

Dell Data Protection

Recovery Guide v8.12/v1.6/v1.3/v1.12/v1.1



Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

© 2016 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 Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools, and Dell Data Protection | Secure Lifecycle suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. 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®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, 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. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of Dell EMC. 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. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, 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. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. 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. This product uses parts of the 7-Zip program. The source code can be found at 7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (7-zip.org/license.txt).

Dell Data Protection Recovery Guide

2017 - 02

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 - Remotely Managed Computer	6
Obtain the Recovery File - Locally Managed Computer	7
Perform a Recovery	7
3 Hardware Crypto Accelerator Recovery	12
Recovery Requirements	12
Overview of the Recovery Process	12
Perform HCA Recovery	12
Obtain the Recovery File - Remotely Managed Computer	12
Obtain the Recovery File - Locally Managed Computer	13
Perform a Recovery	14
4 Self-Encrypting Drive (SED) Recovery	20
Recovery Requirements	20
Overview of the Recovery Process	20
Perform SED Recovery	20
Obtain the Recovery File - Remotely Managed SED Client	20
Obtain the Recovery File - Locally Managed SED Client	21
Perform a Recovery	21
5 General Purpose Key Recovery	25
Recover the GPK	25
Obtain the Recovery File	25
Perform a Recovery	26
6 Encrypted Drive Data Recovery	28
Recover Encrypted Drive Data	28
7 BitLocker Manager Recovery	32
Recover Data	32
8 Password Recovery	34
Recovery Questions	34
Challenge/Response Codes	36
9 External Media Shield Password Recovery	40
Recover Access to Data	40
Self-Recovery	42



10 Secure Lifecycle Recovery	44
Recovery Requirements.....	44
Perform Secure Lifecycle Recovery.....	44
11 Appendix A - Burning the Recovery Environment	48
Burning the Recovery Environment ISO to CD\DVD.....	48
Burning the Recovery Environment on Removable Media.....	48



Getting Started with Recovery

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

- Downloaded copy of the recovery environment software - located in the Windows Recovery Kit folder in the Dell Data Protection installation media
- 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 Data Protection 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 Data Protection product.

Additionally, online support for Dell Data Protection 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 Code available when you call.

For phone numbers outside of the United States, check [Dell ProSupport International Phone Numbers](#).



Policy-Based or File/Folder Encryption Recovery

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 on which you cannot access encrypted data or edit policies.
- A server running Dell Data Protection | Server Encryption that meets either of the preceding conditions.
- A computer on which the Hardware Crypto Accelerator card or the motherboard/TPM must be replaced.

Overview of the Recovery Process

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.

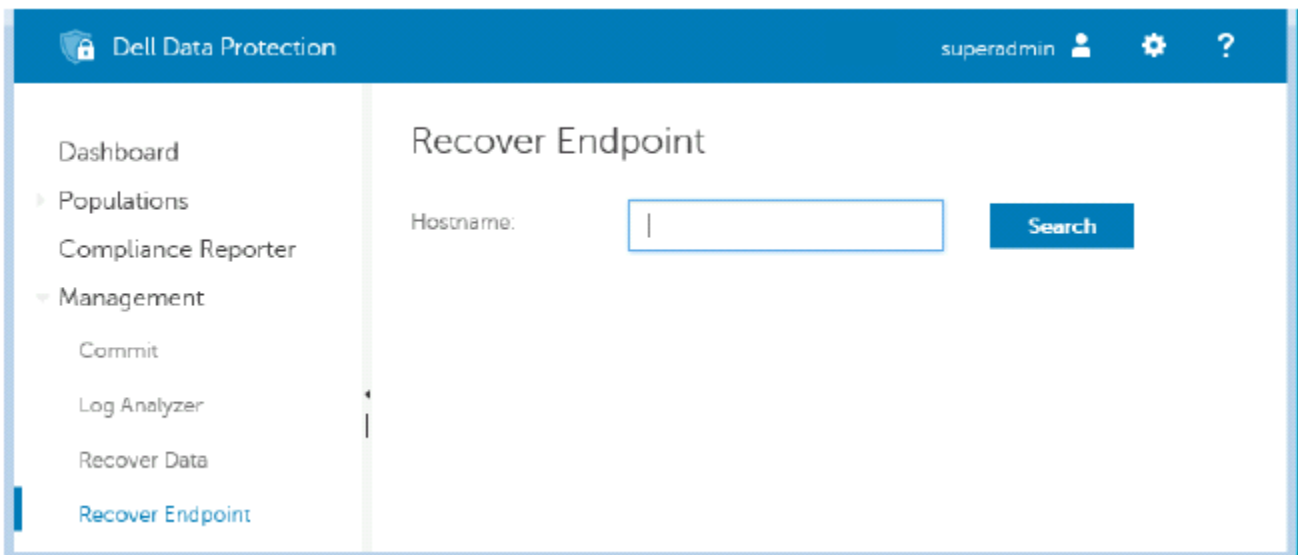
Perform Policy-Based Encryption or FFE Recovery

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

Obtain the Recovery File - Remotely Managed Computer

To download the **<machinename_domain.com>.exe** file:

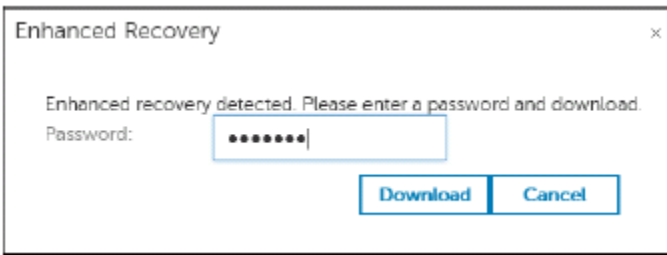
- 1 Open the Remote Management Console and, from the left pane, select **Management > Recover Endpoint**.



- 2 In the Hostname field, enter the fully qualified domain name of the endpoint and click **Search**.
- 3 In the Enhanced Recovery window, enter a recovery Password and click **Download**.

NOTE:

You must remember this password to access the recovery keys.

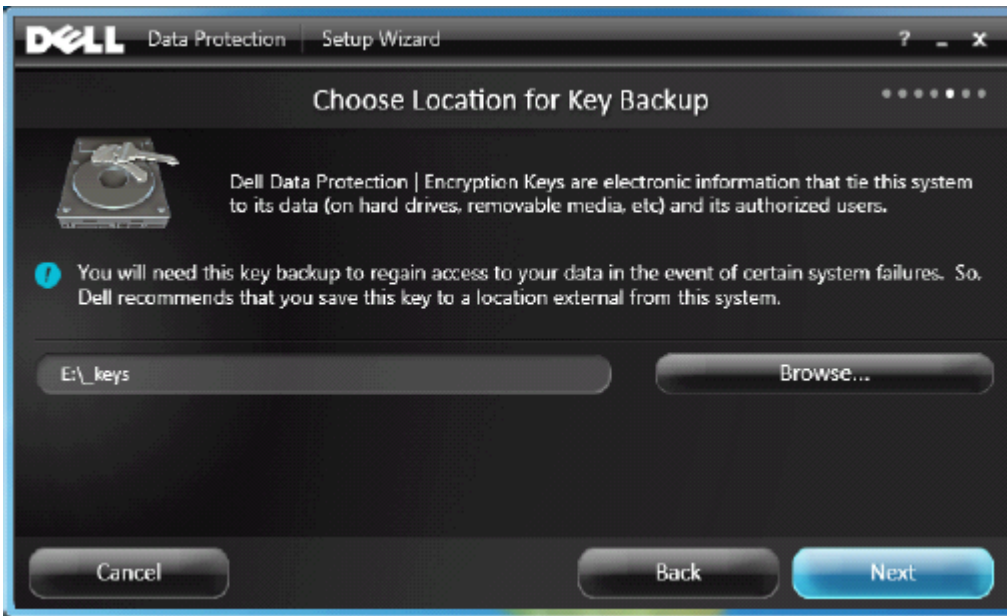


- 4 Copy the **<machinename_domain.com> .exe** file to a location where it can be accessed when booted into WinPE.

Obtain the Recovery File - Locally Managed Computer

To obtain the Personal Edition 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 Personal Edition.

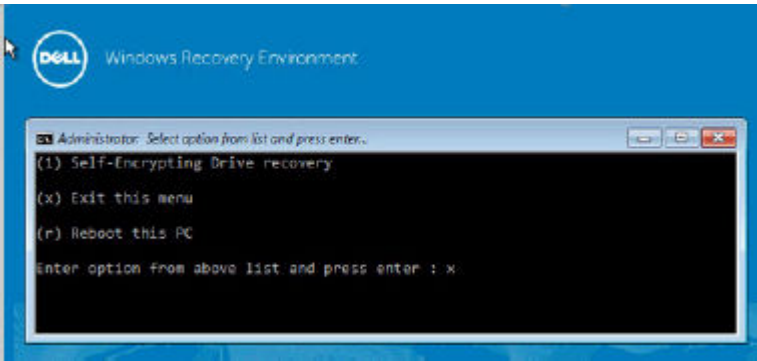


- 2 Copy **LSARecovery_<systemname> .exe** to the target computer (the computer to recover data).

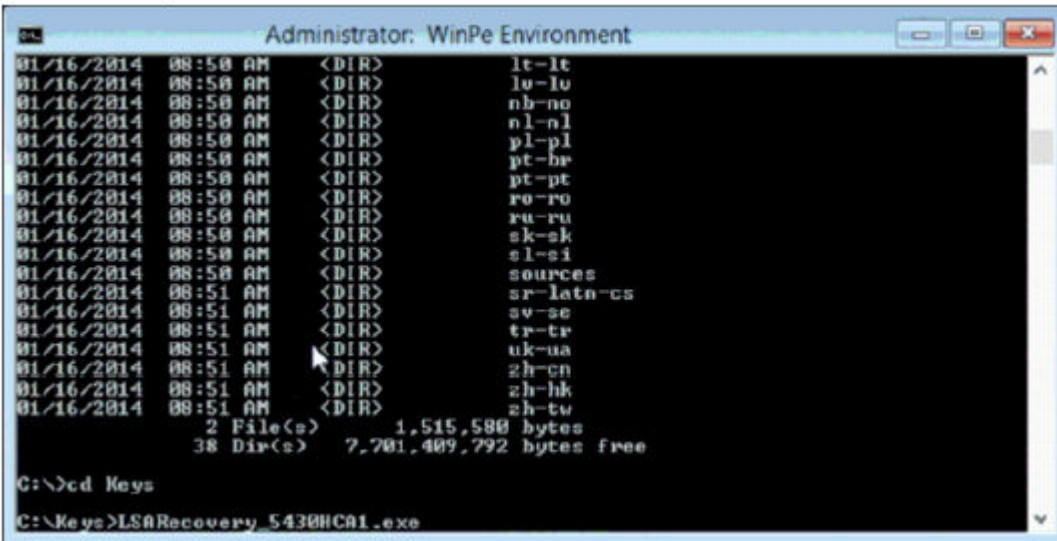
Perform a Recovery

- 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.
- 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.

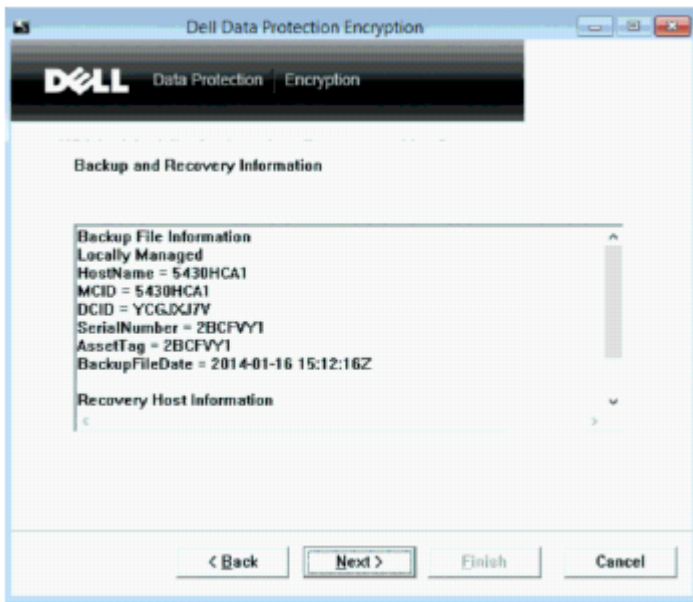
Use this if the Hardware Crypto Accelerator card or the motherboard/TPM must be replaced.





