

# Encryption 복구

Encryption v10.0/Data Guardian v2.0



## 참고, 주의 및 경고

① | **노트:** "참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 중요 정보를 제공합니다.

△ | **주의:** "주의"는 하드웨어 손상이나 데이터 손실의 가능성을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

⚠ | **경고:** "경고"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 알려줍니다.

© 2012-2018 Dell Inc. 저작권 본사 소유. Dell, EMC 및 기타 상표는 Dell Inc. 또는 자회사의 상표입니다. 기타 상표는 각 소유자의 상표일 수 있습니다. Dell Encryption, Endpoint Security Suite Enterprise 및 Data Guardian 문서 세트에 사용된 등록 상표 및 상표, 즉 Dell™ 및 Dell 로고, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® 및 KACE™는 Dell Inc. Cylance®, CylancePROTECT의 상표이고 Cylance 로고는 미국 및 다른 국가에서 Cylance, Inc.의 등록 상표입니다. McAfee® 및 McAfee 로고는 미국 및 기타 국가에서 McAfee, Inc.의 상표 또는 등록 상표입니다. 인텔®, Pentium®, 인텔 Core Inside Duo®, Itanium® 및 Xeon®은 미국 및 기타 국가에서 인텔 Corporation의 등록 상표입니다. Adobe®, Acrobat®, 및 Flash®는 Adobe Systems Incorporated의 등록 상표입니다. Authen tec® 및 Eikon®은 Authen tec의 등록 상표입니다. AMD®는 Advanced Micro Devices, Inc.의 등록 상표입니다. Microsoft®, Windows® 및 Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++®는 미국 및/또는 기타 국가에서 Microsoft Corporation의 상표 또는 등록 상표입니다. VMware®는 미국 또는 기타 국가에서 VMware, Inc.의 등록 상표 또는 상표입니다. Box®는 Box의 등록 상표입니다. Dropbox<sup>SM</sup>는 Dropbox, Inc.의 서비스 표시입니다. Google™, Android™, Google™ Chrome™, Gmail™ 및 Google™ Play는 미국 및 기타 국가에서 Google Inc.의 상표 또는 등록 상표입니다. Apple®, App Store<sup>SM</sup>, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®과 iPod nano®, Macintosh® 및 Safari®는 미국 및/또는 기타 국가에서 Apple, Inc.의 서비스 표시, 상표, 또는 등록 상표입니다. EnCase™ 및 Guidance Software®는 Guidance Software의 상표 또는 등록 상표입니다. Entrust®는 미국 및 기타 국가에서 Entrust®, Inc.의 등록 상표입니다. Mozilla® Firefox®는 미국 및/또는 기타 국가에서 Mozilla Foundation의 등록 상표입니다. iOS®는 미국 및 기타 특정 국가에서 Cisco Systems, Inc.의 상표 또는 등록 상표이며, 라이선스 하에 사용됩니다. Oracle® 및 Java®는 Oracle 및/또는 Oracle 계열사의 등록 상표입니다. Travelstar®는 미국 및 기타 국가에서 HGST, Inc.의 등록 상표입니다. UNIX®는 The Open Group의 등록 상표입니다. VALIDITY™는 미국 및 기타 국가에서 사용되는 Validity Sensors, Inc.의 상표입니다. VeriSign®과 기타 관련 상표는 미국 및 기타 국가에서 VeriSign, Inc.와 그 계열사 또는 자회사의 상표 또는 등록 상표이며, Symantec Corporation에 사용 허가된 상표 또는 등록 상표입니다. KVM on IP®는 Video Products의 등록 상표입니다. Yahoo!®는 Yahoo! Inc. Bing®는 Microsoft Inc. Ask®의 등록 상표입니다. Ask®는 IAC Publishing, LLC의 등록 상표입니다. 기타 이름은 해당 소유자의 상표일 수 있습니다.

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

2018 - 08

개정 A01

<b>1 복구 시작하기.....</b>	<b>5</b>
Dell ProSupport에 문의.....	5
<b>2 정책 기반 또는 파일/폴더 암호화 복구.....</b>	<b>6</b>
복구 프로세스 개요.....	6
정책 기반 암호화 또는 FFE 복구 수행.....	6
복구 파일 가져오기 - 정책 기반 암호화 또는 FFE 암호화 클라이언트.....	6
복구 파일 가져오기 - 로컬로 관리되는 컴퓨터.....	7
복구 수행.....	7
암호화된 드라이브 데이터 복구.....	8
암호화된 드라이브 데이터 복구.....	8
<b>3 HCA(Hardware Crypto Accelerator) 복구.....</b>	<b>10</b>
복구 요구 사항.....	10
복구 프로세스 개요.....	10
HCA 복구 수행.....	10
복구 파일 가져오기 - 원격 관리되는 컴퓨터.....	10
복구 파일 가져오기 - 로컬로 관리되는 컴퓨터.....	11
복구 수행.....	11
<b>4 SED(Self-Encrypting Drive) 복구.....</b>	<b>12</b>
복구 요구 사항.....	12
복구 프로세스 개요.....	12
SED 복구 수행.....	12
복구 파일 가져오기 - 원격으로 관리되는 SED 클라이언트.....	12
복구 파일 가져오기 - 로컬로 관리되는 SED 클라이언트.....	13
복구 수행.....	13
Challenge Recovery(SED 포함).....	13
<b>5 전체 디스크 암호화(FDE) 복구.....</b>	<b>17</b>
복구 요구 사항.....	17
복구 프로세스 개요.....	17
전체 디스크 암호화 복구 수행.....	17
복구 파일 가져오기 - 전체 디스크 암호화 클라이언트.....	17
복구 수행.....	17
전체 디스크 암호화로 챌린지 복구.....	18
<b>6 전체 디스크 암호화 및 Dell 암호화 복구.....</b>	<b>22</b>
복구 요구 사항.....	22
복구 프로세스 개요.....	22
전체 디스크 암호화 및 Dell 암호화된 디스크의 복구 수행.....	22
복구 파일 가져오기 - 전체 디스크 암호화 클라이언트.....	22
복구 파일 가져오기 - 정책 기반 암호화 또는 FFE 암호화 클라이언트.....	23

복구 수행.....	24
전체 디스크 암호화로 챌린지 복구.....	26
<b>7 PBA 장치 제어.....</b>	<b>30</b>
PBA 장치 제어 사용.....	30
<b>8 GPK(General Purpose Key) 복구.....</b>	<b>31</b>
GPK 복구.....	31
복구 파일 가져오기.....	31
복구 수행.....	31
<b>9 BitLocker Manager 복구.....</b>	<b>33</b>
데이터 복구.....	33
<b>10 암호 복구.....</b>	<b>34</b>
복구 질문.....	34
<b>11 Encryption External Media 암호 복구.....</b>	<b>35</b>
데이터 액세스 복구.....	35
자체 복구.....	35
<b>12 Dell Data Guardian 복구.....</b>	<b>37</b>
사전 요구 사항.....	37
Data Guardian 복구 수행.....	37
<b>13 부록 A - 복구 환경 굽기.....</b>	<b>40</b>
복구 환경 ISO에서 CD\DVD로 굽기.....	40
이동식 미디어에서 복구 환경 굽기.....	40

# 복구 시작하기

이 섹션에서는 복구 환경을 생성하는 데 필요한 사항을 세부적으로 설명합니다.

- CD-R, DVD-R 미디어 또는 포맷한 USB 미디어
  - CD 혹은 DVD를 구울 경우 자세한 내용은 [복구 환경 ISO에서 CD\DVD로 굽기](#)를 검토하십시오.
  - USB 미디어를 사용할 경우 자세한 내용은 [이동식 미디어에서 복구 환경 굽기](#)를 검토하십시오.
- 오류가 발생한 장치의 복구 번들
  - 원격으로 관리되는 클라이언트의 경우 다음에 나오는 지침이 Dell Security Management Server에서 복구 번들을 검색하는 방법을 설명합니다.
  - 로컬로 관리되는 클라이언트의 경우 복구 번들 패키지가 공유된 네트워크 드라이브나 외부 미디어에서 설치 중에 생성됩니다. 계속하기 전에 이 패키지를 찾으십시오.

## Dell ProSupport에 문의

877-459-7304(내선번호 4310039)로 전화하면 연중무휴 하루 24시간 Dell 제품에 대한 전화 지원을 받을 수 있습니다.

또한, [dell.com/support](http://dell.com/support)에서 Dell 제품에 대한 온라인 지원도 가능합니다. 온라인 지원에는 드라이버, 매뉴얼, 기술 자문, FAQ 및 최근에 나타나는 문제도 포함됩니다.

올바른 기술 전문가에게 신속히 연결될 수 있도록 전화할 때 서비스 태그 또는 익스프레스 서비스 코드를 준비하십시오.

미국 외부의 전화 번호는 [Dell ProSupport 국제 전화 번호](#)를 확인하십시오.

## 정책 기반 또는 파일/폴더 암호화 복구

암호화된 컴퓨터가 운영 체제로 부팅되지 않을 경우 복구가 필요합니다. 이는 레지스트리가 잘못 수정되거나 암호화된 컴퓨터에서 하드웨어가 변경된 경우 발생합니다.

정책 기반 암호화 혹은 FFE(파일/폴더 암호화) 복구 기능을 사용하면 다음과 같은 항목에 대한 액세스를 복구할 수 있습니다.

- 부팅되지 않았고 SDE 복구를 수행하라는 메시지가 표시되는 컴퓨터
- 컴퓨터에서 STOP 코드 0x6f 또는 0x74가 있는 BSOD를 표시합니다.
- 암호화된 데이터에 액세스할 수 없거나 정책을 편집할 수 있는 컴퓨터
- 위의 조건을 충족하는 Dell Encryption을 실행하는 서버
- Hardware Crypto Accelerator 카드 또는 마더보드/TPM을 교체해야 하는 컴퓨터

① | **노트:** 하드웨어 암호화 가속기는 v8.9.3부터 지원되지 않습니다.

## 복구 프로세스 개요

① | **노트:** 복구에는 32비트 환경이 필요합니다.

장애가 발생한 시스템을 복구하려면 다음을 수행합니다.

- 1 복구 환경을 CD/DVD에 굽거나 부팅이 가능한 USB를 생성합니다. [부록 A - 복구 환경 굽기를 참조하십시오.](#)
- 2 복구 파일을 가져옵니다.
- 3 복구를 수행합니다.

## 정책 기반 암호화 또는 FFE 복구 수행

다음 단계에 따라 Policy-Based 암호화 또는 FFE 복구를 수행합니다.

## 복구 파일 가져오기 - 정책 기반 암호화 또는 FFE 암호화 클라이언트

복구 파일을 다운로드하려면 다음을 수행하십시오.

- 1 <http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers> 에서 Dell 암호화 설치 패키지를 다운로드합니다. 설치 패키지에서 **AdminUtilities** 폴더로 이동하여 **CMGAd.exe**를 엽니다.
- 2 **Dell 서버** 필드에 컴퓨터가 활성화되어 있는 Security Management Server/Security Management Server Virtual을 입력합니다.
- 3 **Dell 관리자** 필드에 포렌식 관리자 권한이 있는 사용자 계정 이름을 입력합니다.
- 4 **암호** 필드에 포렌식 관리자의 암호를 입력합니다.
- 5 **MCID** 필드에 복구하는 장치의 FQDN을 입력합니다.
  - **DCID** 필드는 복구되는 장치의 복구 ID입니다.
- 6 다음을 선택합니다.
- 7 복구 파일을 위한 **암호**를 정의하고 확인합니다. 이 암호는 복구를 수행하는 데 필요합니다.
- 8 **다운로드 대상:** 필드에 복구 번들에 대한 대상 위치를 입력한 후 다음을 선택합니다. 기본적으로 이 위치는 CMGAd.exe가 실행된 디렉터리 안에 있습니다.



9 복구 번들이 다운로드 대상에 지정된 폴더로 다운로드됩니다.

