Encryption Recovery v11.9



January 2024 Rev. A01

Notes, cautions, and warnings

(i) 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.

© 2012-2024 Dell Inc. All rights reserved. Registered trademarks and trademarks used in the Dell Encryption and Endpoint Security Suite Enterprise 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®, Windows Vista®, 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 ^{5M} 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.

Contents

Chapter 1: Getting Started with Recovery	5
Contact Dell ProSupport for Software	5
Chapter 2: Policy-Based or File/Folder Encryption Recovery	6
Perform System Data Encryption or FFE Recovery	6
Overview of the Recovery Process	6
Obtain the Recovery File - Policy-Based Encryption or FFE Encryption Client	6
Obtain the Recovery File - Locally Managed Computer	7
Perform a Recovery	8
Encrypted Drive Data Recovery	
Recover Encrypted Drive Data	
Chapter 3: Hardware Crypto Accelerator Recovery	16
Recovery Requirements	
Overview of the Recovery Process	16
Perform HCA Recovery	16
Obtain the Recovery File - Remotely Managed Computer	
Obtain the Recovery File - Locally Managed Computer	17
Perform a Recovery	18
Chapter 4: Self-Encrypting Drive (SED) Recovery	24
Recovery Requirements	24
Overview of the Recovery Process	24
Perform SED Recovery	24
Obtain the Recovery File - Remotely Managed SED Client	24
Obtain the Recovery File - Locally Managed SED Client	25
Perform a Recovery	25
Challenge Recovery with SED	28
Chapter 5: Full Disk Encryption Recovery	31
Recovery Requirements	
Overview of the Recovery Process	31
Perform Full Disk Encryption Recovery	31
Obtain the Recovery File - Full Disk Encryption Client	
Perform a Recovery	
Challenge Recovery with Full Disk Encryption	
Chapter 6: Full Disk Encryption and Dell Encryption Recovery	
Recovery Requirements	
Overview of the Recovery Process	
Perform Recovery of a Full Disk Encrypted and Dell Encrypted Disk	
Obtain the Recovery File - Full Disk Encryption Client	
Obtain the Recovery File - Policy-Based Encryption or FFE Encryption Client	39
Perform a Recovery	40

Challenge Recovery with Full Disk Encryption	
Chapter 7: PBA Device Control	
Use PBA Device Control	
Chapter 8: General Purpose Key Recovery	47
Recover the GPK	47
Obtain the Recovery File	
Perform a Recovery	
Chapter 9: BitLocker Manager Recovery	
Recover Data	
Chapter 10: Password Recovery	
Recovery Questions	
Chapter 11: Encryption External Media Password Recovery	
Recover Access to Data	55
Self-Recovery	57
Chapter 12: Appendix A - Download the Recovery Environment	59
Chapter 13: Appendix B - Creating Bootable Media	60
Burning the Recovery Environment ISO to CD/DVD	
Burning the Recovery Environment on Removable Media	60

Getting Started with Recovery

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

- CD-R, DVD-R media, or formatted removable media
 - If burning a CD or DVD, review Burning the Recovery Environment ISO to CD/DVD for details.
 - If using removable 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 for Software

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 for Software international phone numbers.



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.

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

Perform System Data Encryption or FFE Recovery

Follow these steps to perform System Data Encryption recovery.

Overview of the Recovery Process

NOTE: For Dell Servers running v10.2.8 and earlier, recovery requires a 32-bit environment. Dell Servers running v10.2.9 and later provide 32-bit and 64-bit recovery bundles.

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.

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

Obtain the recovery file.

The recovery file can be downloaded from the Management Console. To download the Disk Recovery Keys generated when you installed Dell Encryption:

- a. Open the Management Console and, from the left pane, select Populations > Endpoints.
- b. Enter the hostname of the endpoint, then click Search.
- c. Select the name of the endpoint.
- d. Click Device Recovery Keys.

Endpoint De	etail for:				
Details &	Actions	Security Policies	Users	Endpoint Groups	Threat Ev
Endpoint Detail					
Fremove Remove					
Category:	WINDO	WS			
OS/Version:	Microso	ft Windows 10 Enterprise /	10.0.14393		
Processor:	Intel(R)	Core(TM) i7-6700HQ CPU	@ 2.60GHz		
Serial Number:					
Host ID:					
Unique ID:					
Hardware ID:					
Protected:	6/4/19 6	5:55 PM			
Shield Detail			/		
View Effective	Policies 🔍	Device Recovery Keys			
nter a password	to download	I the Device Recovery	Keys.		
Recovery				×	
Recovery of	detected. P	lease enter a passv	word and do	wnload.	
Password:		•••••]		
		Download	Can	cel	

f. Copy the Device Recovery Keys 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.

(i) 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.

	Admi	nistrator: Wi	nPe Environment	-3
01/16/2014	08:50 AM	(DIR)	lt-lt	~
01/16/2014	08:50 AM	(DIR)	10-10	
01/16/2014	08:50 AM	(DIR)	nb-no	
01/16/2014	08:50 AM	<dib></dib>	nl-nl	
01/16/2014	08:50 AM	(DIR>	p1-p1	1.0
01/16/2014	08:50 AM	(DIR)	pt-br	1211
01/16/2014	08:50 AM	(DIR)	pt-pt	
01/16/2014	08:50 AM	(DIR)	ro-ro	
01/16/2014	08:50 AM	(DIR)	ru-ru	
01/16/2014	08:50 AM	(DIR)	sk-sk	
81/16/2014	08:50 AM	(DIR)	sl-si	
01/16/2014	08:50 AM	(DIR)	sources	
01/16/2014	08:51 AM	(DIR)	sr-lata-cs	
01/16/2014	08:51 AM	(DIR)	5V-S6	
01/16/2014	08:51 AM	(DIR)	tr-tr	
01/16/2014	08:51 AM	(DIR)	uk-ua	
01/16/2014	08:51 AM	DIR2	2h-cn	
01/16/2014	08:51 AM	(DIR)	zh-hk	
01/16/2014	08:51 AM	(DIR)	zh-tw	
	2 File(s)	1,515	,580 bytes	
	38 Dir(s)	7,701,409	,792 bytes free	
C:\>cd Keys				
C+> Vous >I Co	Parauanu 5420	1001		~
C- Che ys 2Lon	necevery 5430	ICHT 10 X0		

- 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.

