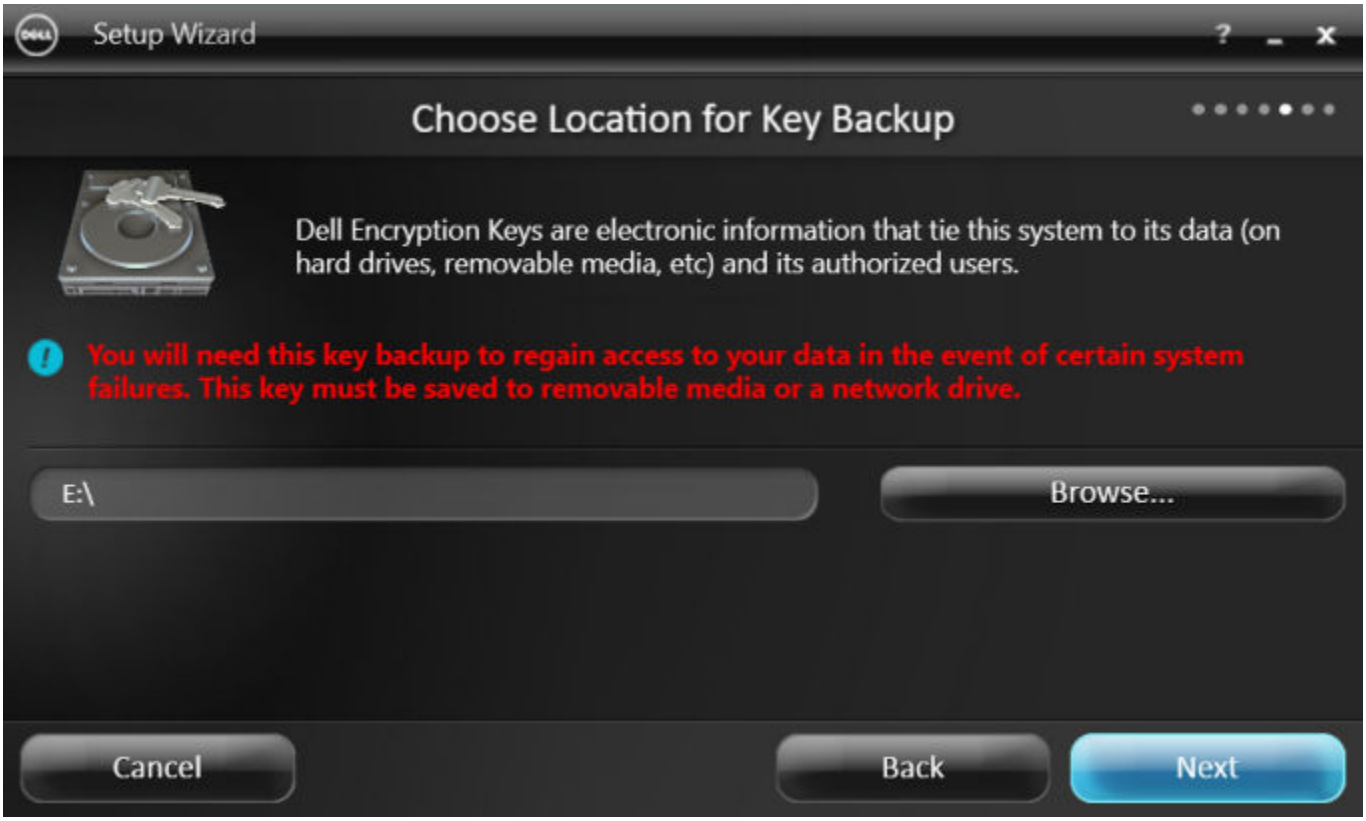
NOTE:
You must remember this password to access the recovery keys.



Obtain the Recovery File - Locally Managed Computer

To obtain the Encryption Personal recovery file:

1 Locate the recovery file named **LSARecovery_<systemname** > **.exe** file. This file was stored on a network drive or removable storage when you went through Setup Wizard while installing Encryption Personal.



2 Copy **LSARecovery_<systemname> > .exe** to the target computer (the computer to recover data).

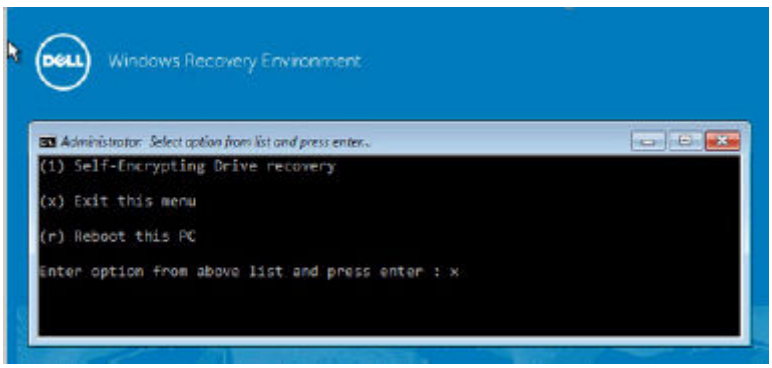
Perform a Recovery

1 Using the bootable media created earlier, boot to that media on a recovery system or on the device with the drive you are attempting to recover.

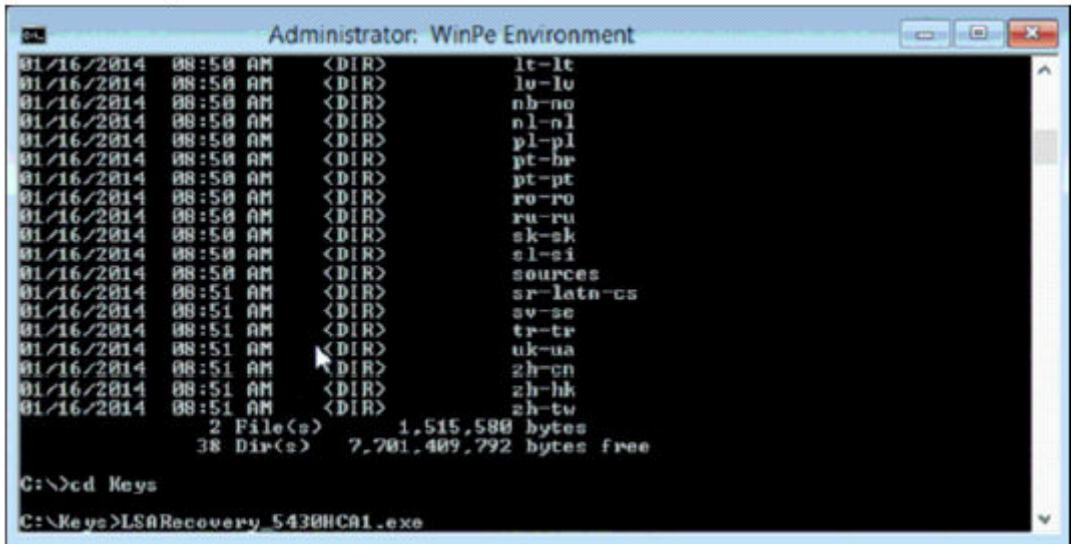
A WinPE Environment opens.

NOTE: Disable SecureBoot before the recovery process. When finished, enable SecureBoot.

2 Type **x** and press **Enter** to get to a command prompt.



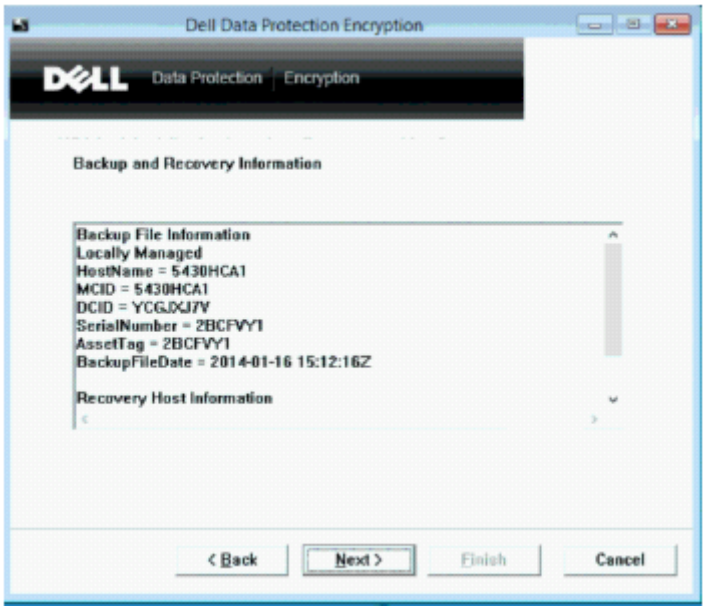
3 Navigate to the saved recovery file and launch it.



4 Select one option:

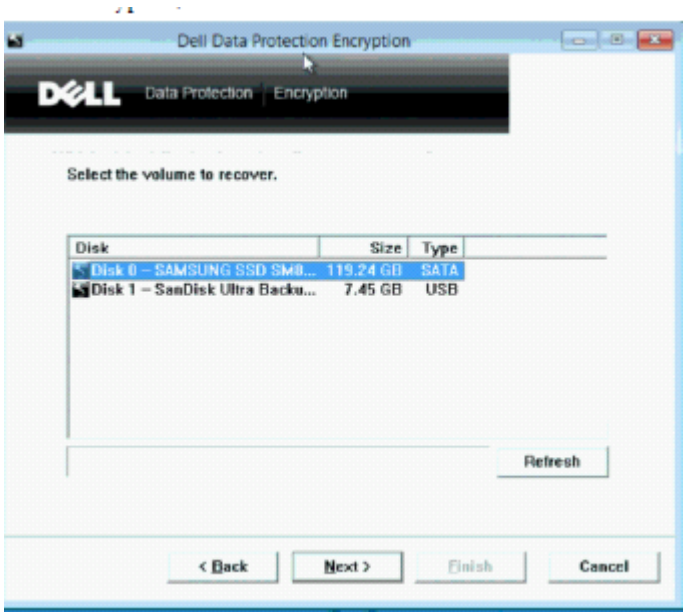
- I want to decrypt my HCA encrypted drive.
- I want to restore access to my HCA encrypted drive.

5 In the Backup and Recovery Information dialog, confirm that the Service Tag or Asset number is correct and click **Next**.



6 In the dialog that lists the computer's volumes, select all applicable drives and click **Next**.
Shift-click or control-click to highlight multiple drives.

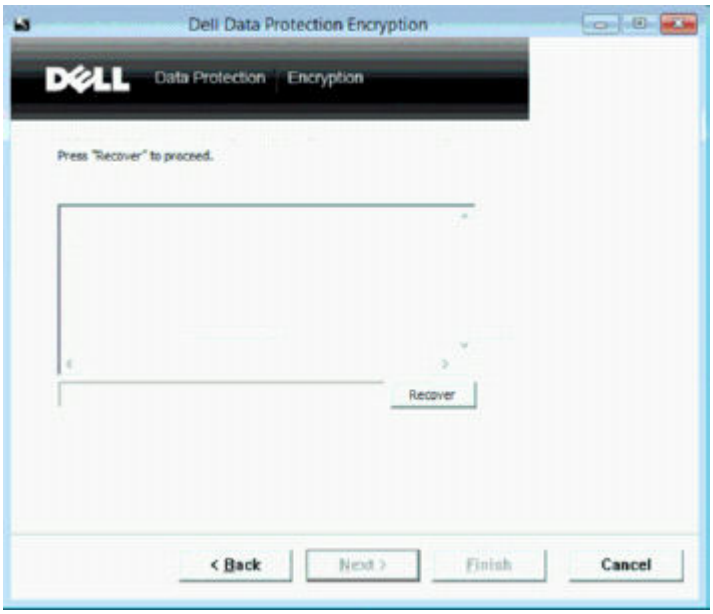
If the selected drive is not HCA encrypted, it will fail to recover.



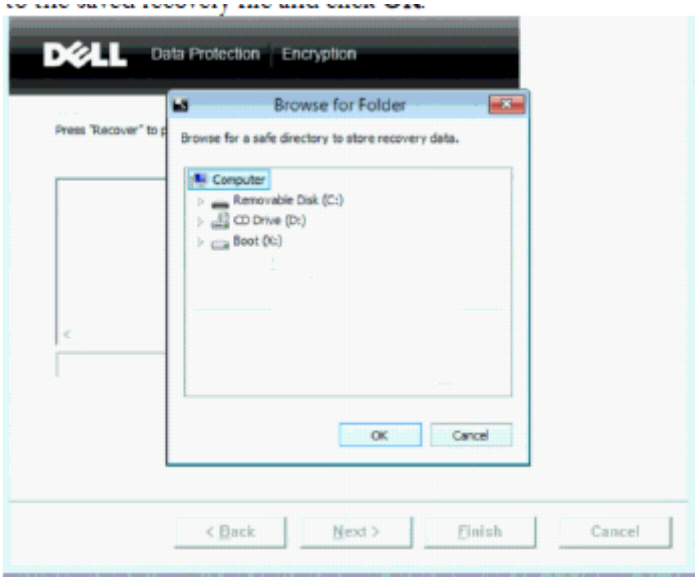
7 Enter your recovery password and click **Next**.
On a remotely managed computer, this is the password provided in step 3 in Obtain the Recovery File - Remotely Managed Computer.

On a locally managed computer, this password is the Encryption Administrator Password set for the system in Personal Edition at the time the keys were escrowed.

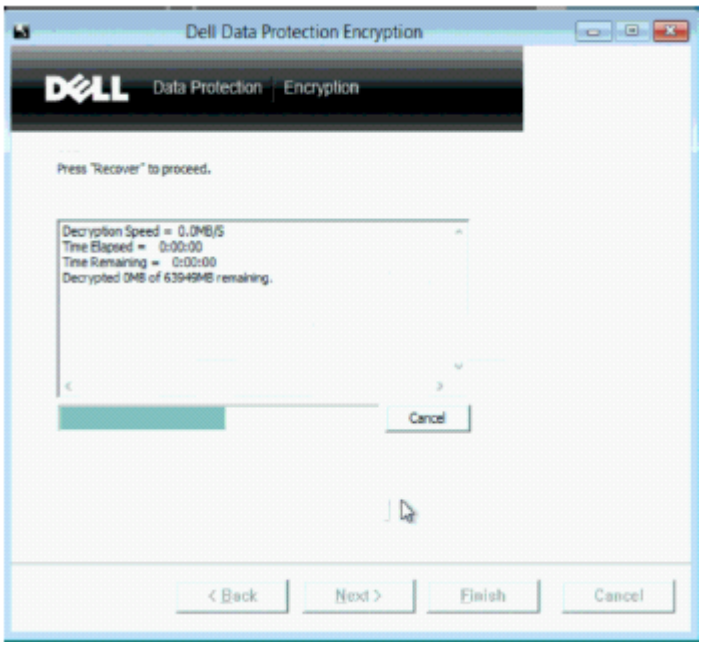
8 In the Recover dialog, click **Recover**. The recovery process begins.



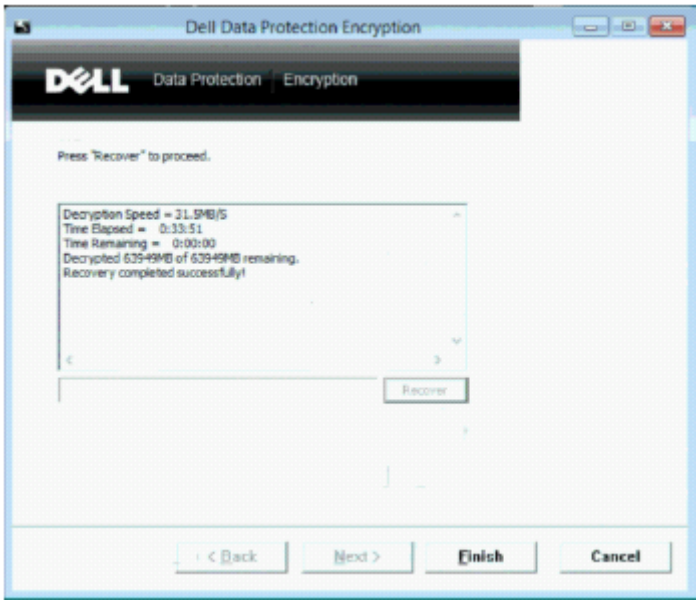
9 When prompted, browse to the saved recovery file and click **OK**.



If you are performing a full decryption, the following dialog displays status. This process may require some time.



10 When the message displays to indicate that recovery completed successfully, click **Finish**. The computer reboots.



After the computer reboots, you should have a fully functioning computer. If problems persist, contact Dell ProSupport.

4

Self-Encrypting Drive (SED) Recovery

With SED Recovery, you can recover access to files on a SED through the following methods:

- Perform a one-time unlock of the drive to bypass the Preboot Authentication (PBA).
- Unlock, then permanently remove the PBA from the drive. Single Sign-On will not function with the PBA removed.
  - With a remotely managed SED client, removing the PBA will require you to deactivate the product from the Remote Management Console if it is necessary to re-enable the PBA in the future.
  - With a locally managed SED client, removing the PBA will require you to deactivate the product inside the OS if it is necessary to re-enable the PBA in the future.

Recovery Requirements

For SED recovery, you need the following:

- Access to the recovery environment ISO
- Bootable CD\DVD or USB media

Overview of the Recovery Process

NOTE: Recovery requires a 64-bit or 32-bit environment based on the BIOS boot mode.

To recover a failed system:

1 Burn the recovery environment onto a CD/DVD or create a bootable USB. See Appendix A - Burning the Recovery Environment.
2 Obtain the Recovery file.
3 Perform the recovery.

Perform SED Recovery

Follow these steps to perform a SED recovery.

