

Dell Data Protection | Encryption

Enterprise Edition 고급 설치 안내서 v8.10.1



범례

△ | 주의: 주의 아이콘은 지시를 따르지 않을 경우 하드웨어 손상 또는 데이터 손실의 가능성이 있음을 나타냅니다.

⚠ | 경고: 경고 아이콘은 재산 피해, 신체 상해 또는 사망의 가능성이 있음을 나타냅니다.

ℹ | 중요, 참고, 팁, 모바일, 또는 비디오: 정보 아이콘은 도움이 되는 정보를 나타냅니다.

© 2016 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools 및 Dell Data Protection | Cloud Edition 문서 세트에 사용된 등록 상표 및 상표들 즉, Dell™ 및 Dell 로고, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® 및 KACE™는 Dell Inc.의 상표입니다. McAfee®와 McAfee 로고는 미국 및 기타 국가에서 McAfee, Inc.의 상표 또는 등록 상표입니다. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® 및 Xeon®은 미국 및 기타 국가에서 Intel 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®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, 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. DropboxSM은 Dropbox, Inc.의 서비스 표시입니다. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® 및 Google™ Play는 미국 및 기타 국가에서 Google Inc.의 상표 또는 등록 상표입니다. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® 및 Siri®는 미국 및/또는 기타 국가에서 Apple, Inc.의 서비스 표시, 상표, 또는 등록 상표입니다. GO ID®, RSA®, SecurID®는 EMC Corporation의 등록 상표입니다. EnCase™ 및 Guidance Software®는 Guidance Software의 상표 또는 등록 상표입니다. Entrust®는 미국 및 기타 국가에서 Entrust®, Inc.의 등록 상표입니다. InstallShield®는 미국, 중국, 유럽 공동체, 홍콩, 일본, 대만, 및 영국에서 Flexera Software의 등록 상표입니다. Micron® 및 RealSSD®는 미국 및 기타 국가에서 Micron Technology, 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. 기타 이름은 해당 소유자의 상표일 수 있습니다. SAMSUNG™은 미국 또는 기타 국가에서 SAMSUNG의 상표입니다. Seagate®는 미국 및/또는 기타 국가에서 Seagate Technology LLC의 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 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.의 등록 상표입니다. 본 제품은 7-Zip 프로그램을 일부 사용합니다. 이 소스 코드는 www.7-zip.org에서 찾아볼 수 있습니다. 라이선스에는 GNU LGPL 라이선스 + unRAR 제한이 적용됩니다(www.7-zip.org/license.txt).

Enterprise Edition 고급 설치 안내서

2016 - 09

개정 A00

1 소개.....	7
시작하기 전에.....	7
이 안내서 사용.....	7
Dell ProSupport에 문의.....	8
2 요구 사항.....	9
모든 클라이언트.....	9
모든 클라이언트 - 필수 구성 요소.....	9
모든 클라이언트 - 하드웨어.....	9
모든 클라이언트 - 언어 지원.....	10
Encryption 클라이언트.....	10
Encryption 클라이언트 필수 구성 요소.....	11
Encryption 클라이언트 하드웨어.....	11
Encryption 클라이언트 운영 체제.....	11
EMS(External Media Shield) 운영 체제.....	11
Server Encryption 클라이언트.....	12
Server Encryption 클라이언트 필수 구성 요소.....	13
Server Encryption 클라이언트 하드웨어.....	13
Server Encryption 클라이언트 운영 체제.....	13
EMS(External Media Shield) 운영 체제.....	14
SED 클라이언트.....	15
OPAL 드라이버.....	15
SED 클라이언트 필수 구성 요소.....	15
OPAL 호환 SED.....	15
SED 클라이언트 운영 체제.....	15
국제 키보드.....	16
Advanced Authentication 클라이언트.....	16
Advanced Authentication 클라이언트 하드웨어.....	16
Advanced Authentication 클라이언트 운영 체제.....	17
BitLocker Manager 클라이언트.....	18
BitLocker Manager 클라이언트 필수 구성 요소.....	18
BitLocker Manager 클라이언트 운영 체제.....	18
Cloud Edition 클라이언트.....	19
Cloud Edition 클라이언트 23.....	19
클라우드 동기화 클라이언트.....	19
웹 브라우저.....	20
클라이언트 운영 체제를 클라우드 Edition.....	20
인증 옵션.....	20
Encryption 클라이언트.....	21
SED 클라이언트.....	21
BitLocker Manager.....	22
3 레지스트리 설정.....	24