Name	Date modified	Type	Size
CmgAd	5/11/2018 6:28 AM	Application	1,469 KB
CmgAlu	5/11/2018 6:28 AM	Application	1,164 KB
CmgAu	5/11/2018 6:28 AM	Application	1,617 KB
CmgCryptoLib.dll	5/11/2018 6:28 AM	Application extens...	608 KB
CmgCryptoLib.mac	5/11/2018 6:28 AM	MAC File	1 KB
FQDN.Dom.ain	5/11/2018 6:34 AM	AIN File	103 KB
WSScan	5/11/2018 6:28 AM	Application	5,330 KB

10 복구 번들 파일을 WinPE로 부팅할 때 액세스할 수 있는 위치에 복사합니다.

## 복구 파일 가져오기 - 로컬로 관리되는 컴퓨터

Encryption Personal 복구 파일을 가져오려면 다음을 수행합니다.

- 1 파일명이 **LSARecovery\_<systemname> .exe**인 복구 파일을 찾습니다. 이 파일은 Encryption Personal을 설치하는 동안 설정 마법사에서 지정한 네트워크 드라이브 또는 이동식 저장소에 저장되어 있습니다.
- 2 대상 컴퓨터(데이터를 복구할 컴퓨터)에 **LSARecovery\_<systemname> .exe**를 복사합니다.

## 복구 수행

- 1 앞에서 만들었던 부팅 가능한 미디어를 사용하여 복구 시스템 또는 복구를 수행할 드라이브가 있는 장치에서 이 미디어로 부팅합니다. WinPE 환경이 열립니다.
  - ① **노트:** 복구 프로세스를 진행하기 전에 **SecureBoot**를 비활성화합니다. 완료되면 **SecureBoot**를 다시 활성화합니다.
- 2 명령 프롬프트를 받으려면 **x**를 입력하고 **Enter** 키를 누릅니다.
- 3 복구 파일로 이동하여 실행합니다.
- 4 다음 옵션 중 하나를 선택합니다.

- 시스템을 부팅하지 못했으며 SDE 복구를 수행하라는 메시지가 표시됩니다.  
이 옵션을 사용하면 OS로 부팅할 때 Encryption 클라이언트에서 수행하는 하드웨어 검사를 다시 빌드할 수 있습니다.
- 시스템에서 암호화된 데이터 액세스 또는 정책 편집을 허용하지 않거나 다시 설치가 진행되고 있습니다.  
Hardware Crypto Accelerator 카드 또는 마더보드/TPM을 교체해야 하는 경우 이 옵션을 사용하십시오.

5 백업 및 복구 정보 대화 상자에서 복구하려는 클라이언트 컴퓨터에 대한 정보가 올바른지 확인하고 **다음**을 클릭하십시오. Dell 이외의 컴퓨터를 복구하는 경우에는 SerialNumber 및 AssetTag 필드가 비어 있습니다.

6 컴퓨터 볼륨이 나열된 대화 상자에서, 해당되는 모든 드라이브를 선택하고 **다음**을 클릭합니다. Shift+클릭하거나 Ctl+클릭하여 여러 드라이브를 선택합니다.

선택한 드라이브가 정책 기반이 아니거나 FFE-암호화되어 있다면 복구에 실패합니다.

7 복구 암호를 입력한 다음 **다음**을 클릭합니다.

원격으로 관리되는 클라이언트와 함께 이는 **복구 파일 - 원격으로 관리되는 컴퓨터 확보의 3단계**에서 제공된 암호입니다.

Encryption Personal에서 이 암호는 키가 에스스로될 때 시스템에 설정된 암호화 관리자 암호입니다.

8 복구 대화 상자에서 **복구**를 클릭합니다. 복구 프로세스가 시작됩니다.

9 설치가 완료되면 **마침**을 클릭합니다.

#### ① 노트:

시스템을 부팅하는 데 사용한 USB 또는 CD\DVD 미디어는 반드시 제거해야 합니다. 이렇게 하지 않으면 복구 환경으로 다시 부팅될 수 있습니다.

10 컴퓨터가 다시 부팅된 후에는 컴퓨터가 완전히 작동됩니다. 문제가 지속되면 Dell ProSupport에 문의하십시오.

## 암호화된 드라이브 데이터 복구

대상 컴퓨터를 부팅할 수 없고 하드웨어 장애가 없는 경우 복구 환경으로 복구되는 컴퓨터에서 데이터 복구를 수행할 수 있습니다. 대상 컴퓨터를 부팅할 수 없고 하드웨어 장애가 있거나 USB 장치일 경우에는 슬레이브 드라이브로 부팅하여 데이터 복구를 수행할 수 있습니다. 드라이브를 슬레이브로 연결하면 파일 시스템이 표시되어 해당 디렉토리를 찾아볼 수 있습니다. 하지만 파일을 열거나 복사하려고 하면 **액세스 거부** 오류가 발생합니다.

## 암호화된 드라이브 데이터 복구

암호화된 드라이브 데이터를 복구하려면 다음을 수행합니다.

- 1 컴퓨터에서 DCID/복구 ID를 가져오려면 다음 옵션 중 하나를 선택합니다.
  - a 일반 암호화된 데이터가 저장되어 있는 폴더에서 WSScan을 실행합니다.  
"일반" 뒤에 8자리로 된 DCID/복구 ID가 표시됩니다.
  - b 원격 관리 콘솔을 열고 끝점에 대한 **세부 정보 및 조치** 탭을 선택합니다.
  - c 끝점 상세정보 화면의 Shield 상세정보 섹션에서 DCID/복구 ID를 찾습니다.
- 2 서버에서 키를 다운로드하려면 Dell Administrative Unlock(**CMGAu**) 유틸리티로 이동하여 실행합니다.  
Dell Administrative Unlock 유틸리티 Dell ProSupport에서 가져올 수 있습니다.
- 3 Dell Administrative Utility(CMGAu) 대화 상자에서 아래와 같은 정보(일부 필드는 미리 입력됨)를 입력하고 **다음**을 클릭합니다.  
**서버:** 서버의 정규화된 호스트 이름. 예:



장치 서버(8.x 이전 클라이언트): <https://<server.organization.com>:8081/xapi>

보안 서버: <https://<server.organization.com>:8443/xapi/>

**Dell 관리:** 포렌식 관리자의 계정 이름(보안 관리 서버/보안 관리 서버 가상에서 활성화됨)

**Dell 관리 암호:** 포렌식 관리자의 계정 암호(보안 관리 서버/보안 관리 서버 가상에서 활성화됨)

**MCID:** MCID 필드를 지웁니다.

**DCID:** 이전에 가져온 DCID/복구 ID입니다.

- 4 Dell Administrative Utility 대화 상자에서 **아니요, 지금 서버에서 다운로드를 수행**을 선택하고 **다음**을 클릭합니다.

**① 노트:**

Encryption 클라이언트가 설치되어 있지 않으면 *Unlock failed(잠금 해제 실패)* 메시지가 나타납니다. Encryption 클라이언트가 설치된 컴퓨터로 이동하십시오.

- 5 다운로드 및 잠금 해제가 완료되면 이 드라이브에서 복구할 파일을 복사합니다. 모든 파일은 읽기 가능합니다. 파일을 복구할 때 까지 **절대 마침을 클릭하지 마십시오.**
- 6 파일을 복구하고 파일을 다시 잠글 준비가 된 후에 **완료**를 클릭하십시오.  
**마침을 클릭하면 암호화된 파일은 더 이상 사용할 수 없습니다.**

## HCA(Hardware Crypto Accelerator) 복구

① **노트:** 하드웨어 암호화 가속기는 v8.9.3부터 지원되지 않습니다.

HCA(Hardware Crypto Accelerator) 복구 기능을 사용하면 다음과 같은 항목에 대한 액세스를 복구할 수 있습니다.

- HCA 암호화된 드라이브의 파일 - 이 방법은 제공된 키를 사용하여 드라이브를 암호 해독합니다. 복구 과정에서 암호 해독할 특정 드라이브를 선택할 수 있습니다.
- 하드웨어 교체 후 HCA 암호화된 드라이브 - 이 방법은 Hardware Crypto Accelerator 카드 또는 마더보드/TPM을 교체한 후에 사용됩니다. 드라이브의 암호를 해독하지 않고 복구를 실행하여 암호화된 데이터에 액세스할 수 있습니다.

### 복구 요구 사항

다음은 HCA 복구를 수행하는 데 필요한 사항입니다.

- 복구 환경 ISO에 대한 액세스(복구에는 32비트 환경이 필요함)
- 부팅 가능한 CD\DVD 또는 USB 미디어

### 복구 프로세스 개요

① **노트:** 복구에는 32비트 환경이 필요합니다.

장애가 발생한 시스템을 복구하려면 다음을 수행합니다.

- 1 복구 환경을 CD/DVD에 굽거나 부팅이 가능한 USB를 생성합니다. [부록 A - 복구 환경 굽기를 참조하십시오.](#)
- 2 복구 파일을 가져옵니다.
- 3 복구를 수행합니다.

### HCA 복구 수행

다음 단계에 따라 HCA 복구를 수행합니다.

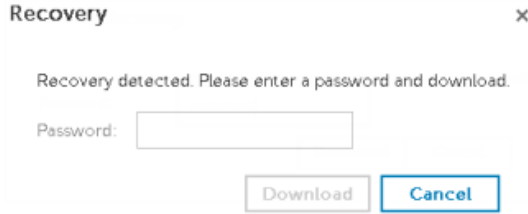
### 복구 파일 가져오기 - 원격 관리되는 컴퓨터

Dell 암호화를 설치했을 때 생성된 <machinename\_domain.com>.exe 파일을 다운로드하려면:

- 1 Remote Management Console을 열고 왼쪽 창에서 **관리 > 끝점 복구**를 선택합니다.
- 2 호스트 이름 필드에 끝점의 정규화된 도메인 이름을 입력하고 **검색**을 클릭합니다.
- 3 복구 창에 복구 암호를 입력하고 **다운로드**를 클릭합니다.

① **노트:**

복구 키에 액세스하려면 이 암호가 필요합니다.



## 복구 파일 가져오기 - 로컬로 관리되는 컴퓨터

Encryption Personal 복구 파일을 가져오려면 다음을 수행합니다.

- 1 파일명이 **LSARecovery\_<systemname> .exe**인 복구 파일을 찾습니다. 이 파일은 Encryption Personal을 설치하는 동안 설정 마법사에서 지정한 네트워크 드라이브 또는 이동식 저장소에 저장되어 있습니다.
- 2 대상 컴퓨터(데이터를 복구할 컴퓨터)에 **LSARecovery\_<systemname> .exe**를 복사합니다.

## 복구 수행

- 1 앞에서 만들었던 부팅 가능한 미디어를 사용하여 복구 시스템 또는 복구를 수행할 드라이브가 있는 장치에서 이 미디어로 부팅합니다.

WinPE 환경이 열립니다.

**① | 노트:** 복구 프로세스를 진행하기 전에 **SecureBoot**를 비활성화합니다. 완료되면 **SecureBoot**를 활성화합니다.

- 2 명령 프롬프트를 받으려면 **x**를 입력하고 **Enter** 키를 누릅니다.
- 3 저장된 복구 파일로 이동하여 실행합니다.
- 4 다음 옵션 중 하나를 선택합니다.
  - HCA로 암호화된 드라이브의 암호를 해독하겠습니다.
  - HCA로 암호화된 드라이브의 액세스를 복구하겠습니다.
- 5 백업 및 복구 정보 대화 상자에서 서비스 태그 또는 자산 번호가 올바른지 확인하고 **다음**을 클릭합니다.
- 6 컴퓨터 볼륨이 나열된 대화 상자에서, 해당되는 모든 드라이브를 선택하고 **다음**을 클릭합니다.  
Shift+클릭하거나 Ctrl+클릭하여 여러 드라이브를 선택합니다.  
선택한 드라이브가 HCA 암호화되어 있지 않으면 복구에 실패합니다.
- 7 복구 암호를 입력한 다음 **다음**을 클릭합니다.  
원격으로 관리되는 컴퓨터에서 이는 [복구 파일 - 원격으로 관리되는 컴퓨터 확보의 3단계](#)에서 제공된 암호입니다.  
로컬로 관리되는 컴퓨터에서, 이 암호는 키가 에스스로될 때 Personal Edition에서 시스템에 설정된 암호화 관리자 암호입니다.
- 8 복구 대화 상자에서 **복구**를 클릭합니다. 복구 프로세스가 시작됩니다.
- 9 메시지가 표시되면 저장된 복구 파일을 찾아보고 **확인**을 클릭합니다.  
전체 암호 해독을 수행하는 경우에는 다음 대화 상자에 상태가 표시됩니다. 이 프로세스에는 시간이 걸릴 수도 있습니다.
- 10 복구가 성공적으로 완료되었다는 메시지가 표시되면 **완료**를 클릭합니다. 컴퓨터가 다시 부팅됩니다.  
컴퓨터가 다시 부팅된 후에는 컴퓨터가 완전히 작동됩니다. 문제가 지속되면 Dell ProSupport에 문의하십시오.