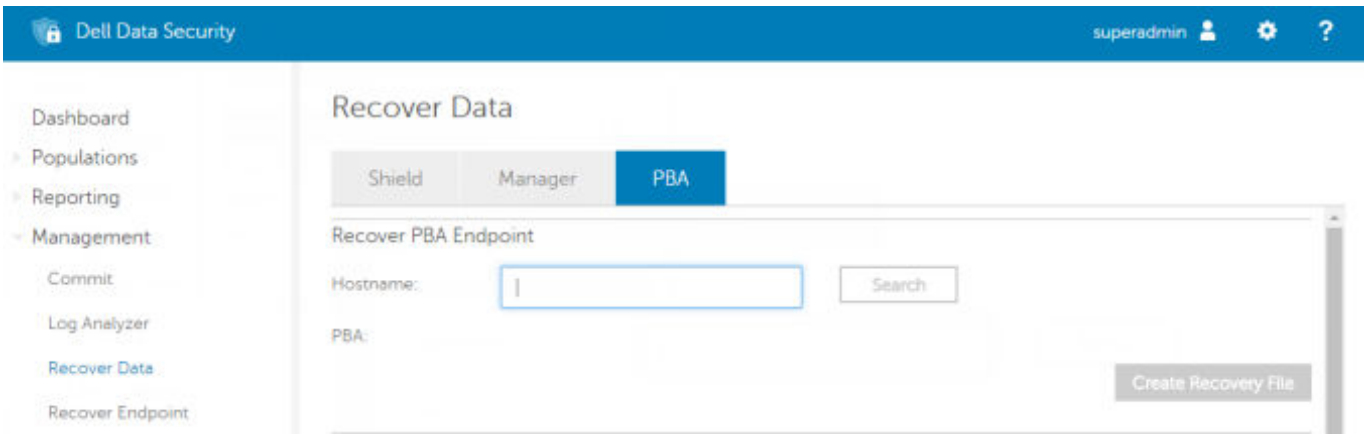
Obtain the Recovery File - Remotely Managed SED Client

Obtain the recovery file.

The recovery file can be downloaded from the Remote Management Console. To download the *<hostname>-sed-recovery.dat* file that was generated when you installed Dell Data Security:

a Open the Remote Management Console and, from the left pane, select **Management > Recover Data** then select the **SED** tab.
b On the Recover Data screen, in the Hostname field, enter the fully qualified domain name of the endpoint, then click **Search**.
c In the SED field, select an option.
d Click **Create Recovery File**.

The **<hostname>-sed-recovery.dat** file is downloaded.



Obtain the Recovery File - Locally Managed SED Client

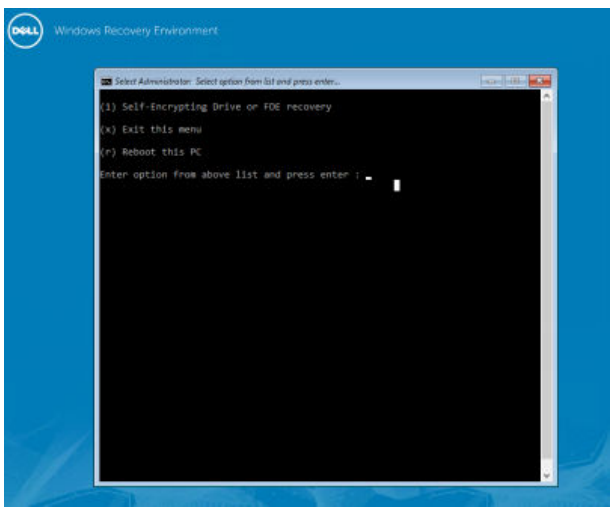
Obtain the recovery file.

The file was generated and is accessible from the backup location you selected when Advanced Authentication was installed on the computer. The filename is *OpalSPkey<systemname>.dat*.

Perform a Recovery

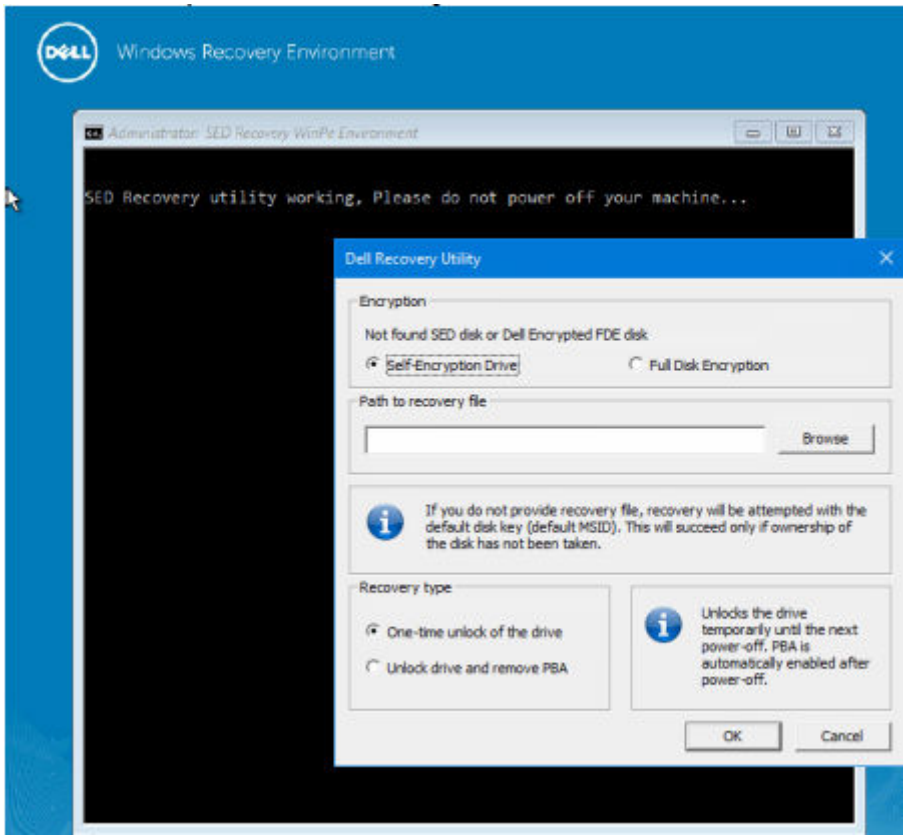
1 Using the bootable media created earlier, boot to that media on a recovery system or on the device with the drive you are attempting to recover. A WinPE environment opens with the recovery application.

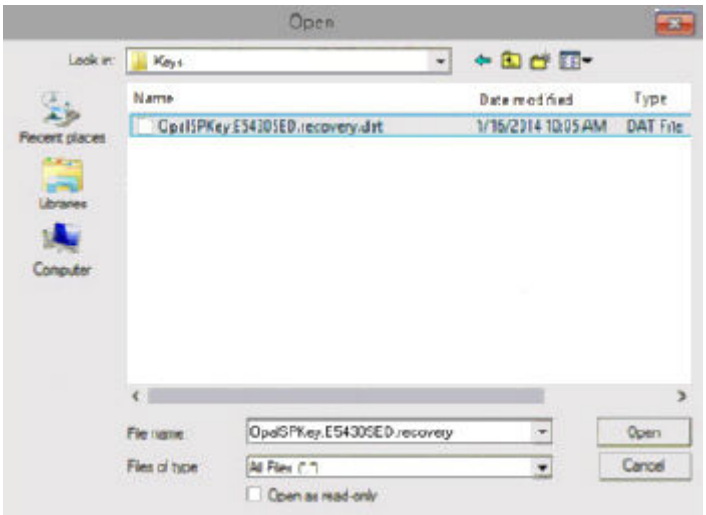
NOTE: Disable SecureBoot before the recovery process. When finished, enable SecureBoot.



2 Choose option one and press **Enter**.

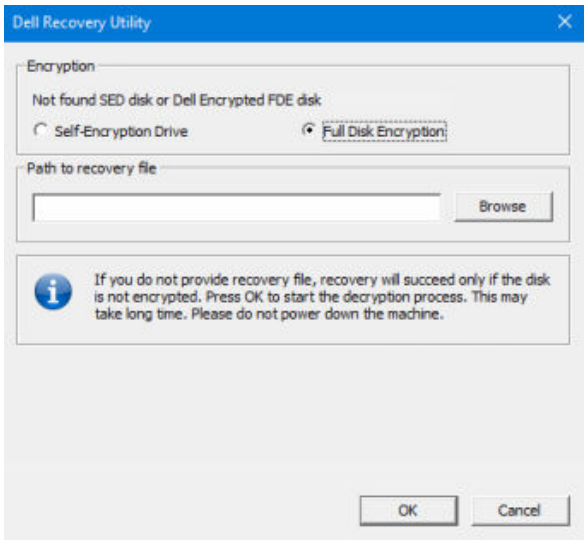
3 Select **Browse**, locate the recovery file, and then click **Open**.

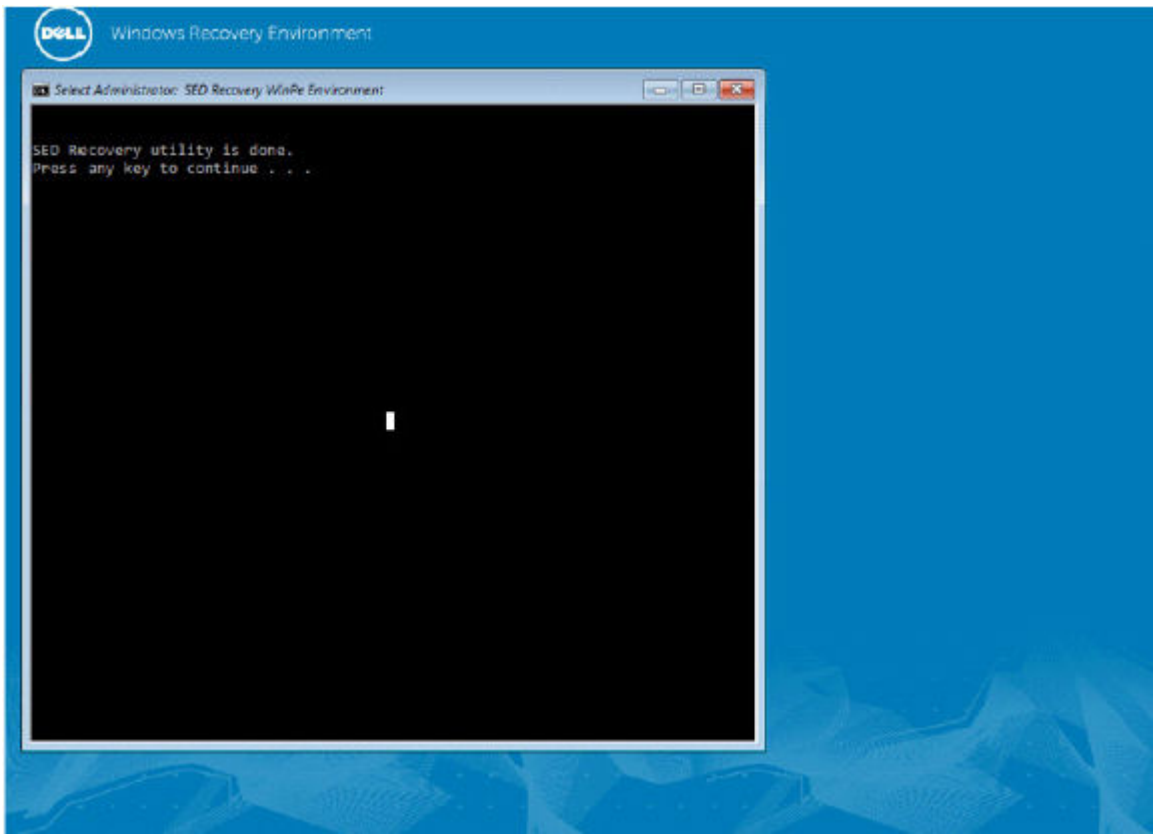




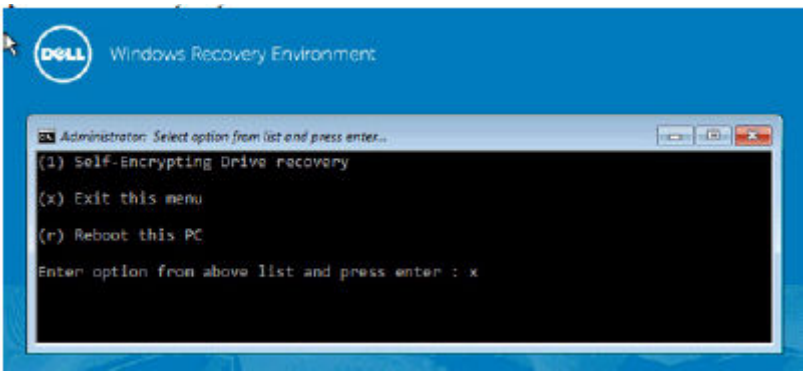
4 Select one option and click **OK**.

- **One-time unlock of the drive** - This method bypasses the PBA.
- **Unlock drive and remove PBA** - This method unlocks, then permanently removes the PBA from the drive. Removing the PBA will require you to deactivate the product from the Remote Management Console (for a remotely managed SED client) or inside the OS (for a locally managed SED client) if it is necessary to re-enable the PBA in the future. Single Sign-On will not function with the PBA removed.





5 Recovery is now completed. Press any key to return to the menu.



6 Press **r** to reboot the computer.

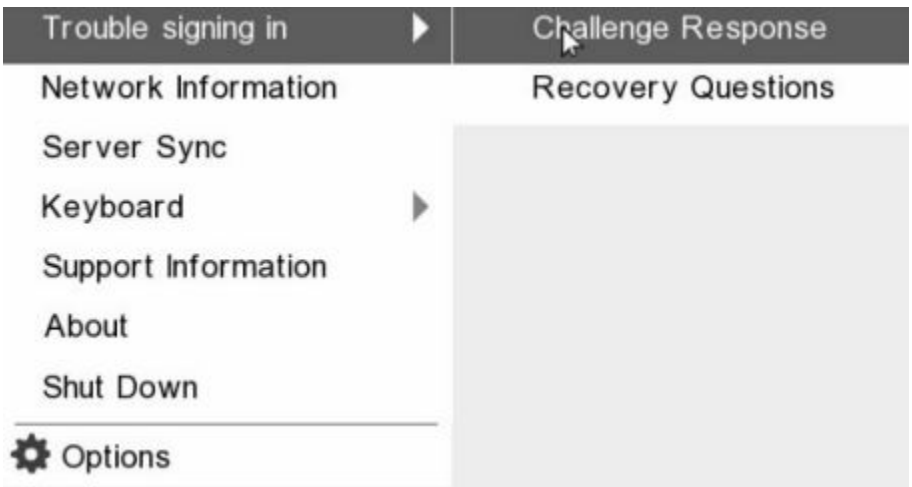
> **NOTE:**
> Be sure to remove any USB or CD\DVD media that was used to boot the computer. Failure to do this may result in booting back into the recovery environment.

7 After the computer reboots, you should have a fully functioning computer. If problems persist, contact Dell ProSupport.

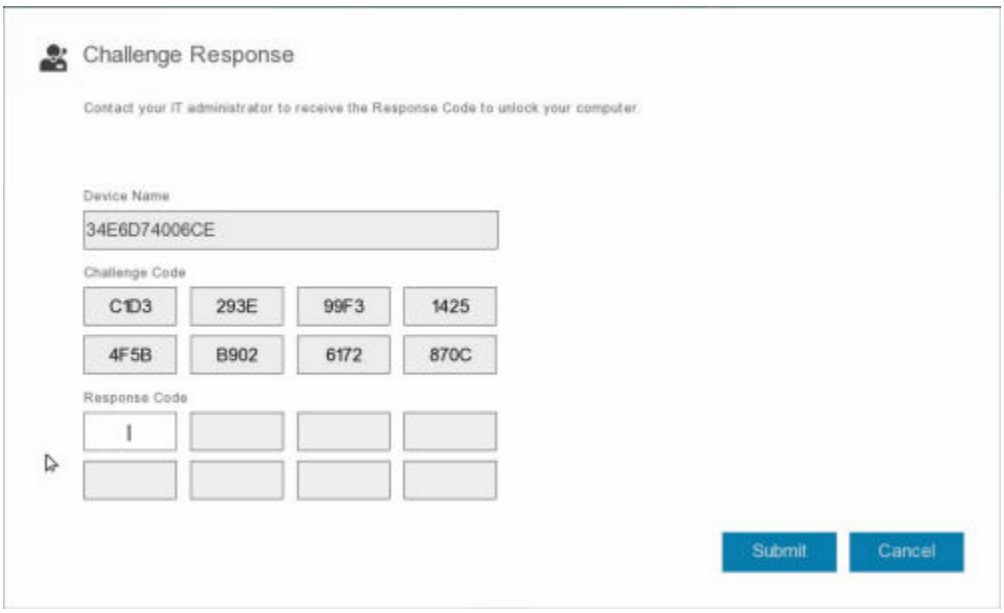
Challenge Recovery with SED

Bypass the PreBoot Authentication Environment

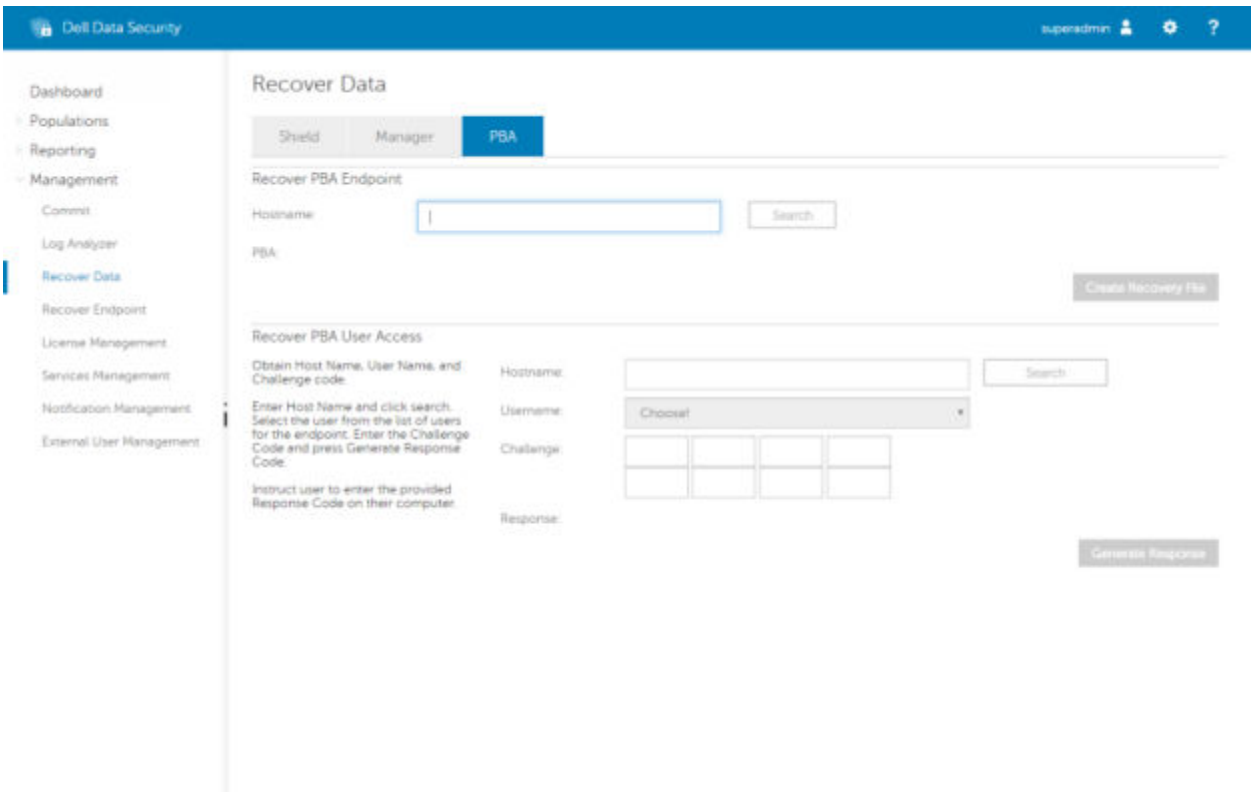
Users forget their passwords and call into the help desk regarding getting through the PBA environment. Use the Challenge/Response mechanism that is built-into the device. This is per-user and is based on a rotating set of alphanumeric characters. The user must enter their name in the **Username** field and then select **Options > Challenge Response**.