1999 F. 1997		
đ	Dell Data Protection Encryption	
Dé	L Data Protection Encryption	Þ
Whic	sh of the following best describes your problem?	
	My system fails to boot and displays a messa perform SDE Recovery.	age asking me to
	My system does not allow me to access encry policies, or is being reinstalled.	vpted data, edit
	○ I want to decrypt my HCA encrypted drive.	
	\cap I want to restore access to my HCA encrypted	drive.
	(Back Next)	Fields Centrel

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.

	Dell Data Protection Encryption	
Déli	Data Protection Encryption	
Backu	ip and Recovery Information	
Back Local Host MCID DCID Seria Asset Back	up File Information ly Managed Name = 5430HCA1 = YC&DXITV INumber = 28CFVY1 INumber = 28CFVY1 ITag = 28CFVY1 uFileDate = 2014-01-16 15:12:16Z	^
Recor	very Host information	. ·
	< Back Einish	Cancel

 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.

63		Dell Data Protectio	n Encryption		
E	XALL •	ala Protection Encry	notion		
_			_		•
	Select the ve	alume to recover.			
	_				
	Disk		Size	Туре	
	Disk 1 -	SanDisk Ultra Backu	7.45 GB	USB	
					Betresh
	1				Pienesn
					1 1
		< Back	Next >	Einish	Cancel

7. Enter your recovery password and click Next.

With a remotely managed client, this is the password provided in step e 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.

	Dell Data Protection Encryption	(a) 0 E
D¢	Data Protection Encryption	
Ple	ease enter your recovery password.	
	Password:	
	< Back Next > E	nish Cancel

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

	Dell Data	Protection Encr	yption	0
Kell	Data Protection	Encryption		
tess Reco	ver" to proceed.			
			~	
i				
			Recover	
	(Back	Net	N Finish	Cancel

9. When recovery is complete, click Finish.

(i) 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 using an alternate boot media. When connecting a drive protected by Dell Encryption to another system that also runs Dell Encryption, files will be viewable when browsing the directories. However, if you attempt

to open or copy a file, an Access Denied error will appear. When connecting a Dell Encrypted drive to a system that does not currently have Dell Encryption installed, attempting to open data will result in cipher text being displayed.

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."

Encr	yption						
Summary: Scanne	d 1 drive(s), 4 folde	er(s) to find 19 en	crypted file(s) to	taling 5617780	96 bytes.		
Clear		Sea	rch		<<	Simple	
	ty Ewed De	i une					
rive Types to Sear	on: Inixed Dr	ives	•				
ncryption Report T	ype: Encrypte	ed Files	•				
2017-07-21 17:35	:13] Commor	1M11HKWL DE	VICE_: "C:\Usen	s\Tech\Desktop	CmgMast	terInstalle	1
2017-07-21 17:35	:13] Commor	1M11HKWL DE	VICE_: "C:\User	s\Tech\Desktop	CmgMast	terInstalle	
2017-07-21 17:35	13] Common	1M11HKWL_DE	VICE : "C:\Usen	s Tech Desktop	CmgMast	terInstalle	
2017 07 21 17.00	13] Commor	1M11HKWL DE	VICE : "C: User	s\Tech\Deskton	CmgMast	terInstalle	
2017-07-21 17:35	1401			a the production of	Contract Forest		
[2017-07-21 17:35	:13] Commor	1M11HKWL DE	VICE_: "C: User	s\Tech\Desktop	CmgMast	terInstalle	
[2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35	:13] Commor :13] Commor	1M11HKWL _DE	VICE_: "C:\Usen VICE_: "C:\Usen	s\Tech\Desktop s\Tech\Desktop	CmgMast CmgMast	terInstalle terInstalle	
[2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35	13] Commor 13] Commor 13] Scan complete	1M11HKWL DE 1M11HKWL DE	VICE_: "C:\User VICE_: "C:\User	s\Tech\Desktop s\Tech\Desktop	CmgMast CmgMast	terInstalle terInstalle	
[2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35	:13] Commor :13] Commor :13] Scan complete :13] Summary: Scanned	1M11HKWL _DE 1M11HKWL _DE	VICE_: "C:\Usen VICE_: "C:\Usen der(s) to find 19	s\Tech\Desktop s\Tech\Desktop encrypted file(s	CmgMast CmgMast	terInstalle terInstalle	
[2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35	13] Commor 13] Commor 13] Scan complete 13] Summary: Scanned	1M11HKWL DE 1M11HKWL DE 1. d 1 drive(s), 4 fok	VICE_: "C:\Usen VICE_: "C:\Usen der(s) to find 19	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast	terInstalle terInstalle 56177809	
2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35	13] Commor 13] Commor 13] Scan complete 13] Summary: Scanned	1M11HKWL_DE 1M11HKWL_DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User VICE_: "C:\User	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle terInstalle 56177809	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35	13 Commor 13 Commor 13 Scan complete 13 Summary: Scanned	1M11HKWL DE 1M11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle terInstalle 56177809	
2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 < Scan Settings	13] Commor 13] Commor 13] Scan complete 13] Summary: Scanned	1M11HKWL DE 1M11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User VICE_: "C:\User	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast	terInstalle 56177809 >	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 consettings Search Path: C:	Users\Tech\Deskto	1M11HKWL DE 1M11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle terInstalle 56177809	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 consettings Search Path: C:	Users\Tech\Deskto	1M11HKWL DE 1M11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User ler(s) to find 19	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle 56177809 	
2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 Scan Settings Search Path: C: [] Outp	USers\Tech\Deskto	1M11HKWL DE 1M11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User ler(s) to find 19	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle 56177809	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 < Scan Settings Search Path: C: ↓ Outp File	Users\Tech\Deskto	1M11HKWL DE 1M11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User ler(s) to find 19	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle 56177809 	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 < Scan Settings Search Path: C: ↓ Outp File Path: C:	Users\Tech\AppDa	ata \Local\Temp\W	VICE_: "C:\User VICE_: "C:\User ler(s) to find 19 SScan.log	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 < Scan Settings Search Path: C: ↓ Outp File Path: C: ↓	Users\Tech\Deskto	1 IM11HKWL DE 1 IM11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User ler(s) to find 19 ler(s) for find 19 SScan.log	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 Search Path: C: V Outp File Path: C: (* Format	Users\Tech\Deskto	ata\Local\Temp\W	VICE_: *C:\User VICE_: *C:\User ler(s) to find 19 SScan.log	s\Tech\Desktop s\Tech\Desktop encrypted file(s Existing File	(CmgMast (CmgMast)totaling 5	terInstalle	
2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 2017-07-21 17:35 < Scan Settings Search Path: C: ↓ Outp File Path: C: ↓ C:	Users\Tech\Deskto Users\Tech\Deskto Users\Tech\Deskto Users\Tech\AppDa	1 IM11HKWL DE 1 IM11HKWL DE d 1 drive(s), 4 fok	VICE_: "C:\User VICE_: "C:\User ler(s) to find 19 SScan.log	s\Tech\Desktop s\Tech\Desktop encrypted file(s	(CmgMast (CmgMast)totaling 5	terInstalle	
[2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 [2017-07-21 17:35 < Scan Settings Search Path: C: ↓ Outp File Path: C: ↓ Outp File Format ↓ Repc ↓ Value	Users\Tech\Deskto Users\Tech\Deskto Users\Tech\Deskto Users\Tech\AppDa Overwrite Existing	ata \Local\Temp\W File	VICE_: "C:\User VICE_: "C:\User VICE_: "C:\User der(s) to find 19 SScan.log C Add to I	s\Tech\Desktop s\Tech\Desktop encrypted file(s Existing File	(CmgMast (CmgMast)totaling 5	terInstalle	