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

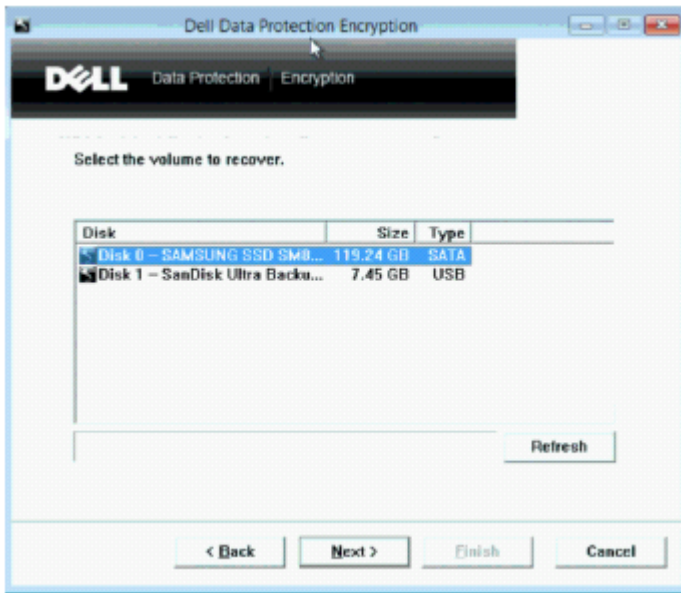
When recovering non-Dell computers, the SerialNumber and AssetTag fields will be blank.



- 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.



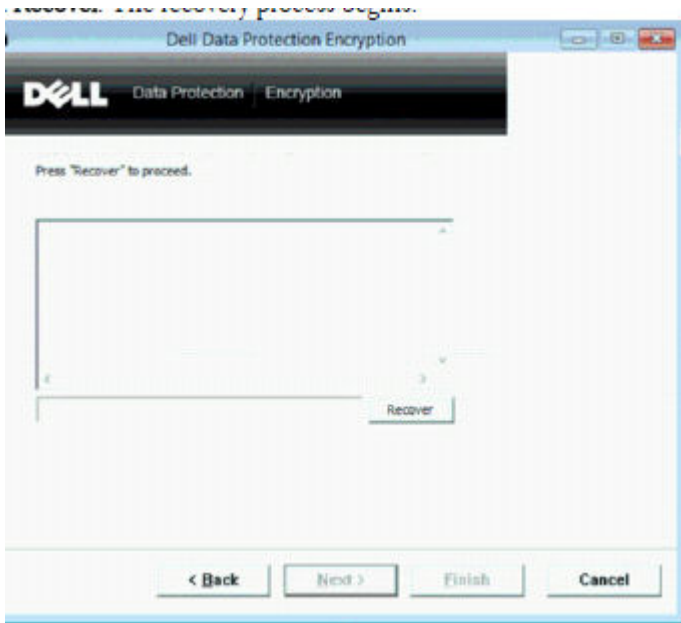


- 7 Enter your recovery password and click **Next**.
With a remotely managed client, this is the password provided in [step 3](#) in [Obtain the Recovery File - Remotely Managed Computer](#).
In Personal Edition, the password is the Encryption Administrator Password set for the system at the time the 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.

Hardware Crypto Accelerator Recovery

With Dell Data Protection 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
- Bootable CD/DVD or USB media

Overview of the Recovery Process

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.

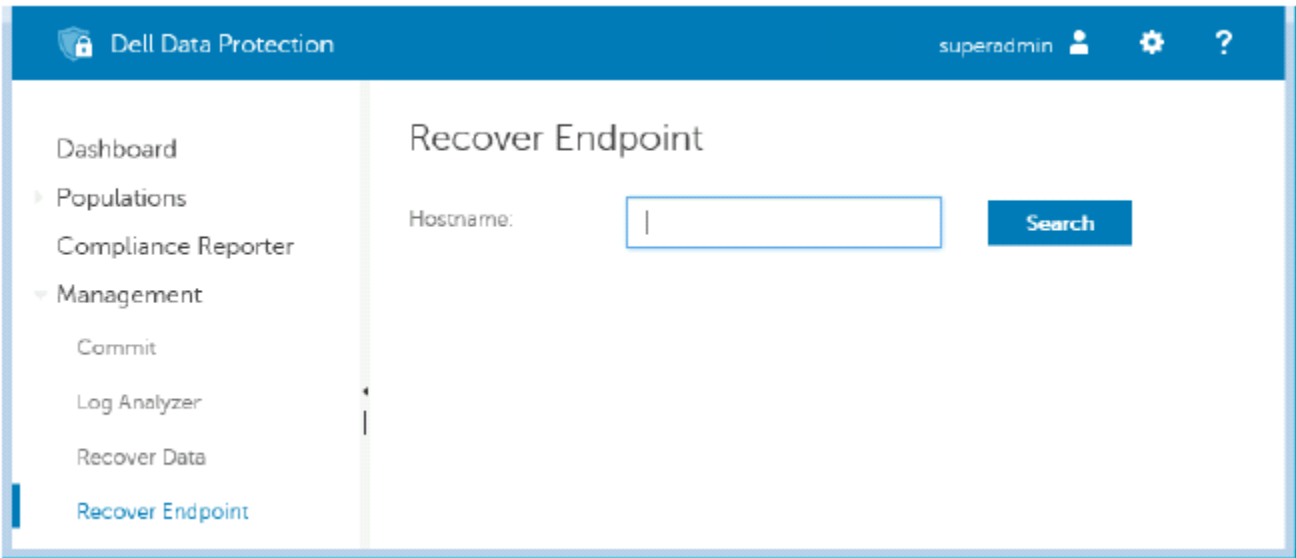
Perform HCA Recovery

Follow these steps to perform an HCA recovery.

Obtain the Recovery File - Remotely Managed Computer

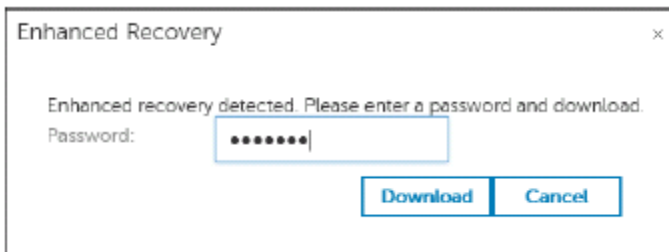
To download the **<machinename_domain.com>.exe** file that was generated when you installed Dell Data Protection:

- 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 Enhanced Recovery window, enter a recovery Password and click **Download**.

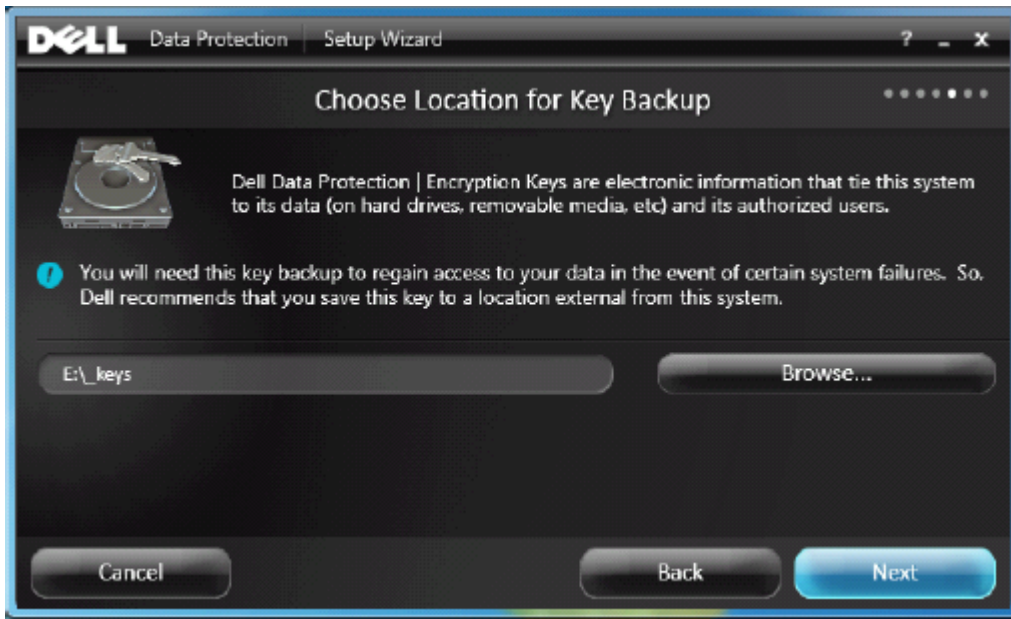
NOTE:
You must remember this password to access the recovery keys.



Obtain the Recovery File - Locally Managed Computer

To obtain the Personal Edition recovery file:

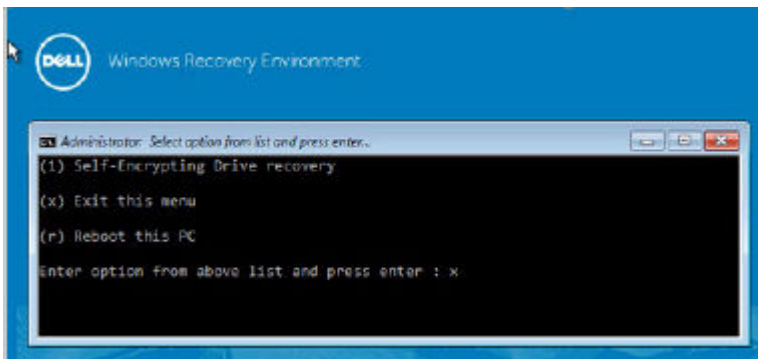
- 1 Locate the recovery file named **LSARecovery_<systemname>.exe** file. This file was stored on a network drive or removable storage when you went through Setup Wizard while installing Personal Edition.



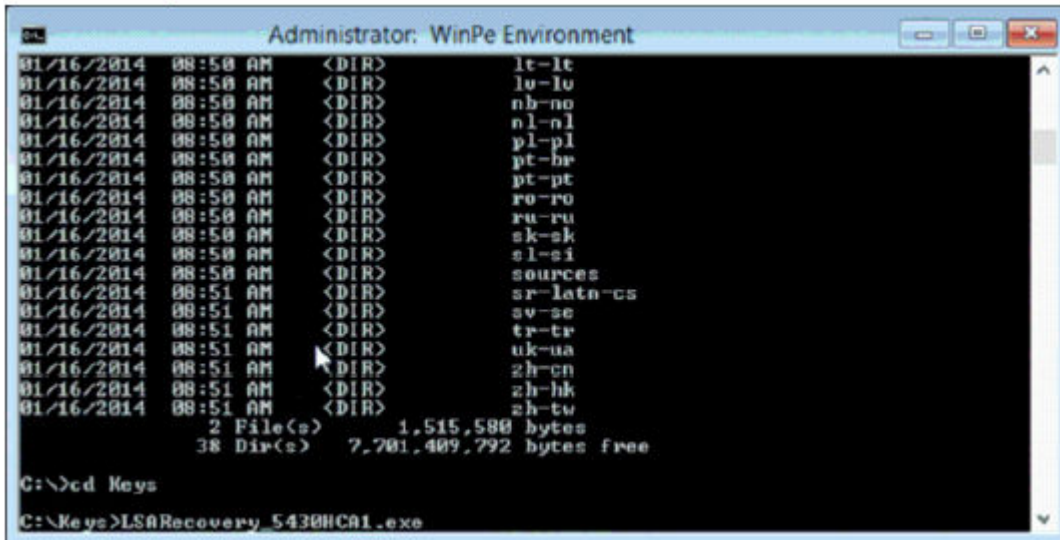
- 2 Copy **LSARecovery_<systemname > .exe** to the target computer (the computer to recover data).