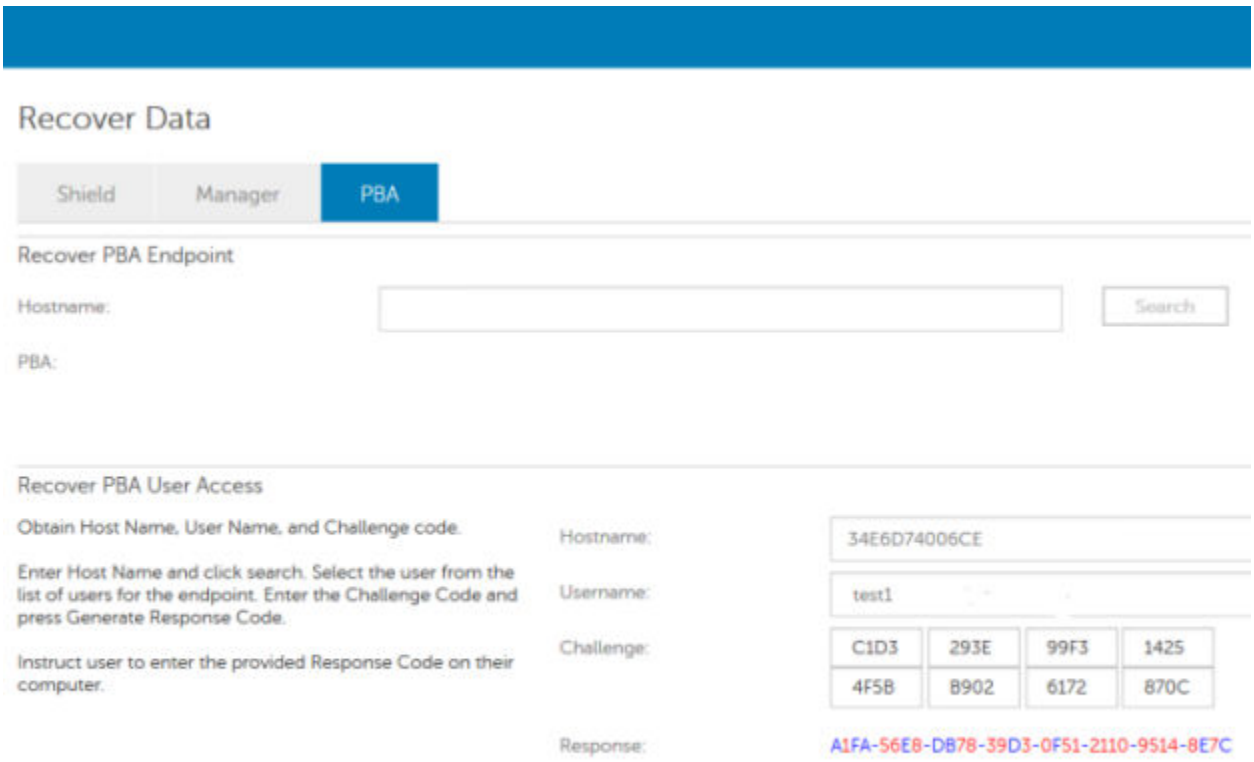
The following information appears after selecting **Challenge Response**.



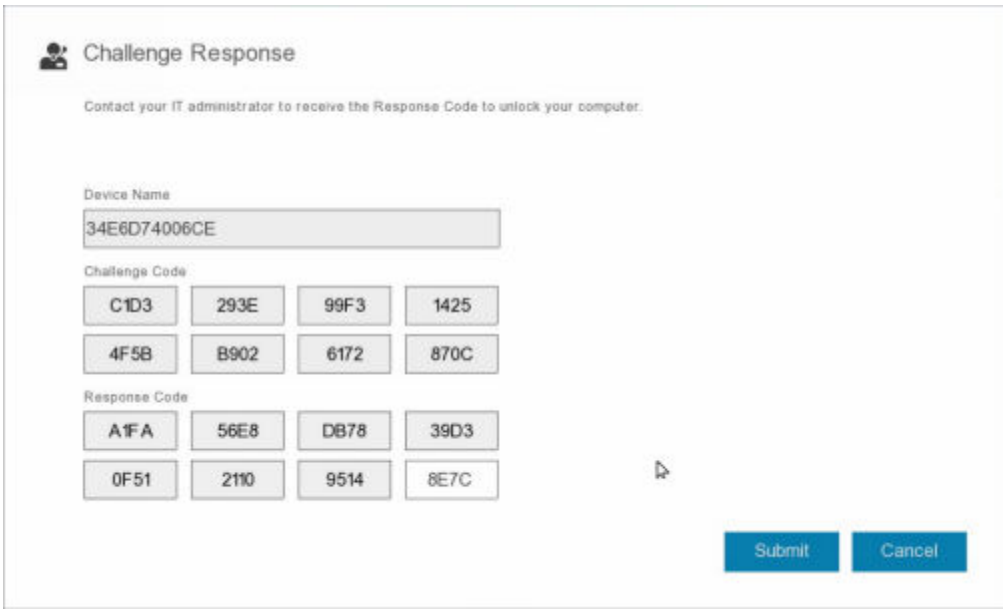
The **Device Name** field is used by the help desk technician within the Remote Management Console to find the correct device, and then a username is selected. This is found within **Management > Recover Data** under the **PBA** tab.



The Challenge Code is provided to the help desk technician who inputs the data, and then clicks the **Generate Response** button.



This resulting data is color-coordinated to help discern between numerals (red) and alphabet characters (blue). This data is read to the end user, who enters it into the PBA environment and then clicks the **Submit** button, moving the user into Windows.



After successful authentication, the following message appears:

Challenge recovery is complete.

5

Full Disk Encryption Recovery

Recovery enables you to recover access to files on a drive encrypted with Full Disk Encryption.

NOTE: Decryption should not be interrupted. If decryption is interrupted, data loss may occur.

Recovery Requirements

For Full Disk Encryption recovery, you need the following:

- Access to the recovery environment ISO
- Bootable CD\DVD or USB media

Overview of the Recovery Process

NOTE: Recovery requires a 64-bit environment.

To recover a failed system:

1 Burn the recovery environment onto a CD/DVD or create a bootable USB. See Appendix A - Burning the Recovery Environment.
2 Obtain the Recovery file.
3 Perform the recovery.

Perform Full Disk Encryption Recovery

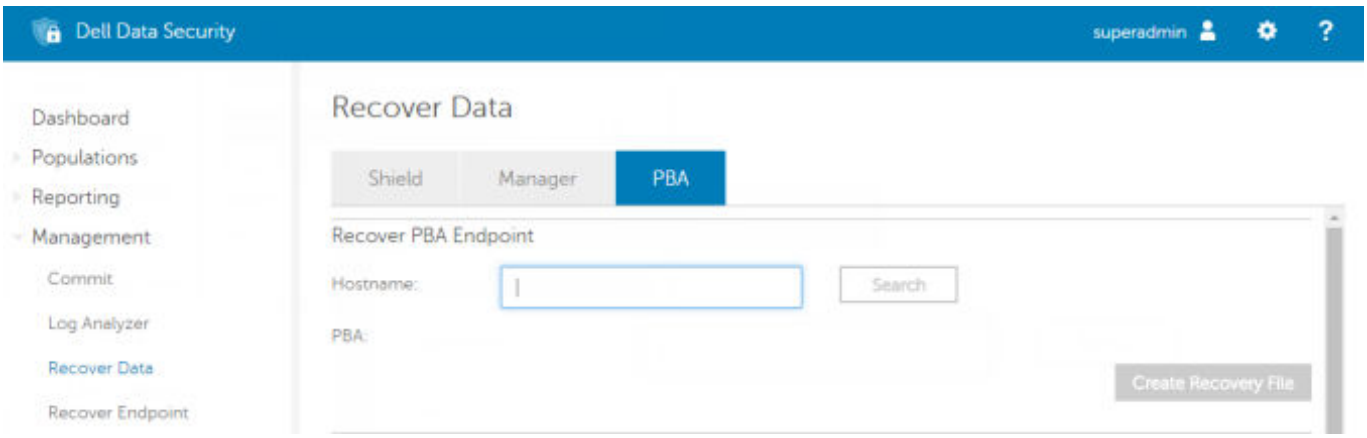
Follow these steps to perform a Full Disk Encryption recovery.

Obtain the Recovery File - Full Disk Encryption Client

Obtain the recovery file.

Download the recovery file from the Remote Management Console. To download the *<hostname>-sed-recovery.dat* file that was generated when you installed Dell Data Security:

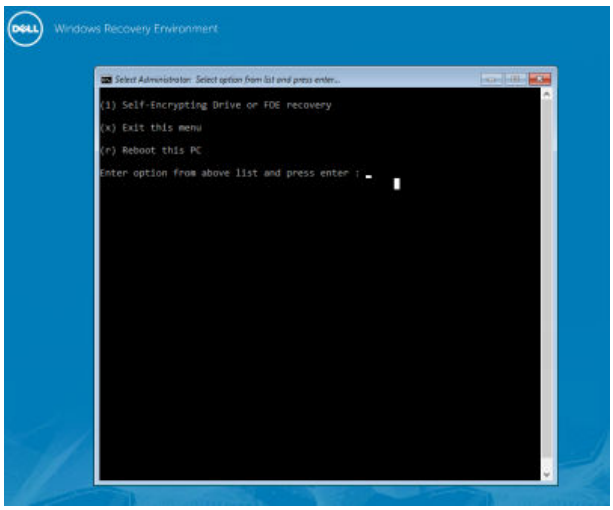
a Open the Remote Management Console and, from the left pane, select **Management > Recover Data** then select the **PBA** tab.
b On the Recover Data screen, in the Hostname field, enter the fully qualified domain name of the endpoint, then click **Search**.
c In the SED field, select an option.
d Click **Create Recovery File**.
The **<hostname>-sed-recovery.dat** file is downloaded.



Perform a Recovery

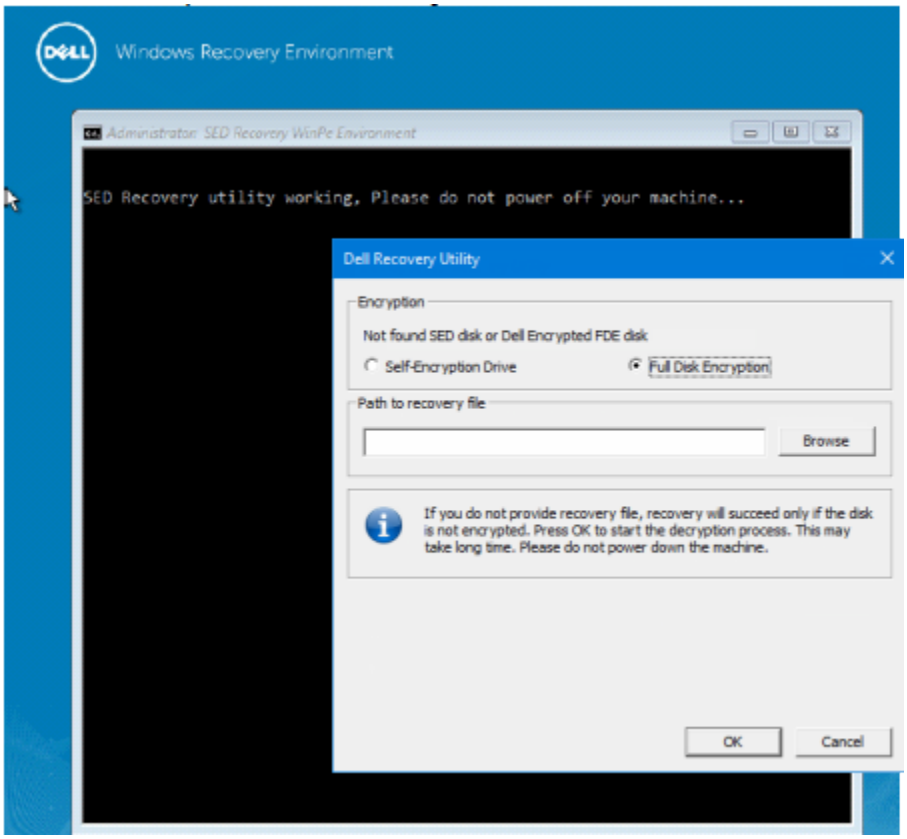
1 Using the bootable media created earlier, boot to that media on a recovery system or on the device with the drive you are attempting to recover. A WinPE environment opens with the recovery application.

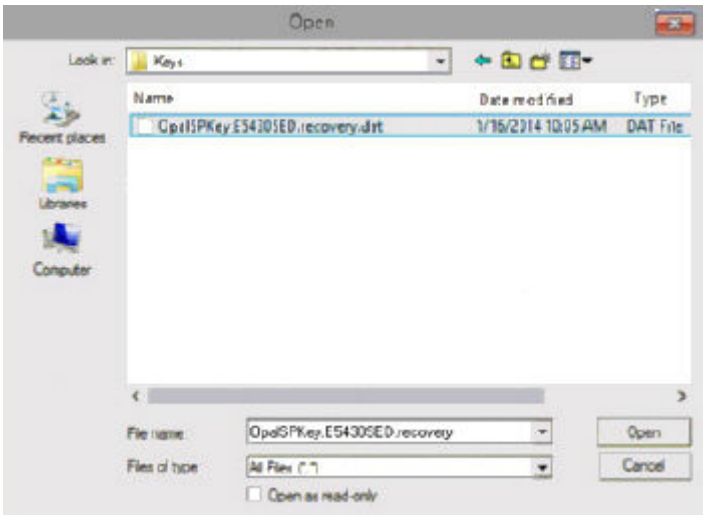
NOTE: Disable SecureBoot before the recovery process. When finished, re-enable SecureBoot.



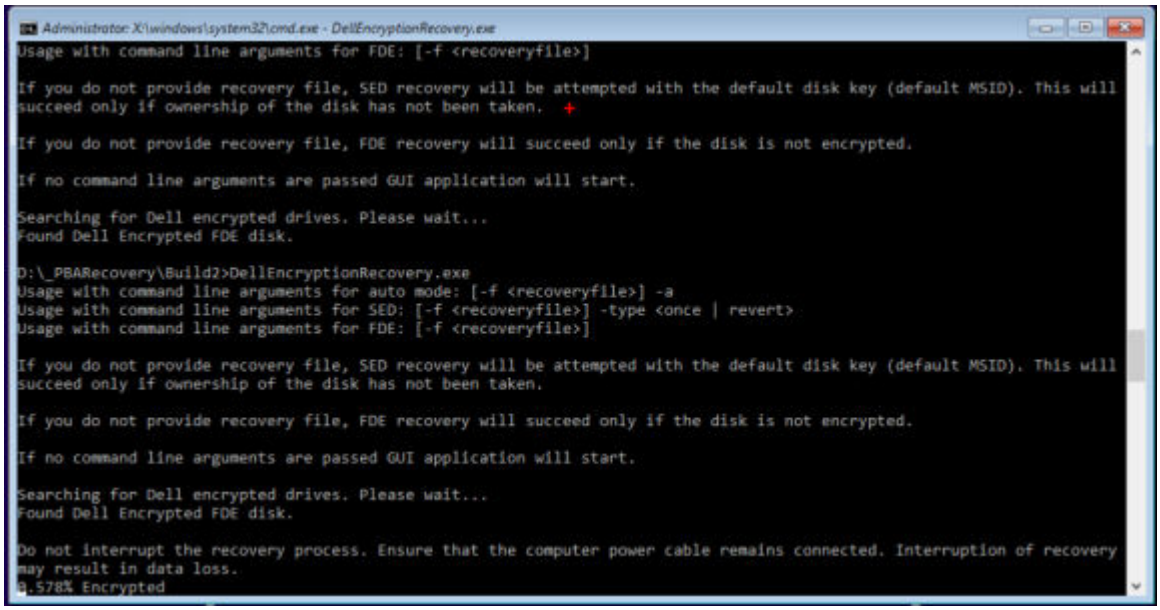
2 Choose option one and press **Enter**.