- 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.

300 - DDPE -	• 64bit Utilities • Dell-Offline-Admin-64	bit-8.1.0.482 • • 🛂 🗍	Search Dell-Offline-Ad	min-64bit-8	
Organize - 🗟 Open	New folder			III • 13	0
* Favorites	Name +	Date modified	Туре	Size	
Desktop	JE Documentation	10/16/2013 4:27 PM	File foilder		
👍 Downloads	CmgAd	9/11/2013 10:09 AM	Application	1,389 KB	
Secent Places	CmgAlu	9/11/2013 10:09 AM	Application	992 KB	
	📉 CmgAu	9/11/2013 10:09 AM	Application	1,482 KB	
Call Libraries	CmgCryptoLib.dll	7/10/2012 6:08 PM	Application extens	608 KB	
Documents	CmgCryptoLib.mac	7/10/2012 6:08 PM	MAC IFile	1 KB	

 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.

Dél	Data Pro	lection End	ryption	
Device Server	https://ddpe.dp	e.com:xxxx/xap	v	i i
Dell Admin:	superadmin			
Password:				
MCID:	1			1
DCID:	ENDTEFDZ			

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

Dell Administ	trative U	tility	1
D¢	LL	Data Protection Encryption	
Have you alw	eady perf	ormed a download for this MCID?	
C Yes, work	c offline w	ith a previously downloaded file.	
1* No, perto	m a dow	nioad from a server now.	

(i) NOTE:

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

< Back Next >

Cancel

 When download and unlock are complete, copy files you need to recover from this drive. All files are readable. Do <u>not</u> 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

(i) 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

(i) 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.

Dell Administrative Download

Deell En	cryption	
Device Server Dell Admin: Password:	https://server.domain.com:8443/xapi/ Forensic@Dom.ain	
MCID: DCID:	FQDN.Dom.ain ABCD1234	
	< Back Next >	Cancel

 \times

- 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**.

(i) NOTE:

You must remember this password to access the recovery keys.

Recovery	×
Recovery detected	Please enter a password and download.
rasarota.	Download Cancel

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.

(i) 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.

	Administrat	or: WinPe Environment	-25
01/16/2014	08:50 AM (DIR)	lt-lt	~
01/16/2014	08:50 AM <dir></dir>	1 u -1 u	
01/16/2014	08:50 AM <dir></dir>	nb-no	
01/16/2014	08:50 AM <dir></dir>	nl-nl	
01/16/2014	08:50 AM <dir></dir>	p1-p1	110
01/16/2014	08:50 AM (DIR)	pt-br	100
01/16/2014	08:50 AM (DIR)	pt-pt	
01/16/2014	08:50 AM <dir></dir>	ro-ro	
01/16/2014	08:50 AM <dir></dir>	ru-ru	
01/16/2014	08:50 AM <dir></dir>	sk-sk	
81/16/2014	08:50 AM (DIR)	sl-si	
01/16/2014	08:50 AM (DIR)	sources	
01/16/2014	08:51 AM <dir></dir>	sr-lata-cs	
01/16/2014	08:51 AM <dir></dir>	sv-se	
01/16/2014	08:51 AM <dir></dir>	tr-tr	
01/16/2014	08:51 AM (DIR)	uk≁ua	
01/16/2014	08:51 AM DIR	2h-cn	
01/16/2014	08:51 AM <dir></dir>	zh-hk	
01/16/2014	88:51 AM <dir></dir>	zh-tw	
	2 File(s)	1,515,580 bytes	
	38 Dir(s) 7,7	81,409,792 bytes free	
G: >cd Keys			
C:\Keys>LSA	Recovery_5430HCA1.	2X0	~