Encryption 클라이언트 레지스트리 설정.....	24
SED 클라이언트 레지스트리 설정.....	27
Advanced Authentication 클라이언트 레지스트리 상태.....	29
BitLocker Manager 클라이언트 레지스트리 설정.....	29
Cloud Edition 클라이언트 레지스트리 설정.....	30
4 마스터 설치 프로그램을 사용하여 설치.....	31
마스터 설치 프로그램을 사용하여 대화형으로 설치.....	31
마스터 설치 프로그램을 사용하여 명령줄을 통해 설치.....	32
5 마스터 설치 프로그램을 사용하여 설치 제거.....	34
마스터 설치 프로그램 설치 제거.....	34
명령줄 설치 제거.....	34
6 하위 설치 프로그램을 사용하여 설치.....	35
드라이버 클라이언트 설치.....	36
명령줄 설치.....	36
Encryption 클라이언트 설치.....	36
명령줄 설치.....	37
Server Encryption 클라이언트 설치.....	38
Server Encryption 대화형 설치.....	39
명령줄을 사용하여 Server Encryption 설치.....	40
Server Encryption 활성화.....	41
SED Management 및 Advanced Authentication 클라이언트 설치.....	43
명령줄 설치.....	43
Cloud Edition 설치.....	44
명령줄 설치.....	44
BitLocker Manager 클라이언트 설치.....	44
명령줄 설치.....	45
7 하위 설치 프로그램을 사용하여 설치 제거.....	46
Encryption 및 Server Encryption 클라이언트 설치 제거.....	47
프로세스.....	47
명령줄 설치 제거.....	47
External Media Edition 설치 제거.....	49
SED 및 Advanced Authentication 클라이언트 설치 제거.....	49
프로세스.....	49
PBA 비활성화.....	49
SED 클라이언트 및 Advanced Authentication 클라이언트 설치 제거.....	50
BitLocker Manager 클라이언트 설치 제거.....	50
명령줄 설치 제거.....	50
Cloud Edition 설치 제거.....	50
명령줄 설치 제거.....	50
8 일반적으로 사용되는 시나리오.....	51
Encryption 클라이언트 및 Advanced Authentication.....	52
SED 클라이언트(Advanced Authentication 포함) 및 External Media Shield.....	52



SED 클라이언트(Advanced Authentication 포함), External Media Edition, 및 Cloud Edition.....	53
Encryption 클라이언트 및 Cloud Edition.....	53
BitLocker Manager 및 External Media Shield.....	54
BitLocker Manager, External Media Edition 및 Cloud Edition.....	54
SED 클라이언트(Advanced Authentication 포함), Encryption 클라이언트 및 Cloud Edition.....	55
9 다운로드할 소프트웨어.....	56
10 일회용 암호, SED UEFI, BitLocker의 사전 설치 구성.....	57
TPM 초기화.....	57
UEFI 컴퓨터의 사전 설치 구성.....	57
UEFI 부팅 전 인증이 진행되는 동안 네트워크 연결 활성화.....	57
레거시 옵션 ROM 비활성화.....	57
BitLocker PBA 파티션 설정을 위한 사전 설치 구성.....	58
11 권한 부여 활성화를 위해 도메인 컨트롤러에서 GPO 설정.....	59
12 마스터 설치 프로그램에서 하위 설치 프로그램 추출.....	60
13 EE Server에 대해 활성화된 Encryption 클라이언트 설치 제거를 위한 Key Server 구성.....	61
서비스 패널 - 도메인 계정 사용자 추가.....	61
Key Server 구성 파일 - EE Server 통신에 대한 사용자 추가.....	61
예시 구성 파일:.....	62
서비스 패널 - Key Server 서비스 재시작.....	62
원격 관리 콘솔 - Forensic Administrator 추가.....	63
14 Administrative Download Utility 사용(CMGAd).....	64
Forensic 모드로 Administrative Download Utility 사용.....	64
관리 모드로 Administrative Download Utility 사용.....	64
15 Server Encryption 구성.....	66
Server Encryption 사용.....	66
활성화 로그인 대화 상자 사용자 지정.....	66
Server Encryption EMS 정책 설정.....	67
암호화된 서버 인스턴스 일시 중단.....	67
16 Cloud Edition을 위한 서버 구성.....	69
Cloud Edition을 위한 VE Server 구성.....	69
Cloud Edition을 위한 EE Server 구성.....	69
Cloud Storage Protection Provider 프로필 관리.....	70
허용 목록/거부 목록에서 사용자 허용/거부.....	70
17 Dropbox for Business에서 Cloud Edition 사용.....	72
업무 및 개인 계정을 위한 정책.....	72
업무 및 개인 폴더.....	73
팀원 계정 원격 삭제.....	73
보고서 실행.....	74