3 Select **Browse**, locate the recovery file, and then click **Open**.


Windows Recovery Environment
Administrator: SED Recovery WinPe Environment
SED Recovery utility working, Please do not power off your machine...
Dell Recovery Utility
Encryption
Not found SED disk or Dell Encrypted FDE disk
Self-Encryption Drive
Full Disk Encryption
Path to recovery file
Browse
If you do not provide recovery file, recovery will succeed only if the disk is not encrypted. Press OK to start the decryption process. This may take long time. Please do not power down the machine.
OK
Cancel

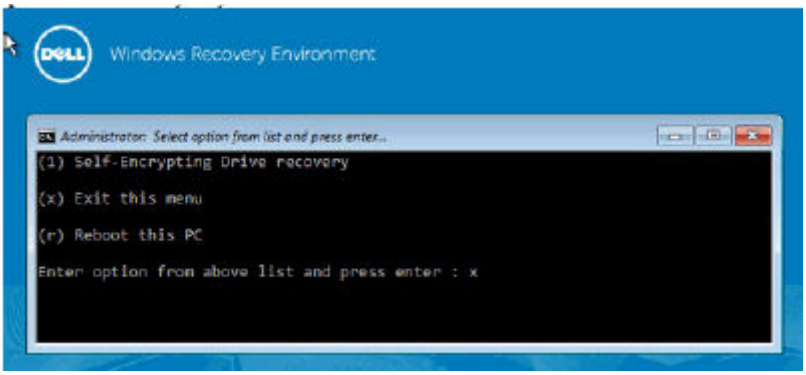

Open
Look in:
Keys
Recent places
Libraries
Computer
Name
Date modified
Type
OpalSPKey.E5430SED.recovery.dat
1/16/2014 10:05 AM
DAT File
File name:
OpalSPKey.E5430SED.recovery
Open
Files of type:
All Files (*.*)
Cancel
Open as read-only

4 Click **OK**.



.

5 Recovery is now completed. Press any key to return to the menu.



6 Press **r** to reboot the computer.

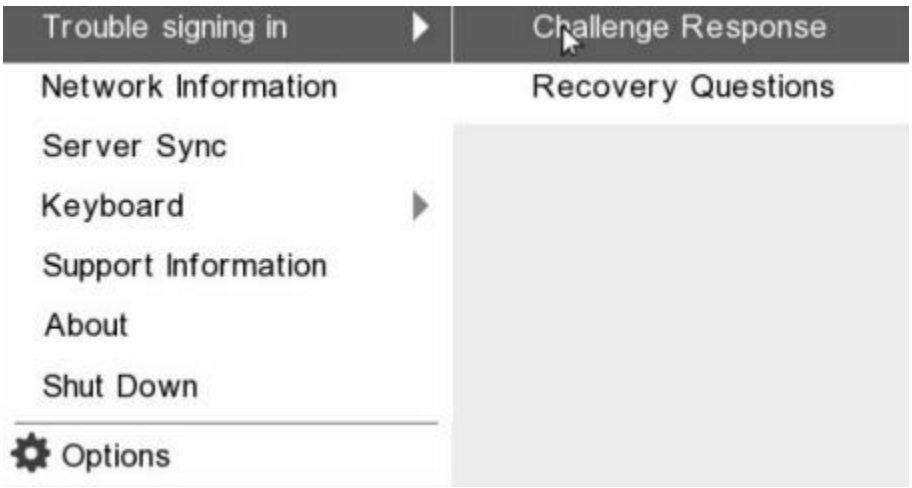
> **NOTE:**
> Be sure to remove any USB or CD\DVD media that was used to boot the computer. Failure to do this may result in booting back into the recovery environment.

7 After the computer reboots, you should have a fully functioning computer. If problems persist, contact Dell ProSupport.

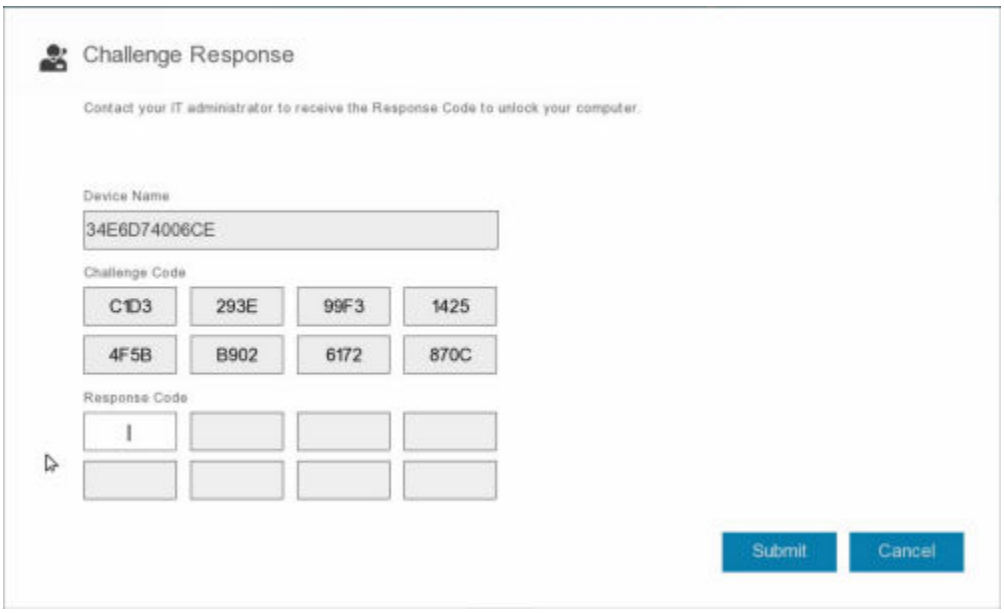
Challenge Recovery with Full Disk Encryption

Bypass the Preboot Authentication Environment

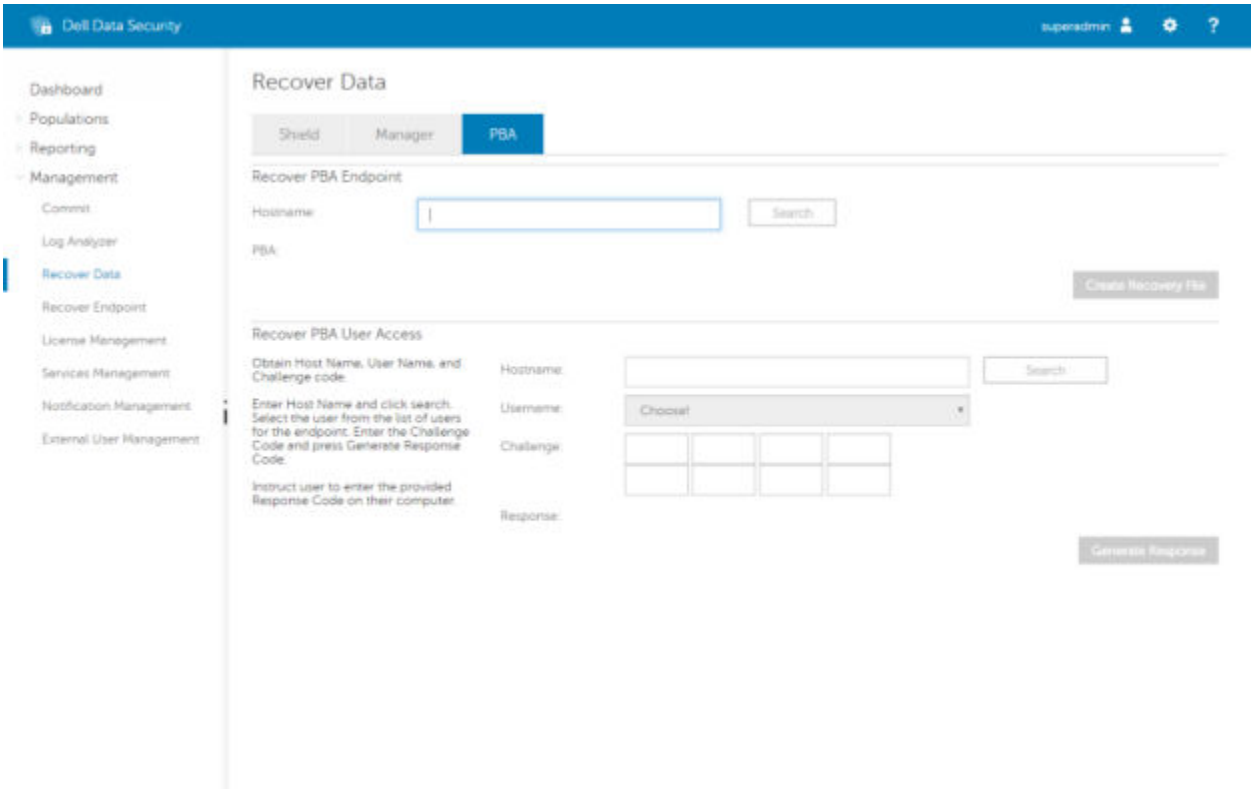
Users forget their passwords and call into the help desk regarding getting through the PBA environment. Use the Challenge/Response mechanism that is built-into the device. This is per-user and is based on a rotating set of alphanumeric characters. The user must enter their name in the **Username** field and then select **Options > Challenge Response**.



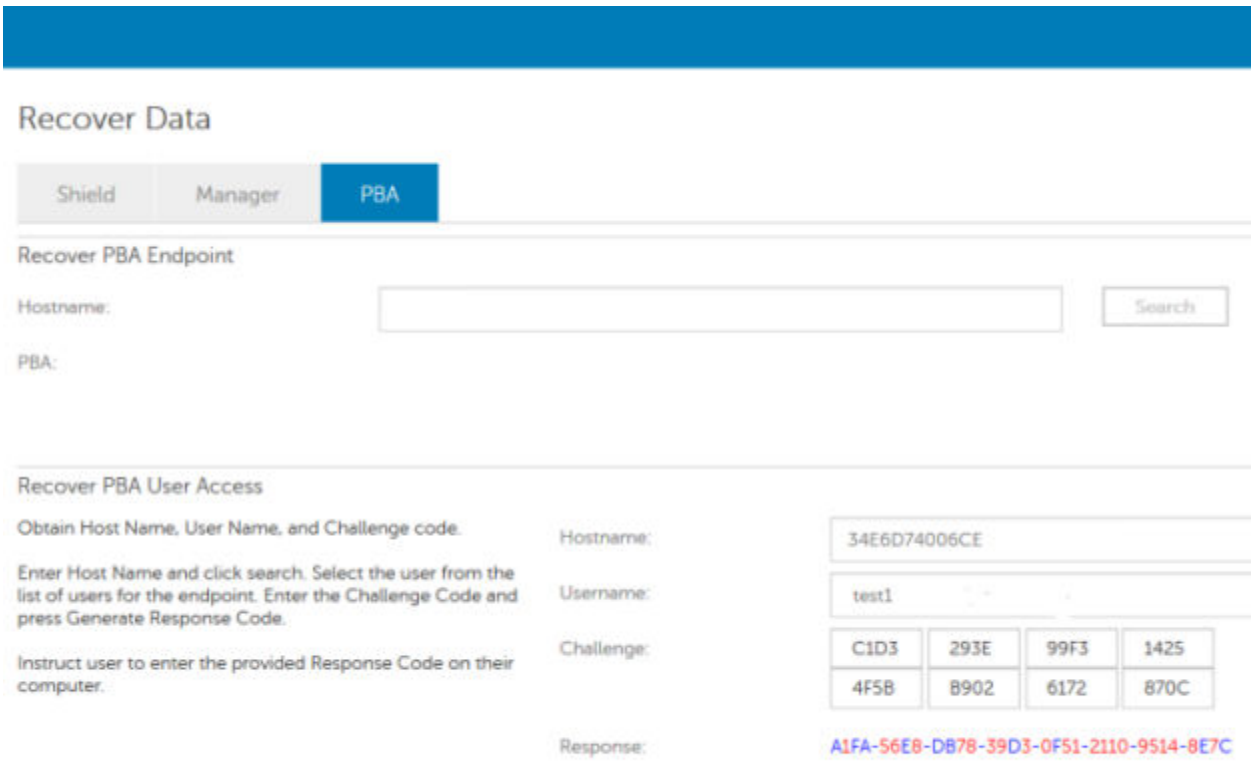
The following information appears after selecting **Challenge Response**.



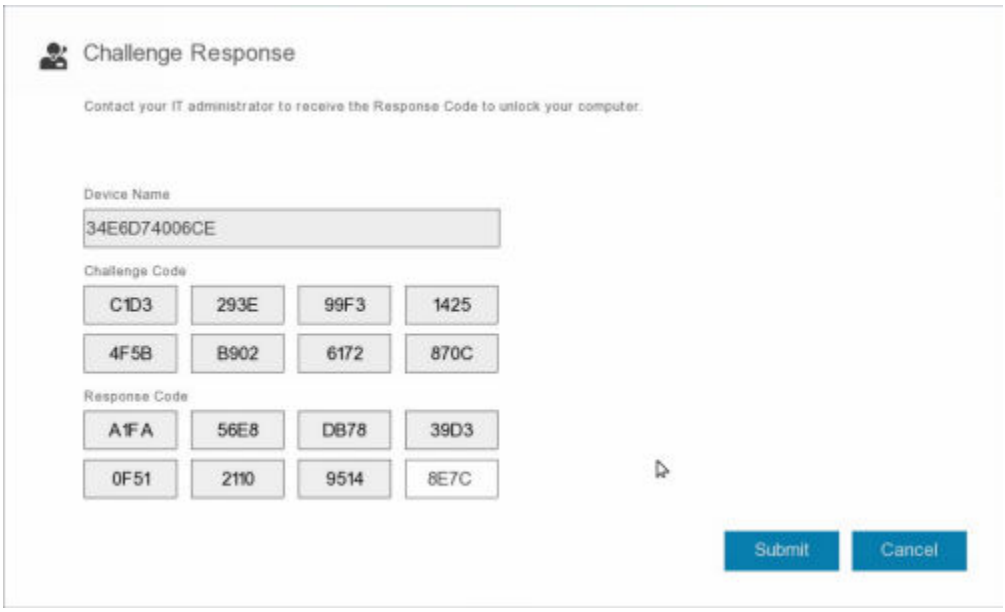
The **Device Name** field is used by the help desk technician within the Remote Management Console to find the correct device, and then a username is selected. This is found within **Management > Recover Data** under the **PBA** tab.



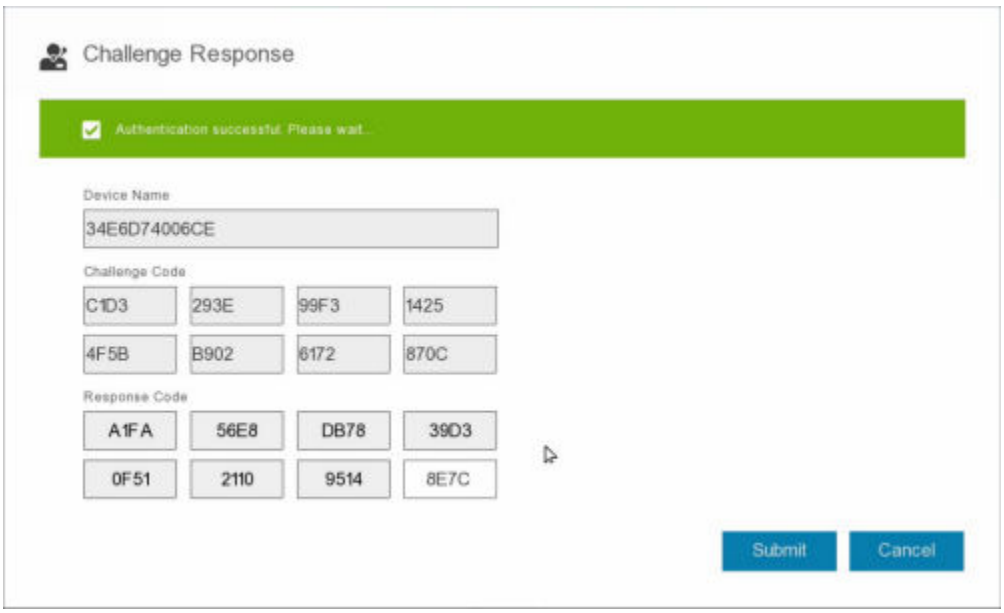
The Challenge Code is provided to the help desk technician who inputs the data, and then clicks the **Generate Response** button.



This resulting data is color-coordinated to help discern between numerals (red) and alphabet characters (blue). This data is read to the end user, who enters it into the PBA environment and then clicks the **Submit** button, moving the user into Windows.



After successful authentication, the following message appears:



Challenge recovery is complete.

6

Full Disk Encryption and Dell Encryption Recovery

This chapter details the recovery steps required to recover access to Dell Encryption protected files on a disk protected with Full Disk Encryption.

NOTE: Decryption should not be interrupted. If decryption is interrupted, data loss may occur.

Recovery Requirements

For Full Disk Encryption and Dell Encryption recovery, you need the following:

- Access to the recovery environment ISO
- Bootable CD\DVD or USB media

Overview of the Recovery Process

NOTE: Recovery requires a 64-bit environment.

To recover a failed system:

1 Burn the recovery environment onto a CD/DVD or create a bootable USB. See Appendix A - Burning the Recovery Environment.
2 Obtain the Recovery files for Dell Encryption and Full Disk Encryption.
3 Perform the recovery.