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

-	Dell Data Protection Encryption	a i n 💼
	D&LL Data Protection Encryption	D
Г	Which of the following best describes your problem?	
	My system fails to boot and displays a message asking me to perform SDE Recovery.	
	My system does not allow me to access encrypted data, edit policies, or is being reinstalled.	
	$\widehat{\mbox{\ \ e}}$) want to decrypt my HCA encrypted drive.	
	Γ^{\ast}) want to restore access to my HCA encrypted drive.	
	Clinck Next > Finish	Cencel

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

-	Dell Data Protection Encryption	
	DELL Data Protection Encryption	
	Backup and Recovery Information	
	Backup File Information Locally Managed HostName = 5430HCA1 MCID = 5430HCA1 DCID = YCGLXJ7V SerialNumber = 2BCFVY1 AssetTag = 2BCFVY1 BackupFileDate = 2014-01-16 15:12:16Z	
	Recovery Host Information	>
	< Back Einish	Cancel

 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.

	11 · · ·
63	Dell Data Protection Encryption
	DELL Data Protection Encryption
	Select the volume to recover.
	Disk Size Type
	S Disk 0 - SAMSUNG SSD SM0 119.24 GB SATA
	Refresh
	< Back Next > Einish Cancel

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.

ð	De	II Data Prot	ection Encryption	n	0 0 0
DĘ	LL Data Pr	olection E	ncryption		
Ple	ase enter your	recovery pa	ssword.		
	Password:				
		(Back	Next >	Finish	Cancel

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

	Dell Data Protection Encryption	0 0
Dél	Data Protection Encryption	
Press Theo	cover" to proceed.	
6	Recover	
	< Back Next > Finish	Cancel

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

Press "Recover" to p	Browse for Folder
c	Computer → Removable Disk (C:) → All CD Drive (D:) → Boot (k:)
	OK Cancel

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

Dell Data Protection Encryption	
Dista Protection Encryption	
Press "Recover" to proceed.	
Decryption Speed = 0.0MB/S ^ Time Elepted = 0:00:00 Time Remaining = 0:00:00 Decrypted 0MB of 63949MB remaining.	
< > Cancel	
L Date	
< Beck Next > Einish	Cancel

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

Dell Data Protection	Encryption
Deta Protection Encrypt	ion
Page "Barrup" to proved	
nes recire uproces.	
Decryption Speed = 31.5MB/S Time Bapsed = 0:33:51 Time Remaining = 0:00:00 Decryption Speed = 0:00:00	-
Recovery completed successfully!	
	Recover
(< Back	Next > Einish Cancel
	geod > Einish Cancel

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 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: For Dell Servers running v10.2.8 and earlier, recovery requires a 32-bit environment. Dell Servers running v10.2.9 and later provide 32-bit and 64-bit recovery bundles.

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.

Dell Data Security					superadmin 🔒	٠	?
Dashboard	Recover [Data					
Populations Reporting	Shield	Manager	РВА				
Management	Recover PBA B	ndpoint					
Commit	Hostname:	1		Search			
Log Analyzer	PBA:						
Recover Data					Create Recov		e i
Recover Endpoint							

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.

(i) 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.

C Administrator	SED Recovery WinP	e Enveranment	
SED Recovery	utility work	ing, Please do not power off y	bur machine
		Dell Recovery Utility	
		Encryption Not found SED disk or Dell Encrypted FDB (* Self-Encryption Drive)	disk C Full Disk Encryption
		Path to recovery file	
			Browse
		If you do not provide recovery default disk key (default MSID) the disk has not been taken.	file, recovery will be attempted with the This will succeed only if ownership of
		Recovery type One-time unlock of the drive Unlock drive and remove PBA	Unlocks the drive temporarily until the next power-off. PBA is automatically enabled after power-off.
			OK Cancel
		Open	
Look	r: Kest	Open	
Look	e: Keys Name	Open 👻 🍝 🗈	i 🗗 🖬 🕶
Look Pecet place	e: 🔛 Køys Name GpillSPKej	Open v 🗲 🗲 Date / vE54305ED.recovery.dat 1/16/2	ed fiel Type 14 1005AM DAT File
Look Pecet place Librares Librares Conputer	in: Koys Name Gp(ISPKe)	Open v & C Dater v£54205ED.recovery.dat 1/16/2	ved find Type DI4 1005AM DAT File
Look Pecet place Ubranes Looputer	er: Roys Name GpdSPKey	Open v & C Dater v£54205ED.recovery.dat V15/2	ved find Type DI4 10:05 AM DAT File
Look Pecert place Ubranes Computer	e: Aoys Name GpillSPKe CpillSPKe	Open Date r yE34305ED.recovery.dit V136/2 OpdSPKey.E54305ED.recovery	Copen

- 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.

	Encryption	
	Not found SED disk or Dell Encrypted FDE disk	
	C Self-Encryption Drive Full Disk Encryption	
	Path to recovery file	
	l L	Browse
	If you do not provide recovery file, recovery will succeed is not encrypted. Press OK to start the decryption proces take long time. Please do not power down the machine.	only if the disk is. This may
	OK	Cancel
Windows Recovery Er	wironment	
Carl and the second sec		3
Select Administrator: SED Recovery Wi	ife frivatiment	
CED Recovery utility is done		
Press any key to continue .		
		ALS A ALSO ALSO
- Part - Part		

Dell Recovery Utility

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



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

(i) 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

(i) NOTE: The Challenge Response recovery method is available only to domain user accounts.