18 문제 해결	75
모든 클라이언트 - 문제 해결.....	75
Encryption 및 Server Encryption 클라이언트 문제 해결.....	75
Windows 10 Anniversary Update로 업그레이드.....	75
서버 운영 체제에서 활성화.....	75
(선택 사항) Encryption Removal Agent 로그 파일 생성.....	77
TSS 버전 찾기.....	78
EMS와 PCS 상호 작용.....	78
WSScan 사용.....	78
WSProbe 사용.....	81
Encryption Removal Agent 상태 확인.....	82
SED 클라이언트 문제 해결.....	83
초기 액세스 코드 정책 사용.....	83
문제 해결을 위해 PBA 로그 파일 생성.....	83
Dell ControlVault 드라이버.....	84
Dell ControlVault 드라이버 및 펌웨어 업데이트.....	84
Cloud Edition v8.x.....	86
세부 정보 화면 사용.....	86
고급 세부 정보 화면 사용.....	86
로그 파일 보기.....	86
임시 폴더 관리 권한 제공.....	86
자주 묻는 질문.....	86
UEFI 컴퓨터.....	87
네트워크 연결 문제 해결.....	87
TPM 및 BitLocker.....	88
TPM 및 BitLocker 오류 코드.....	88
19 용어집	118



소개

이 안내서는 Encryption 클라이언트, SED Management 클라이언트, Advanced Authentication, BitLocker Manager 및 Cloud Edition을 설치하고 구성하는 방법에 대해 자세히 설명합니다.

모든 정책 정보와 그 설명은 AdminHelp에서 찾으시기 바랍니다.

시작하기 전에

1 클라이언트를 배포하기 전에 EE Server/VE Server를 설치하십시오. 아래 나열된 안내서에서 해당되는 안내서를 찾아 지침을 따른 후 이 안내서의 지침을 따르십시오.

- [DDP Enterprise Server 설치 및 마이그레이션 설명서](#)
- [DDP Enterprise Server – Virtual Edition 빠른 시작 안내서 및 설치 안내서](#)

정책이 원하는 대로 설정되었는지 확인합니다. ?에서 사용할 수 있는 AdminHelp를 통해 검색합니다. ?는 화면 맨 오른쪽에 있습니다. AdminHelp는 정책을 설정 및 수정하고 EE Server/VE Server에서의 옵션을 이해할 수 있도록 돕는 페이지 수준의 도움말입니다.

- 2 이 문서의 [요구 사항](#) 장을 읽고 숙지하십시오.
- 3 최종 사용자에게 클라이언트를 배포하십시오.

이 안내서 사용

다음 순서에 따라 이 안내서를 사용합니다.