Perform Recovery of a Full Disk Encrypted and Dell Encrypted Disk

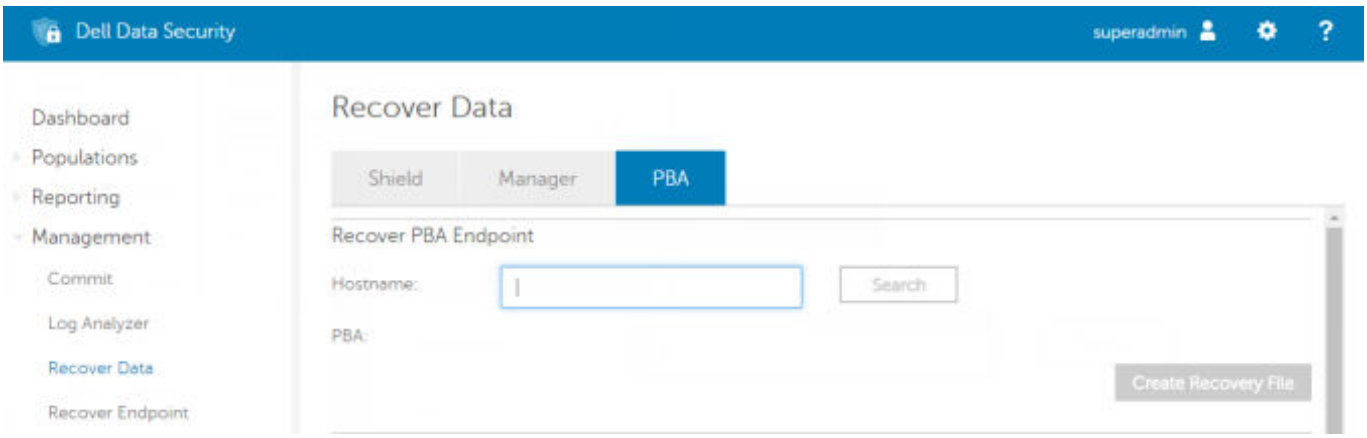
Follow these steps to perform recovery of a Full Disk Encrypted and Dell Encrypted disk.

Obtain the Recovery File - Full Disk Encryption Client

Obtain the recovery file.

Download the recovery file from the Remote Management Console. To download the *<hostname>-sed-recovery.dat* file that was generated when you installed Dell Data Security:

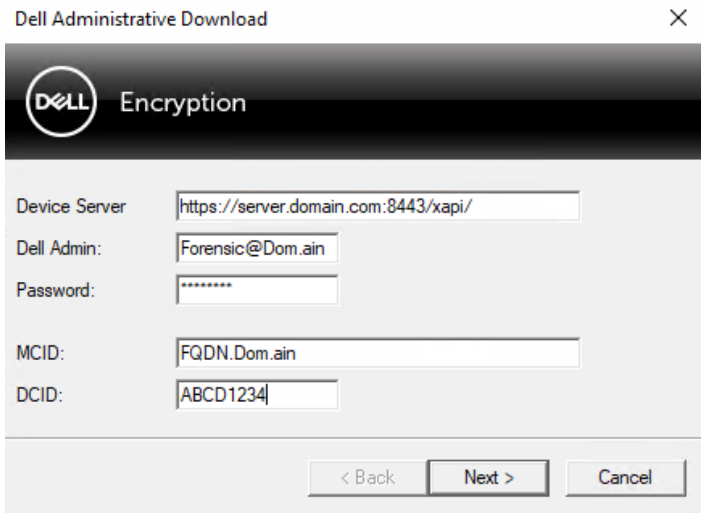
a Open the Remote Management Console and, from the left pane, select **Management > Recover Data** then select the **PBA** tab.
b On the Recover Data screen, in the Hostname field, enter the fully qualified domain name of the endpoint, then click **Search**.
c In the SED field, select an option.
d Click **Create Recovery File**.
The **<hostname>-sed-recovery.dat** file is downloaded.



Obtain the Recovery File - Policy-Based Encryption or FFE Encryption Client

To download the recovery file:

1 Download the Dell Encryption installation package from http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Navigate to the **AdminUtilities** folder in the installation package and open **CMGAd.exe**.



2 In the **Dell Server** field, enter the Security Management Server/Security Management Server Virtual the computer was activated against.

3 In the **Dell Admin** field, enter a user account name with Forensic Administrator privileges.

4 In the **Password** field, enter the password for the Forensic Administrator.

5 In the **MCID** field, enter the FQDN of the device being recovered.

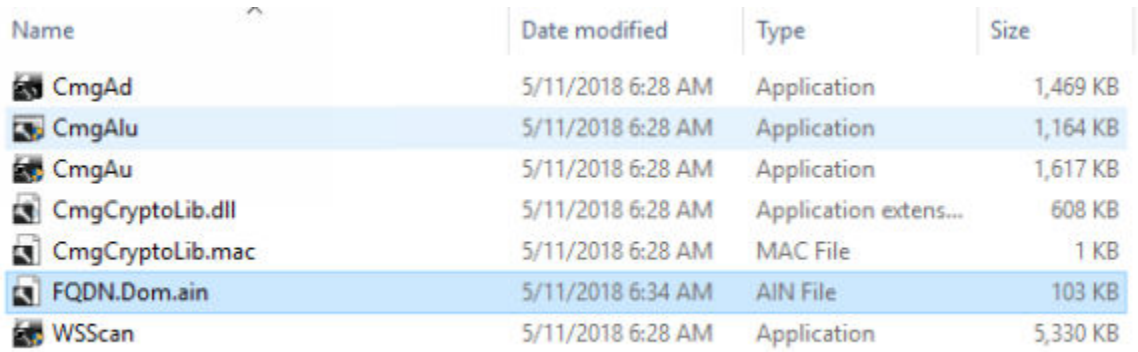
- The **DCID** field is the Recovery ID of the device being recovered.

6 Select **Next**.

7 Define and confirm a **Passphrase** for the recovery file. This Passphrase is needed to perform recovery.

8 In the **Download To:** field, enter a destination location for the recovery bundle then select **Next**. By default, this will be in the directory from which CMGAd.exe was run.

9 The recovery bundle downloads to the folder specified in **Download To:**.

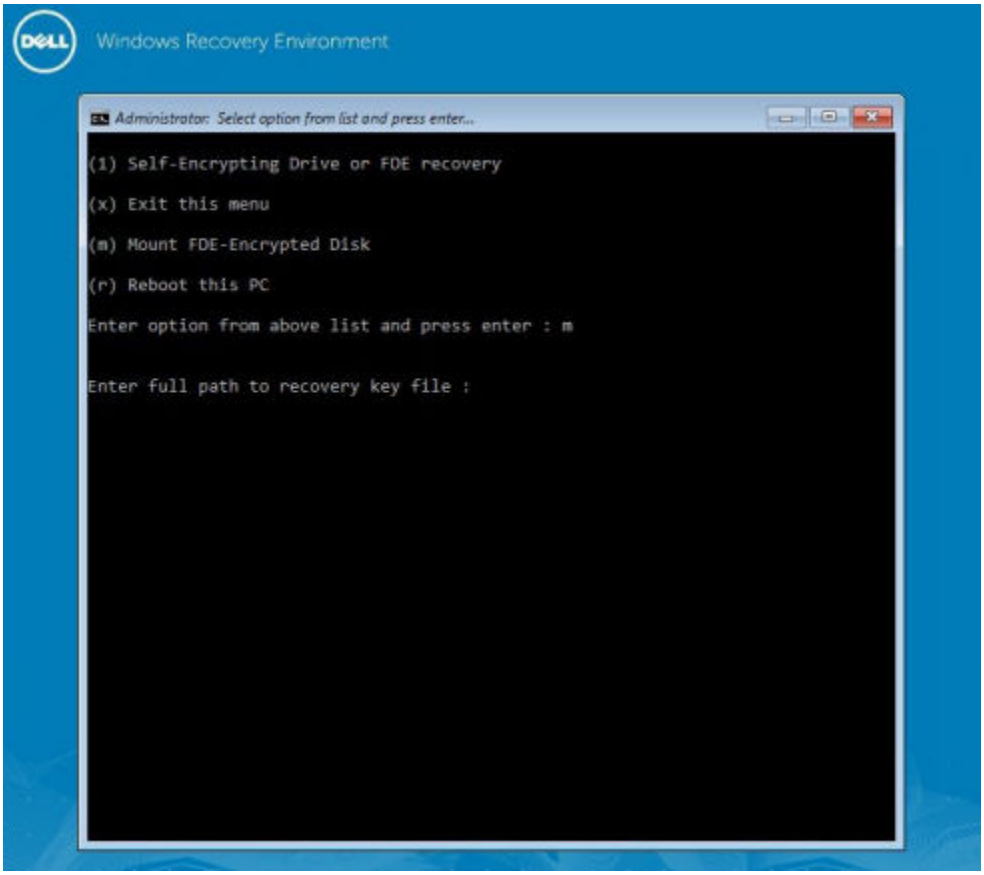


10 Copy the recovery bundle file to a location where it can be accessed when booted into WinPE.

Perform a Recovery

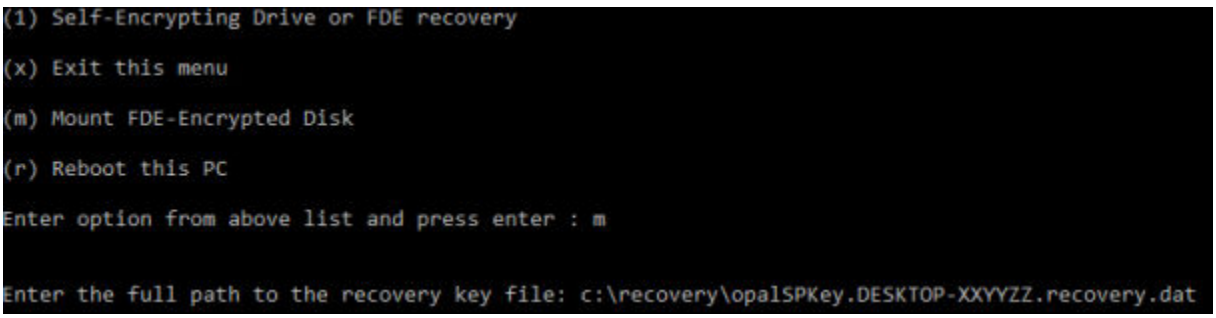
1 Using the bootable media created earlier, boot to that media on a recovery system or on the device with the drive you are attempting to recover. A WinPE environment opens with the recovery application.

NOTE: Disable SecureBoot before the recovery process. When finished, re-enable SecureBoot.



2 Choose option three and press **Enter**.

3 When prompted, Enter the recovery file name and location .



4 Using the Recovery Key, the Full Disk encrypted disk is mounted.

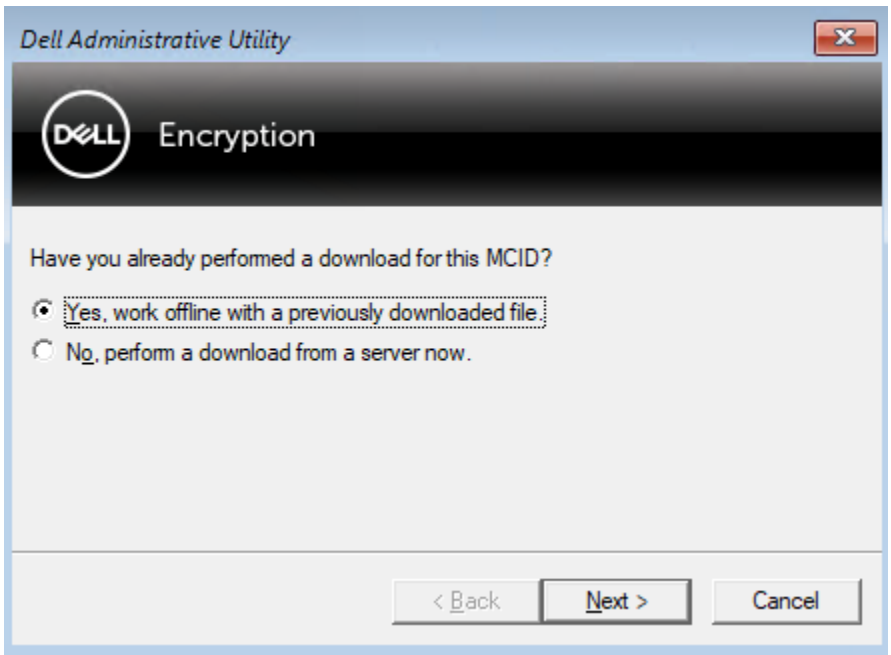
```
Enter option from above list and press enter : m


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
```

.

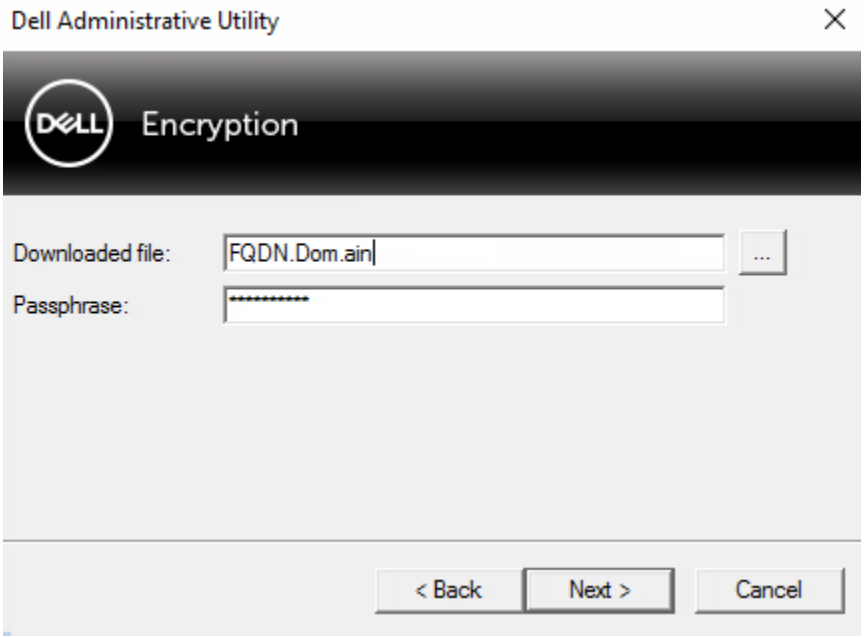
5 Navigate to the CMGAu.exe utility using the following command: `cd DDPEAdminUtilities\`

6 Launch the CMGAu.exe using the following command: `\DDPEAdminUtilities>CmgAu.exe`

Select **Yes, work offline with a previously downloaded file**.



7 In the **Downloaded file:** field, enter the location of the **Recovery Bundle** then enter the **Passphrase** of the Forensic Administrator and select **Next**.



When recovery is complete, click **Finish**.

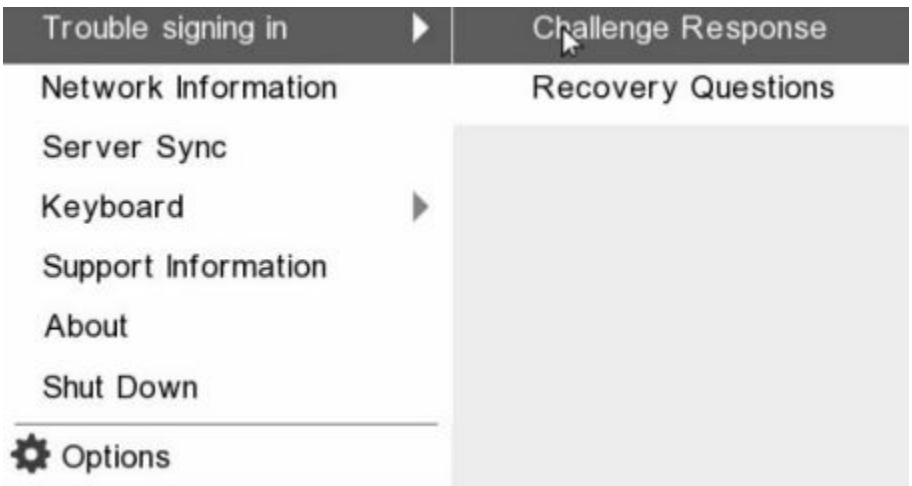
NOTE:
Be sure to remove any USB or CD\DVD media that was used to boot the computer. Failure to do this may result in booting back into the recovery environment.