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



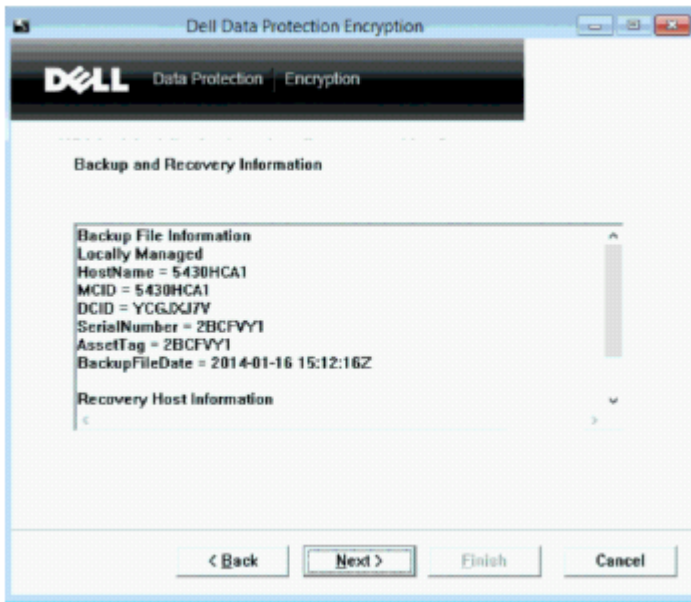
- 3 Navigate to the saved recovery file and launch it.



- 4 Select one option:
- I want to decrypt my HCA encrypted drive.
 - I want to restore access to my HCA encrypted drive.

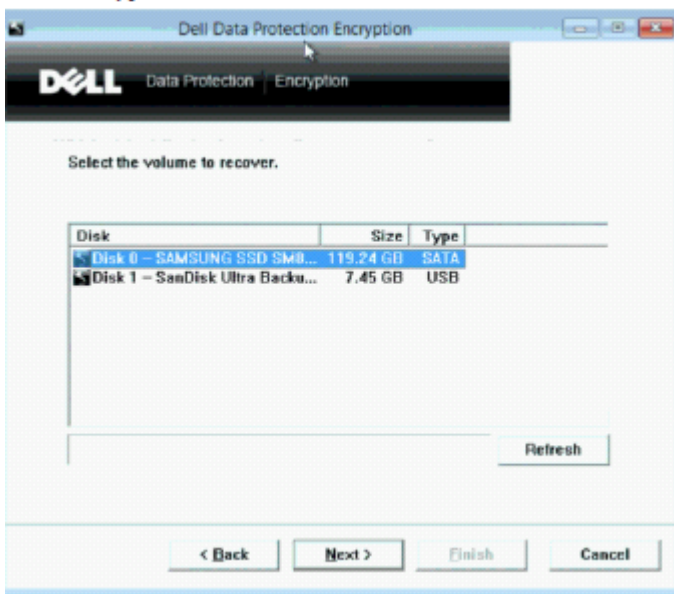


- 5 In the Backup and Recovery Information dialog, confirm that the Service Tag or Asset number is correct and click **Next**.



- 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.

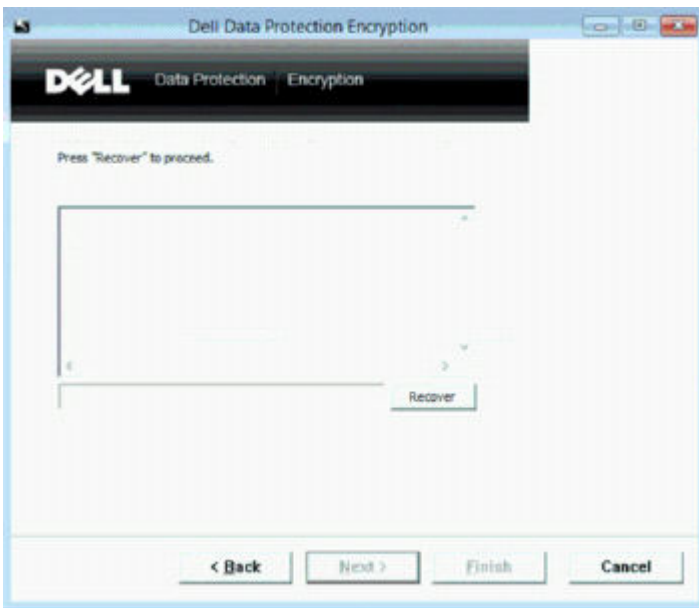


- 7 Enter your recovery password and click **Next**.
On a remotely managed computer, this is the password provided in [step 3](#) in [Obtain the Recovery File - Remotely Managed Computer](#).

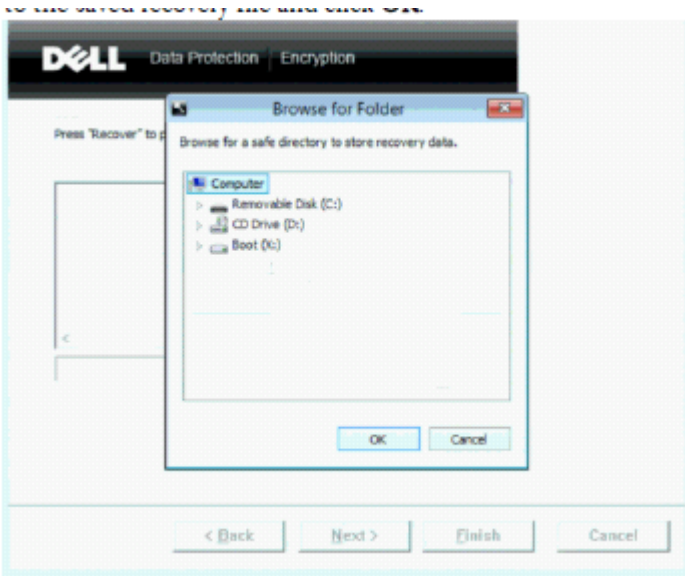
On a locally managed computer, this password is the Encryption Administrator Password set for the system in Personal Edition at the time the keys were escrowed.



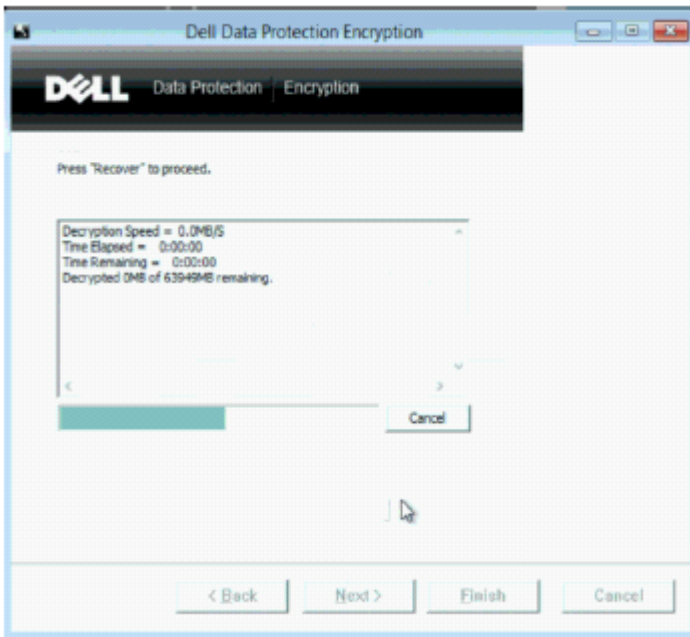
- 8 In the Recover dialog, click **Recover**. The recovery process begins.



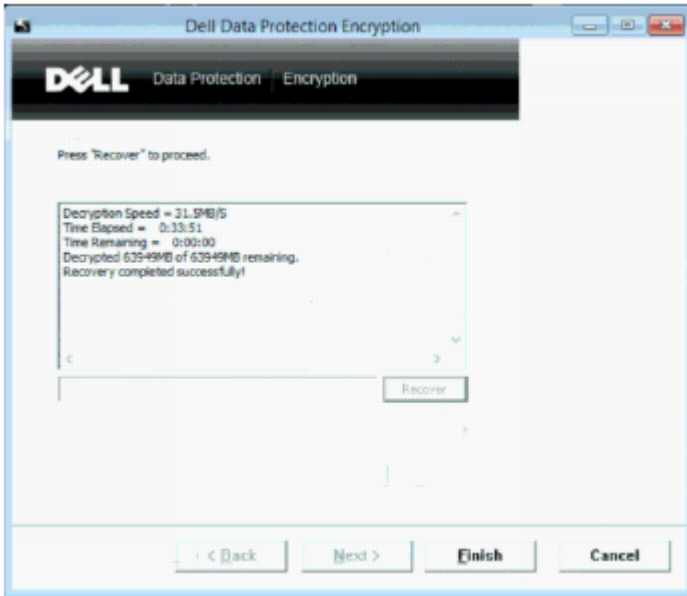
- 9 When prompted, browse to the saved recovery file and click **OK**.



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.



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 and remove Preboot Authentication (PBA).
 - With a remotely managed SED client, the PBA can later be enabled again through the Remote Management Console.
 - With a locally managed SED client, the PBA can be enabled through the Security Tools Administrator Console.
- 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

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.

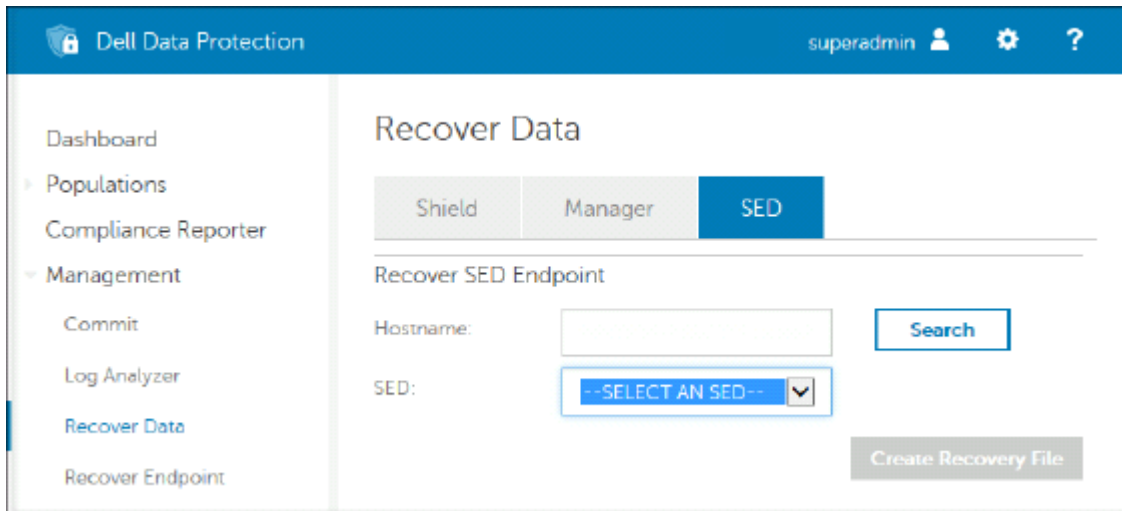
Obtain the Recovery File - Remotely Managed SED Client

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 Protection:

- 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.



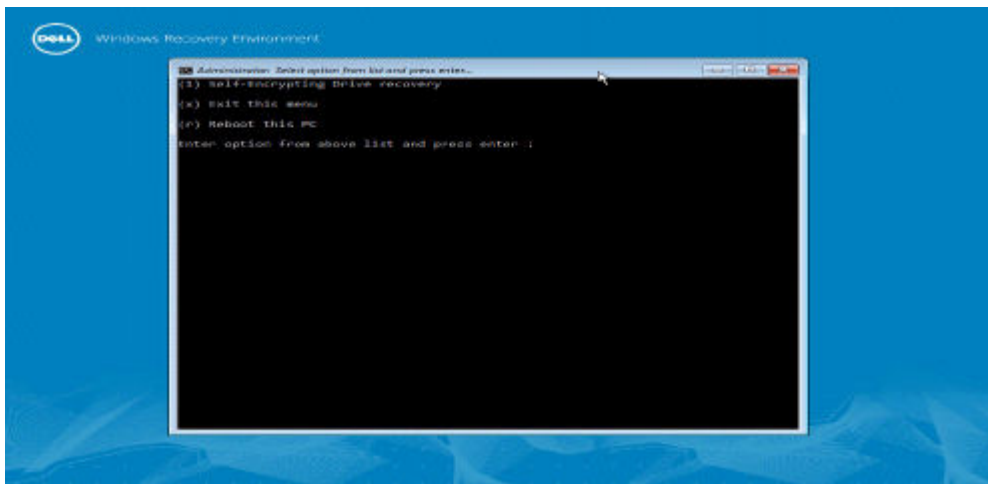
Obtain the Recovery File - Locally Managed SED Client

Obtain the recovery file.