- 클라이언트 필수 구성 요소, 컴퓨터 하드웨어 및 소프트웨어 정보, 제한 사항 그리고 제한 기능에 필요한 특수 레지스트리 변경에 대해서는 [요구 사항](#)을 참조하십시오.
- 필요하다면 [OTP\(일회용 암호\)](#), [SED UEFI](#) 및 [BitLocker](#)에 대한 [설치 전 구성](#)을 참조하십시오.
- 클라이언트에 Dell Digital Delivery(DDD) 사용 권한이 부여되는 경우, [사용 권한을 활성화하도록 도메인 컨트롤러에서 GPO를 설정](#)을 참조하십시오.
- 마스터 설치 프로그램을 사용하여 클라이언트를 설치할 경우, 다음을 참조하십시오.
 - [마스터 설치 프로그램을 사용하여 대화형으로 설치](#)
- 또는
 - [마스터 설치 프로그램을 사용하여 명령줄을 통해 설치](#)
- 하위 설치 프로그램을 사용하여 클라이언트를 설치하는 경우, 하위 설치 프로그램의 실행 파일들을 마스터 설치 프로그램에서 반드시 추출해야 합니다. [마스터 설치 프로그램에서 하위 설치 프로그램 추출](#)을 참조한 다음, 여기로 되돌아옵니다.
 - 명령줄을 사용하여 하위 설치 프로그램을 설치하십시오.
 - [드라이버 클라이언트 설치](#) - TPM(Trusted Platform Module)이 내장된 컴퓨터에 Encryption 클라이언트를 설치할 경우 또는 Dell 하드웨어에 Encryption 클라이언트를 설치할 경우, 이 지침을 적용하십시오.
 - [Encryption 클라이언트 설치](#) - 컴퓨터가 네트워크에 연결되어 있는지 아니면 네트워크와의 연결이 분리되었거나 분실 내지 도난되었는지 여부에 관계없이 보안 정책을 실행하는 구성 요소에 해당되는 Encryption 클라이언트를 설치할 경우, 이 지침을 적용하십시오.
 - [SED Management 및 Advanced Authentication 클라이언트 설치](#) - 이 지침을 적용하여 SED에 대한 암호화 소프트웨어를 설치합니다. SED가 자체 암호화를 제공하는 하지만 해당 암호화 및 정책을 관리할 플랫폼은 없습니다. SED Management를



사용하면 모든 정책, 저장 그리고 암호화 키 검색을 단일 콘솔에서 이용할 수 있기 때문에 분실 또는 무단 액세스 발생 시 컴퓨터가 무방비로 노출될 위험을 줄입니다.

Advanced Authentication 클라이언트는 SED용 PBA, SSO(Single Sign-On), 지문 및 암호 등과 같은 사용자 자격 증명을 비롯한 여러 인증 방법을 관리합니다. 또한 웹 사이트 및 응용 프로그램에 액세스할 수 있는 Advanced Authentication 기능도 제공합니다.

- **Cloud Edition 설치** - 이 지침을 적용하여 Cloud Edition 클라이언트를 설치합니다. Dropbox, Dropbox for Business, Box, OneDrive 등과 같은 공용 클라우드 서비스에 저장된 데이터를 보호합니다. 데이터는 파일이 클라우드 내부 및 외부로 이동 될 때 완벽하게 암호화됩니다.
- **BitLocker Manager 클라이언트 설치** - BitLocker 배포의 보안을 강화하고 소유 비용을 간소화하여 절감할 수 있도록 설계된 BitLocker Manager 클라이언트를 설치하려면 이 지침을 적용하십시오.

이 노트: 대부분의 하위 설치 프로그램은 대화형으로 설치할 수 있지만 이 안내서에서는 설치에 대한 설명을 제공하지 않습니다.

- 가장 널리 사용되는 시나리오에 관한 설명은 **널리 사용되는 시나리오**를 참조하십시오.

Dell ProSupport에 문의

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

또한, dell.com/support에서 Dell Data Protection 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 코드를 준비하십시오.

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

요구 사항

모든 클라이언트

이 요구 사항은 모든 클라이언트에 적용됩니다. 다른 섹션에 나열된 요구 사항은 특정 클라이언트에 적용됩니다.

- 배포 시에는 IT 모범 사례를 따라야 합니다. 예를 들어, 초기 테스트에서 테스트 환경을 통제하고 사용자에게 대해 시간별 배포를 수행해야 합니다.
- 설치/업그레이드/설치 제거를 수행하는 사용자 계정은 로컬 또는 도메인 관리자여야 하며, 관리자 권한은 Microsoft SMS 또는 Dell KACE 등의 배포 도구를 사용하여 임시로 할당할 수 있습니다. 관리자 이외의 사용자는 상승된 권한을 가진 경우에도 지원되지 않습니다.
- 설치/설치 제거를 시작하기 전에 중요한 데이터를 모두 백업하십시오.
- 설치가 진행되는 동안에는 외부(USB) 드라이브 삽입 또는 제거를 비롯하여 컴퓨터를 변경하지 마십시오.
- 마스터 설치 프로그램 클라이언트에 DDD(Dell Digital Delivery) 사용 권한이 부여되는 경우 아웃바운드 포트 443이 EE Server/VE Server와 통신할 수 있는지 확인하십시오. 어떠한 이유로든 포트 443이 차단된 경우 권한 부여 기능이 작동하지 않습니다. 하위 설치 프로그램을 사용하여 설치하는 경우 DDD는 사용되지 않습니다.
- 최신 문서 자료와 기술 권고사항에 대해서는 www.dell.com/support를 정기적으로 확인하시기 바랍니다.