8 After the computer reboots, you should have access to encrypted files. If problems persist, contact Dell ProSupport.

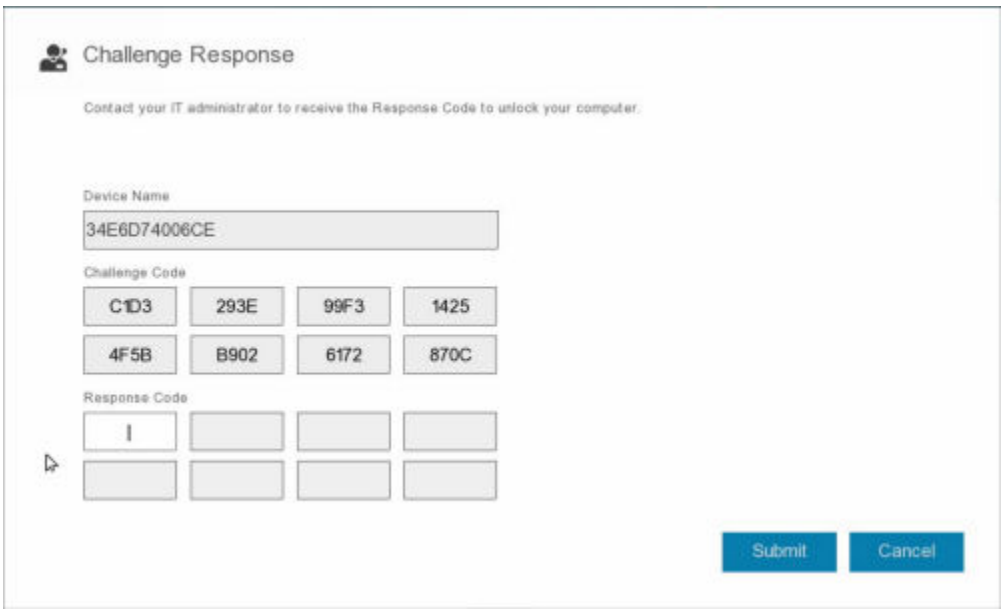
Challenge Recovery with Full Disk Encryption

Bypass the Preboot Authentication Environment

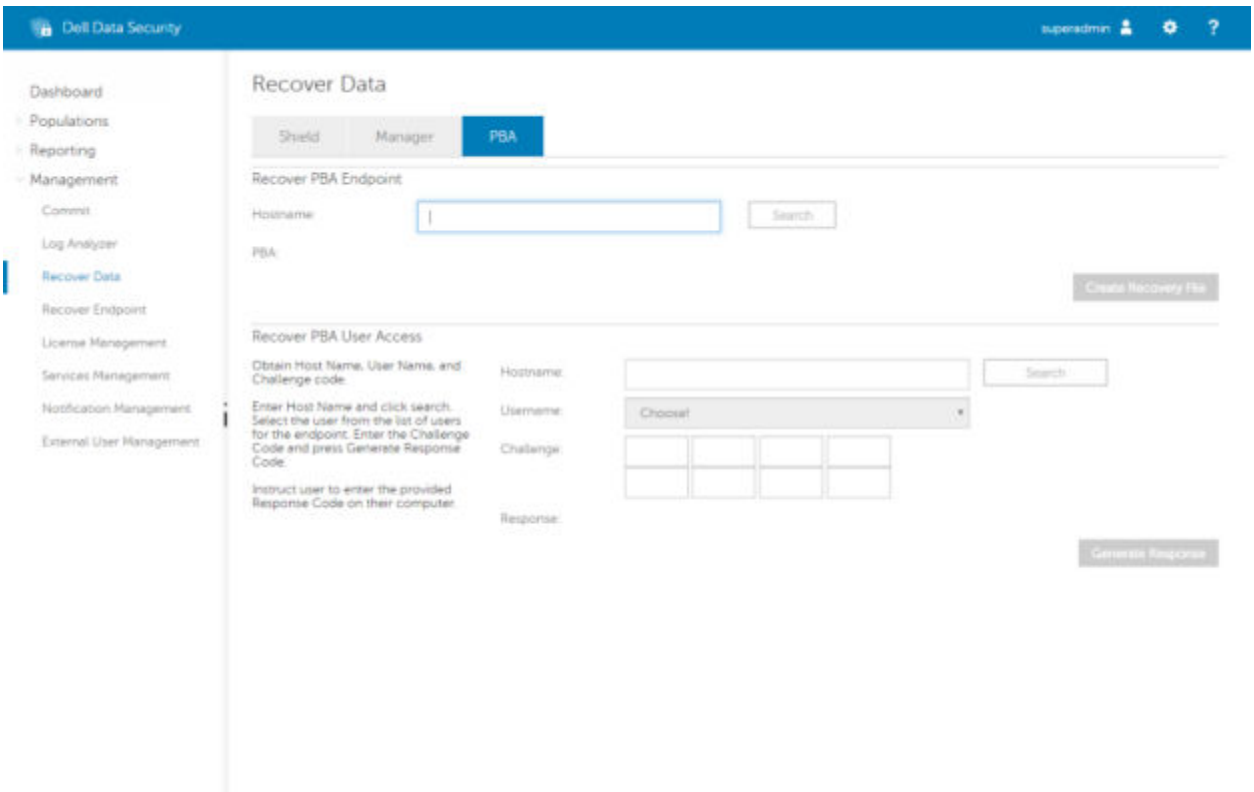
Users forget their passwords and call into the help desk regarding getting through the PBA environment. Use the Challenge/Response mechanism that is built-into the device. This is per-user and is based on a rotating set of alphanumeric characters. The user must enter their name in the **Username** field and then select **Options > Challenge Response**.



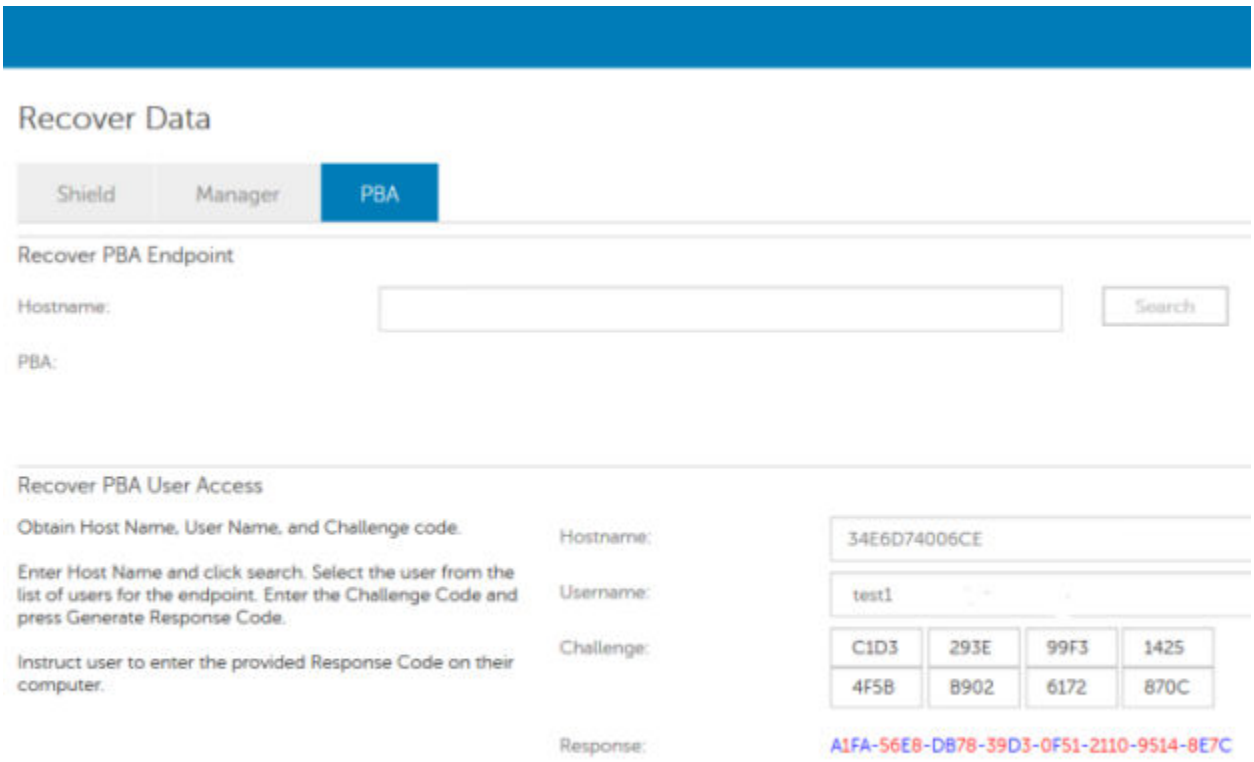
The following information appears after selecting **Challenge Response**.



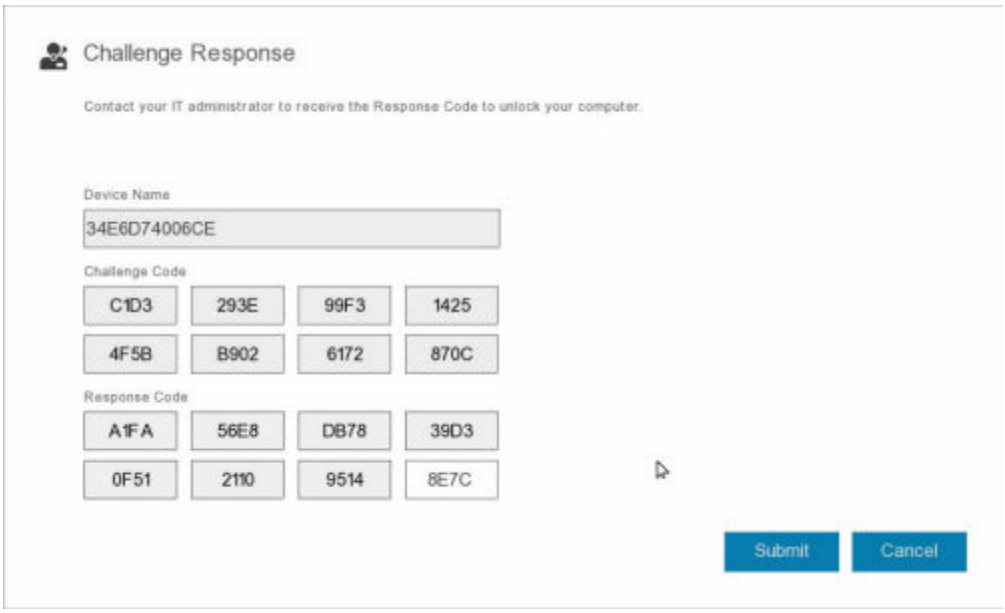
The **Device Name** field is used by the help desk technician within the Remote Management Console to find the correct device, and then a username is selected. This is found within **Management > Recover Data** under the **PBA** tab.



The Challenge Code is provided to the help desk technician who inputs the data, and then clicks the **Generate Response** button.



This resulting data is color-coordinated to help discern between numerals (red) and alphabet characters (blue). This data is read to the end user, who enters it into the PBA environment and then clicks the **Submit** button, moving the user into Windows.



After successful authentication, the following message appears:

Challenge recovery is complete.

7

PBA Device Control

PBA Device Control applies to endpoints encrypted with SED or Full Disk Encryption.

Use PBA Device Control

PBA commands for a specific endpoint are carried out in the PBA Device Control area. Each command has a priority ranking. A command with a higher priority rank cancels commands of lower priorities in the enforcement queue. For a list of command priority rankings, see *AdminHelp* available by clicking the ? in the Remote Management Console. The PBA Device Controls are available on the Endpoint Details page of the Remote Management Console.

The following commands are available in PBA Device Control:

- **Lock** - Locks the PBA screen and prevents any user from logging into the computer.
- **Unlock** - Unlocks the PBA screen after it has been locked on this endpoint, either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.
- **Remove Users** - Removes all users from the PBA.
- **Bypass Login** - Bypasses the PBA screen one time to allow a user into the computer without authenticating. The user will still need to login to Windows after PBA has been bypassed.
- **Wipe** - The Wipe command functions as a “restore to factory state” for the encrypted drive. The Wipe command can be used to re-purpose a computer or, in an emergency situation, wipe the computer, making the data permanently unrecoverable. Ensure that this is the desired behavior before invoking this command. For Full Disk Encryption, the Wipe command cryptographically erases the drive and the PBA is removed. For SED, the Wipe command cryptographically erases the drive and the PBA displays "Device Locked". To re-purpose the SED, remove the PBA with the SED Recovery app.

8

General Purpose Key Recovery

The General Purpose Key (GPK) is used to encrypt part of the registry for domain users. However, during the boot process, in rare cases, it might become corrupted and fail to unseal. If so, the following errors display in the CMGShield.log file on the client computer:

```
[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
```

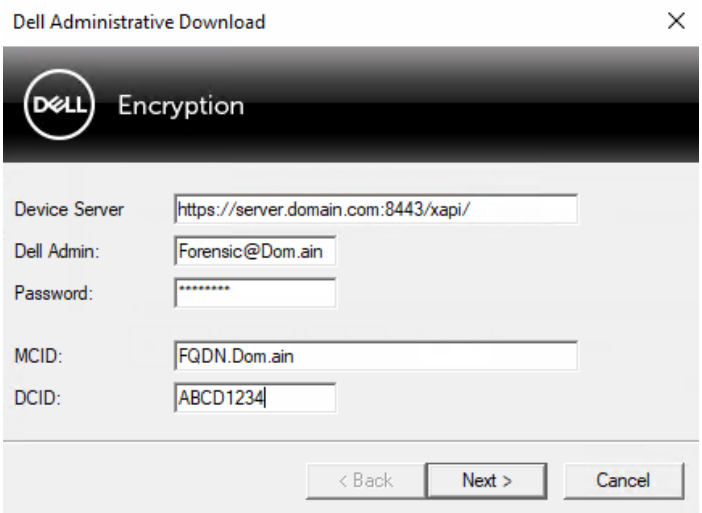
If the GPK fails to unseal, the GPK must be recovered by extracting it from the recovery bundle that is downloaded from the Dell Server.

Recover the GPK

Obtain the Recovery File

To download the **<machinename_domain.com>.exe** file that was generated when you installed Dell Data Security:

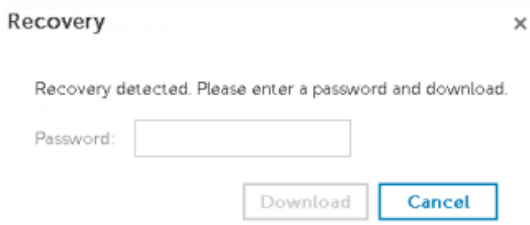
1 Open the Remote Management Console and, from the left pane, select **Management** > **Recover Endpoint**.



2 In the Hostname field, enter the fully qualified domain name of the endpoint and click **Search**.

3 In the Recovery window, enter a recovery Password and click **Download**

NOTE:
You must remember this password to access the recovery keys.



The **<machinename_domain.com>.exe** file is downloaded.

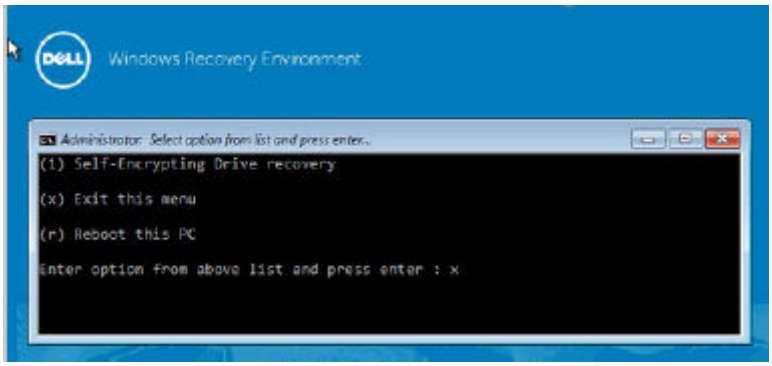
Perform a Recovery

1 Create bootable media of the recovery environment. For instructions, see Appendix A - Burning the Recovery Environment.

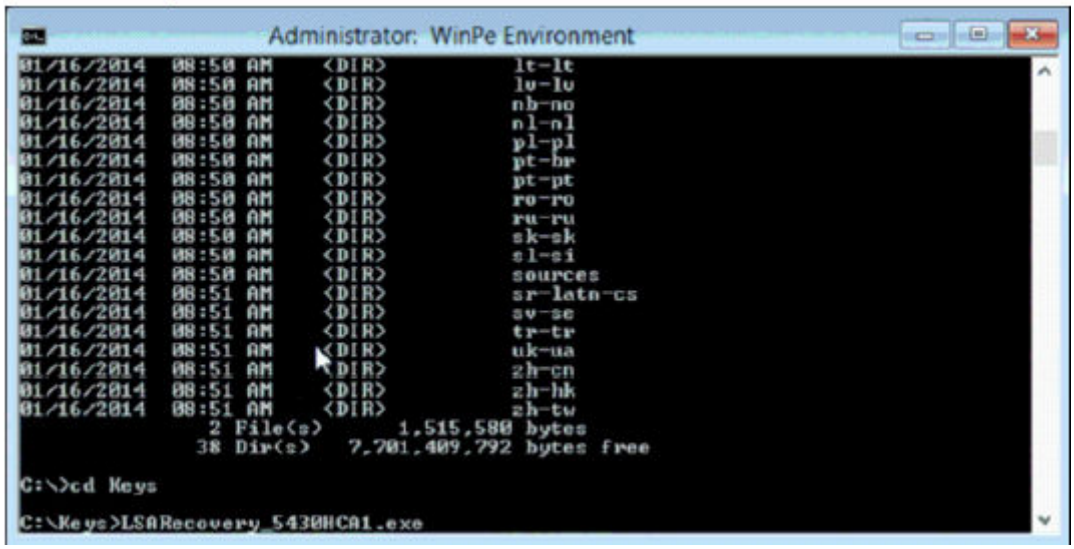
NOTE: Disable SecureBoot before the recovery process. When finished, enable SecureBoot.

2 Boot to that media on a recovery system or on the device with the drive you are attempting to recover.
A WinPE Environment opens.

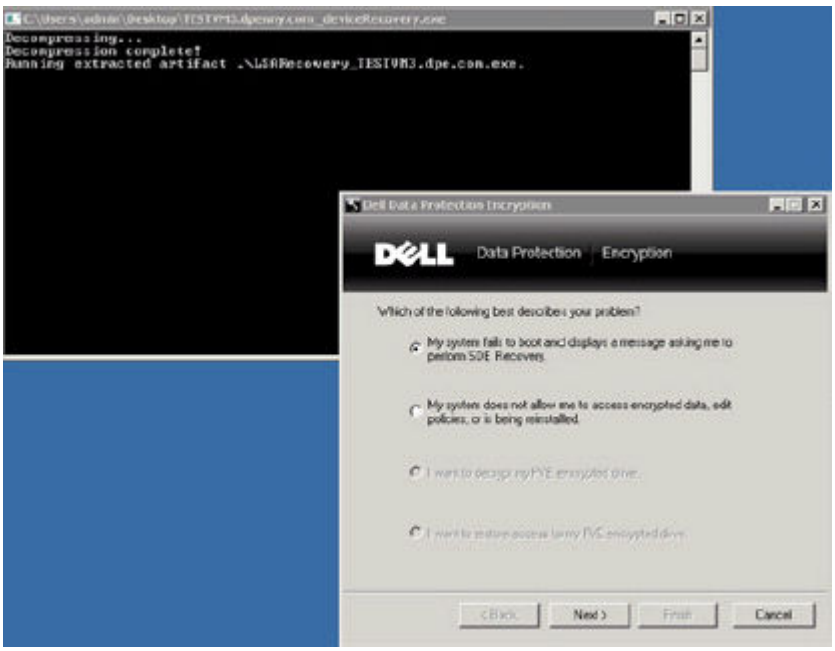
3 Enter **x** and press **Enter** to get to a command prompt.



4 Navigate to the recovery file and launch it.

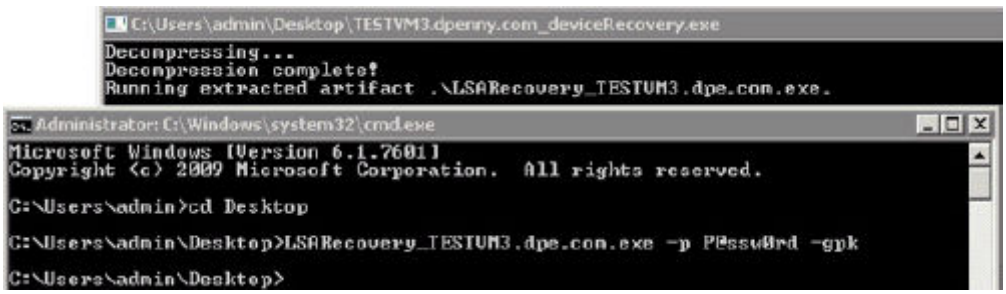


An Encryption client diagnostic dialog opens and the recovery file is being generated in the background.