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**.

Trouble signing in		Challenge Response
Network Information		Recovery Questions
Server Sync		
Keyboard	•	
Support Information		
About		
Shut Down		
Options		

The following information appears after selecting Challenge Response.

34E6D7400	6CE				
Challenge Code					
C1D3	293E	99F3	1425		
4F5B	B902	6172	870C		
Response Code	0				
1					

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.

Dell Data Security		superadmin 🛔 🗢 ?
Dashboard Populations Reporting Management Commit Log Analyzer	Recover Data Shield Manager PBA Recover PBA Endpoint I Search PBA I Search	
Recover Endpoint Licerne Management Services Management Notification Management External User Management	Recover PBA User Access Hostname Distain Host Name, User Name, and Challenge code. Hostname Enser Host Name and click sench. Select the user from the list of users for the explort, Enter the Challenge Code and press Generate Response Code. Username Instruct user to enter the provided Response Code on their computer. Challenge	Citata Necovery File Smirch Generalis Response

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

lecover Data						
Shield Manager	PBA					
ecover PBA Endpoint						
ostname.						Search
BA:						
ecover PBA User Access						
BA: ecover PBA User Access Ibtain Host Name, User Name, and	d Challenge code.	Hostname:	34E6D74	1006CE		
ecover PBA User Access Ibtain Host Name, User Name, and Inter Host Name and click search, it of users for the endpoint. Enter ress Generate Response Code.	d Challenge code. Select the user from the the Challenge Code and	Hostname: Username:	34E6D74	1006CE		
BA: ecover PBA User Access btain Host Name, User Name, and iter Host Name and click search, t of users for the endpoint. Enter ess Generate Response Code. struct user to enter the provided	d Challenge code. Select the user from the the Challenge Code and Response Code on their	Hostname: Username: Challenge:	34E6D74 test1 C1D3	293E	99F3	1425

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.

opinaet four in	i adminiscrator ci	o receive the Re	sponse Code to uni	ick your compu	tor	
34E6D7400	6CE					
Challenge Cod	9					
C1D3	293E	99F3	1425			
4F5B	B902	6172	870C			
Response Cod	a					
A1FA	56E8	DB78	39D3			
0F51	2110	9514	8E7C		4	

After successful authentication, the following message appears:

Authent	cation successfu	t Please wait				
Device Name	6					
34E6D740	06CE					
Challenge Co	de					
C1D3	293E	99F3	1425			
4F5B	B902	6172	870C			
Response Co	>de					
A1FA	56E8	DB78	39D3			
0F51	2110	9514	8E7C	4		

Challenge recovery is complete.

Full Disk Encryption Recovery

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

(i) 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

(i) 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.

Dell Data Security					superadmin 🔒	٠	?
Dashboard	Recover [Data					
Populations Reporting	Shield	Manager	РВА				
Management	Recover PBA B	ndpoint					
Commit	Hostname:	1		Search			
Log Analyzer	PBA:						
Recover Data					Create Recov		e i
Recover Endpoint							

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.

(i) 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 R	ecovery Envir	onment		
GG Administrator S	ED Recovery WinP	e Environment		
SED Recovery u	utility work:	ing, Please do not power	off your machine	
		Dell Recovery Utility		×
		Encryption		
		Not found SED disk or Dell Encry	vpted FDE disk	
		Rath to recovery file	(* Full Disk Encrypto	ū
				Browse
		If you do not provide is not encrypted. Pres take long time. Please	recovery file, recovery will succe as OK to start the decryption pro do not power down the machine	eed only if the disk cess. This may t.
			ок	Cancel
		Open		
Look in	📕 Keys	•	+ 🗈 🗗 🗊-	
2.5	Name	CS4305ED Increases July	Date modified Typ	e Ede
Recert places	Spinent			
	¢			>
	File name	OpdSPKey.E5430SED recovery	- Open	
	Files of type	All Flex (")	Caro	

4. Click OK.



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

 Self-Encrypting Drive recovery Exit this menu 	er	🛋 Administrator: Select option from list and pres
x) Exit this menu		 Self-Encrypting Drive recover
		(x) Exit this menu
r) Reboot this PC		(r) Reboot this PC

6. Press r to reboot the computer.

(i) 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**.

Trouble signing in		Challenge Response
Network Information		Recovery Questions
Server Sync		
Keyboard	•	
Support Information		
About		
Shut Down		
Options	_	

The following information appears after selecting Challenge Response.

	Device Name					
	34E6D7400	6CE				
	Challenge Code	(
	C1D3	293E	99F3	1425		
	4F5B	B902	6172	870C		
	Response Code	0				
	1					
ŧ.						

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.

Dell Data Security		superadmin 🛔 🗢 ?
Dashboard Populations Reporting Management Commit Log Ansiyser	Recover Data Sheeld Manager PBA Recover PBA Endpoint Hostname I FBA	
Recover Endpoint Uceme Management Services Management Notification Management External User Management	Recover PBA User Access Ditain Host Name, User Name, and Challenge code. Enser Host Name and click search. Select the user from the list of users for the andport. Enser the Challenge Code and press Generate Response Code on their computer. Instruct user to enter the provided Response Code on their computer.	Greenie Response

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

ecover [Data						
Shield	Manager	PBA					
scover PBA E	indpoint						
ortname							Search
Grade har time .							
BA:							
IA: ecover PBA L	Jser Access						
BA: ecover PBA (Ibtain Host Nar	Jser Access ne, User Name, and	Challenge code.	Hostname:	34E6D74	1006CE		
BA: BA: btain Host Narr tof users for the ress Generate F	Jser Access ne, User Name, and e and click search. S he endpoint. Enter t Response Code.	Challenge code. Select the user from the the Challenge Code and	Hostname: Username:	34E6D74 test1	1006CE		
ecover PBA L btain Host Nam tof users for ti ess Generate F struct user to e	Jser Access ne, User Name, and e and click search. S he endpoint. Enter t Response Code. enter the provided F	Challenge code. Select the user from the the Challenge Code and Response Code on their	Hostname: Username: Challenge:	34E6D74 test1 C1D3	293E	99F3	1425

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.