모든 클라이언트 - 필수 구성 요소

- 마스터 설치 프로그램 및 하위 설치 클라이언트(Microsoft .Net Framework 4.5 Client Profile만 필요로 하는 Cloud Edition 하위 설치 프로그램은 제외)에 대해서는 Microsoft .Net Framework 4.0(또는 그 이상)의 전체 버전이 필요합니다. 설치 프로그램은 Microsoft .Net Framework 구성 요소를 설치하지 않습니다.

Dell에서 배송된 모든 컴퓨터에는 전체 버전의 Microsoft .Net Framework 4.5이 미리 설치되어 있습니다. 하지만 Dell 하드웨어에 설치하지 않거나 이전 Dell 하드웨어에서 Security Tools를 업그레이드하는 경우에는, Security Tools를 설치하기 전에 어떤 버전의 Microsoft .Net이 설치되어 있는지 확인한 후 필요에 따라 버전을 업데이트해야만 설치/업그레이드에 따른 문제를 방지할 수 있습니다. 설치되어 있는 Microsoft .Net의 버전을 확인하려면 설치하고자 하는 컴퓨터에서 다음 지침을 따르십시오: [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx) 전체 버전의 Microsoft .Net Framework 4.5를 설치하려면 <https://www.microsoft.com/en-us/download/details.aspx?id=30653>으로 이동하십시오.

- Dell ControlVault용 드라이버 및 펌웨어, 지문 판독기 및 스마트 카드는(아래 참조) 마스터 설치 프로그램 또는 하위 설치 프로그램 실행 파일에 포함되어 있지 않습니다. 드라이버 및 펌웨어는 최신 상태로 유지해야 하며, <http://www.dell.com/support>에서 컴퓨터 모델을 선택하여 다운로드하십시오. 인증 하드웨어에 따라 적절한 드라이버 및 펌웨어를 다운로드하십시오.

- Dell ControlVault
- NEXT 생체 인식 지문 드라이버
- 유효 지문 판독기 495 드라이버
- O2Micro 스마트 카드 드라이버

Dell 이외의 하드웨어에 설치하는 경우 해당 벤더의 웹 사이트에서 업데이트된 드라이버 및 펌웨어를 다운로드하십시오. Dell ControlVault 드라이버 설치 지침은 [Dell ControlVault 드라이버 및 펌웨어 업데이트](#)에 제시되어 있습니다.

모든 클라이언트 - 하드웨어

- 다음 표에 지원되는 컴퓨터 하드웨어가 나와 있습니다.



- 최소 하드웨어 요구 사항은 운영 체제의 최소 사양을 충족시켜야 합니다.

모든 클라이언트 - 언어 지원

- Encryption, Cloud Edition 및 BitLocker Manager 클라이언트는 MUI(다국어 사용자 인터페이스)와 호환되며 다음 언어를 지원합니다.

언어 지원

- EN - 영어
- ES - 스페인어
- FR - 프랑스어
- IT - 이탈리아어
- DE - 독일어
- JA - 일본어
- KO - 한국어
- PT-BR - 포르투갈어, 브라질
- PT-PT - 포르투갈어, 포르투갈(이베리아)

- SED 및 Advanced Authentication 클라이언트는 MUI(다국어 사용자 인터페이스)와 호환되며 다음 언어를 지원합니다. UEFI 모드와 Preboot Authentication은 러시아어, 중국어(번체) 또는 중국어(간체)로 지원되지 않습니다.