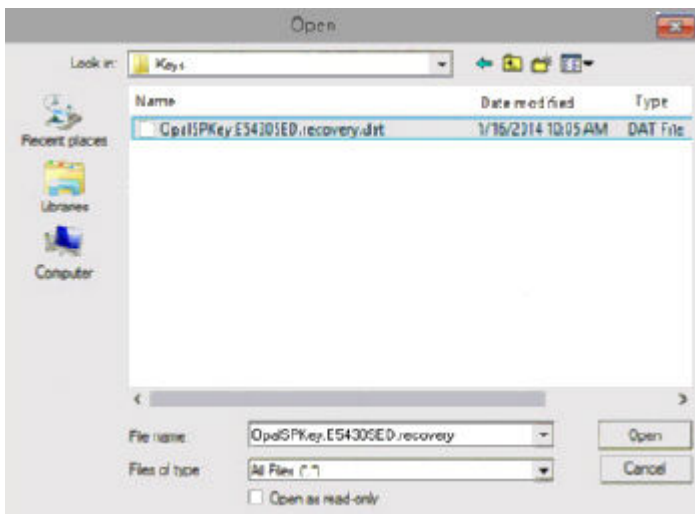
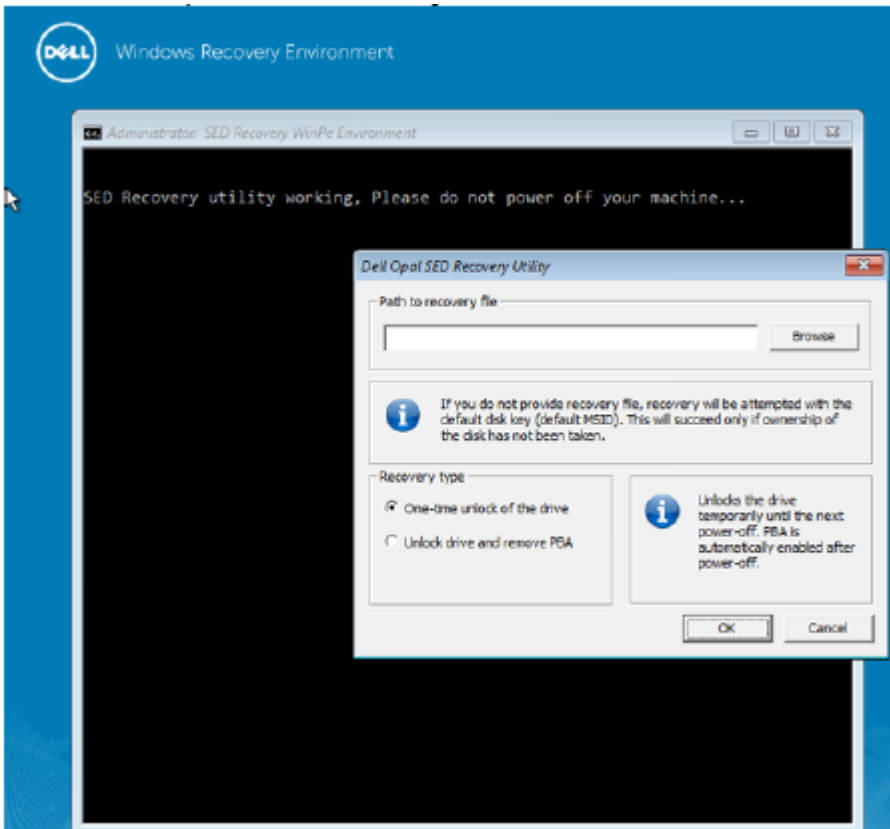
The file was generated and is accessible from the backup location you selected when Dell Data Protection | Security Tools was installed on the computer. The filename is *OpalSPkey<systemname>.dat*.

Perform a Recovery

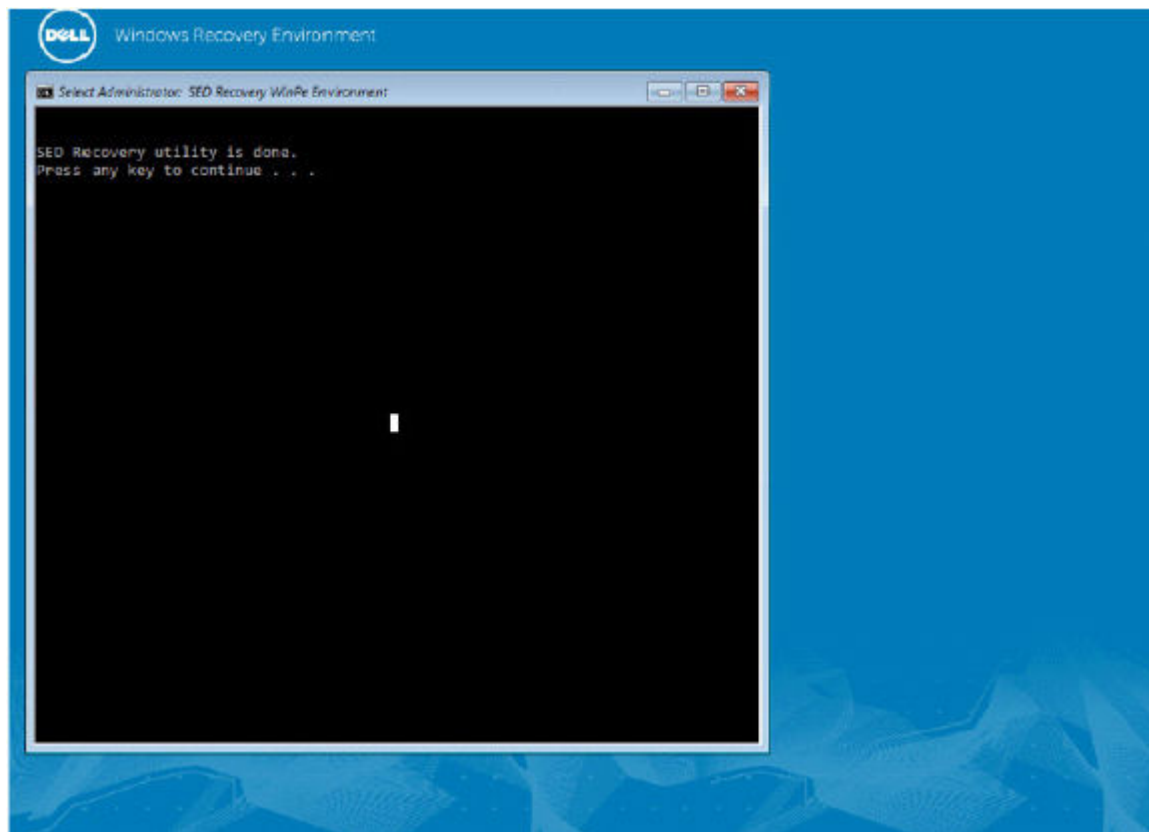
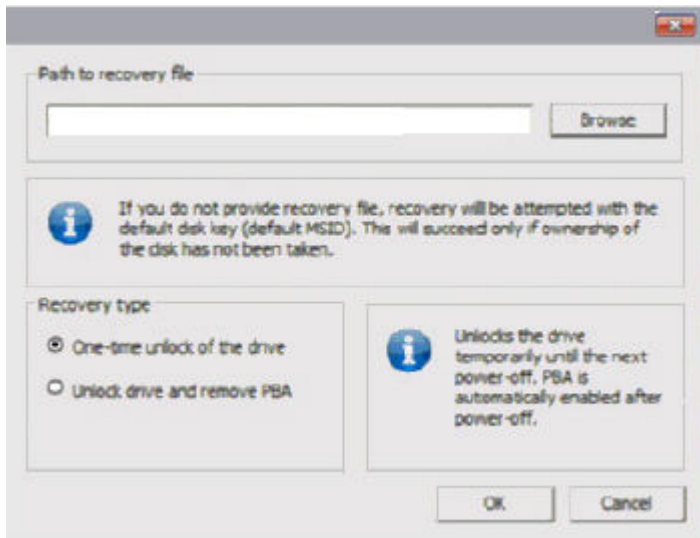
- 1 Using the bootable media created earlier, boot to that media on a recovery system or on the device with the drive you are attempting to recover. A WinPE environment opens with the recovery application.



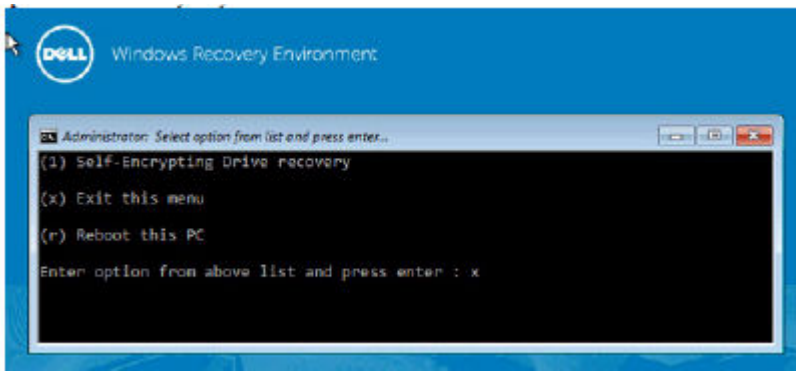
- 2 Choose option one and press **Enter**.
- 3 Select **Browse**, locate the recovery file, and then click **Open**.



- 4 Select one option and click **OK**.
- **One-time unlock of the drive** - This method bypasses and removes the PBA. Later, it can be enabled again through the Remote Management Console (for a remotely managed SED client) or through the Security Tools Administrator Console (for a locally managed SED client).
 - **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.