5 At an administrative command prompt, run **<machinename_domain.com** > **.exe** > **-p <password** > **-gpk**

It returns the GPKRCVR.txt for your computer.



6 Copy the **GPKRCVR.txt** file to the root of the OS drive of the computer.

7 Reboot the computer.

The GPKRCVR.txt file will be consumed by the operating system and will regenerate the GPK on that computer.

8 If prompted, reboot again.

9

BitLocker Manager Recovery

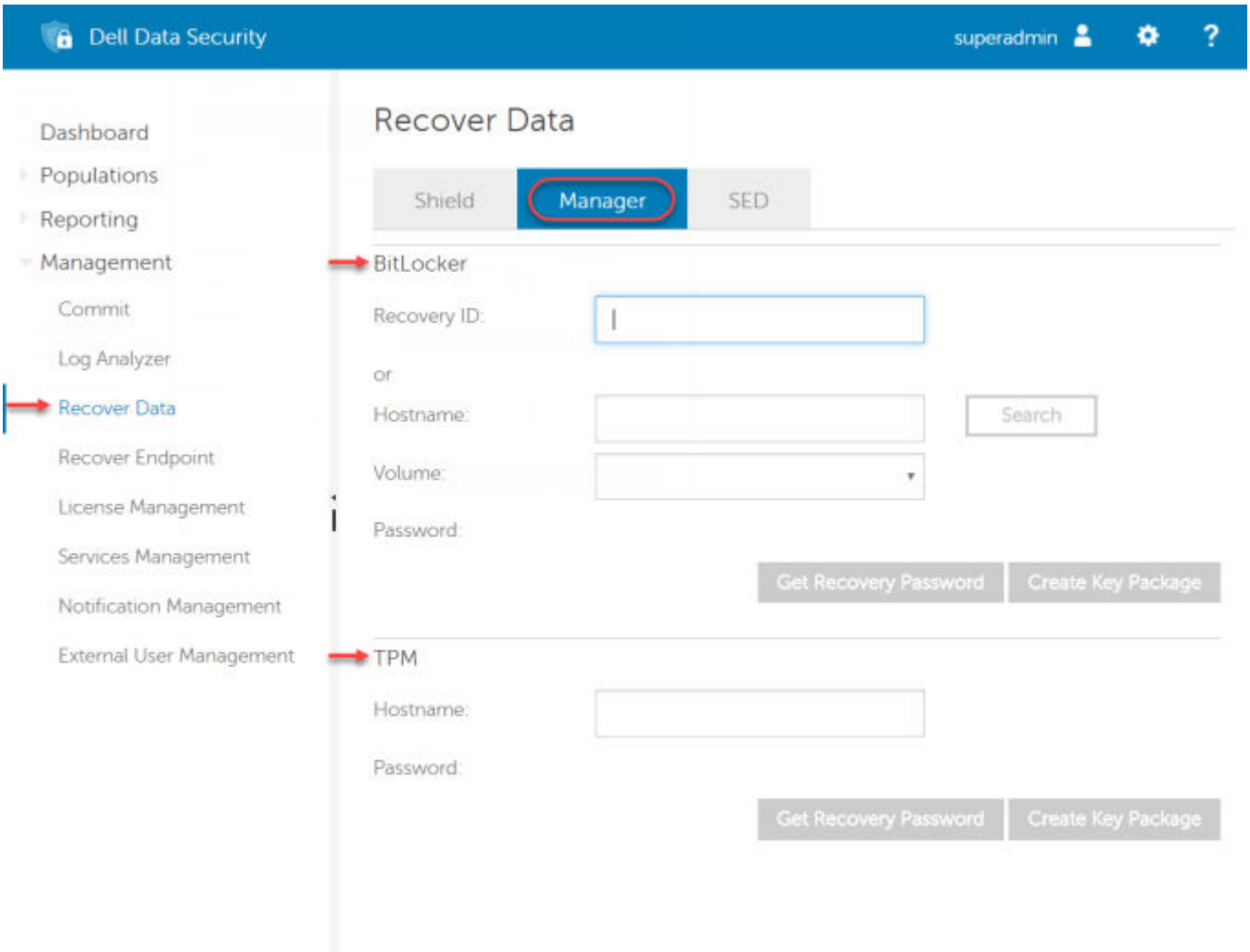
To recover data, you obtain a recovery password or key package from the Remote Management Console, which then allows you to unlock data on the computer.

Recover Data

1 As a Dell Administrator, log in to the Remote Management Console.

2 In the left pane, click **Management** > **Recover Data**.

3 Click the **Manager** tab.



4 For *BitLocker*:

Enter the **Recovery ID** received from BitLocker. Optionally, if you enter the Hostname and Volume, the Recovery ID is populated.

Click **Get Recovery Password** or **Create Key Package**.

Depending on how you want to recover, you will use this recovery password or key package to recover data.

For the *TPM*:

Enter the **Hostname**.

Click **Get Recovery Password** or **Create Key Package**.

Depending on how you want to recover, you will use this recovery password or key package to recover data.

5 To complete the recovery, see Microsoft's Instructions for Recovery.

NOTE:

If BitLocker Manager does not "own" the TPM, the TPM password and key package are not available in the Dell database. You will receive an error message stating that Dell cannot find the key, which is the expected behavior.

To recover a TPM that is "owned" by an entity other than BitLocker Manager, you should follow the process to recover the TPM from that specific owner or follow your existing process for the TPM recovery.

10

Password Recovery

Users commonly forget their password. Fortunately, there are multiple ways for users to regain access to a computer with Preboot Authentication when they do.

- The Recovery Questions feature offers question- and- answer-based authentication.
- Challenge/Response Codes lets users work with their Administrator to regain access to their computer. This feature is available only to users who have computers that are managed by their organization.

Recovery Questions

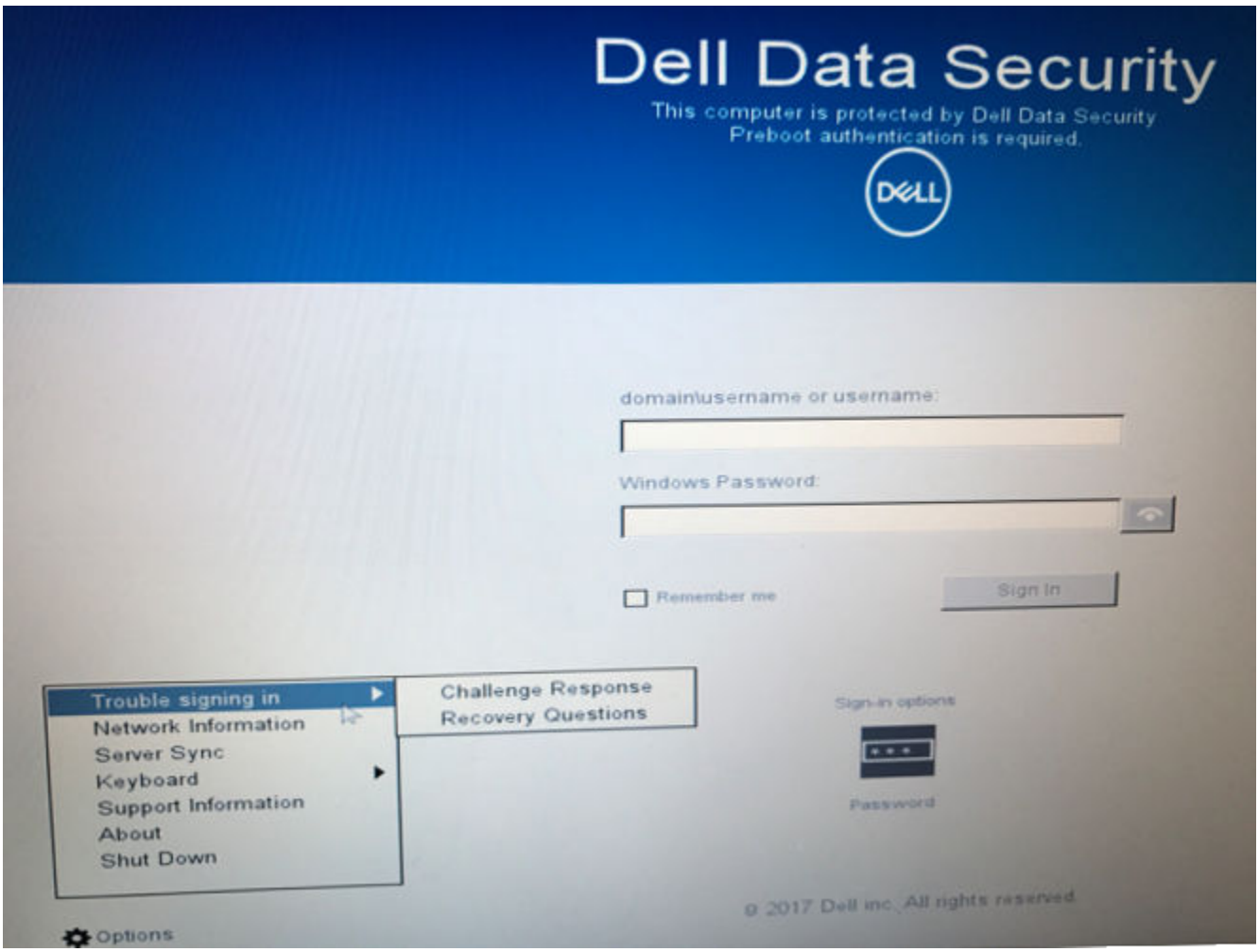
The first time a user signs in to a computer, he is prompted to answer a standard set of questions that the Administrator has configured. After enrolling his answers to these questions, the next time he forgets his password, the user is prompted for the answers. Assuming he has answered the questions correctly, he is able to sign in and regain access to Windows.

Prerequisites

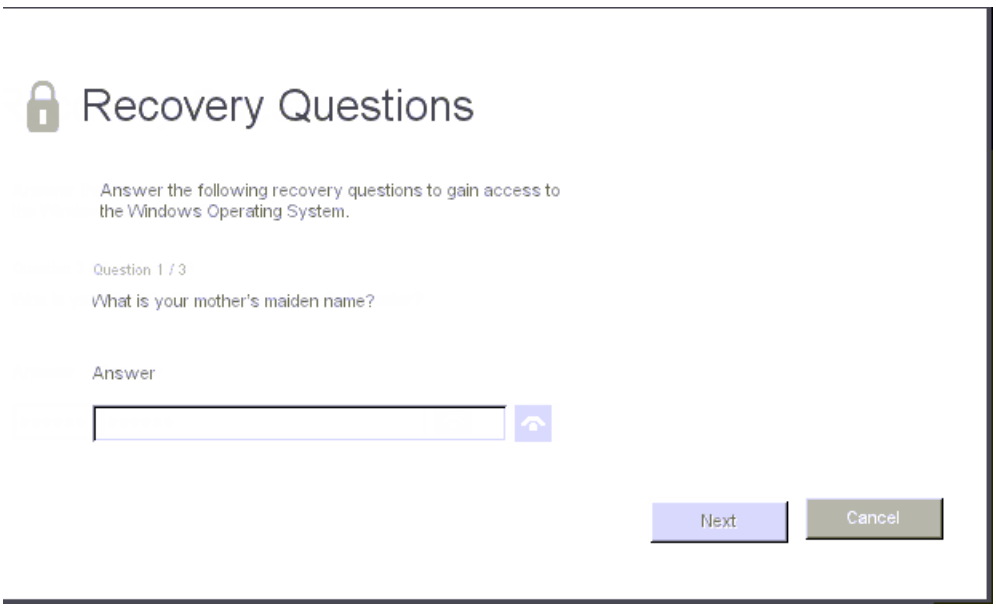
- Recovery Questions must be set up by the Administrator.
- The user must have enrolled his answers to the questions.
- Before clicking the **Trouble Signing In** menu option, the user must enter a valid user name and domain.

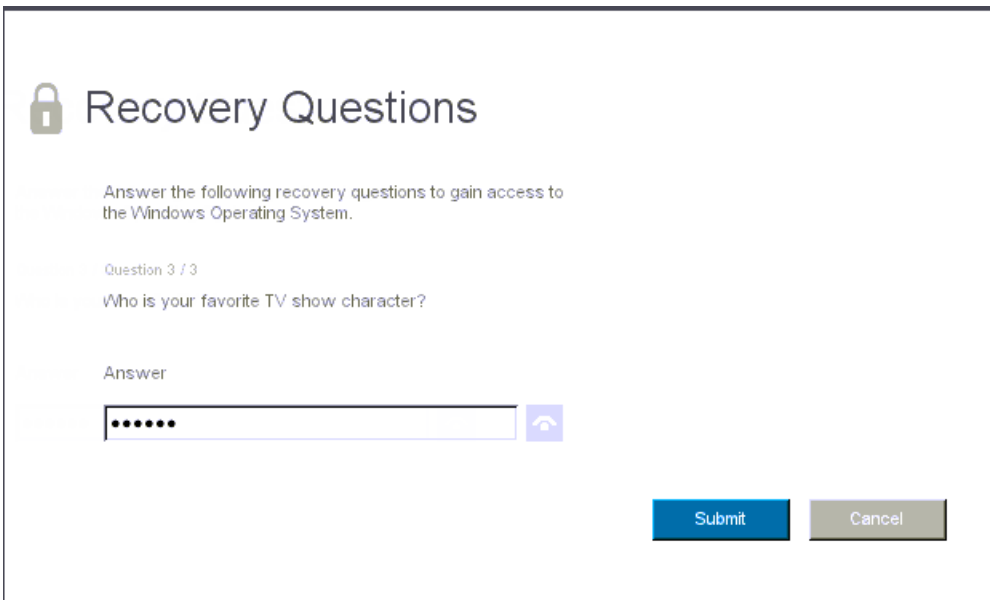
To access the Recovery Questions from the PBA sign-in screen:

1 Enter a valid domain name and user name.
2 At the bottom left side of the screen, click **Options** > **Trouble Signing In**.



3 When the Q&A dialog appears, enter the answers that you supplied when you enrolled in Recovery Questions the first time you signed in.




Recovery Questions
Answer the following recovery questions to gain access to the Windows Operating System.
Question 3 / 3
Who is your favorite TV show character?
Answer
Submit
Cancel

Encryption External Media Password Recovery

Encryption External Media gives you the ability to protect removable storage media both in and outside of your organization by allowing users to encrypt USB flash drives and other removable storage media. The user assigns a password to each removable media device they want to protect. This section describes the process for recovering access to an encrypted USB storage device when a user forgets a device's password.

Recover Access to Data

When a user incorrectly types his password so many times that he exceeds the allowed number of password attempts, the USB device is placed into Manual Authentication mode.

Manual Authentication is the process of providing codes from the client to an administrator who is logged into the Dell Server.

When in Manual Authentication mode, the user has two options to reset his password and recover access to his data.

The administrator provides an Access Code to the client, allowing the user to reset his password and regain access to his encrypted data.

1 When prompted for your password, click the **I Forgot** button.

The confirmation dialog appears.

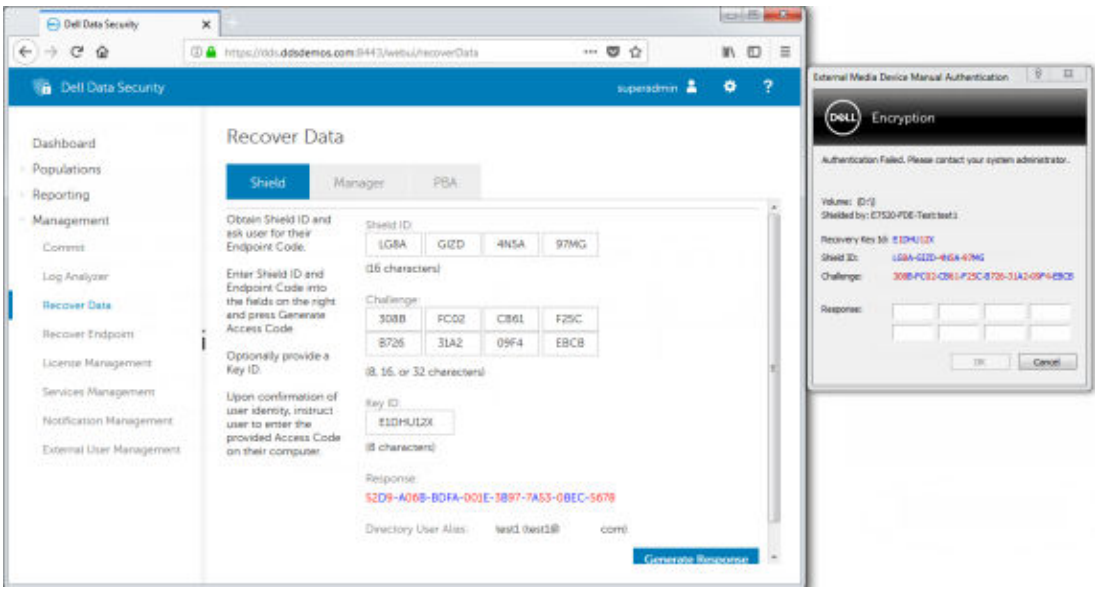
2 Click **Yes** to confirm. After confirmation, the device goes into Manual Authentication mode.

3 Contact the Help Desk Administrator and give him the codes that appear in the dialog.

4 As a Help Desk Administrator, log into the Remote Management Console - the Help Desk Administrator's account must have Help Desk privileges.