언어 지원

- EN - 영어
- FR - 프랑스어
- IT - 이탈리아어
- DE - 독일어
- ES - 스페인어
- JA - 일본어
- KO - 한국어
- ZH-CN - 중국어(간체)
- ZH-TW - 중국어(번체)/대만
- PT-BR - 포르투갈어, 브라질
- PT-PT - 포르투갈어, 포르투갈(이베리아)
- RU - 러시아어

Encryption 클라이언트

- 클라이언트 컴퓨터가 네트워크에 연결되어 있어야 활성화할 수 있습니다.
- 초기 암호화 시간을 줄려면 Windows 디스크 정리 마법사를 실행하여 임시 파일 및 기타 불필요한 데이터를 모두 제거합니다.
- 암호화 스윙이 처음 실행되는 동안, 사용자가 없는 시간에 컴퓨터가 절전 모드로 전환되지 않도록 절전 모드를 해제하십시오. 절전 상태의 컴퓨터에서는 암호화 및 암호 해독이 발생되지 않습니다.
- 이중 부팅 구성은 다른 운영 체제의 시스템 파일을 암호화하여 작업을 방해할 수 있으므로 Encryption 클라이언트는 이중 부팅 구성을 지원하지 않습니다.
- v8.0 이전 구성 요소는 마스터 설치 프로그램으로 업그레이드할 수 없습니다. 마스터 설치 프로그램에서 하위 설치 프로그램을 추출하고 구성 요소를 개별적으로 업그레이드합니다. 추출 지침을 보려면 **마스터 설치 프로그램에서 하위 설치 프로그램 추출**을 참조하십시오.
- 이제 Encryption 클라이언트가 Audit 모드를 지원합니다. Audit 모드를 사용하면 관리자는 타사 SCCM 또는 유사 솔루션을 사용하여 Encryption 클라이언트를 배포하는 대신, 암호화 기업 이미지의 일부로서 Encryption 클라이언트를 배포할 수 있습니다. 기본적으로 이미지가 완전히 배포된 후에는 활성화가 진행되지 않습니다.
- Encryption 클라이언트는 McAfee, Symantec 클라이언트, Kaspersky, MalwareBytes에 맞게 테스트를 거쳤으며 호환 가능합니다. 이러한 바이러스 백신 공급자를 위한 하드 코딩된 제외가 제공되므로 바이러스 백신 스캔과 암호화 간의 불일치를 방지할 수 있습니다. 또한 Encryption 클라이언트는 Microsoft Enhanced Mitigation Experience Toolkit에 맞게 테스트를 거쳤습니다.



여기에 나열되지 않은 바이러스 백신 공급자를 조직에서 사용하고 있는 경우 [KB article SLN298707](#)이나 [Dell ProSupport](#)에 연락을 참조하여 도움을 받으십시오.

- TPM은 GPK 키 봉인에 사용됩니다. 따라서 Encryption 클라이언트를 실행하는 경우, 클라이언트 컴퓨터에 새 운영 체제를 설치하기 전에 BIOS에서 TPM을 삭제하십시오.
- Encryption 클라이언트가 설치된 상태에서는 내부 운영 체제 업그레이드가 지원되지 않습니다. Encryption 클라이언트를 설치 제거 및 암호 해독하고, 새 운영 체제로 업그레이드한 후, Encryption 클라이언트를 다시 설치합니다.

추가적으로 운영 체제 재설치는 지원되지 않습니다. 운영 체제를 재설치하려는 경우 대상 컴퓨터를 백업하고, 컴퓨터를 초기화하고, 운영 체제를 설치한 뒤 다음의 설정된 복구 절차에 따라 암호화된 데이터를 복구합니다.

Encryption 클라이언트 필수 구성 요소

- 마스터 설치 프로그램에서 Microsoft Visual C++ 2012 업데이트 4를 설치합니다(컴퓨터에 이미 설치되어 있지 않은 경우). **하위 설치 프로그램을 사용할 때는** Encryption 클라이언트를 설치하기 전에 이 구성 요소를 설치해야 합니다.

필수 구성 요소

- Visual C++ 2012 업데이트 4 이상의 재배포 가능 패키지(x86 및 x64)

Encryption 클라이언트 하드웨어

- 다음 표에 지원되는 하드웨어가 나와 있습니다.

내장 하드웨어(선택 사항)

- TPM 1.2 또는 2.0

Encryption 클라이언트 운영 체제

- 다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제(32 및 64비트)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7, 응용 프로그램 호환성 템플릿 포함(하드웨어 암호화는 지원되지 않음)
- Windows 8: Enterprise, Pro
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (하드웨어 암호화는 지원되지 않음)
- Windows 10: Education, Enterprise, Pro
- VMware Workstation 5.5 이상

① **노트:** UEFI 모드는 **Windows 7, Windows Embedded Standard 7 또는 Windows Embedded 8.1 Industry Enterprise**에서 지원되지 않습니다.