# SED(Self-Encrypting Drive) 복구

SED 복구 기능을 사용하여 다음 방법을 통해 SED의 파일에 대한 액세스를 복구할 수 있습니다.

- 드라이브의 1회 잠금 해제를 수행하여 PBA(부팅 전 인증)를 무시합니다.
- 드라이브의 잠금을 해제하고 드라이브에서 PBA를 영구 제거합니다. PBA가 제거된 상태에서는 SSO(Single Sign-On)이 작동되지 않습니다.
  - 원격으로 관리되는 SED 클라이언트에서, PBA를 제거할 때는 Remote Management Console에서 제품을 비활성화해야 나중에 PBA를 다시 활성화할 수 있습니다.
  - 로컬로 관리되는 SED 클라이언트에서, PBA를 제거할 때는 OS 내부에서 제품을 비활성화해야 나중에 PBA를 다시 활성화할 수 있습니다.

## 복구 요구 사항

다음은 SED 복구를 수행하는 데 필요한 사항입니다.

- 복구 환경 ISO에 대한 액세스
- 부팅 가능한 CD\DVD 또는 USB 미디어

## 복구 프로세스 개요

① | **노트:** 복구에는 BIOS 부팅 모드 기반의 64비트 또는 32비트 환경이 필요합니다.

장애가 발생한 시스템을 복구하려면 다음을 수행합니다.

- 1 복구 환경을 CD/DVD에 굽거나 부팅이 가능한 USB를 생성합니다. [부록 A - 복구 환경 굽기를 참조하십시오.](#)
- 2 복구 파일을 가져옵니다.
- 3 복구를 수행합니다.

## SED 복구 수행

다음 단계에 따라 SED 복구를 수행합니다.

### 복구 파일 가져오기 - 원격으로 관리되는 SED 클라이언트

복구 파일을 가져옵니다.

복구 파일은 Remote Management Console에서 다운로드할 수 있습니다. Dell Data Security를 설치할 때 생성된 `<hostname>-sed-recovery.dat` 파일을 다운로드하기:

- a 원격 관리 콘솔을 열고 왼쪽 창에서 **관리 > 데이터 복구**를 선택한 후 **SED** 탭을 선택합니다.
- b 데이터 복구 화면의 호스트 이름 필드에서 끝점의 정규화된 도메인 이름을 입력한 다음 **검색**을 클릭합니다.
- c SED 필드에서 옵션을 선택합니다.
- d **복구 파일 만들기**를 클릭합니다.

`<hostname>- sed- recovery.dat` 파일이 다운로드됩니다.

# 복구 파일 가져오기 - 로컬로 관리되는 SED 클라이언트

복구 파일을 가져옵니다.

이 파일은 컴퓨터에 고급 인증을 설치할 때 생성되었으며 선택한 백업 위치에서 액세스할 수 있습니다. 파일 이름은 `OpalSPkey<systemname>_dat`입니다.

## 복구 수행

- 1 앞에서 만들었던 부팅 가능한 미디어를 사용하여 복구 시스템 또는 복구를 수행할 드라이브가 있는 장치에서 이 미디어로 부팅합니다. 복구 응용 프로그램에서 WinPE 환경이 열립니다.

**① | 노트:** 복구 프로세스를 진행하기 전에 **SecureBoot**를 비활성화합니다. 완료되면 **SecureBoot**를 활성화합니다.

- 2 옵션 1을 선택하고 **Enter**키를 누릅니다.
- 3 **찾아보기**를 선택하고, 복구 파일을 찾은 다음, **열기**를 클릭합니다.
- 4 옵션 하나를 선택하고 **확인**을 클릭합니다.
  - **드라이브의 일회용 잠금 해제** - 이 방법은 PBA를 무시합니다.
  - **드라이브를 잠금 해제하고 PBA 제거** - 이 방법은 잠금 해제한 후, 드라이브에서 PBA를 영구적으로 제거합니다. PBA를 제거할 때는 Remote Management Console(원격으로 관리되는 SED 클라이언트의 경우) 또는 OS 내에서(로컬로 관리되는 SED 클라이언트의 경우) 제품을 비활성화해야 나중에 PBA를 다시 활성화할 수 있습니다. PBA가 제거된 상태에서는 SSO(Single Sign-On)이 작동되지 않습니다.
- 5 이제 복구가 완료됩니다. 아무 키나 눌러 메뉴로 돌아갑니다.
- 6 **r**을 눌러 컴퓨터를 재부팅합니다.

**① | 노트:**

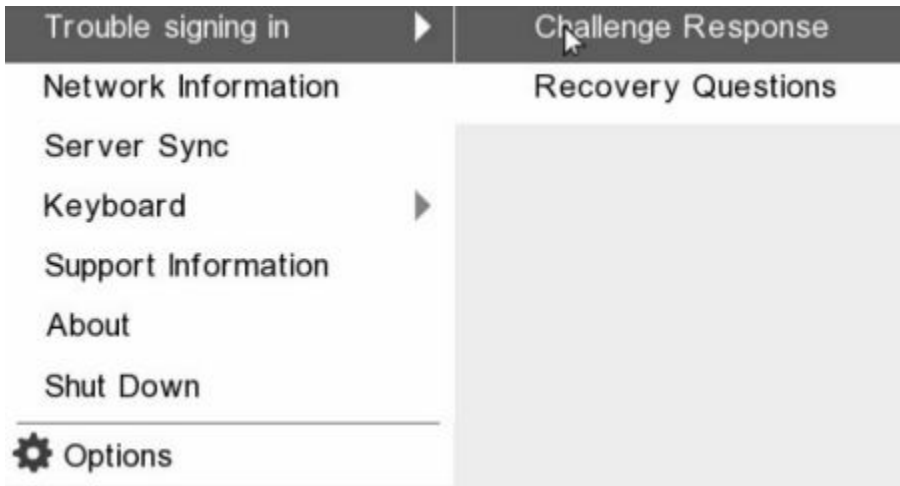
컴퓨터를 부팅하는 데 사용한 USB 또는 CD/DVD 미디어는 반드시 제거해야 합니다. 이렇게 하지 않으면 복구 환경으로 다시 부팅될 수 있습니다.

- 7 컴퓨터가 다시 부팅된 후에는 컴퓨터가 완전히 작동됩니다. 문제가 지속되면 Dell ProSupport에 문의하십시오.

## Challenge Recovery(SED 포함)

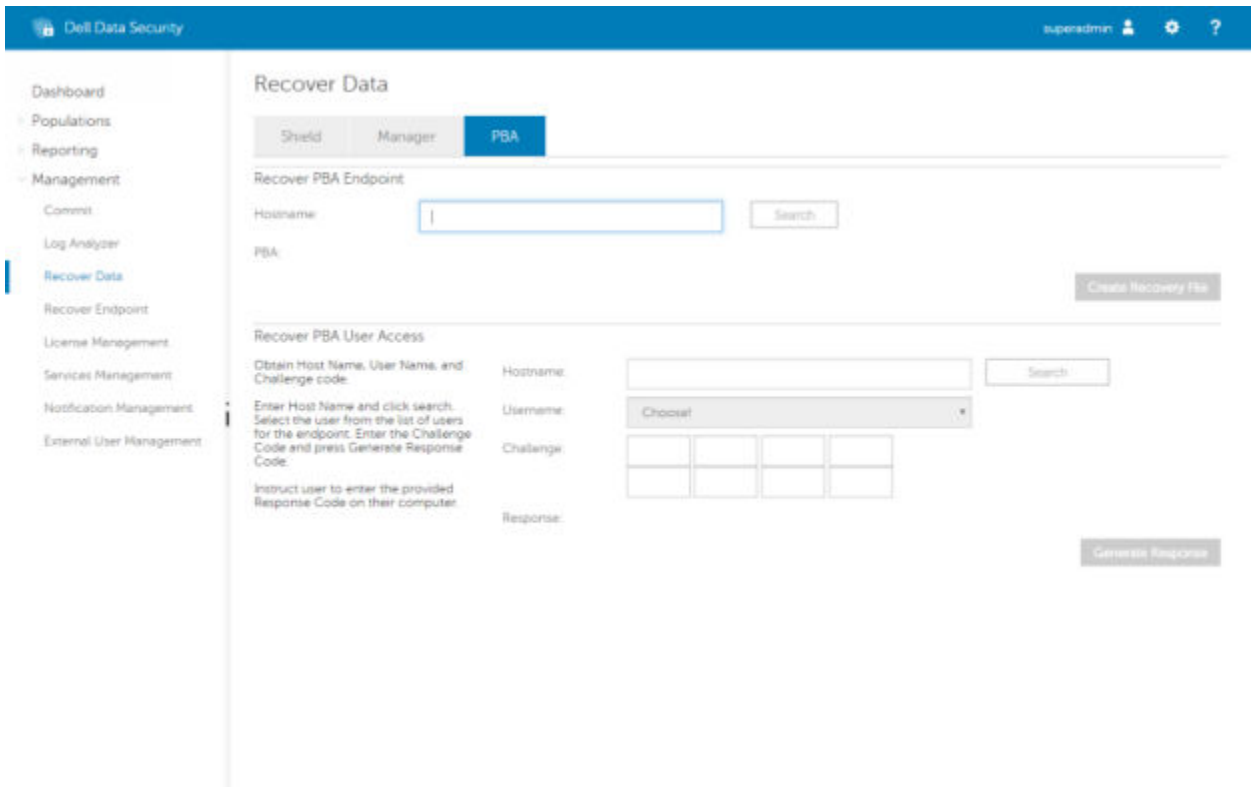
### 부팅 전 인증 환경 무시

사용자가 암호를 분실하여 PBA 환경 통과와 관련하여 헬프 데스크에 전화를 합니다. 장치에 내장된 의문 제기/응답 메커니즘을 사용하십시오. 이 메커니즘은 사용자별로 이루어지며 교대되는 영숫자 문자 집합을 기반으로 합니다. **사용자 이름** 필드에 사용자가 자신의 이름을 입력한 다음, **옵션 > 챌린지 응답**을 선택해야 합니다.

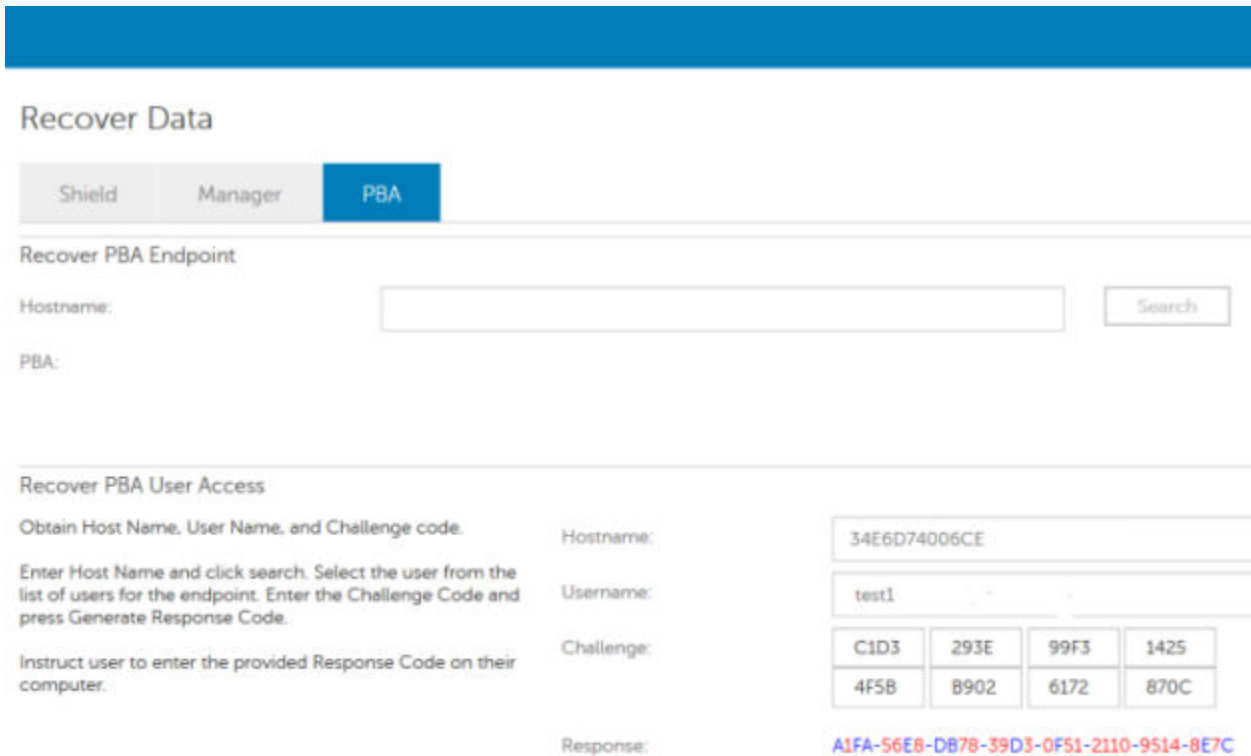


챌린지 응답을 선택하면 다음 정보가 표시됩니다.