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
```

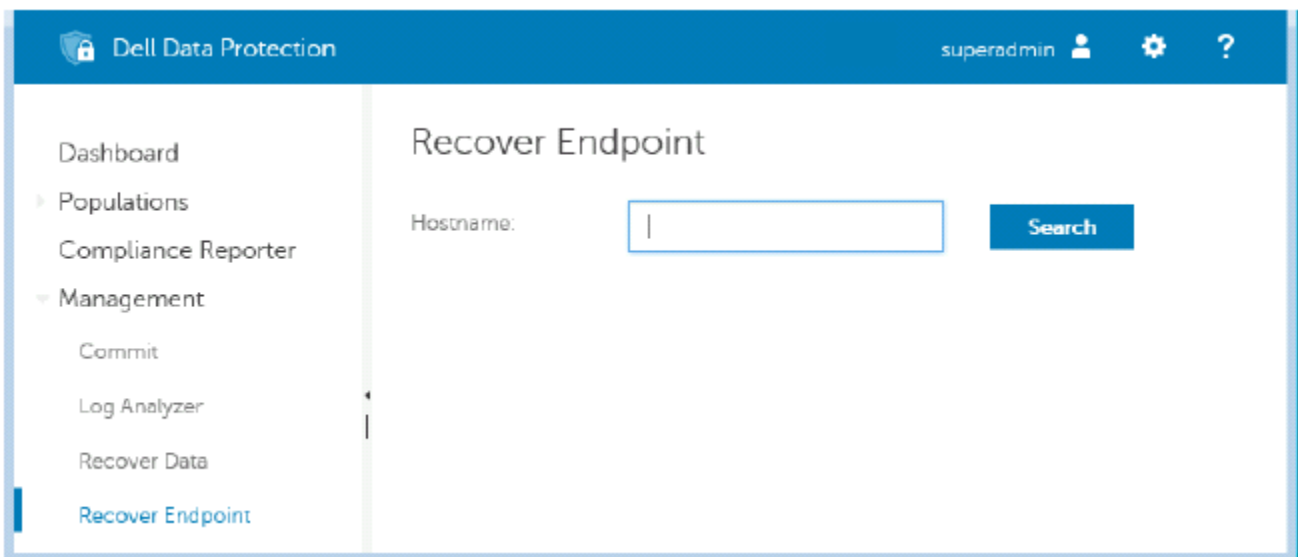
If the GPK fails to unseal, the GPK must be recovered by extracting it from the recovery bundle that is downloaded from the Server.

Recover the GPK

Obtain the Recovery File

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

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

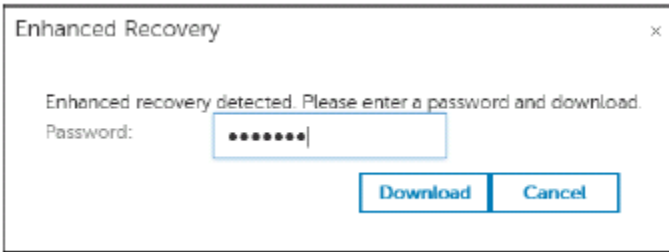


- 2 In the Hostname field, enter the fully qualified domain name of the endpoint and click **Search**.
- 3 In the Enhanced Recovery window, enter a recovery Password and click **Download**

NOTE:

You must remember this password to access the recovery keys.

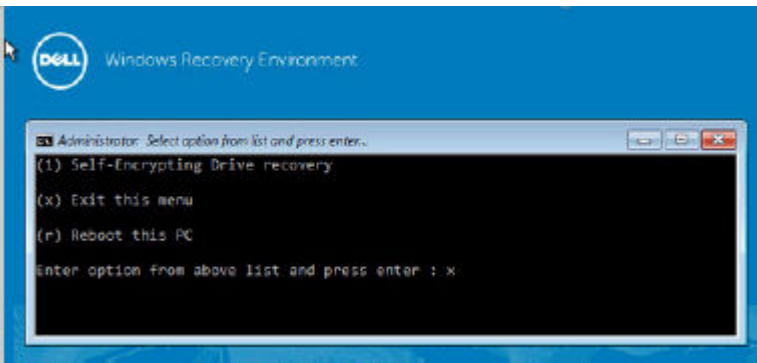




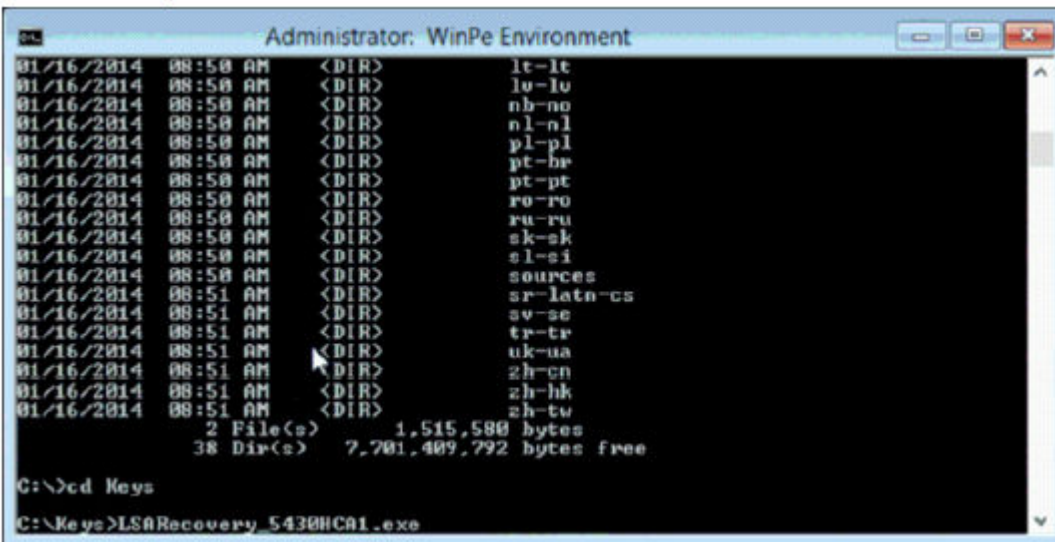
The <machinename_domain.com>.exe file is downloaded.

Perform a Recovery

- 1 Create bootable media of the recovery environment. For instructions, see [Appendix A - Burning the Recovery Environment](#).
- 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.

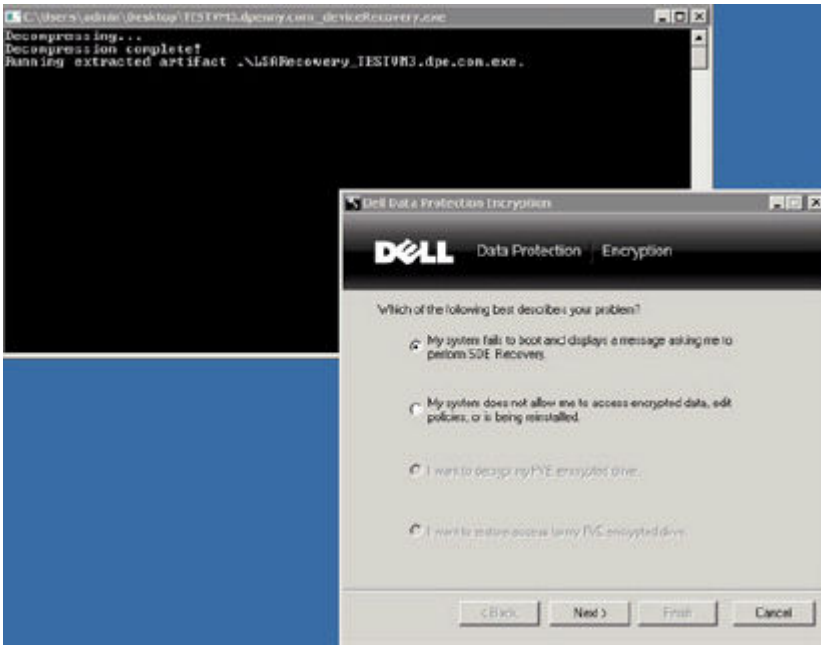


- 4 Navigate to the recovery file and launch it.

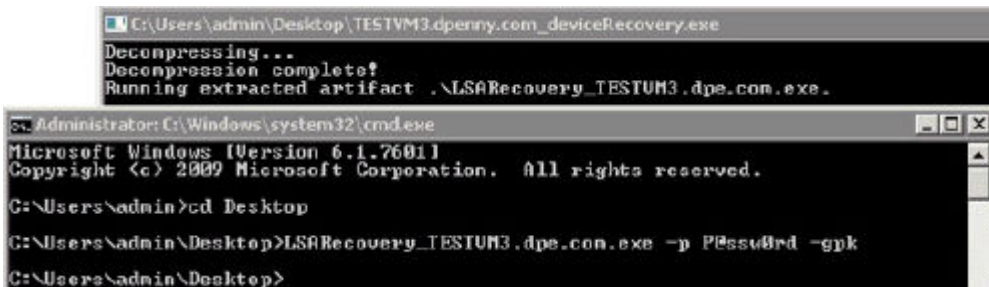


An Encryption client diagnostic dialog opens and the recovery file is being generated in the background.





- 5 At an administrative command prompt, run `<machinename_domain.com> .exe > -p <password> -gpk`
It returns the GPKRCVR.txt for your computer.

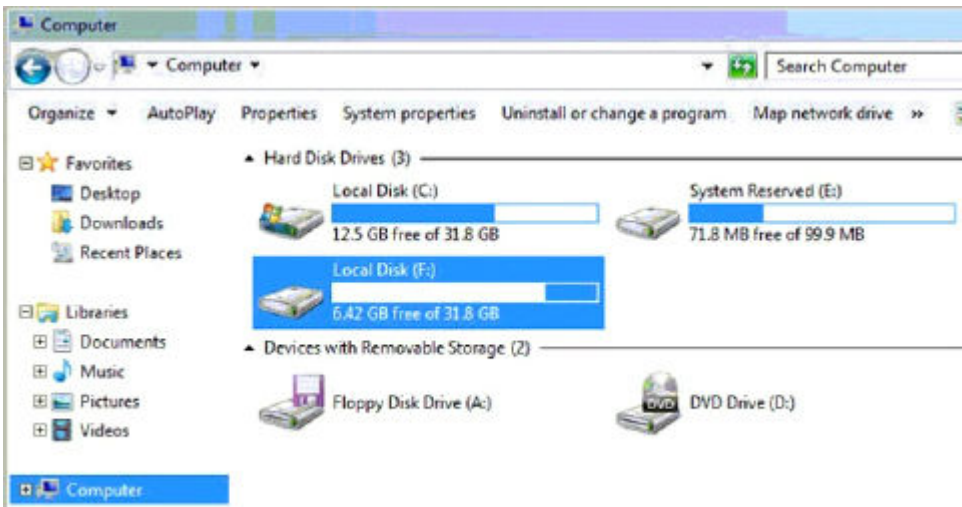


- 6 Copy the **GPKRCVR.txt** file to the root of the OS drive of the computer.
- 7 Reboot the computer.
The GPKRCVR.txt file will be consumed by the operating system and will regenerate the GPK on that computer.
- 8 If prompted, reboot again.



Encrypted Drive Data Recovery

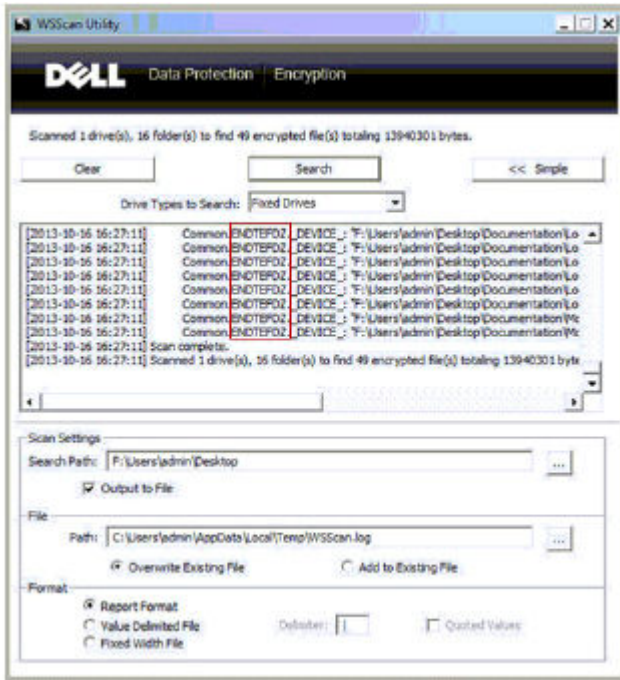
If the target computer is not bootable and no hardware failure exists, data recovery can be accomplished on the computer booted into a recovery environment. If the target computer is not bootable and has failed hardware or is a USB device, data recovery can be accomplished by booting into a slaved drive. 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.



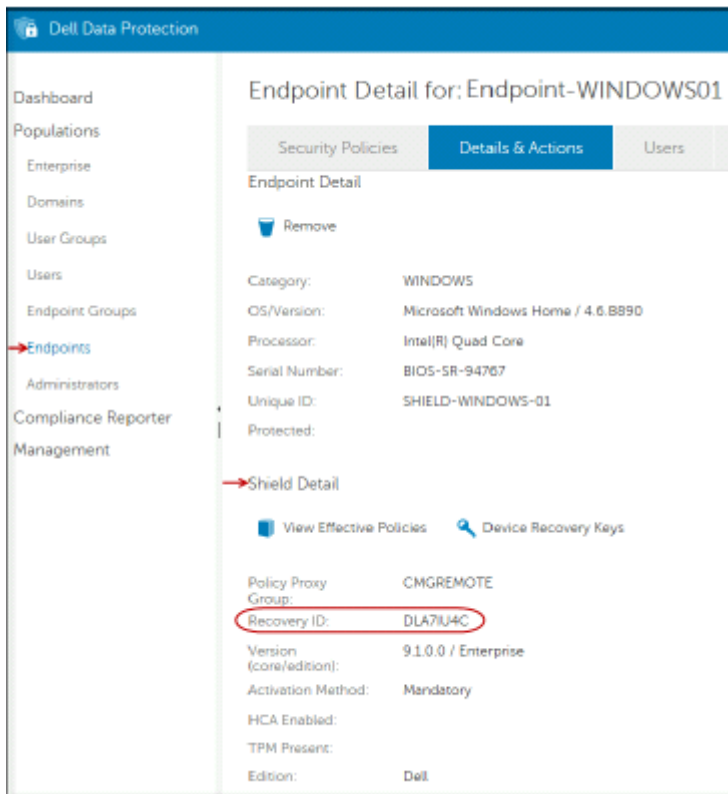
Recover Encrypted Drive Data

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."

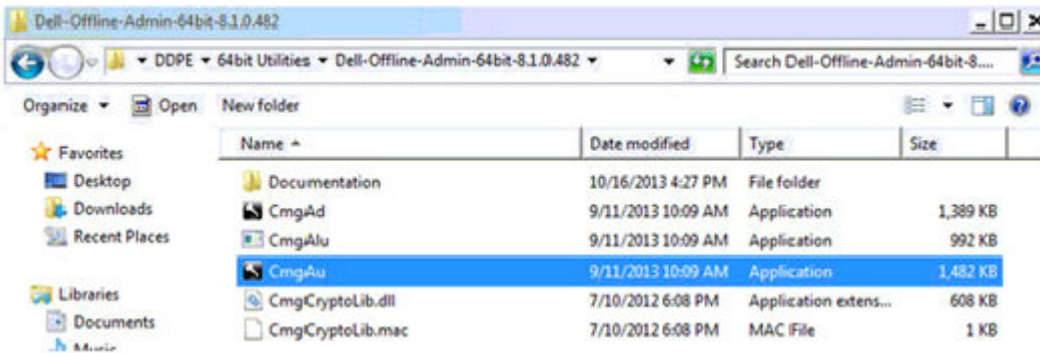


- b Open the Remote Management Console, and select the **Details & Actions** tab for the endpoint.
- c In the Shield Detail section of the Endpoint Detail screen, locate the DCID/Recovery ID.



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

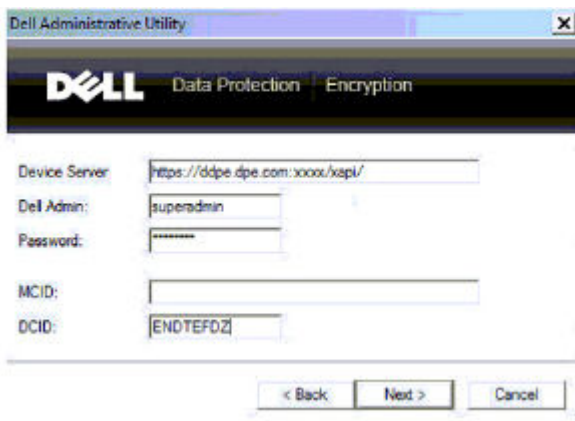
Security Server: **https://<server.organization.com>:8443/xapi/**

Dell Admin: The account name for the Forensic Administrator (enabled in the Server)

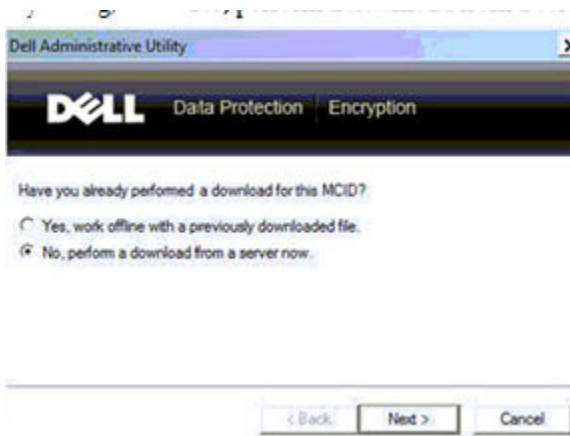
Dell Admin Password: The account password for the Forensic Administrator (enabled in the Server)

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.**

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.

The screenshot shows the 'Recover Data' interface in the Dell Data Protection console. The left navigation pane includes 'Management' > 'Recover Data'. The main content area has three tabs: 'Shield', 'Manager' (selected and circled in red), and 'SED'. Under the 'Manager' tab, there are two sections: 'BitLocker' and 'TPM'. Each section has input fields for 'Recovery ID', 'Hostname', 'Volume', and 'Password'. The 'BitLocker' section also includes a 'Search' button. Below the input fields are two buttons: 'Get Recovery Password' and 'Create Key Package'.

- 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.



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

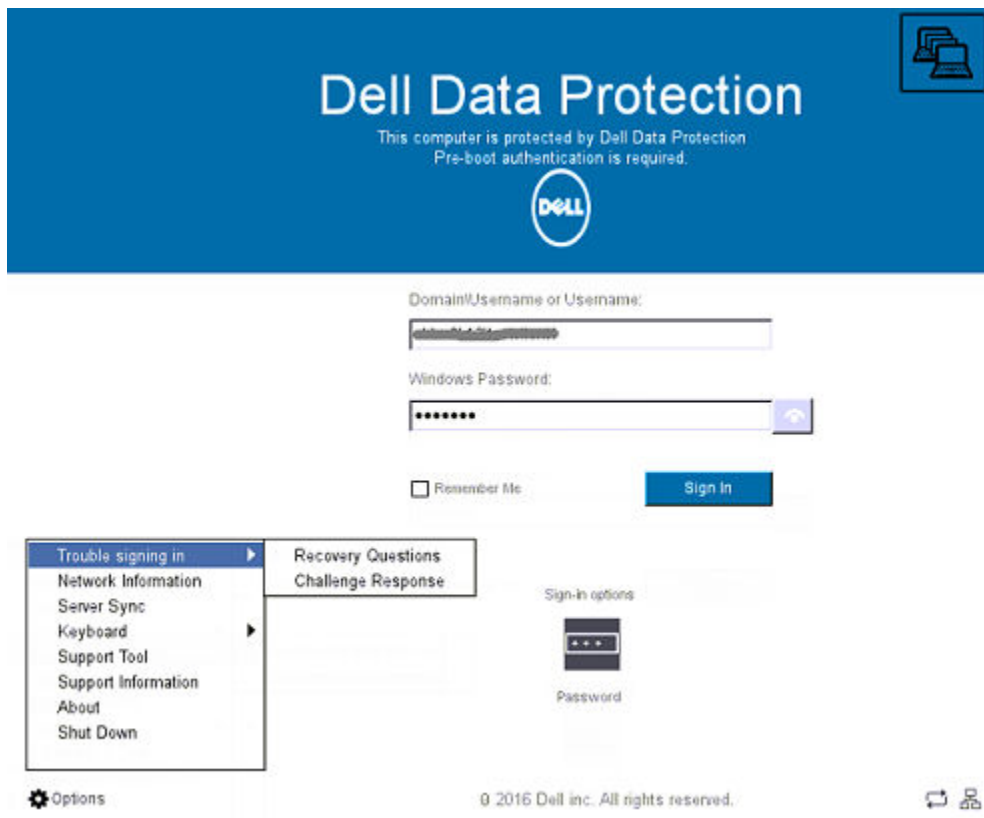
The first time a user signs in to a computer, he is prompted to answer a standard set of questions that the Administrator has configured. After enrolling his answers to these questions, the next time he forgets his password, the user is prompted for the answers. Assuming he has answered the questions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

Prerequisites

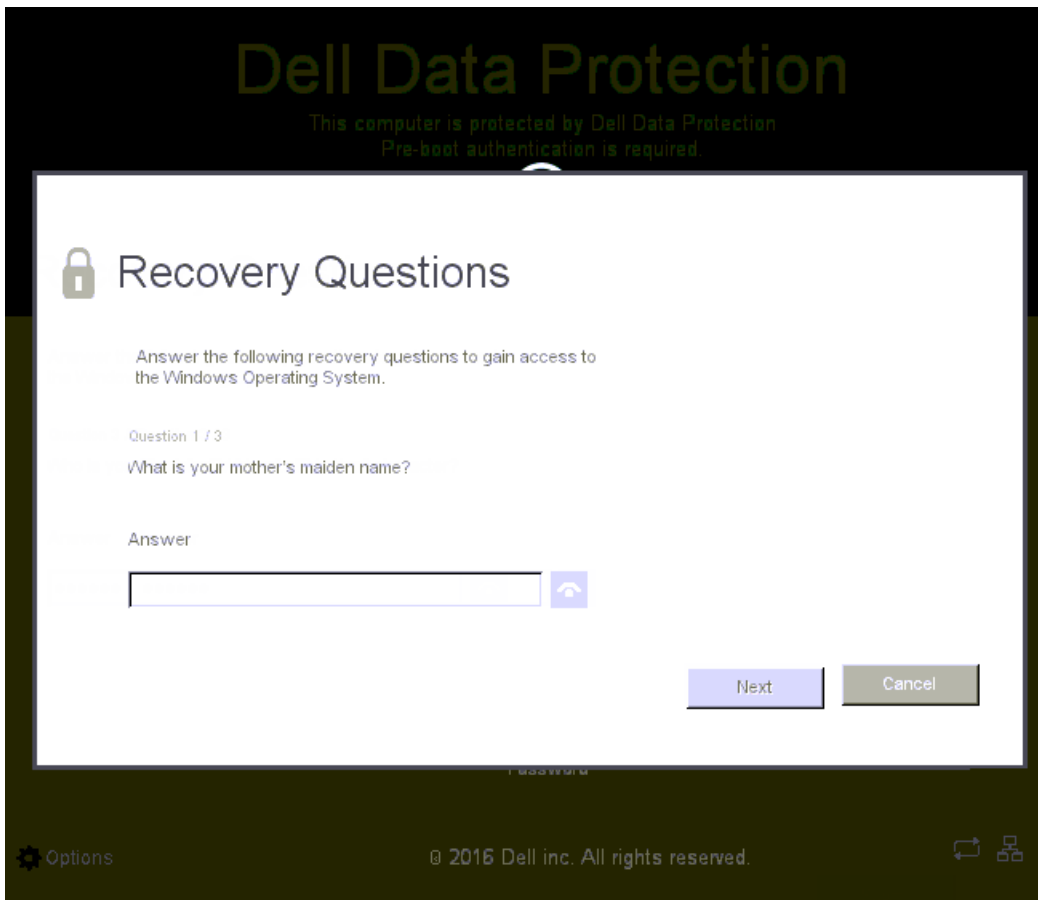