5 Navigate to the **Recover Data** menu option on the left pane.

6 Enter the codes provided by the end-user.

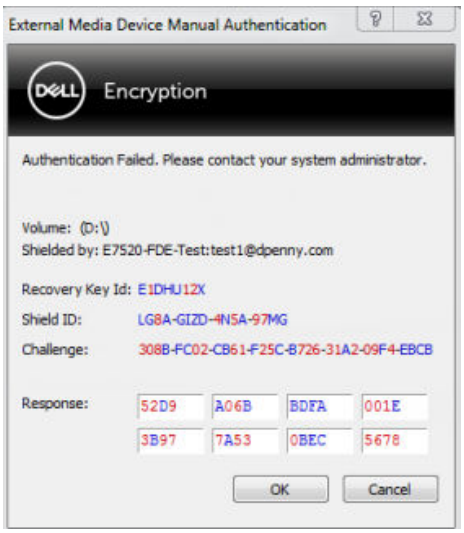


7 Click the **Generate Response** button at the bottom right-hand corner of the screen.

8 Give the user the Access Code.

NOTE:

Be sure to manually authenticate the user prior to providing an Access Code. For example, ask the user a series of questions over the phone that only that person would know, such as "What is your employee ID number?" Another example: request that the user come to the Help Desk to provide identification to ensure they are the owner of the media. Failure to authenticate a user prior to providing an Access Code over the phone could allow an attacker to gain access to encrypted removable media.



9 Reset your password for the encrypted media.

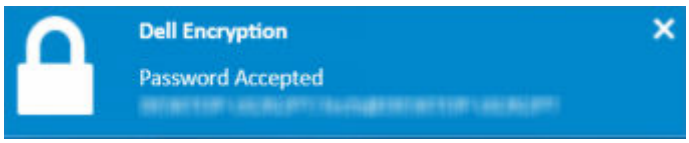
The user is prompted to reset his password for the encrypted media.

Self-Recovery

The drive must be inserted back into the machine that originally encrypted it for the Self-Recovery to work. As long as the media owner is authenticated to the protected Mac or PC, the client detects the loss of key material and prompts the user to re-initialize the device. At that time, the user can reset their password and regain access to their encrypted data. This process may resolve issues with partially corrupted media.

1 Sign in to a Dell Data Security encrypted workstation as the media owner.
2 Insert the encrypted removable storage device.
3 When prompted, enter a new password to re-initialize the removable storage device.

If successful, a small notification appears to indicate that the password was accepted.



4 Navigate to the storage device and confirm access to the data.

12

Dell Data Guardian Recovery

The recovery tool allows:

- Decryption of:
  - Dell Data Guardian Protected Office files with any supported format - Protected Office Document encryption, Data Classification encryption, or Cloud Service Provider protection.
  - Files formats listed in the Basic File Protection policy, if enabled.
- Manual escrow of key material
- Ability to check for tampered files
- Ability to force decryption of protected Office documents where someone tampered with the file's wrapper, for example, the protected Office file's cover page in the cloud or on a device that does not have Data Guardian

NOTE:
You can use the Windows Recovery Tool with files created on Mac, mobile, or web portal platforms.

Prerequisites

Prerequisites include:

- Microsoft .Net Framework 4.5.2 running on the endpoint to be recovered.
- The forensic administrator role must be assigned in the Management Console for the administrator performing the recovery.

Perform Data Guardian Recovery

Follow these steps to perform a recovery of Data Guardian's protected Office documents. You can recover one computer at a time.

IMPORTANT:
To avoid losing content in case of corruption, decrypt copies of the files, not the original files.

Perform a Recovery from Windows, a USB Flash Drive, or Network Drive

To perform a recovery:

1 From the Dell installation media, copy **RecoveryTools.exe** to one of these:

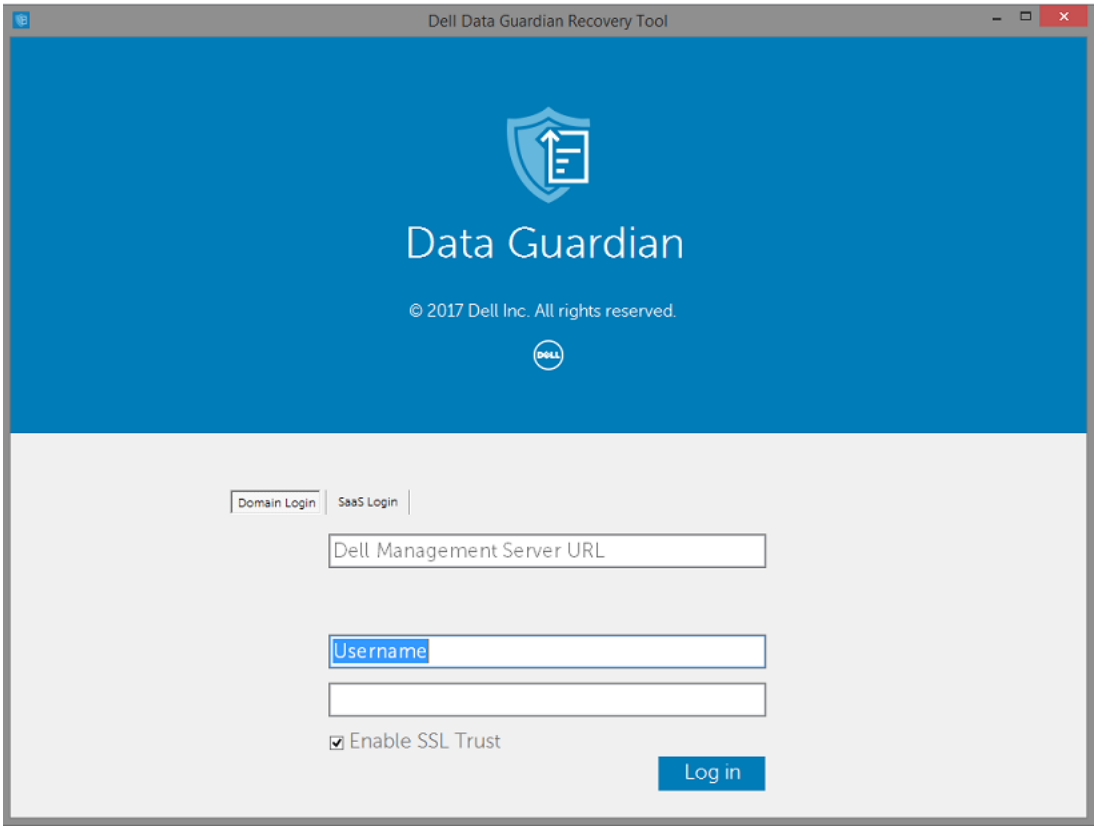
- Computer - Copy the .exe to the computer on which Office documents will be recovered.
- USB - Copy the .exe to the USB flash drive and run it from the USB flash drive.
- Network drive

IMPORTANT:
As administrator, be sure to copy only the **RecoveryTools.exe** and not the installer. The **RecoveryTools.exe** performs better if no sweep or decryption is running.

2 Double-click **RecoveryTools.exe** to launch the recovery tool.

3 On the Data Guardian Recovery Tool window, select **Domain Login**.

NOTE:
The SaaS Login option for a hosted solution is for a future release.



4 Enter the Dell Server FQDN in this format:
server.domain.com

NOTE:
A prefix and suffix are automatically added to the FQDN.

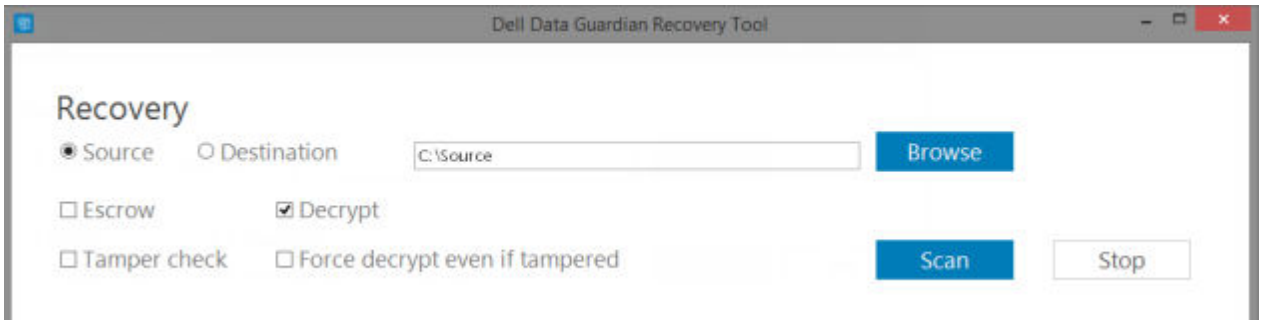
5 Enter the user name in UPN format and the password.

Click **Log in**.

NOTE:
Do not clear the *Enable SSL Trust* check box unless your administrator tells you to.

NOTE:
If you are not a forensic administrator and enter credentials, a message displays indicating you do not have login rights.

6 If you are a forensic administrator, the recovery tool opens.



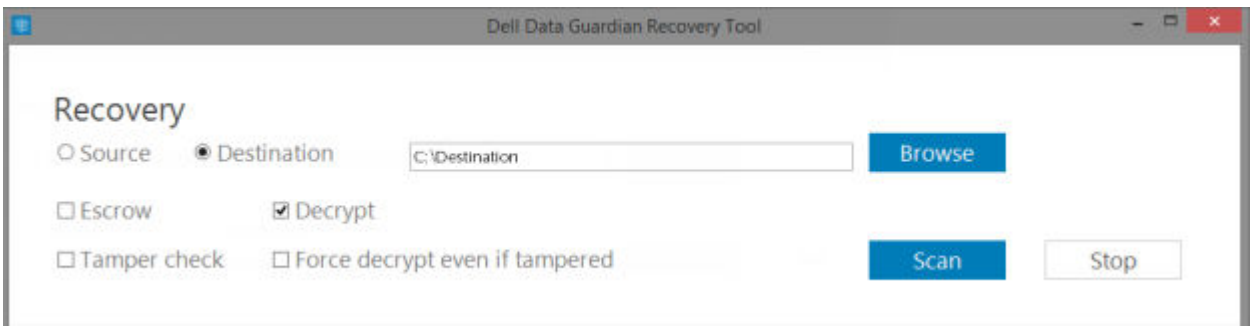
7 Select **Source**.

> **NOTE:**
> You must browse to a source and a destination, but you can select these in either order.

8 Click **Browse** to select the folder or drive to be recovered.

9 Click **OK**.

10 Click **Destination**, an empty folder for the decrypted or recovered files.



11 Click **Browse** to select a destination, such as an external device, a directory location, or the Desktop.

12 Click **OK**.

13 Select one or more check boxes based on what you want to recover.

Options	Description
Escrow	• Recover offline-generated keys that could not be escrowed to the Dell Server. • If a hard drive fails while the user is offline from the network, use the slaved drive to recover data and non-escrowed keys from the computer.
Decrypt	Point the recovery tool to a directory that contains protected Office documents to decrypt them. **NOTE:** As a best practice, decrypt copies of the files, not originals, in case corruption occurs. Optionally, if tampering has occurred, select one or both of these options (see below for details): • **Tamper check** - checks for tampered files but does not decrypt them. • **Tamper check** and **Force decrypt even if tampered** - checks for tampered files and if the wrapper of a protected Office document was tampered with, Data Guardian repairs the wrapper and decrypts the Office document.

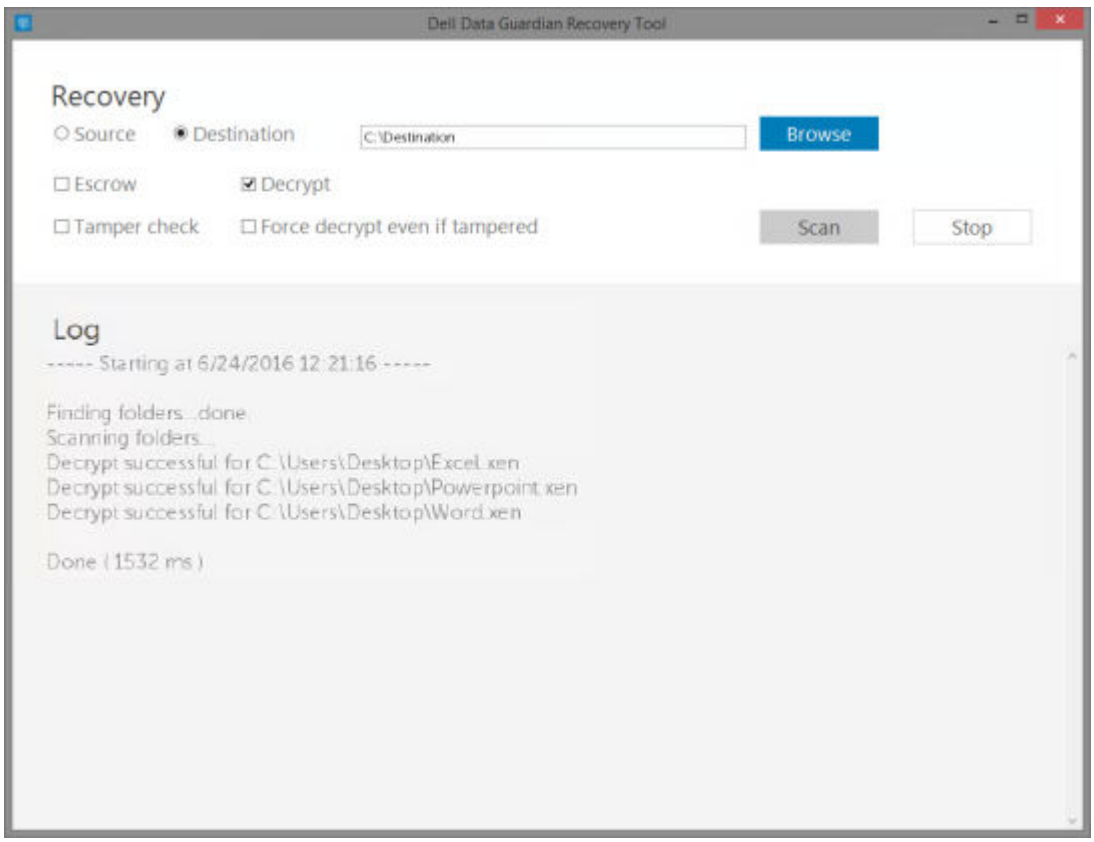
Options	Description
Tamper check	Detects files that have been tampered with and logs them or notifies you. Logs the author that tampered with the file. It does not decrypt the files.
Force decrypt even if tampered	To select this option, you must also select **Tamper check**. If an unauthorized person tampered with the wrapper of a protected Office document, such as the cover page, either in the cloud or on a device that does not have Data Guardian, select this option to repair the wrapper and to force decryption of the protected Office file. **NOTE:** If someone tampered with the encrypted Office .xen file within the wrapper, the file cannot be recovered.

Each protected Office document has a hidden watermark that contains a history of the original user and computer name and any other computer name that modified the file. By default, the recovery tool checks the hidden watermarks and adds a text file with a list of all authors to a *HiddenWatermark* folder in the logs.

14 After selections are complete, click **Scan**.

The Log area displays:

- Folders found and scanned within the selected source
- Whether decryption, per file, was successful or failed
- The name of the last author of a file



The recovery tool adds the recovered files to the selected destination. You can open and view the files

View data from Hidden Audit Trail

For Windows, if the Hidden Audit Trail policy for protected Office documents is enabled, user information is captured in the file metadata. To view this data, use the Recovery Tool:

1 Launch the Recovery Tool.
   - For **Source**, browse to a folder that contains protected Office documents with hidden audit data. The Recovery Tool copies the folder and subfolder structure, decrypting any protected Office documents that have hidden audit data.
   - Before browsing to a **Destination**, you can create a folder, Decrypted files, and then browse to that.
2 Select **Decrypt**.
3 After selections are complete, click **Scan**.

   The folder selected as the Destination contains a dated *Recovered Files* folder with the following:
   - Decrypted protected Office files
   - *Audit Trail* folder, created by the Recovery Tool, with a .txt file for each decrypted file. Each .txt file has a log that lists information of the decrypted file, such as authors, last author, time stamps.

Appendix A - Burning the Recovery Environment

You can download the Master Installer.

Burning the Recovery Environment ISO to CD\DVD

The following link contains the process needed to use Microsoft Windows 7, Windows 8, or Windows 10 to create a bootable CD or DVD for the recovery environment.

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

Burning the Recovery Environment on Removable Media

To create a bootable USB, us the following instructions:

Legacy boot:

1 Connect a USB drive to the system.
2 Open an administrative command prompt.
3 Enter the Diskpart utility by typing **diskpart**.
4 Find the target disk to modify by typing **list disk**. Disks will be designated by number.
5 Select the appropriate disk using the command **select disk #** where # is the disk number to corresponding drive indicated by the previous step.
6 Wipe the disk by issuing a **clean** command. This will purge the drive of data by wiping the File Table.
7 Create a partition for the boot image to reside.
   a The **create partition primary** command generates a primary partition on the drive.
   b The **select partition 1** command select the new partition.
   c Use the following command to quick format the drive with the NTFS file system: **format FS=NTFS quick**.
8 The drive must be marked as a bootable drive. Use the **active** command to mark the drive as bootable.
9 To move files directly to the drive, assign an available letter to the drive with the **assign** command.
10 The drive will automatically mount, and the contents of the ISO file can be copied to the root of the drive.

After the ISO contents have completely copied, the drive is bootable and can be used for recovery.

EUFI Boot:

1 Connect a USB drive to the system.
2 Open an administrative command prompt.
3 Enter the Diskpart utility by typing **diskpart**.
4 Find the target disk to modify by typing **list disk**. Disks will be designated by number.
5 Select the appropriate disk using the command **select disk #** where # is the disk number to corresponding drive indicated by the previous step.
6 Wipe the disk by issuing a **clean** command. This will purge the drive of data by wiping the File Table.
7 Create a partition for the boot image to reside.

a The **create partition primary** command generates a primary partition on the drive.

b The **select partition 1** command select the new partition.

c Use the following command to quick format the drive with the FAT32 file system: **format FS=FAT32 quick**.

8 The drive must be marked as a bootable drive. Use the **active** command to mark the drive as bootable.

9 To move files directly to the drive, assign an available letter to the drive with the **assign** command.

10 The drive will automatically mount, and the contents of the ISO file can be copied to the root of the drive.

After the ISO contents have completely copied, the drive is bootable and can be used for recovery.