장치 이름 필드는 Remote Management Console의 헬프데스크 기술자가 올바른 장치를 찾는 데 사용되며 사용자 이름이 선택됩니다. 이는 **PBA** 탭의 **관리 > 데이터 복구** 탭에서 찾을 수 있습니다.



데이터를 입력하고 **응답 생성** 단추를 클릭한 헬프 데스크 기술자에게 챌린지 코드가 제공됩니다.



이 결과 데이터는 숫자(빨간색)와 영문자(파란색)를 구별하는 데 도움이 되도록 색상으로 조정됩니다. 이 데이터를 최종 사용자가 읽습니다. 최종 사용자는 이 데이터를 PBA 환경에 입력한 다음 **제출** 단추를 클릭하여 사용자를 Windows로 이동합니다.

**Challenge Response**

Contact your IT administrator to receive the Response Code to unlock your computer.

Device Name  
34E6D74006CE

Challenge Code

C1D3	293E	99F3	1425
4F5B	B902	6172	870C

Response Code

A1FA	56E8	DB78	39D3
0F51	2110	9514	8E7C

Submit Cancel

인증에 성공하면 다음 메시지가 표시됩니다.

**Challenge Response**

Authentication successful. Please wait...

Device Name  
34E6D74006CE

Challenge Code

C1D3	293E	99F3	1425
4F5B	B902	6172	870C

Response Code

A1FA	56E8	DB78	39D3
0F51	2110	9514	8E7C

Submit Cancel

챌린지 복구가 완료되었습니다.



## 전체 디스크 암호화(FDE) 복구

복구를 사용하면 전체 디스크 암호화로 암호화된 드라이브의 파일에 대한 액세스를 복구할 수 있습니다.

① **노트:** 암호 해독을 중단하지 않아야 합니다. 암호 해독이 중단되는 경우 데이터가 손실될 수 있습니다.

### 복구 요구 사항

전체 디스크 암호화 복구의 경우 다음이 필요합니다.

- 복구 환경 ISO에 대한 액세스
- 부팅 가능한 CD\DVD 또는 USB 미디어

### 복구 프로세스 개요

① **노트:** 복구에는 64비트 환경이 필요합니다.

장애가 발생한 시스템을 복구하려면 다음을 수행합니다.

- 1 복구 환경을 CD/DVD에 굽거나 부팅이 가능한 USB를 생성합니다. [부록 A - 복구 환경 굽기를 참조하십시오.](#)
- 2 복구 파일을 가져옵니다.
- 3 복구를 수행합니다.

## 전체 디스크 암호화 복구 수행

다음 단계에 따라 전체 디스크 암호화 복구를 수행합니다.

### 복구 파일 가져오기 - 전체 디스크 암호화 클라이언트

복구 파일을 가져옵니다.

Remote Management Console에서 복구 파일을 다운로드합니다. Dell Data Security를 설치할 때 생성된 `<hostname>-sed-recovery.dat` 파일을 다운로드하기:

- a Remote Management Console을 열고 왼쪽 창에서 **관리 > 데이터 복구**를 선택한 후 **PBA** 탭을 선택합니다.
- b 데이터 복구 화면의 호스트 이름 필드에서 끝점의 정규화된 도메인 이름을 입력한 다음 **검색**을 클릭합니다.
- c SED 필드에서 옵션을 선택합니다.
- d **복구 파일 만들기**를 클릭합니다.

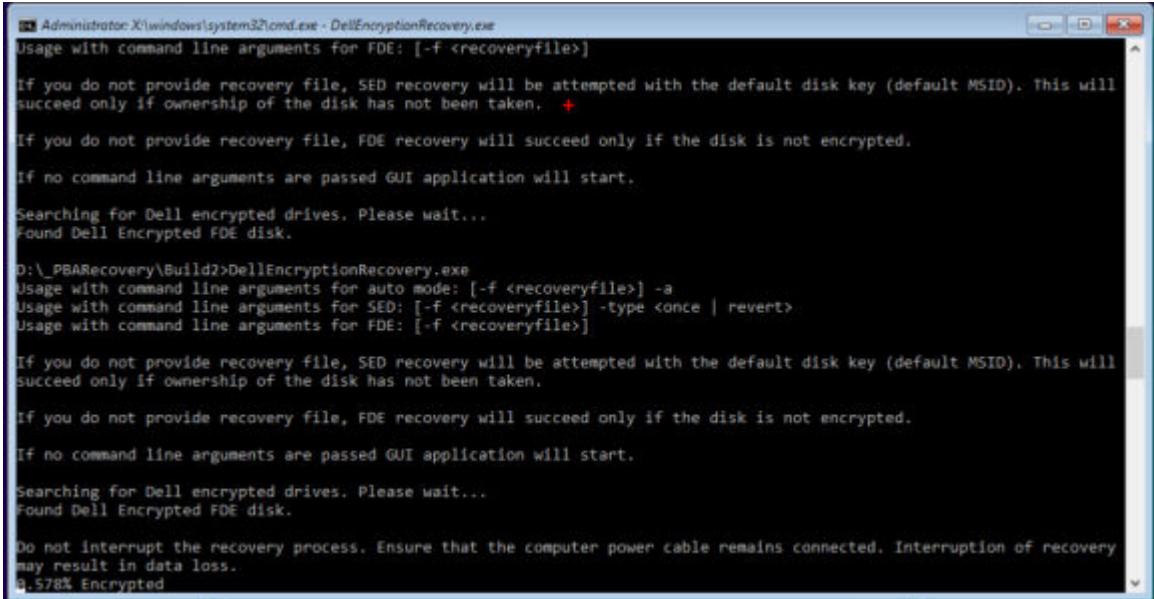
`<hostname>- sed- recovery.dat` 파일이 다운로드됩니다.

### 복구 수행

- 1 앞에서 만들었던 부팅 가능한 미디어를 사용하여 복구 시스템 또는 복구를 수행할 드라이브가 있는 장치에서 이 미디어로 부팅합니다. 복구 응용 프로그램에서 WinPE 환경이 열립니다.

① **노트:** 복구 프로세스를 진행하기 전에 **SecureBoot**를 비활성화합니다. 완료되면 **SecureBoot**를 다시 활성화합니다.

- 2 옵션 1을 선택하고 **Enter**키를 누릅니다.
- 3 **찾아보기**를 선택하고, 복구 파일을 찾은 다음, **열기**를 클릭합니다.
- 4 **확인**을 클릭합니다.



```
Administrator: X:\windows\system32\cmd.exe - DellEncryptionRecovery.exe
Usage with command line arguments for FDE: [-f <recoveryfile>]

If you do not provide recovery file, SED recovery will be attempted with the default disk key (default MSID). This will
succeed only if ownership of the disk has not been taken. +

If you do not provide recovery file, FDE recovery will succeed only if the disk is not encrypted.

If no command line arguments are passed GUI application will start.

Searching for Dell encrypted drives. Please wait...
Found Dell Encrypted FDE disk.

D:\_PBAREcovery\Build2>DellEncryptionRecovery.exe
Usage with command line arguments for auto mode: [-f <recoveryfile>] -a
Usage with command line arguments for SED: [-f <recoveryfile>] -type <once | revert>
Usage with command line arguments for FDE: [-f <recoveryfile>]

If you do not provide recovery file, SED recovery will be attempted with the default disk key (default MSID). This will
succeed only if ownership of the disk has not been taken.

If you do not provide recovery file, FDE recovery will succeed only if the disk is not encrypted.

If no command line arguments are passed GUI application will start.

Searching for Dell encrypted drives. Please wait...
Found Dell Encrypted FDE disk.

Do not interrupt the recovery process. Ensure that the computer power cable remains connected. Interruption of recovery
may result in data loss.
9.578% Encrypted
```

- 5 이제 복구가 완료됩니다. 아무 키나 눌러 메뉴로 돌아갑니다.
- 6 **r**을 눌러 컴퓨터를 재부팅합니다.

① **노트:**

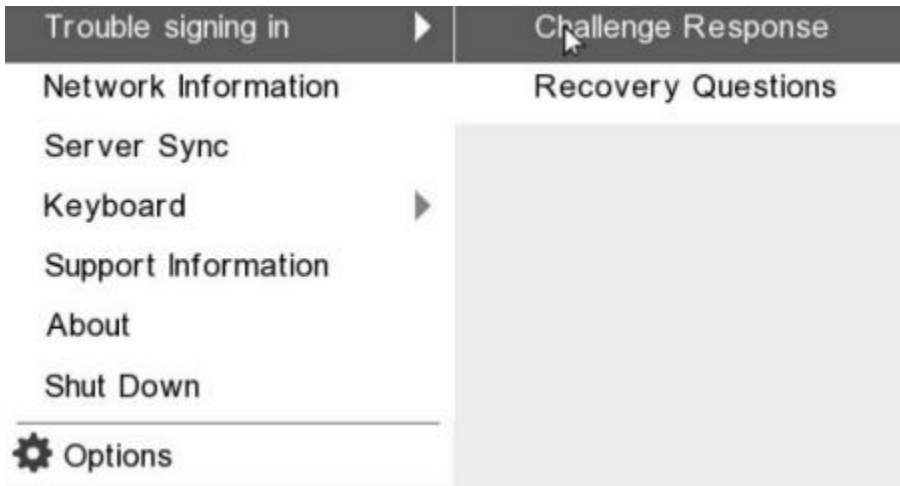
컴퓨터를 부팅하는 데 사용한 USB 또는 CD/DVD 미디어는 반드시 제거해야 합니다. 이렇게 하지 않으면 복구 환경으로 다시 부팅될 수 있습니다.

- 7 컴퓨터가 다시 부팅된 후에는 컴퓨터가 완전히 작동됩니다. 문제가 지속되면 Dell ProSupport에 문의하십시오.