- Recovery Questions must be set up by the Administrator.
- The user must have enrolled his answers to the questions.
- Before clicking the **Trouble Signing In** menu option, the user must enter a valid user name and domain.

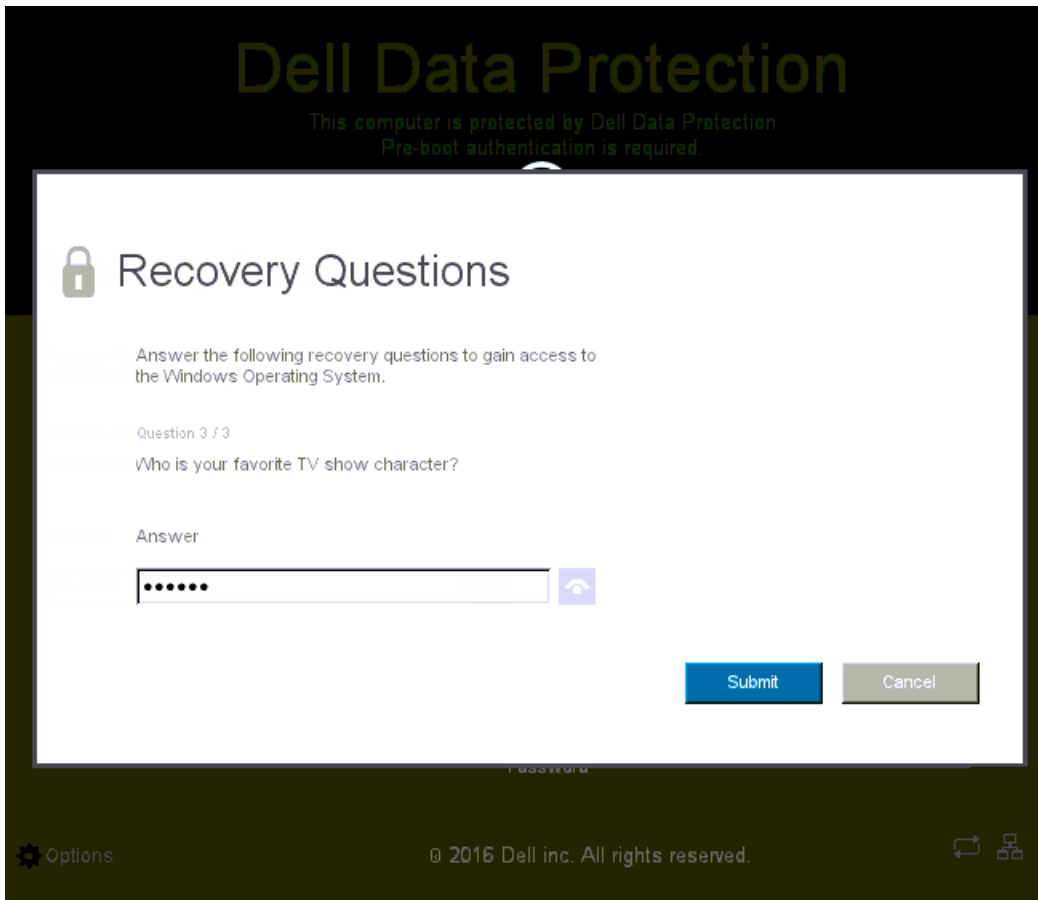
To access the Recovery Questions from the PBA sign-in screen:

- 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.





Challenge/Response Codes

Challenge/Response recovery can be used to authenticate through PBA to access Windows. Challenge/Response can be used in the following scenarios:

- When a user does not remember the answers supplied at time of Recovery Questions enrollment.
- The Administrator has not enabled the Recovery Questions feature.
- A user is remote with no network connectivity and cannot receive an unlock command from the Security Server through SED Device Controls

A user can get to the Challenge/Response screen by clicking the **Trouble Signing In** option or by entering his password incorrectly, exceeding the password failure limit without the network cable plugged in. If Recovery Questions have been disabled, the **Trouble Signing In** option opens the Challenge/Response screen directly.

Requirement

- Challenge/Response recovery is available only to domain computers that are remotely managed by your organization or enterprise.

Prerequisites

- Disconnect the computer from the network before answering either Recovery Questions or entering Challenge/Response codes.
- Before clicking Trouble Signing In, enter a valid user name and domain.

To use Challenge/Response recovery

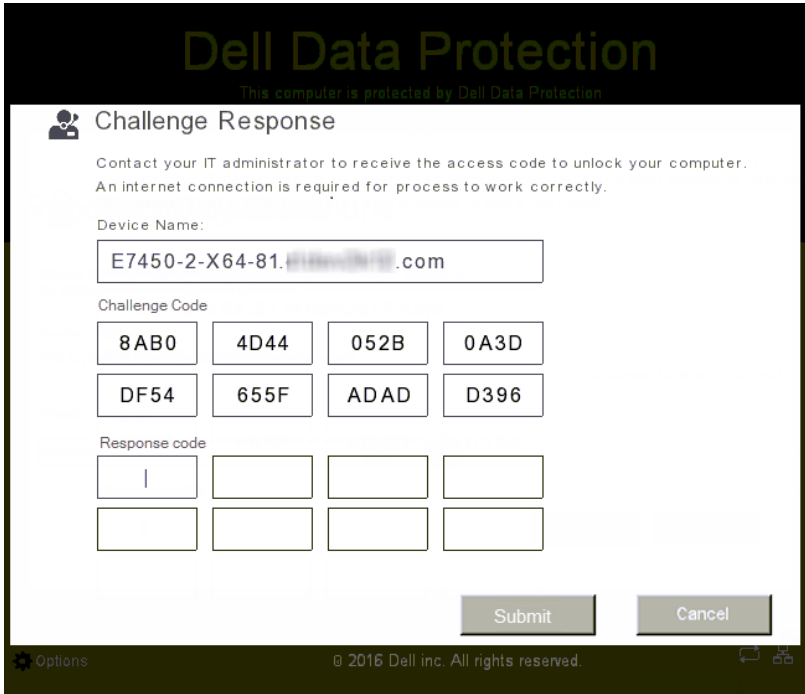
- 1 The user clicks the **Options** link to display the menu.
- 2 The user clicks **Trouble Signing In > Challenge/Response**.



NOTE:

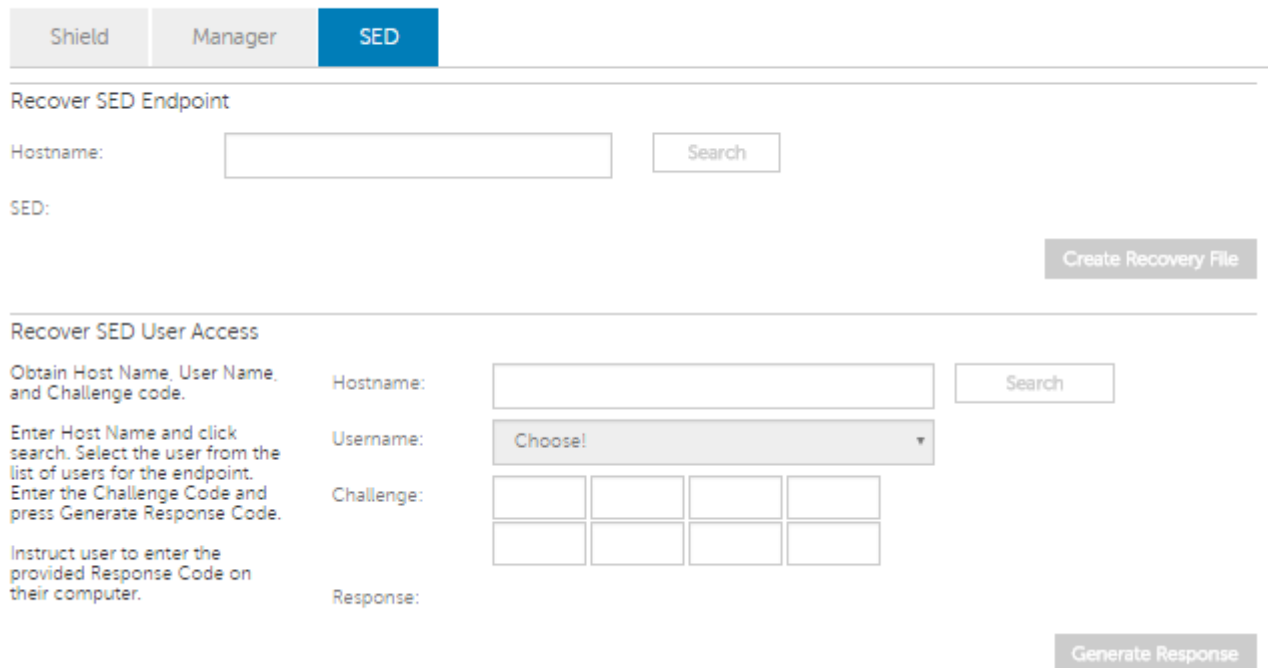
The Challenge/Response option is only available on computers that are managed by an enterprise. If the computer is non-domain, the Challenge/Response option does not appear on the menu.

- 3 When prompted, the user contacts the Help Desk and gives the Administrator the Device Name (host name) and Challenge Code.



- 4 The Administrator opens the Remote Management Console, clicks **Management > Recover Data**, and then clicks **SED** from the top menu.

Recover Data



- Under Recover SED User Access, the Administrator enters the **Host Name** obtained from the user, and clicks **Search**.
- The Administrator selects the user name who is asking for help:

Recover SED User Access

Obtain Host Name, User Name, and Challenge code.

Enter Host Name and click search. Select the user from the list of users for the endpoint. Enter the Challenge Code and press Generate Response Code.

Instruct user to enter the provided Response Code on their computer.

Hostname:

Search

Username:

Challenge:

1234	5678	9012	

Response:

Generate Response

- Enter the device code obtained from the user into the **Challenge** field and click **Generate Response**.

Recover SED User Access

Obtain Host Name, User Name, and Challenge code.

Enter Host Name and click search. Select the user from the list of users for the endpoint. Enter the Challenge Code and press Generate Response Code.

Instruct user to enter the provided Response Code on their computer.

Hostname:

Search

Username:

Challenge:

1234	5678	9012	4424
7422	3344	2233	1122

Response:

Generate Response

- Give the generated response code to the user.



NOTE:

These codes are not case sensitive. The numbers are shown in red and the letters in blue.

Recover SED User Access

Obtain Host Name, User Name, and Challenge code.

Enter Host Name and click search. Select the user from the list of users for the endpoint. Enter the Challenge Code and press Generate Response Code.

Instruct user to enter the provided Response Code on their computer.

Hostname:

Search

Username:

Challenge:

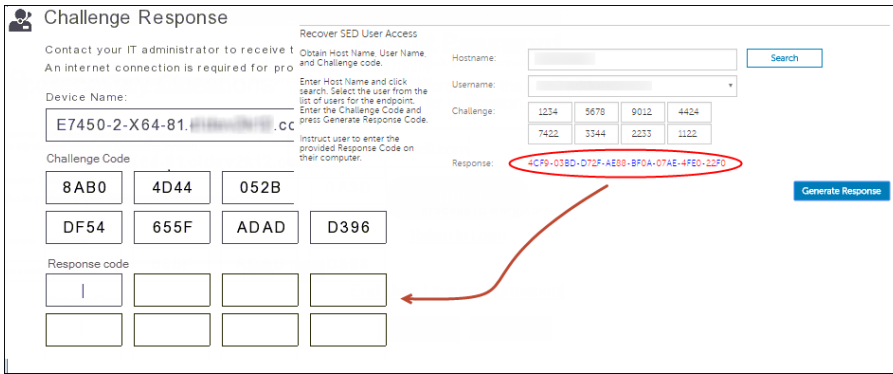
1234	5678	9012	4424
7422	3344	2233	1122

Response: 4CF9-03BD-D72F-AE88-BF0A-07AE-4FE0-22F0

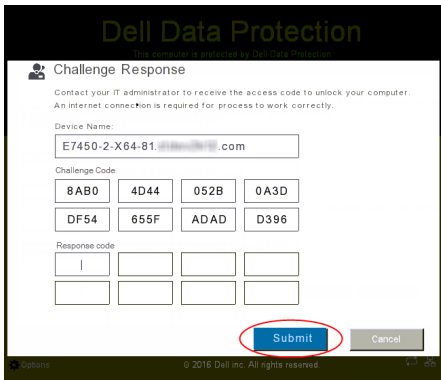
Generate Response