EMS(External Media Shield) 운영 체제

- 다음 표에는 EMS로 보호되는 미디어에 대한 액세스가 지원되는 운영 체제가 자세히 나와 있습니다.

① **노트:** EMS를 호스팅하려면 외장형 미디어에 약 **55MB**의 사용 가능한 공간과 암호화할 파일 중 최대 크기의 파일에 해당하는 여유 공간이 있어야 합니다.



① **노트:**

Windows XP는 EMS Explorer를 사용할 때만 지원됩니다.

EMS로 보호받는 미디어(32 및 64비트)에 대한 액세스가 지원되는 Windows 운영 체제

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

EMS로 보호되는 미디어에 대한 액세스가 지원되는 Mac 운영 체제(64비트 커널)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.0

Server Encryption 클라이언트

Server Encryption은 서버 모드로 실행되는 컴퓨터에 사용됩니다(특히 파일 서버).

- Server Encryption은 Dell Data Protection | Enterprise Edition 및 Dell Data Protection | Endpoint Security Suite Enterprise와만 호환됩니다.
- Server Encryption은 다음을 제공합니다.
 - 소프트웨어 암호화
 - 이동식 저장소 암호화
 - 포트 제어

① **노트:**

서버에서 포트 제어를 지원해야 합니다.

서버 포트 제어 시스템 정책은 보호되는 서버의 이동식 미디어에 영향을 줍니다(예: USB 장치별로 서버의 USB 포트의 액세스 및 사용 제어). USB 포트 정책은 외장형 USB 포트에 적용됩니다. 내장형 USB 포트 기능은 USB 포트 정책의 영향을 받지 않습니다. USB 포트 정책이 비활성화되어 있으면 클라이언트 USB 키보드 및 마우스가 작동되지 않으며, 이 정책이 적용되기 전에 Remote Desktop Connection이 설정된 경우가 아니라면 사용자가 컴퓨터를 사용할 수 없게 됩니다.

Server Encryption은 다음에서 사용됩니다.

- 로컬 드라이브를 사용하는 파일 서버
- 서버 운영 체제 또는 비서버 운영 체제를 단순 파일 서버로 실행하는 가상 머신(VM) 게스트
- 지원되는 구성:
 - RAID 5 또는 10 드라이브가 장착된 서버, RAID 0(스트라이핑) 및 RAID 1(미러링)은 서로 독립적으로 지원됩니다.
 - 멀티 테라바이트(TB) RAID 드라이브가 장착된 서버
 - 컴퓨터를 종료하지 않고도 변경할 수 있는 드라이브가 장착된 서버
 - Server Encryption은 테스트를 거쳤으며 McAfee VirusScan, Symantec 클라이언트, Kaspersky Anti-Virus 및 MalwareBytes Anti-Malware와 호환됩니다. 바이러스 백신 스캐닝과 암호화 간의 불일치를 방지하기 위해 바이러스 백신 공급자를 위해 하드 코딩된 제외가 제공됩니다. 여기에 나열되지 않은 바이러스 백신 공급자를 조직에서 사용하고 있는 경우 KB 문서 [SLN298707](#)을 참조하거나 [Dell ProSupport](#)에 연락하여 도움을 받으십시오.

지원 안 됨

Server Encryption은 다음에서 사용하지 않습니다.