## 전체 디스크 암호화로 챌린지 복구

### 부팅 전 인증 환경 무시

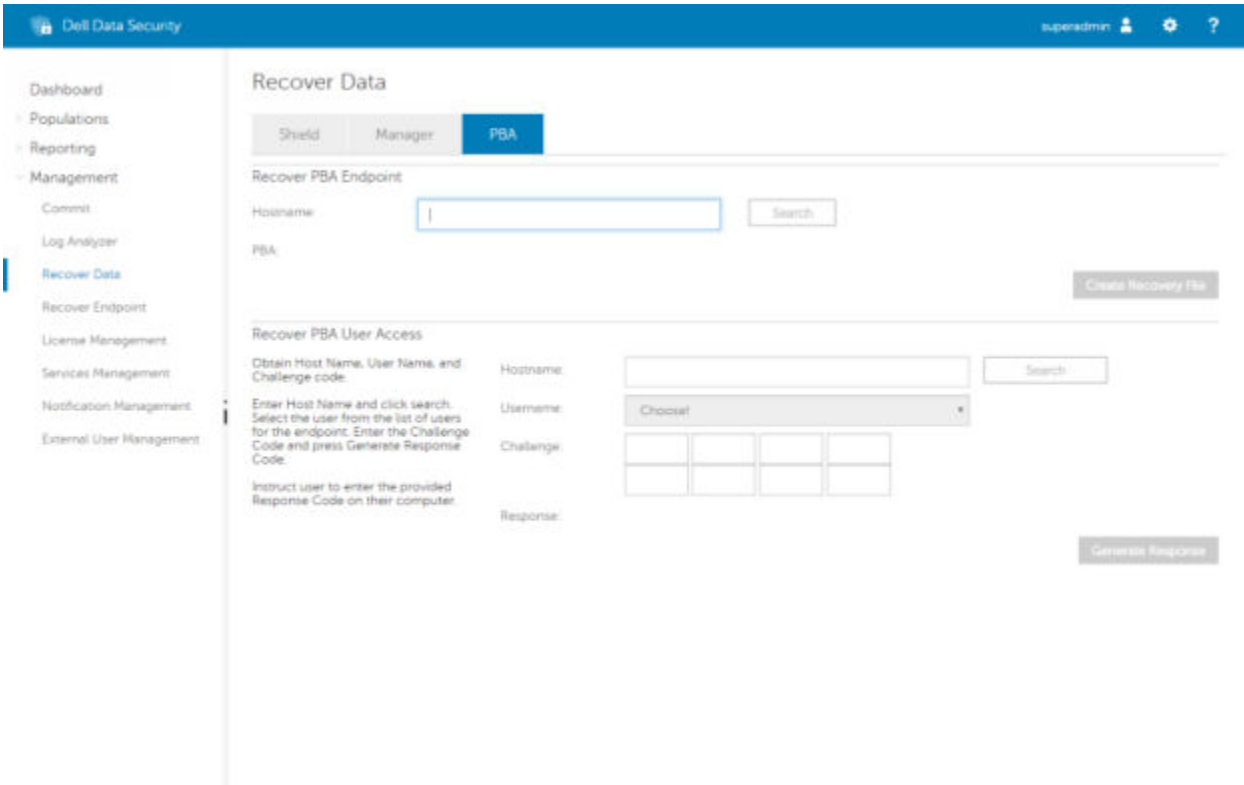
사용자가 암호를 분실하여 PBA 환경 통과와 관련하여 헬프 데스크에 전화를 합니다. 장치에 내장된 의문 제기/응답 메커니즘을 사용하십시오. 이 메커니즘은 사용자별로 이루어지며 교대되는 영숫자 문자 집합을 기반으로 합니다. **사용자 이름** 필드에 사용자가 자신의 이름을 입력한 다음, **옵션 > 챌린지 응답**을 선택해야 합니다.



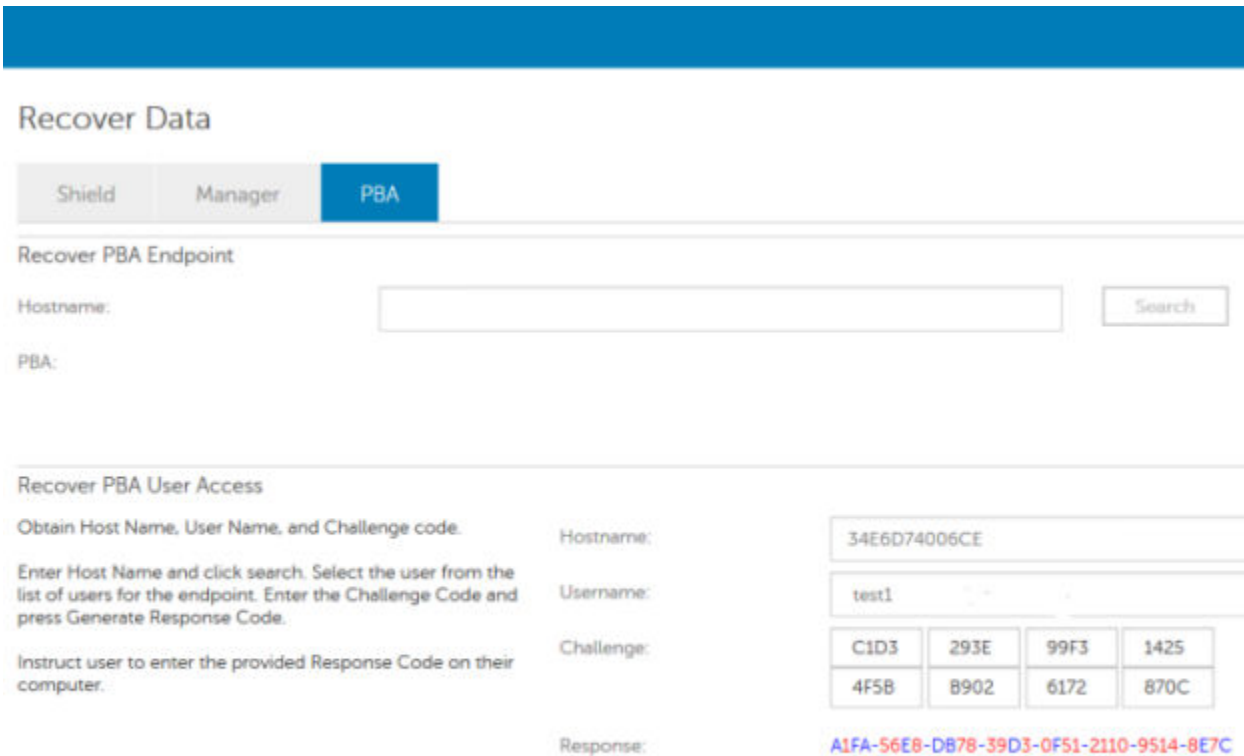
챌린지 응답을 선택하면 다음 정보가 표시됩니다.

 A screenshot of the 'Challenge Response' form. At the top, it says 'Challenge Response' with a user icon and 'Contact your IT administrator to receive the Response Code to unlock your computer.' Below this, there is a 'Device Name' field containing '34E6D74006CE'. Under 'Challenge Code', there are two rows of buttons: the first row has 'C1D3', '293E', '99F3', and '1425'; the second row has '4F5B', 'B902', '6172', and '870C'. Under 'Response Code', there are two rows of input boxes, with the first box in the first row containing the letter 'I'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

장치 이름 필드는 Remote Management Console의 헬프데스크 기술자가 올바른 장치를 찾는 데 사용되며 사용자 이름이 선택됩니다. 이는 PBA 탭의 관리 > 데이터 복구 탭에서 찾을 수 있습니다.



데이터를 입력하고 **응답 생성** 단추를 클릭한 헬프 데스크 기술자에게 챌린지 코드가 제공됩니다.



이 결과 데이터는 숫자(빨간색)와 영문자(파란색)를 구별하는 데 도움이 되도록 색상으로 조정됩니다. 이 데이터를 최종 사용자가 읽습니다. 최종 사용자는 이 데이터를 PBA 환경에 입력한 다음 **제출** 단추를 클릭하여 사용자를 Windows로 이동합니다.

**Challenge Response**

Contact your IT administrator to receive the Response Code to unlock your computer.

Device Name  
34E6D74006CE

Challenge Code

C1D3	293E	99F3	1425
4F5B	B902	6172	870C

Response Code

A1FA	56E8	DB78	39D3
0F51	2110	9514	8E7C

Submit Cancel

인증에 성공하면 다음 메시지가 표시됩니다.

**Challenge Response**

Authentication successful. Please wait...

Device Name  
34E6D74006CE

Challenge Code

C1D3	293E	99F3	1425
4F5B	B902	6172	870C

Response Code

A1FA	56E8	DB78	39D3
0F51	2110	9514	8E7C

Submit Cancel

챌린지 복구가 완료되었습니다.

## 전체 디스크 암호화 및 Dell 암호화 복구

이 장에서는 전체 디스크 암호화로 보호되는 Dell 암호화 보호된 파일에 대한 액세스를 복구하는 데 필요한 복구 단계를 상세히 설명합니다.

① **노트:** 암호 해독을 중단하지 않아야 합니다. 암호 해독이 중단되는 경우 데이터가 손실될 수 있습니다.

### 복구 요구 사항

전체 디스크 암호화 및 Dell 암호화 복구의 경우 다음이 필요합니다.

- 복구 환경 ISO에 대한 액세스
- 부팅 가능한 CD/DVD 또는 USB 미디어

### 복구 프로세스 개요

① **노트:** 복구에는 64비트 환경이 필요합니다.

장애가 발생한 시스템을 복구하려면 다음을 수행합니다.

- 1 복구 환경을 CD/DVD에 굽거나 부팅이 가능한 USB를 생성합니다. [부록 A - 복구 환경 굽기를 참조하십시오.](#)
- 2 Dell 암호화 및 전체 디스크 암호화에 대한 복구 파일을 가져옵니다.
- 3 복구를 수행합니다.

## 전체 디스크 암호화 및 Dell 암호화된 디스크의 복구 수행

전체 디스크 암호화 및 Dell 암호화된 디스크의 복구를 수행하려면 다음과 같은 단계를 따르십시오.

### 복구 파일 가져오기 - 전체 디스크 암호화 클라이언트

복구 파일을 가져옵니다.

Remote Management Console에서 복구 파일을 다운로드합니다. Dell Data Security를 설치할 때 생성된 `<hostname>-sed-recovery.dat` 파일을 다운로드하기:

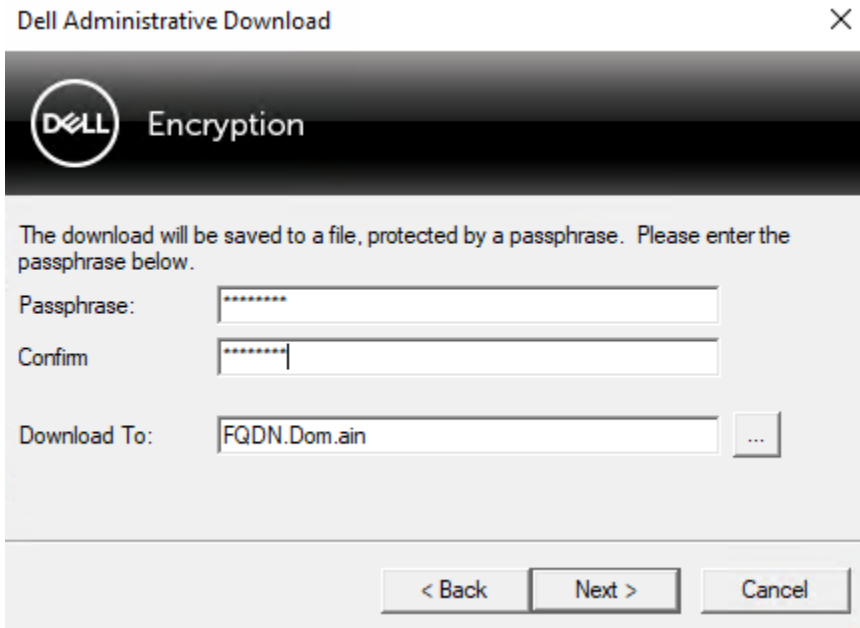
- a Remote Management Console을 열고 왼쪽 창에서 **관리 > 데이터 복구**를 선택한 후 **PBA** 탭을 선택합니다.
- b 데이터 복구 화면의 호스트 이름 필드에서 끝점의 정규화된 도메인 이름을 입력한 다음 **검색**을 클릭합니다.
- c SED 필드에서 옵션을 선택합니다.
- d **복구 파일 만들기**를 클릭합니다.

`<hostname>- sed- recovery.dat` 파일이 다운로드됩니다.

# 복구 파일 가져오기 - 정책 기반 암호화 또는 FFE 암호화 클라이언트

복구 파일을 다운로드하려면 다음을 수행하십시오.