Device Name							
enge Code	6. 1						
C1D3	293E	99F3	1425				
F5B	B902	6172	870C				
onse Code	,						
1FA	56E8	DB78	39D3				
DEE4	2110	9514	8E7C				
	is Name 6D7400 sngs Code 1D3 F58 sonse Code	e Name 6D74006CE enge Code 1D3 293E F58 B902 onse Code NFA 56E8	28 Name 6D74006CE enge Code 7D3 293E 99F3 F58 B902 6172 onse Code NFA 56E8 DB78	e Name 6D74006CE enge Code 2D3 293E 99F3 1425 F58 B902 6172 870C conse Code NFA 56E8 DB78 39D3	a Name 6D74006CE enge Code 2D3 293E 99F3 1425 F58 B902 6172 870C ranse Code VFA 56E8 DB78 39D3	e Name 6D74006CE enge Code 1D3 293E 99F3 1425 F58 B902 6172 870C conse Code NFA 56E8 DB78 39D3	a Name 6D74006CE enge Code 203E 99F3 1425 F58 B902 6172 870C onse Code NFA 56E8 DB78 39D3

After successful authentication, the following message appears:

Authent	cation successfu	. Please wait				
Device Name						
34E6D740	006CE					
Challenge Co	de					
C1D3	293E	99F3	1425			
4F5B	B902	6172	870C			
Response Ca	ode					
A1FA	56E8	DB78	39D3	N		
0F51	2110	9514	8E7C	14		

Challenge recovery is complete.

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.

(i) 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

(i) NOTE: Full Disk Encryption recovery requires a 64-bit environment. For Dell Servers running v10.2.8 and earlier, Policy-Based Encryption and FFE recovery requires a 32-bit environment. Dell Servers running v10.2.9 and later provide 32-bit and 64-bit recovery bundles.

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.

Dell Data Security					superadmin 💄	٠
Dashboard	Recover I	Data				
Populations Reporting	Shield	Manager	РВА			
Management	Recover PBA I	Endpoint				
Commit	Hostname:	1		Search		
Log Analyzer	PBA:					
Recover Data					Create Recov	
Recover Endpoint						

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

Obtain the recovery file.

The recovery file can be downloaded from the Management Console. To download the Disk Recovery Keys generated when you installed Dell Encryption:

- a. Open the Management Console and, from the left pane, select **Populations > Endpoints**.
- **b.** Enter the hostname of the endpoint, then click **Search**.
- c. Select the name of the endpoint.
- d. Click Device Recovery Keys.

Endpoint De	etail for:				
Details &	Actions	Security Policies	Users	Endpoint Groups	Threat Events
Endpoint Detail					
TRemove					
Category:	WINDO	WS			
OS/Version	Microso	ft Windows 10 Enterprise /	10.0.14393		
Processor:	Intel(R)	Core(TM) i7-6700HQ CPU	@ 2.60GHz		
Serial Number:					
Host ID:					
Jnique ID:					
Hardware ID:					
Protected:	6/4/19 (5:55 PM			
Shield Detail			/		
View Effective	Policies 🔍	Device Recovery Keys			

e. Enter a password to download the Device Recovery Keys.

Recovery	y
----------	---

Recovery detected. Please enter a password and download.

Password:	•••••	
	Download	Cancel

f. Copy the Device Recovery Keys 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.
 - **(i) NOTE:** Disable SecureBoot before the recovery process. When finished, re-enable SecureBoot.

Administrator: Select option from list and press enter	
(1) Self-Encrypting Drive or FDE recovery	
(x) Exit this menu	
(m) Mount FDE-Encrypted Disk	
(r) Reboot this PC	
Enter option from above list and press enter : m	
Enter full path to recovery key file :	

- 2. Choose option three and press Enter.
- 3. When prompted, Enter the recovery file name and location .

Self-Encrypting Drive or FDE recovery
 (x) Exit this menu
 (m) Mount FDE-Encrypted Disk
 (r) Reboot this PC
 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

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



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.

Dell Administrative Utility		×
Encryption	_	-
Have you already performed a down	nload for this MCID? sly downloaded file. server now.	
	< <u>B</u> ack <u>N</u> ext	> Cancel

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

Dell Administrative Utility

Deell Enc	ryption	-	-	-
Downloaded file: Passphrase:	FQDN.Dom.ain			
		< Back	Next >	Cancel

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.

 \times

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**.

Trouble signing in		Challenge Response
Network Information		Recovery Questions
Server Sync		
Keyboard	•	
Support Information		
About		
Shut Down		
Options	_	

The following information appears after selecting Challenge Response.

	Contact Your II	warminal wor to	receive the rost	poise code to t	ioox your comparer		
	Device Name						
	34E6D7400	6CE					
	Challenge Code						
	C1D3	293E	99F3	1425			
	4F5B	B902	6172	870C			
	Response Code	0					
	1						
4							

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.