- The user enters the response code into the **Response code** fields on the PBA sign-in screen. This is an example of a user-entered response code:





10 Click the right arrow to continue, and to authenticate past the PBA screen.



11 Click **Submit**.

A user can authenticate past PBA using the Challenge/Response feature only one time. After a computer restart, the PBA layer resumes protecting the computer and resumes prompting the user to sign in on the PBA screen.

NOTE:

After the user has displayed the Challenge/Response dialog, the user must complete the Challenge/Response sequence to regain access to the system. If the user turns off the computer, and attempts to log back in - even with the correct password - PBA re-prompts the user with the Challenge/Response dialog.



External Media Shield Password Recovery

External Media Shield (EMS) 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 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.

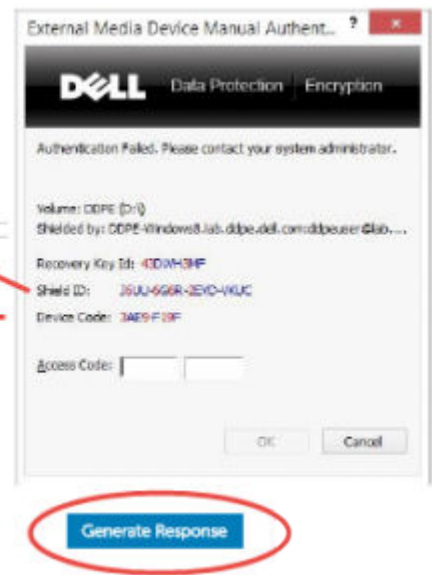
- Contact the Help Desk Administrator and give him the codes that appear in the dialog.



- As a Help Desk Administrator, log into the Remote Management Console - the Help Desk Administrator's account must have Help Desk privileges.
- Navigate to the **Recover Data** menu option on the left pane.
- Enter the codes provided by the end-user.

Recover Data

Shield	Manager	SED
Obtain Shield ID and ask user for their Endpoint Code.	Shield ID:	J6UU 6G6R 2EVD VKUC
Enter Shield ID and Endpoint Code into the fields on the right and press Generate Access Code.	Challenge:	3AE9 F19F
Optionally provide a Key ID.	Key ID:	
Upon confirmation of user identity, instruct user to enter the provided Access Code on their computer.	Response:	
	Directory User Alias:	



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



Recover Data

The 'Recover Data' interface is divided into three tabs: Shield, Manager, and SED. The 'Shield' tab is active. It contains instructions and a form for recovering data. The form fields are:

- Shield ID: 36UU, 6G6R, 2EVD, VKUC
- Challenge: 3AEP, F19F, [empty], [empty]
- Key ID: [empty]
- Response: 18FC-4FD3
- Directory User Alias: DDP-USER (DDPUSER@organization.com)

A red arrow points from the 'Response' field to a 'Generate Response' button in a separate window titled 'External Media Device Media Auth...'. The 'Generate Response' button is circled in red.

- 9 Reset your password for the encrypted media.

The 'Password Reset' dialog box is titled 'Password Reset' and features the Dell Data Protection Encryption logo. It contains the following text and fields:

Failed password attempts detected, do you wish to reset the device's password?

Volume: DDPE (D:)

New Password: [password field]

Retype Password: [password field]

Buttons: OK, Cancel

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

Self-Recovery

Self-Recovery is the process of resetting the password for an encrypted removable media device by inserting the drive back into a protected machine where the owner of the media is logged in. 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.

- 1 Sign in to a Dell Data Protection 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.

Secure Lifecycle Recovery

The recovery tool allows:

- Decryption of protected Office files

This includes files up to triple encryption - With more than one way to encrypt files, occasionally a file is double or triple encrypted. If the user opens the file, an error message instructs them to contact their administrator to recover them.

- 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 Secure Lifecycle

Recovery Requirements

Requirements include:

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

Perform Secure Lifecycle Recovery

Follow these steps to perform a recovery of Secure Lifecycle's protected Office documents.

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

To perform a recovery:

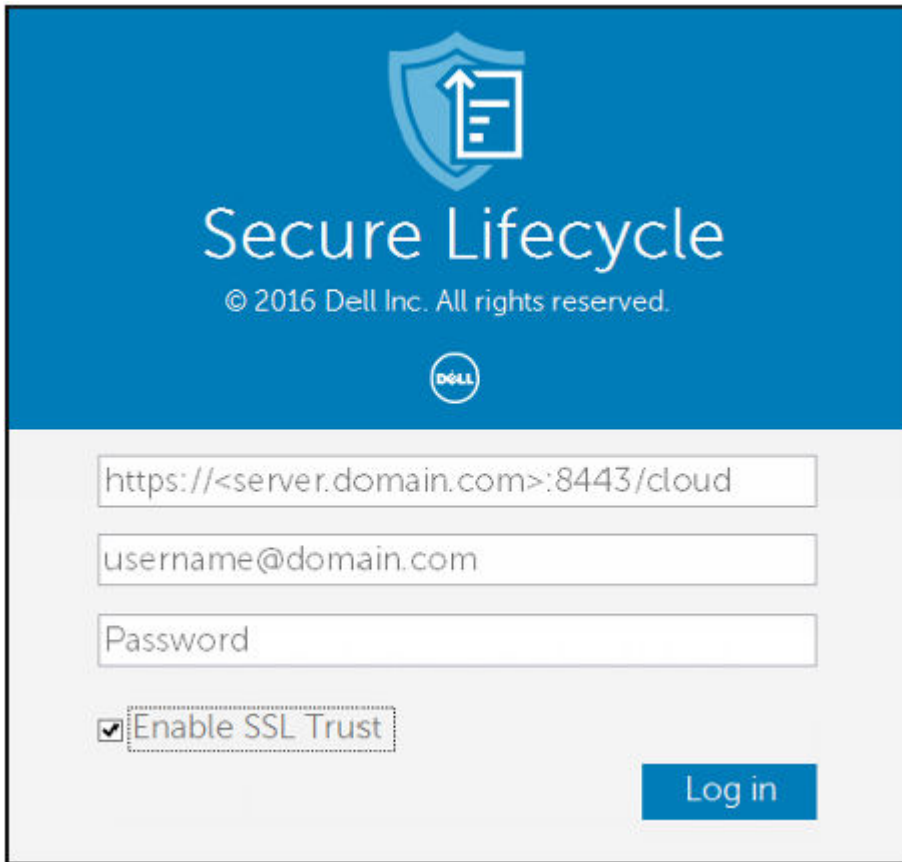
- 1 From the Dell installation media, copy **RecoveryTools.exe** to one of these:
 - Computer - Copy the .exe to the computer on which Office documents will be recovered.