- 1 <http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers> 에서 Dell 암호화 설치 패키지를 다운로드합니다. 설치 패키지에서 **AdminUtilities** 폴더로 이동하여 **CMGAd.exe**를 엽니다.
- 2 **Dell 서버** 필드에 컴퓨터가 활성화되어 있는 Security Management Server/Security Management Server Virtual을 입력합니다.
- 3 **Dell 관리자** 필드에 포렌식 관리자 권한이 있는 사용자 계정 이름을 입력합니다.
- 4 **암호** 필드에 포렌식 관리자의 암호를 입력합니다.
- 5 **MCID** 필드에 복구하는 장치의 FQDN을 입력합니다.
  - **DCID** 필드는 복구되는 장치의 복구 ID입니다.
- 6 다음을 선택합니다.
- 7 복구 파일을 위한 **암호**를 정의하고 확인합니다. 이 암호는 복구를 수행하는 데 필요합니다.
- 8 **다운로드 대상:** 필드에 복구 번들에 대한 대상 위치를 입력한 후 다음을 선택합니다. 기본적으로 이 위치는 CMGAd.exe가 실행된 디렉터리 안에 있습니다.



- 9 복구 번들이 **다운로드 대상:**에 지정된 폴더로 다운로드됩니다.

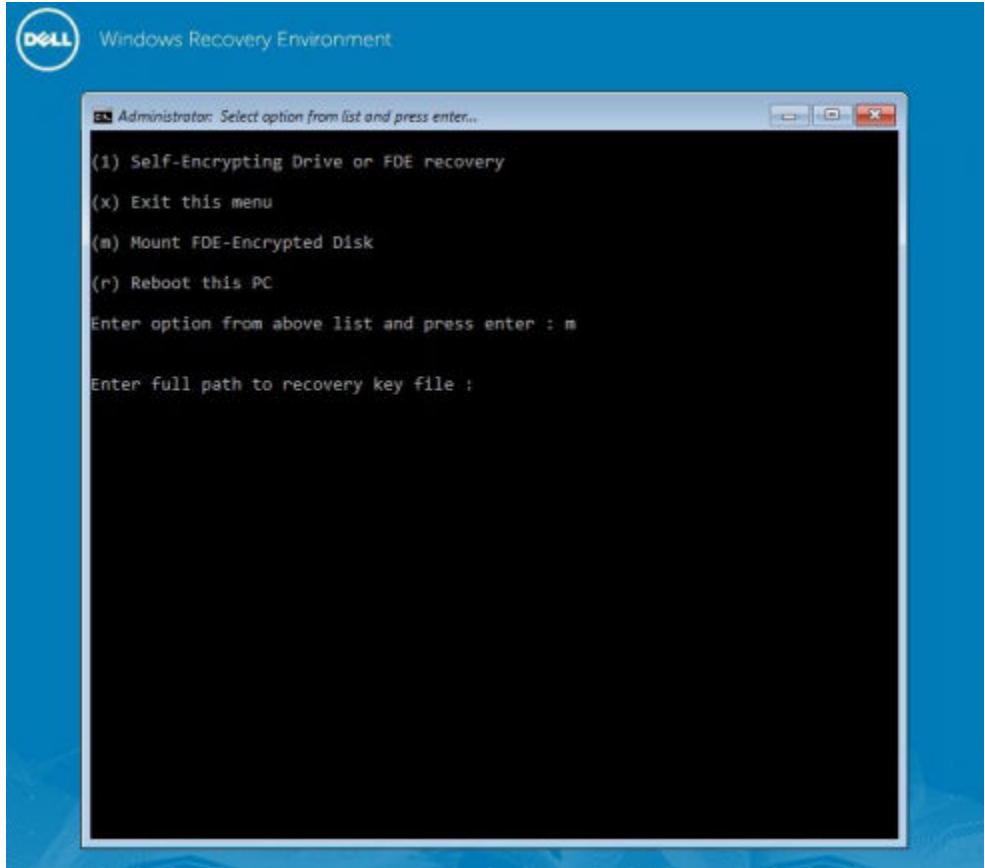
Name	Date modified	Type	Size
CmgAd	5/11/2018 6:28 AM	Application	1,469 KB
CmgAlu	5/11/2018 6:28 AM	Application	1,164 KB
CmgAu	5/11/2018 6:28 AM	Application	1,617 KB
CmgCryptoLib.dll	5/11/2018 6:28 AM	Application extens...	608 KB
CmgCryptoLib.mac	5/11/2018 6:28 AM	MAC File	1 KB
FQDN.Dom.ain	5/11/2018 6:34 AM	AIN File	103 KB
WSScan	5/11/2018 6:28 AM	Application	5,330 KB

- 10 복구 번들 파일을 WinPE로 부팅할 때 액세스할 수 있는 위치에 복사합니다.

# 복구 수행

1 앞에서 만들었던 부팅 가능한 미디어를 사용하여 복구 시스템 또는 복구를 수행할 드라이브가 있는 장치에서 이 미디어로 부팅합니다. 복구 응용 프로그램에서 WinPE 환경이 열립니다.

① **노트:** 복구 프로세스를 진행하기 전에 **SecureBoot**를 비활성화합니다. 완료되면 **SecureBoot**를 다시 활성화합니다.



- 2 옵션 3을 선택하고 **Enter** 키를 누릅니다.
- 3 메시지가 표시되면 복구 파일 이름 및 위치를 입력합니다.
- 4 복구 키를 사용하여 전체 디스크 암호화된 디스크가 마운트됩니다.



```

Enter option from above list and press enter : m

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

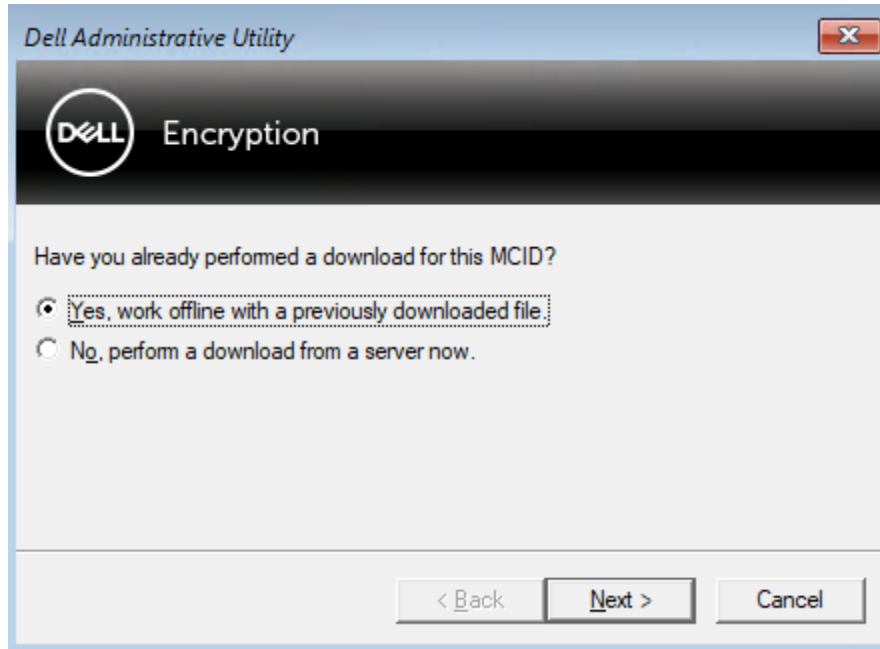
Recoveryfile loaded
----- Disk 0 -----
Cylinders      = 15566
Tracks/cylinder = 255
Sectors/track  = 63
Bytes/sector   = 512
Disk size      = 128035676160 (Bytes)
               = 119.24 GB
--> Disk 0, returned status.....: EDriverStatus_Success
----- Disk 1 -----
Cylinders      = 973
Tracks/cylinder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

```

5 cd DDPEAdminUtilities\ 명령을 사용하여 CMGAu.exe 유틸리티로 이동합니다.

6 \DDPEAdminUtilities>CmgAu.exe 명령을 사용하여 CMGAu.exe를 실행합니다.

예, 이전에 다운로드한 파일을 가지고 오프라인으로 작업을 선택합니다.



7 다운로드된 파일: 필드에 복구 번들의 위치를 입력한 후 포렌식 관리자의 암호를 입력하고 다음을 선택합니다.

설치가 완료되면 **마침**을 클릭합니다.

**① 노트:**

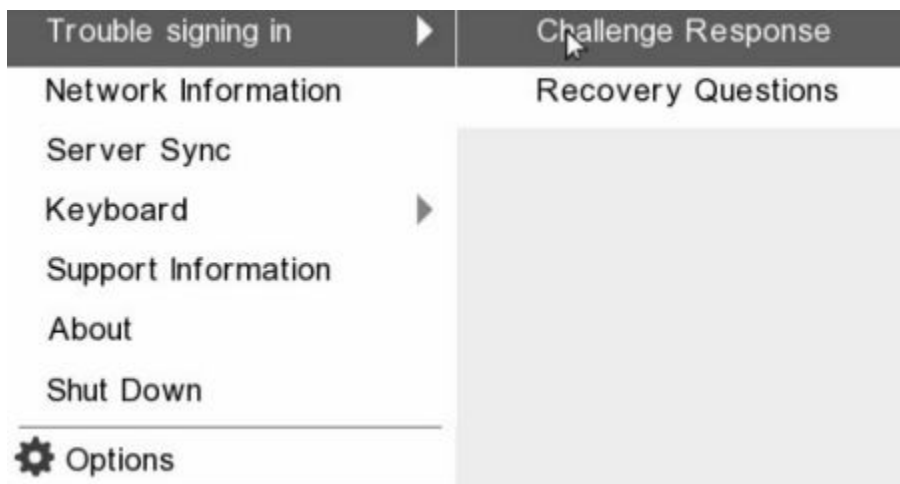
컴퓨터를 부팅하는 데 사용한 USB 또는 CD/DVD 미디어는 반드시 제거해야 합니다. 이렇게 하지 않으면 복구 환경으로 다시 부팅될 수 있습니다.

- 8 컴퓨터가 다시 부팅된 후에는 암호화된 파일에 액세스할 수 있습니다. 문제가 지속되면 Dell ProSupport에 문의하십시오.

## 전체 디스크 암호화로 챌린지 복구

### 부팅 전 인증 환경 무시

사용자가 암호를 분실하여 PBA 환경 통과와 관련하여 헬프 데스크에 전화를 합니다. 장치에 내장된 의문 제기/응답 메커니즘을 사용하십시오. 이 메커니즘은 사용자별로 이루어지며 교대되는 영숫자 문자 집합을 기반으로 합니다. **사용자 이름** 필드에 사용자가 자신의 이름을 입력한 다음, **옵션 > 챌린지 응답**을 선택해야 합니다.



**챌린지 응답**을 선택하면 다음 정보가 표시됩니다.

### Challenge Response

Contact your IT administrator to receive the Response Code to unlock your computer.

Device Name  
34E6D74006CE

Challenge Code

C1D3	293E	99F3	1425
4F5B	B902	6172	870C

Response Code

I			

Submit Cancel

장치 이름 필드는 Remote Management Console의 헬프데스크 기술자가 올바른 장치를 찾는 데 사용되며 사용자 이름이 선택됩니다. 이는 PBA 탭의 관리 > 데이터 복구 탭에서 찾을 수 있습니다.

Dell Data Security | superadmin

### Recover Data

Shield Manager **PBA**

Recover PBA Endpoint

Hostname:  Search

PBA:  Create Recovery File

Recover PBA User Access

Obtain Host Name, User Name, and Challenge code. Hostname:  Search

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. Username:  Challenge: 


 Response:

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

데이터를 입력하고 응답 생성 단추를 클릭한 헬프 데스크 기술자에게 챌린지 코드가 제공됩니다.

## Recover Data

Shield   Manager   **PBA**

---

Recover PBA Endpoint

Hostname:

PBA:

### Recover PBA 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:

Username:

C1D3	293E	99F3	1425
4F5B	B902	6172	870C

Challenge:

Response: **A1FA-56E8-DB78-39D3-0F51-2110-9514-8E7C**

이 결과 데이터는 숫자(빨간색)와 영문자(파란색)를 구별하는 데 도움이 되도록 색상으로 조정됩니다. 이 데이터를 최종 사용자가 읽습니다. 최종 사용자는 이 데이터를 PBA 환경에 입력한 다음 **제출** 단추를 클릭하여 사용자를 Windows로 이동합니다.

### Challenge Response

Contact your IT administrator to receive the Response Code to unlock your computer.

Device Name

Challenge Code

C1D3	293E	99F3	1425
4F5B	B902	6172	870C

Response Code

A1FA	56E8	DB78	39D3
0F51	2110	9514	8E7C

인증에 성공하면 다음 메시지가 표시됩니다.