Dell Data Security		superadman 🛔 🗢 ?
Dashboard Populations Reporting	Recover Data Sheld Manager PBA	
Management Commit Log Analyzer Recover Data	Recover PBA Endpoint Holimame I Sierch PBA:	Create Recovery Har
Recover Endpoint Liceme Management Services Management Notification Management Esternal User Management	Recover PBA User Access Datain Host Name, User Name, and Challenge code. Hostname. Enter Host Name and click search. Select the user from the list of users for the endpoint. Enter the Challenge Code. Userneme: Chocsel Code. Instruct user to enter the provided Response Code on their computer. Challenge Image: Training Code. Response Code on their computer. Response: Feature: Image: Training Code.	Smith Server the Response

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

Recover Data

Shield	Manager	PBA					
Recover PBA E	indpoint						
fostname:							Search
PBA:							
Recover PBA L	Jser Access						
Recover PBA L Obtain Host Nan	Jser Access ne, User Name, and	Challenge code.	Hostname:	34E6D74	1006CE		
Recover PBA L Obtain Host Nam Inter Host Name st of users for the press Generate F	Jser Access ne, User Name, and e and click search. S he endpoint. Enter t Response Code.	Challenge code. elect the user from the he Challenge Code and	Hostname: Username:	34E6D74 test1	1006CE		
Recover PBA L Obtain Host Nam Enter Host Name ist of users for th press Generate F Instruct user to a	Jser Access ne, User Name, and e and click search. S he endpoint. Enter t Response Code.	Challenge code. elect the user from the he Challenge Code and lesponse Code on their	Hostname: Username: Challenge:	34E6D74 test1 C1D3	293E	99F3	1425
Recover PBA L Dbtain Host Name ist of users for th press Generate F Instruct user to e computer.	Jser Access ne, User Name, and e and click search. S he endpoint. Enter t Response Code. enter the provided R	Challenge code. elect the user from the he Challenge Code and lesponse Code on their	Hostname: Username: Challenge:	34E6D74 test1 C1D3 4F5B	293E 8902	99F3 6172	1425 870C

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.

Davies Name					
34E6D7400	6CE				
Challenge Code					
C1D3	293E	99F3	1425		
4F5B	B902	6172	870C		
Response Code	0				
A1FA	56E8	DB78	39D3		
0F51	2110	9514	8E7C	4	
			has a set of the set o		

After successful authentication, the following message appears:

Authent	cation successfu	/ Please wait				
Device Name						
34E6D740	006CE					
Challenge Co	ide					
C1D3	293E	99F3	1425			
4F5B	B902	6172	870C			
Response Co	ode					
A1FA	56E8	DB78	39D3			
0F51	2110	9514	8E7C	15		

Challenge recovery is complete.

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 Locked". To re-purpose the SED, remove the PBA with the SED Recovery app.

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.

Dell Administra	tive Download			×
	ncryption	-	-	-
Device Server Dell Admin:	https://server.do Forensic@Dom.a	main.com:8443 iin	/xapi/	
Password: MCID:	FQDN.Dom.ain			
DCID:	JABCD1234	< Back	Next >	Cancel

- 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.

Recovery		×
Recovery detected.	Please enter a password an	d download.
Password:		
	Download	Cancel

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

Perform a Recovery

- 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.
- 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.

I contract of the Community	Administrator: WinPe	Environment	×
01/16/2014 08:50 AM	<dir></dir>	lt-lt	6
01/16/2014 08:50 AM	<dir></dir>	10-10	
01/16/2014 08:50 AM	<dir></dir>	nb-no	
01/16/2014 08:50 AM	<dir></dir>	nl-nl	
01/16/2014 08:50 AM	<dir></dir>	p1-p1	1000
01/16/2014 08:50 AM	<dir></dir>	pt-he	10110
01/16/2014 08:50 AM	<dir></dir>	pt-pt	
01/16/2014 08:50 AM	<dir></dir>	ro-ro	
01/16/2014 08:50 AM	<dir></dir>	<u>หน-หน</u>	
01/16/2014 08:50 AM	<dir></dir>	sk-sk	
01/16/2014 08:50 AM	<dir></dir>	sl-si	
01/16/2014 08:50 AM	<dir></dir>	sources	
01/16/2014 08:51 AM	<dir></dir>	sr-lata-cs	
01/16/2014 08:51 AM	<dir></dir>	3V-20	
01/16/2014 08:51 AM	<dir></dir>	tr-tr	
01/16/2014 08:51 AM	VDIR>	uk-ua	
01/16/2014 08:51 AM	CDIR>	2h-cn	
01/16/2014 08:51 AM	<dir></dir>	zh-hk	
01/16/2014 08:51 AM	<dir></dir>	zh-tw	
2 Fil	e(s) 1,515,580	d hytes	
38 Dir	(s) 7,701,409,792	2 bytes free	
G:∖>cd Keys			
C:\Keys>LSARecovery_	5430HCA1.exe		۷

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.

C:\Users\admin\Desktop\TESTVM3.dpenny.com_deviceRecovery.exe	
Decompressing Decompression complete? Running extracted artifact .\LSARecovery_TESTVM3.dpe.com.exe.	
Administrator: C:\Windows\system32\cmd.exe	_ 🗆 X
Microsoft Windows (Version 6.1.7601) Copyright <c> 2009 Microsoft Corporation. All rights reserved.</c>	-
C:\Users\admin>cd Desktop	
C:\Users\admin\Desktop>LSARecovery_TESIUM3.dpe.con.exe -p P@ssw&rd -gpk	
C:\Users\admin\Desktop>	

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 Management Console, which then allows you to unlock data on the computer.

Recover Data

- 1. As a Dell Administrator, log in to the Management Console.
- 2. In the left pane, click Management > Recover Data.
- 3. Click the Manager tab.