 - USB - Copy the .exe to the USB flash drive and run it from the USB flash drive.
 - Network drive
- 2 Double-click **RecoveryTools.exe** to launch the recovery tool.
- 3 On the Secure Lifecycle window, enter the DDP Server URL in this format:

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

NOTE:

Replace <server.domain.com> with the fully qualified host name of the DDP Server that manages Secure Lifecycle on that endpoint. To locate the DDP Server URL, click the Secure Lifecycle icon in the system tray and click **Details**. The upper-left corner of the Details screen displays the Server URL.

- 4 Enter the User name and Password, and click **Log in**.



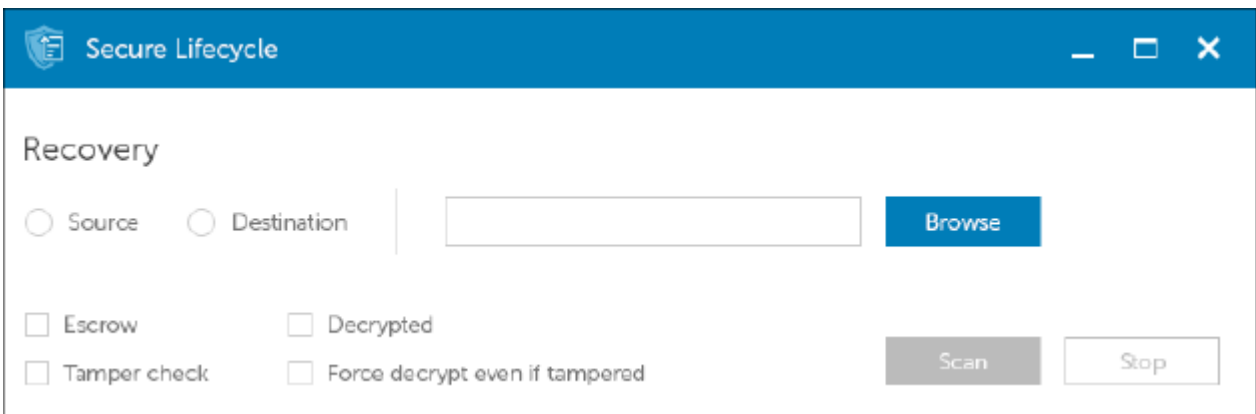
The image shows the Secure Lifecycle login interface. At the top, there is a blue header with a shield icon containing a document and an arrow, the text "Secure Lifecycle", and the copyright notice "© 2016 Dell Inc. All rights reserved." Below the header is the Dell logo. The main form area has a light gray background and contains the following elements:

- A text input field with the placeholder "https://<server.domain.com>:8443/cloud".
- A text input field with the placeholder "username@domain.com".
- A text input field with the placeholder "Password".
- A checked checkbox labeled "Enable SSL Trust".
- A blue "Log in" button.

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.

If you are a Forensic Administrator, the recovery tool opens.



The image shows the "Secure Lifecycle" Recovery tool window. The title bar includes the Dell logo, the text "Secure Lifecycle", and standard window controls (minimize, maximize, close). The main content area is titled "Recovery" and contains:

- Two radio buttons: "Source" (selected) and "Destination".
- A text input field for the selected option, followed by a blue "Browse" button.
- Four checkboxes: "Escrow", "Decrypted", "Tamper check", and "Force decrypt even if tampered".
- A gray "Scan" button and a white "Stop" button.

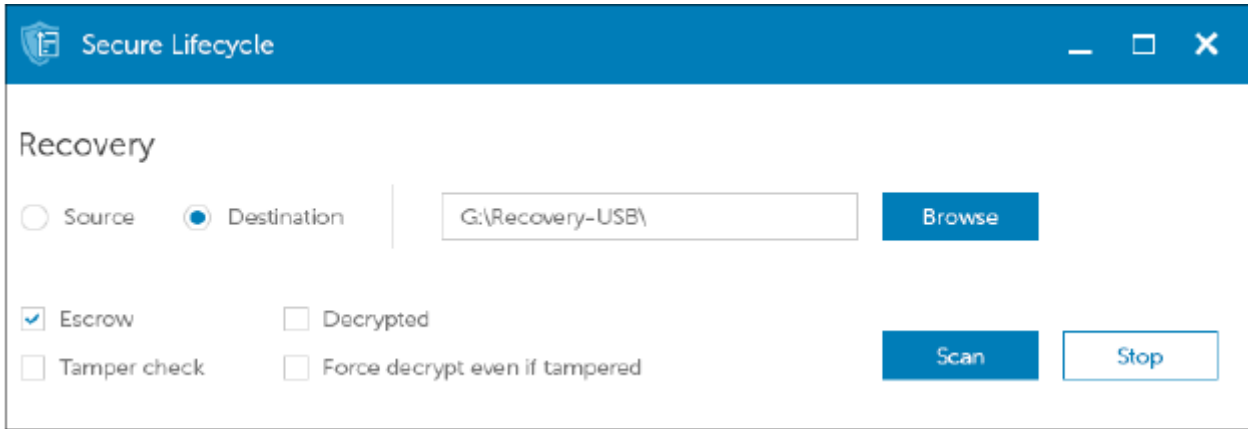
5 Select **Source**.

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

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



- 7 Click **OK**.
- 8 Click **Destination**



- 9 Click **Browse** to select a destination, such as an external device, a directory location, or the Desktop.
- 10 Click **OK**.
- 11 Select one or more check boxes based on what you want to recover.

Options	Description
Escrow	<ul style="list-style-type: none"> • Recover offline-generated keys that could not be escrowed to the DDP 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.
Decrypted	<p>Point the recovery tool to a directory that contains protected Office documents to decrypt them.</p> <p>Optionally, if tampering has occurred, select one or both of these options (see below for details):</p> <ul style="list-style-type: none"> • 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, Secure Lifecycle repairs the wrapper and decrypts the Office document.
Tamper check	<p>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.</p>
Force decrypt even if tampered	<p>To select this option, you must also select Tamper check.</p> <p>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 Secure Lifecycle, select this option to repair the wrapper and to force decryption of the protected Office file.</p> <p>Note: If someone tampered with the encrypted Office .xen file within the wrapper, the file cannot be recovered.</p>

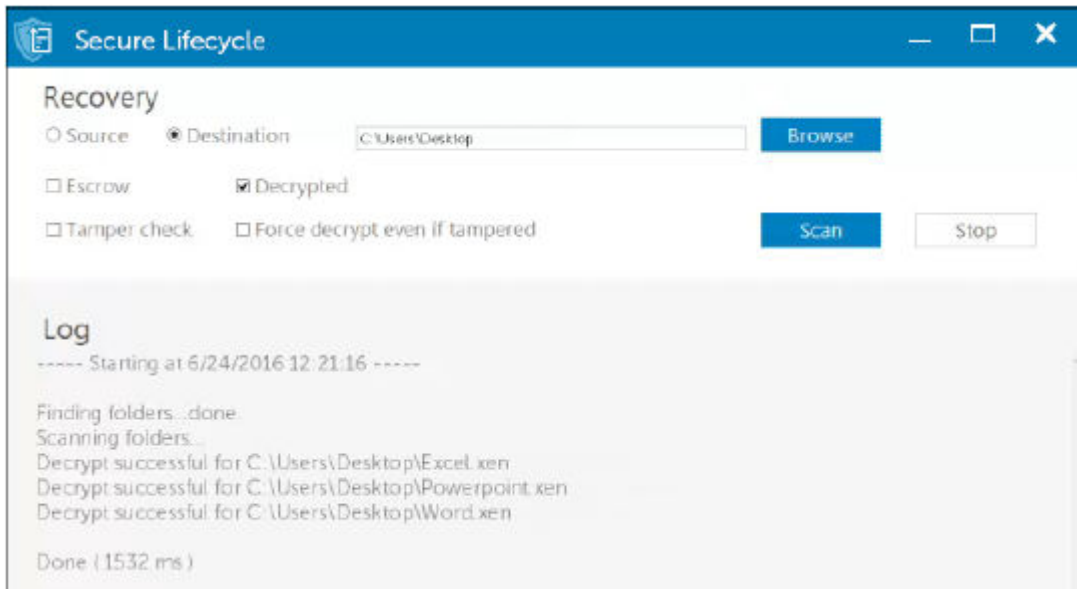
Each protected Office document has a hidden watermark that contains a history of the original user and computer name and any other computer name that modified the file. By default, the recovery tool checks the hidden watermarks and logs the information.

- 12 After selections are complete, click **Scan**.



The Log area displays:

- Folders found and scanned within the selected source
- Whether decryption was successful or failed



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

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, follow the instructions in this Microsoft article:

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