## Challenge Response

Authentication successful. Please wait...

Device Name

34E6D74006CE

Challenge Code

C1D3

293E

99F3

1425

4F5B

B902

6172

870C

Response Code

A1FA

56E8

DB78

39D3

0F51

2110

9514

8E7C

4

Submit

Cancel

챌린지 복구가 완료되었습니다.

## PBA 장치 제어

PBA 장치 제어는 SED 또는 전체 디스크 암호화로 암호화된 끝점에 적용됩니다.

### PBA 장치 제어 사용

특정 끝점에 대한 PBA 명령은 PBA 장치 제어 영역에서 실행됩니다. 각 명령에는 우선 순위 등급이 있습니다. 우선 순위 등급이 가장 높은 명령은 시행 큐에서 우선 순위가 낮은 명령을 취소합니다. 명령 우선 순위 등급 목록은 Remote Management Console에서 물음표 (?)를 클릭하면 제공되는 *AdminHelp*를 참조하십시오. PBA 장치 제어는 Remote Management Console의 끝점 세부 정보 페이지에서 사용할 수 있습니다.

PBA 장치 제어에서 다음 명령을 사용할 수 있습니다.

- **잠금** - PBA 화면을 잠그고 사용자가 컴퓨터에 로그인하지 못하도록 합니다.
- **잠금 해제** - 잠금 명령을 전송하거나 정책에서 허용하는 최대 인증 시도 횟수를 초과하여 이 끝점에서 PBA 화면이 잠긴 경우에 이 화면을 잠금 해제할 수 있습니다.
- **사용자 제거** - PBA에서 모든 사용자를 제거합니다.
- **로그인 무시** - PBA 화면을 한 번 무시하여 사용자가 인증 없이 컴퓨터에 액세스할 수 있도록 허용합니다. PBA를 건너뛰었다라도 사용자는 Windows에 로그인해야 합니다.
- **초기화** - 초기화 명령은 암호화된 드라이브에 대해 "출고 시 상태로 복원"처럼 작동합니다. 삭제 명령은 컴퓨터의 용도를 다시 지정하거나, 응급 상황에서 컴퓨터를 삭제해 데이터를 영구히 복구할 수 없게 만드는 데 사용할 수 있습니다. 이 명령을 호출하기 전에 원하는 동작인지 확인하십시오. 전체 디스크 암호화의 경우 초기화 명령은 드라이브를 암호화 방식으로 지우고 PBA가 제거됩니다. SED의 경우 초기화 명령은 드라이브를 암호화 방식으로 지우고 PBA는 "장치 잠금"을 표시합니다. SED를 다시 사용하려면 SED 복구 앱으로 PBA를 제거합니다.

## GPK(General Purpose Key) 복구

GPK(General Purpose Key) 복구는 도메인 사용자의 레지스트리 부분을 암호화하는 데 사용됩니다. 드물기는 하지만, 부팅 과정 중에 손상되어 암호를 해독하지 못할 수도 있습니다. 이 경우에는 클라이언트 컴퓨터의 CMGShield.log 파일에 다음과 같은 오류가 표시됩니다.

```
[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
```

GPK의 암호 해독에 실패하면, Dell Server에서 다운로드한 복구 번들에서 GPK를 추출하여 복구해야 합니다.

## GPK 복구

### 복구 파일 가져오기

Dell Data Security를 설치했을 때 생성된 <machinename\_domain.com>.exe 파일을 다운로드하려면:

- 1 Remote Management Console을 열고 왼쪽 창에서 **관리 > 끝점 복구**를 선택합니다.
- 2 호스트 이름 필드에 끝점의 정규화된 도메인 이름을 입력하고 **검색**을 클릭합니다.
- 3 복구 창에서 복구 암호를 입력하고 **다운로드**를 클릭합니다.

#### ① 노트:

복구 키에 액세스하려면 이 암호가 필요합니다.

<machinename\_domain.com>.exe 파일이 다운로드됩니다.

### 복구 수행

- 1 복구 환경의 부팅 가능한 미디어를 생성합니다. 자세한 지침은 **부록 A - 복구 환경 굽기**를 참조하십시오.
  - ① 노트: 복구 프로세스를 진행하기 전에 **SecureBoot**를 비활성화합니다. 완료되면 **SecureBoot**를 활성화합니다.
- 2 복구 시스템에 있거나 드라이브가 있고 복구하려는 장치에 미디어를 부팅합니다. WinPE 환경이 열립니다.
- 3 명령 프롬프트를 받으려면 **x**를 입력하고 **Enter** 키를 누릅니다.
- 4 복구 파일로 이동하여 실행합니다. Encryption 클라이언트 진단 대화 상자가 열리고 백그라운드에서 복구 파일이 생성됩니다.
- 5 관리자 명령 프롬프트에서 <machinename\_domain.com> .exe > -p <password> -gpk를 실행합니다. 그러면 컴퓨터용 GPKRcvr.txt가 반환됩니다.
- 6 **gpkrcvr.txt** 파일을 컴퓨터의 OS 드라이브의 루트에 복사합니다.

- 7 컴퓨터를 재부팅합니다.  
GPKRCVR.txt 파일이 운영 체제에 사용되어 해당 컴퓨터에 GPK를 다시 생성합니다.
- 8 메시지가 표시되면 다시 부팅합니다.



# BitLocker Manager 복구

데이터를 복구하려면 원격 관리 콘솔에서 복구 암호 또는 키 패키지를 얻은 다음 컴퓨터의 데이터를 잠금 해제합니다.

## 데이터 복구

- 1 Dell 관리자로 Remote Management Console에 로그인합니다.
- 2 왼쪽 창에서 **관리 > 데이터 복구**를 클릭합니다.
- 3 **관리자** 탭을 클릭합니다.
- 4 *BitLocker*인 경우:  
BitLocker에서 받은 **복구 ID**를 입력합니다. 선택적으로 호스트 이름과 볼륨을 입력할 경우 복구 ID가 채워집니다.

**복구 암호 또는 키 생성 패키지를** 클릭합니다.

선호하는 복구 방법에 따라 이 복구 암호 또는 키 패키지를 사용하여 데이터를 복구합니다.

*TPM*인 경우:

**호스트 이름을** 입력합니다.

**복구 암호 또는 키 생성 패키지를** 클릭합니다.

선호하는 복구 방법에 따라 이 복구 암호 또는 키 패키지를 사용하여 데이터를 복구합니다.

- 5 복구를 완료하려면 **복구 관련 Microsoft의 지침**을 참조하십시오.

### ① **노트:**

BitLocker Manager가 TPM을 "소유"하지 않을 경우 Dell 데이터베이스에서 TPM 암호 및 키 패키지를 사용할 수 없습니다. Dell에서 키를 찾을 수 없다는 오류 메시지가 표시됩니다. 이는 예상된 동작입니다.

BitLocker Manager 이외의 엔터티가 "소유"하는 TPM을 복구하려면 해당 소유자로부터 TPM을 복구하는 절차를 따르거나 기존 TPM 복구 프로세스를 따라야 합니다.

## 암호 복구

사용자는 일반적으로 본인의 암호를 잊어버립니다. 사용자가 부팅 전 인증 단계에서 컴퓨터에 대한 액세스 권한을 다시 부여 받을 수 있는 다양한 방법이 있습니다.

- 복구 질문 기능은 질문 및 응답 기반 인증을 제공합니다.
- 의문 제기/응답 코드는 사용자가 관리자와 함께 자신의 컴퓨터에 다시 액세스할 수 있도록 도와줍니다. 이 기능은 조직이 관리하는 컴퓨터가 있는 사용자만 사용할 수 있습니다.

### 복구 질문

사용자가 컴퓨터에 처음 로그인할 때, 사용자는 관리자가 구성한 일련의 표준 질문에 대답해야 합니다. 질문에 대한 대답을 입력하고 나면, 나중에 암호를 잊어버리더라도 사용자는 대답을 입력하면 됩니다. 사용자가 질문을 정확히 입력한다면 로그인해서 Windows 액세스 권한을 다시 얻을 수 있습니다.

#### 필수 구성 요소

- 관리자는 복구 질문을 설정해두어야 합니다.
- 사용자는 질문에 대한 답을 입력하였습니다.
- **로그인 문제** 메뉴 옵션을 클릭하기 전에 사용자는 유효한 사용자 이름과 도메인을 입력해야 합니다.

PBA 화면에서 복구 질문에 접근하기:

- 1 유효한 도메인 이름과 사용자 이름을 입력합니다.
- 2 화면 왼쪽 하단에서 **옵션 > 로그인 문제**를 클릭합니다.
- 3 Q&A 대화 상자가 나타나면 처음에 로그인할 때 복구 질문에 입력했던 대답을 입력합니다.

## Encryption External Media 암호 복구

Encryption External Media는 사용자가 USB 플래시 드라이브 및 기타 이동식 저장 미디어를 암호화하도록 하여 이동식 저장 미디어를 조직 안팎으로 보호해 줍니다. 사용자는 보호하려는 이동식 미디어 장치 하나당 암호 하나를 지정합니다. 이 섹션은 사용자가 장치의 암호를 잊었을 때, 암호화된 USB Storage Device에 대한 액세스를 복구하는 프로세스를 설명합니다.

### 데이터 액세스 복구

사용자가 올바르게 않은 자신의 암호를 허용되는 수를 초과하여 입력하는 경우 USB 장치는 수동 인증 모드로 전환됩니다.

**수동 인증**은 Dell Server에 로그인되어 있는 클라이언트에서 관리자에게 코드 제공을 제공하는 프로세스입니다.

수동 인증 모드에 있을 때 사용자는 암호를 재설정하고 데이터에 대한 액세스를 복구하는 2개의 옵션이 필요합니다.

관리자는 사용자가 자신의 암호를 재설정하고 암호화된 데이터에 대한 액세스를 다시 확보하도록 액세스 코드를 제공합니다.

- 1 암호에 대한 메시지가 표시되면, **암호 분실** 단추를 클릭합니다.  
확인 대화 상자가 나타납니다.
- 2 **예**를 클릭하여 확인합니다. 확인 후에 장치는 수동 인증 모드로 전환됩니다.
- 3 도움말 책상 관리자에게 문의하여 대화 상자에 나타나는 코드를 알려 주십시오.
- 4 헬프 데스크 관리자는 원격 관리 콘솔에 로그인합니다. 헬프 데스크 관리자의 계정은 헬프 데스크 권한이 있어야 합니다.
- 5 왼쪽 창의 **데이터 복구** 메뉴 옵션을 탐색합니다.
- 6 최종 사용자가 제공하는 코드를 입력합니다.
- 7 화면의 오른쪽 맨 아래에 있는 **응답 생성** 단추를 클릭합니다.
- 8 사용자에게 액세스 코드를 부여합니다.

#### ① 노트:

액세스 코드를 제공하기 전에 수동으로 사용자를 인증하십시오. 예를 들어, 전화로 사용자에게 "귀하의 ID는 무엇입니까?"와 같이 본인만 알 수 있는 질문을 하십시오. 또 다른 예: 사용자가 미디어의 소유자인지 확인하기 위해 신원 확인을 제공하는 헬프 데스크로 오라고 요청하십시오. 전화상으로 액세스 코드를 제공하기 전에 사용자 인증에 실패한 경우 공격자는 암호화된 이동식 미디어에 액세스할 수 있습니다.

- 9 암호화된 미디어에 대한 암호를 재설정하십시오.  
사용자는 암호화된 미디어의 암호를 재설정해야 합니다.

### 자체 복구

자체 복구가 작동하도록 하려면 원래 암호화한 시스템에 드라이브를 다시 삽입해야 합니다. 미디어 소유자가 보호되는 MAC 또는 PC에 인증을 받으려면 클라이언트는 키 자료의 손실을 탐지하고 사용자가 장치를 재시작하도록 요구합니다. 사용자는 암호를 재설정하고 암호화된 데이터에 다시 액세스할 수 있습니다. 이 프로세스에서 부분적으로 손상된 미디어 문제를 해결할 수 있습니다.

- 1 Dell Data Security 암호화 워크스테이션에 미디어 소유주로 로그인합니다.
- 2 암호화된 이동식 저장 장치를 삽입합니다.
- 3 메시지가 나타나면 이동식 저장소 장치를 다시 초기화하도록 새 암호를 입력합니다.