👘 Dell Data Security				superadmi	n 🛔	٠	?
Dashboard	Recover Data						
 Populations Reporting 	Shield Manag	er SED					
Management							
Commit	Recovery ID:						
Log Analyzer	or						
Recover Data	Hostname:			Searc	h		
Recover Endpoint	Volume:						
License Management	Password						
Services Management	-0.00000000000		Get Recovery Parri	word	iaata Va	v Pareka	10.0
Notification Management			Get Necovery 1955		eate Ne	y Facilia	ngie
External User Management							
	Hostname.						
	Password:						
				word Cr			ige

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 one of the following:
 - Windows 7
 - Windows 8
 - Windows 10

(i) 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**.

domainlusername or username Windows Password Windows Password Permember me Sign in Sign in Sign in Sign in options Sign in options Sign in options		Dell Data Sec This computer is protected by Dell Dat Preboot authentication is require	Curity ta Security red.
Trouble signing in Challenge Response Recovery Questions Sign-in options Network Information Recovery Questions Sign-in options Server Sync Image: Sign-in options		domain\username or username: Windows Password:	
Support Information Password About Shut Down	Trouble signing in Network Information Server Sync Keyboard Support Information About Shut Down	Challenge Response Recovery Questions	

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 1 / 3 What is your mother's maiden name?	
Answer	
	Next Cancel

Recovery Questions

Answer the following recovery questions to gain access to the Windows Operating System.

 \sim

Question 373

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.

nter External Media I	Password	8 23
Encry	ption	
Please enter the pass device.	word assigned to this e	xternal media
If you calent "Cancel"	you will have full acces	
data on the device, bu data.	ut you will have no acce	is to encrypted
data on the device, bu data. Volume: (D:1)	it you will have no acce	is to unencrypted iss to encrypted
data on the device, bu data. Volume: (D:1) Password:	ut you will have no acce	is to unencrypted iss to encrypted





- 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.

External Media	Device Manual Authentication
Deeu E	ncryption
Authentication	Failed. Please contact your system administrator.
Volume: (D:\) Shielded by: E	7520 FDE-Test:test1@dpenny.com
Recovery Key	Id: E1DHU12X
Shield ID:	LG8A-GIZD-4N5A-97MG
Challenge:	3088-FC02-CB61-F25C-B726-31A2-09F4-EBCB
Response:	
	OK Cancel

- **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.

😑 Dell Data Security	×	-						(col)	15 - 1 3 -	1
€) ⇒ ♥ @	0	https://dds.ddsdemos.com	9443/webul/	ncoverOata			♡ ☆	11/	© ≡	
Dell Data Security							superadmin 🛔	٠	?	Externel Media Device Manual Authentication
Dashboard		Recover Data								Cost Encryption
Populations										Authentication Failed. Please cantact your system administrator
Reporting		Shield Ma	nager	28A						Mary Dril
Management		Obtain Shield ID and	Sheld ID						- ñ-	Shelded by: 07530-PDE-Text:text1
Commit		Endpoint Code.	LG8A	GED	ANSA.	97MG				Reavery fee bit #104010X
Log Analyzer		Enter Shield ID and	(16 charact	ersl						Challenge 308-PCID-CRU-PICK-0795
Recover Data		Endpoint Code into the fields on the right	Challenge							and the second s
Bacquet Endnoim		and press Generate Access Code	3088	FC02	C861	F25C				
Concern Management	1	Optionally provide a	B726	31A2	09F4	EBCB				I will cont
Licente Management		Key ID.	(8, 16, or 3)	2 character	s)				8	
Services Management		Upon confirmation of user identity, instruct	Rey ID							
Notification Management		user to enter the provided Access Code	EIDHUL	23						
External User Management		on their computer.	6 characte	ers)						
			Response.							
			\$2D9-A06	B-BDFA-00	0E-3897-74	\$3-08EC-5	578			
			Directory L	her Alus	test1 the	1110	com).			
							Generate R	neonse	-	

- 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.

	Device Mar	nual Auther	ntication	8 23
Deell E	Incryptio	n		
Authentication	Failed. Pleas	e contact y	our system (administrator.
Volume: (D:\) Shielded by: E	7520-FDE-Te	st:test1@d;	enny.com	
necovery ney	LG8A-GE	2D-4N5A-97	MG	
Shield ID:				
Shield ID: Challenge:	308B-FC	02-CB61-F2	5C-8726-31	A2-09F4-EBCE
Shield ID: Challenge: Response:	3088-FC	02-CB61-F2	5C-8726-31	001E

9. Reset your password for the encrypted media.

Password Reset		?	\times
Encrypti	on		
Failed password atter device's password?	mpts detected, do you	u wish to r	eset the
Volume: (E:\)			
New	•••••		
Retype Password:	•••••		
	ОК	Са	ncel

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.

Password Reset		?	\times
Deell Encryp	tion		
Failed password att device's password?	empts detected, do yo	u wish to re	eset the
Volume: (E:\)			
New	•••••		
Retype Password:	•••••		
	ОК	Car	ncel

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.

Appendix A - Download the Recovery Environment

The pre-built WinPE Recovery environment can be downloaded here or requested through Dell ProSupport. Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product. For more information about recovery, see this KB article 130790.

For phone numbers outside of the United States, see Dell ProSupport for Software international phone numbers.

Appendix B - Creating Bootable Media

Use this appendix to create bootable media.

Burning the Recovery Environment ISO to CD/DVD

The following link contains the process needed to use Microsoft Windows 7 to create a bootable CD or DVD for the recovery environment. If you are using Windows 10 or later, see Burning the Recovery Environment on Removable Media.

https://support.microsoft.com/windows/create-installation-media-for-windows

Burning the Recovery Environment on Removable Media

Download the latest recovery ISO here. To create a bootable USB, us the following instructions:

Legacy boot:

- 1. Connect a USB drive to the computer.
- 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 are 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 automatically mounts, and the contents of the ISO file can be copied to the root of the drive.

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

EUFI Boot:

- 1. Connect a USB drive to the computer.
- 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 automatically mounts, and the contents of the ISO file can be copied to the root of the drive.

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