작업에 성공하면 암호가 수락되었다고 알리는 작은 알림창이 나타납니다.

- 4 저장소 장치로 이동하고 데이터에 대한 액세스를 확인합니다.

## Dell Data Guardian 복구

복구 도구를 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 암호화 해제:
  - 지원되는 모든 형식의 보호된 Office 파일 - Data Guardian의 보호된 Office 문서 암호화 및 해당 클라우드 서비스 공급자 보호로 보호되는 파일은 복구할 수 있습니다.
  - 활성화된 경우 기본 파일 보호 정책에 파일 형식이 나열되어 있습니다.
- 핵심 자료의 수동 에스스로
- 변조된 파일 확인 기능
- 클라우드 혹은 Data Guardian이 없는 장치에 있는 보호된 Office 문서 파일의 표지 페이지와 같이 누군가가 파일 래퍼로 변조한 보호된 Office 문서를 강제로 해독할 수 있습니다.

### ① 노트:

Mac, 모바일 또는 웹 포털 플랫폼에서 생성된 파일에 Windows 복구 도구를 사용할 수 있습니다.

## 사전 요구 사항

필수 조건은 다음과 같습니다.

- 끝점에서 실행 중인 Microsoft .Net Framework 4.5.2를 복구할 수 있습니다.
- 포렌식 관리자 역할은 복구를 수행하는 관리자를 위해 Management Console에서 할당되어야 합니다.

## Data Guardian 복구 수행

다음 단계에 따라 Data Guardian의 보호된 Office 문서 복구를 수행하십시오. 한 번에 하나의 컴퓨터만 복구할 수 있습니다.

### ① 중요:

손상이 발생한 경우에 콘텐츠를 손실하지 않으려면 원본 파일이 아닌 파일의 사본을 해독합니다.

### Windows, USB 플래시 드라이브 또는 네트워크 드라이브에서 복구 수행

복구 수행하기:

- 1 Dell 설치 미디어에서 **RecoveryTools.exe**를 다음 중 하나로 복사합니다.
  - 컴퓨터 - .exe를 Office 문서가 복구될 컴퓨터에 복사합니다.
  - USB - USB 플래시 드라이브로 .exe 파일을 복사하고 USB 플래시 드라이브에서 실행.
  - 네트워크 드라이브

### ① 중요:

관리자 권한으로 **RecoveryTools.exe**만 복사해야 합니다(설치 프로그램은 복사하지 않음). **RecoveryTools.exe**는 스윙 또는 암호 해독이 실행되지 않고 있을 때 더 잘 작동합니다.

- 2 **RecoveryTools.exe**를 두 번 클릭하여 복구 도구를 시작합니다.
- 3 Data Guardian 복구 도구 창에서 **도메인 로그인(Domain Login)**을 선택합니다.

① **노트:**

호스팅된 솔루션을 위한 SaaS 로그인 옵션은 향후 출시 예정입니다.

- 4 Dell Server FQDN을 이 형식으로 입력합니다.  
server.domain.com

① **노트:**

접두사 및 접미사가 FQDN에 자동으로 추가됩니다.

- 5 사용자 이름과 암호를 입력하고 **로그인**을 클릭합니다.

① **노트:**

관리자가 요구하는 경우를 제외하고 *SSL 인증서 활성화* 확인란을 선택 해제하지 마십시오.

① **노트:**

포렌식 관리자가 아닌데도 자격 증명을 입력하는 경우, 로그인 권한이 없다고 알려주는 메시지가 표시됩니다.

- 6 포렌식 관리자의 경우 복구 도구가 실행됩니다.
- 7 소스를 선택합니다.

① **노트:**

소스 및 대상을 찾아야 하지만, 순서에 상관없이 선택할 수 있습니다.

- 8 **찾아보기**를 클릭하여 폴더 혹은 복구할 드라이브를 선택합니다.
- 9 **확인**을 클릭합니다.
- 10 암호 해독되었거나 복구된 파일용의 빈 폴더인 **대상**을 클릭합니다.
- 11 외부 장치, 디렉터리 위치 혹은 데스크탑과 같은 대상을 선택하려면 **찾아보기**를 클릭합니다.
- 12 **확인**을 클릭합니다.
- 13 복구하고자 하는 대상을 기반으로 하는 상자를 1개 이상 선택합니다.

**옵션**

**설명**

에스크로

- Dell Server로 에스크로할 수 없으며 오프라인으로 생성된 키를 복구합니다.
- 사용자가 네트워크 상에서 오프라인일 때 하드 드라이브가 작동이 되지 않을 경우, 컴퓨터에서 데이터와 에스크로되지 않은 키를 복구하려면 슬레이브 드라이브를 사용합니다.

암호 해독

보호된 Office 문서의 암호를 해독하려면 문서를 포함하는 디렉터리에 보호 도구를 지정합니다.

① **노트:**

손상이 발생한 경우 파일의 원본이 아니라 사본 암호를 해독하는 것이 좋습니다.

선택적으로 변경이 발생했다면 다음 옵션 중 하나 혹은 모두를 선택합니다(자세한 사항은 아래 참조).

- **무단 변경 확인** - 변경된 파일을 검사하지만 암호를 해독하지는 않습니다.
- **무단 변경 확인 및 무단 변경되어도 강제 암호 해독** - 변경된 파일을 검사합니다. 보호된 Office 문서의 래퍼가 변경된 경우, Data Guardian은 래퍼를 수리하고 Office 문서의 암호를 해독합니다.

## 옵션

## 설명

무단 변경 확인

변조된 파일을 감지하고 로그하거나 사용자에게 알립니다. 파일을 변조한 작성자를 기록합니다. 파일의 암호를 해독하지 않습니다.

무단 변경되어도 강제 암호 해독

이 옵션을 선택하려면 **무단 변경 확인**을 선택해야 합니다.

승인 받지 않은 사람이 클라우드에 있거나 Data Guardian이 없는 장치에 있는 표지 페이지와 같은 보호된 Office 문서의 래퍼를 변경하는 경우, 래퍼를 수리하고 보호된 Office 문서의 암호를 강제로 해독하려면 옵션을 선택하십시오.

### ① 노트:

래퍼 내에 있는 암호화된 Office .xen 파일을 변경하는 경우, 파일은 복구될 수 없습니다.

각 보호된 Office 문서는 원래 사용자의 기록, 컴퓨터 이름, 파일을 변경한 기타 컴퓨터 이름을 포함하는 숨겨진 워터마크가 있습니다. 기본적으로 복구 도구는 숨겨진 워터마크를 확인하고 로그의 *HiddenWatermark* 폴더에 모든 작성자 목록이 있는 텍스트 파일을 추가합니다.

14 선택을 완료하면 **스캔**을 클릭합니다.

로그 영역에 다음과 같은 사항이 표시됩니다.

- 검색되고 스캔된 폴더 내의 선택된 소스
- 암호 해독이 파일별로 성공적으로 수행되었는지 여부
- 파일의 마지막 작성자 이름

복구 도구는 선택한 대상에 복구된 파일을 추가합니다. 파일을 열고 볼 수 있습니다.

## 숨겨진 감사 추적의 데이터 보기

Windows의 경우 보호된 Office 문서의 숨겨진 감사 추적 정책을 사용하면 파일 메타데이터에 사용자 정보가 수집됩니다. 이 데이터를 보려면 복구 도구를 사용하십시오.

1 복구 도구를 실행합니다.

- 소스의 경우 숨겨진 감사 데이터가 있는 보호된 Office 문서가 들어있는 폴더를 찾습니다. 복구 도구는 폴더 및 하위 폴더 구조를 복사하고 숨겨진 감사 데이터가 있는 보호된 Office 문서를 해독합니다.
- **대상**으로 이동하기 전에 암호 해독된 파일이라는 폴더를 생성한 다음 해당 폴더로 이동할 수 있습니다.

2 **암호 해독**을 선택합니다.

3 선택을 완료하면 **스캔**을 클릭합니다.

대상으로 선택된 폴더에는 날짜가 있는 **복구된 파일** 폴더가 다음과 함께 들어 있습니다.

- 암호 해독되고 보호된 Office 파일
- 복구 도구가 생성한 **감사 추적** 폴더(암호 해독된 각 파일에 대한 .txt 파일 포함) 작성자, 최종 작성자, 시간 스탬프와 같이 암호 해독된 파일의 정보를 나열하는 로그가 각 .txt 파일에 있습니다.

## 부록 A - 복구 환경 굽기

마스터 설치 프로그램을 다운로드할 수 있습니다.

### 복구 환경 ISO에서 CD\DVD로 굽기

다음 링크에는 복구 환경을 위한 부팅 가능한 CD 또는 DVD를 생성하기 위해 Microsoft Windows 7, Windows 8 또는 Windows 10을 사용하는 데 필요한 프로세스가 포함되어 있습니다.

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

### 이동식 미디어에서 복구 환경 굽기

부팅 가능한 USB를 만들려면 다음 지침을 따르십시오.

레거시 부팅:

- 1 USB 드라이브를 시스템에 연결합니다.
- 2 관리자 명령 프롬프트를 엽니다.
- 3 **diskpart**를 입력하여 Diskpart 유틸리티를 시작합니다.
- 4 **list disk**를 입력하여 수정할 대상 디스크를 찾습니다. 디스크는 번호로 지정됩니다.
- 5 **select disk #** 명령을 사용하여 해당 디스크를 선택하십시오. 여기서 #은 이전 단계에서 표시된 해당 드라이브의 디스크 번호입니다.
- 6 **clean** 명령을 실행하여 디스크를 지우십시오. 이렇게 하면 파일 테이블을 지워 데이터 드라이브가 제거됩니다.
- 7 부트 이미지가 상주할 파티션을 만듭니다.
  - a **create partition primary** 명령이 드라이브에 기본 파티션을 생성합니다.
  - b **select partition 1** 명령이 새 파티션을 선택합니다.
  - c **format FS=NTFS quick** 명령을 사용하여 NTFS 파일 시스템으로 드라이브를 빠르게 포맷하십시오.
- 8 드라이브는 부팅 가능한 드라이브로 표시되어야 합니다. **active** 명령을 사용하여 드라이브를 부팅 가능으로 표시하십시오.
- 9 파일을 드라이브로 직접 옮기려면 **assign** 명령을 사용하여 드라이브에 사용 가능한 문자를 할당하십시오.
- 10 드라이브가 자동으로 마운트되고 ISO 파일의 내용을 드라이브의 루트에 복사할 수 있습니다.

ISO 내용이 완전히 복사되면 드라이브가 부팅 가능하며 복구에 사용할 수 있습니다.

UEFI 부팅:

- 1 USB 드라이브를 시스템에 연결합니다.
- 2 관리자 명령 프롬프트를 엽니다.
- 3 **diskpart**를 입력하여 Diskpart 유틸리티를 시작합니다.
- 4 **list disk**를 입력하여 수정할 대상 디스크를 찾습니다. 디스크는 번호로 지정됩니다.
- 5 **select disk #** 명령을 사용하여 해당 디스크를 선택하십시오. 여기서 #은 이전 단계에서 표시된 해당 드라이브의 디스크 번호입니다.
- 6 **clean** 명령을 실행하여 디스크를 지우십시오. 이렇게 하면 파일 테이블을 지워 데이터 드라이브가 제거됩니다.
- 7 부트 이미지가 상주할 파티션을 만듭니다.
  - a **create partition primary** 명령이 드라이브에 기본 파티션을 생성합니다.



- b **select partition 1** 명령이 새 파티션을 선택합니다.
  - c **format FS=FAT32 quick** 명령을 사용하여 FAT32 파일 시스템으로 드라이브를 빠르게 포맷하십시오.
- 8 드라이브는 부팅 가능한 드라이브로 표시되어야 합니다. **active** 명령을 사용하여 드라이브를 부팅 가능으로 표시하십시오.
  - 9 파일을 드라이브로 직접 옮기려면 **assign** 명령을 사용하여 드라이브에 사용 가능한 문자를 할당하십시오.
  - 10 드라이브가 자동으로 마운트되고 ISO 파일의 내용을 드라이브의 루트에 복사할 수 있습니다.
- ISO 내용이 완전히 복사되면 드라이브가 부팅 가능하며 복구에 사용할 수 있습니다.