- Dell Data Protection Server 또는 Dell Data Protection Server용 데이터베이스를 실행 중인 서버



- Server Encryption은 Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Personal Edition 또는 Dell Data Protection | Security Tools와 호환되지 않습니다.
- Server Encryption은 SED Management 또는 BitLocker Manager 클라이언트에서 지원되지 않습니다.
- Server Encryption으로 들어가거나 나가는 마이그레이션은 지원되지 않습니다. Dell Data Protection | External Media Edition에서 Server Encryption으로 업그레이드하려면 Server Encryption을 설치하기 전에 이전 제품 또는 제품을 완전히 설치 제거해야 합니다.
- VM 호스트(일반적으로 VM 호스트 하나에 여러 개의 VM 게스트가 있음)
- 도메인 컨트롤러
- Exchange Server
- 데이터베이스를 호스팅하는 서버(SQL, Sybase, SharePoint, Oracle, MySQL, Exchange 등)
- 다음 기술 중 하나를 사용하는 서버:
 - 복원 파일 시스템
 - 유동 파일 시스템
 - Microsoft 스토리지 공간
 - SAN/NAS 네트워크 스토리지 솔루션
 - iSCSI 연결 장치
 - 중복 제거 소프트웨어
 - 하드웨어 중복 제거
 - 분할 RAID(단일 RAID에 있는 여러 볼륨)
 - SED 드라이브(RAID 및 비-RAID)
 - 키오스크용 자동 로그인(Windows OS 7, 8/8.1)
 - Microsoft Storage Server 2012
- 이중 부팅 구성은 다른 운영 체제의 시스템 파일을 암호화하여 작업을 방해할 수 있으므로 Server Encryption은 이중 부팅 구성을 지원하지 않습니다.
- 내부 운영 체제 업그레이드는 Server Encryption에서 지원되지 않습니다. 운영 체제를 업그레이드하려면 Server Encryption을 설치 제거 및 해독하고 새 운영 체제로 업그레이드한 뒤 Server Encryption을 다시 설치하십시오.

또한 운영 체제 재설치는 지원되지 않습니다. 운영 체제를 재설치하고 싶은 경우 대상 컴퓨터를 백업하고, 컴퓨터를 초기화하고, 운영 체제를 설치한 뒤 다음 복구 절차에 따라 암호화된 데이터를 복구합니다. 암호화된 데이터 복구에 대한 자세한 내용은 복구 안내서를 참조하십시오.

Server Encryption 클라이언트 필수 구성 요소

- Server Encryption 클라이언트를 설치하기 전에 이 구성 요소를 설치해야 합니다.

필수 구성 요소

- Visual C++ 2012 업데이트 4 이상의 재배포 가능 패키지(x86 및 x64)

Server Encryption 클라이언트 하드웨어

최소 하드웨어 요구 사항은 운영 체제의 최소 사양을 충족시켜야 합니다.

Server Encryption 클라이언트 운영 체제

다음 표에 지원되는 운영 체제가 나와 있습니다.

운영 체제(32 및 64비트)

- Windows 7 SP0-SP1: Home, Enterprise, Professional, Ultimate



운영 체제(32 및 64비트)

- Windows 8.0: Enterprise, Pro
- Windows 8.1 - Windows 8.1 업데이트 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

지원되는 서버 운영 체제

- Windows Server 2008 SP2: Standard Edition, Hyper-V 포함 또는 불포함 Datacenter Edition, Hyper-V 포함 또는 불포함 Enterprise Edition, Foundation Server Edition
- Windows Server 2008 R2 SP1: Standard Edition, Hyper-V 포함 또는 불포함 Datacenter Edition, Hyper-V 포함 또는 불포함 Enterprise Edition, Foundation Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition

UEFI 모드가 지원되는 운영 체제

- Windows 8: Enterprise, Pro
- Windows 8.1 - Windows 8.1 업데이트 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

① **노트:** 지원되는 UEFI 컴퓨터의 기본 메뉴에서 재시작을 선택하면 컴퓨터가 다시 시작되고 두 가지 로그인 화면 중 하나가 표시됩니다. 표시되는 로그인 화면은 컴퓨터 플랫폼 아키텍처에 따라 다릅니다.

EMS(External Media Shield) 운영 체제

다음 표에는 EMS로 보호되는 미디어에 대한 액세스가 지원되는 운영 체제가 자세히 나와 있습니다.

① **노트:** EMS를 호스팅하려면 외장형 미디어에 약 55MB의 사용 가능한 공간과 암호화할 파일 중 최대 크기의 파일에 해당하는 여유 공간이 있어야 합니다.

① **노트:**

Windows XP는 EMS Explorer를 사용할 때만 지원됩니다.

EMS로 보호받는 미디어(32 및 64비트)에 대한 액세스가 지원되는 Windows 운영 체제

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

지원되는 서버 운영 체제

- Windows Server 2008 SP1 이상
- Windows Server 2012 R2

EMS로 보호되는 미디어에 대한 액세스가 지원되는 Mac 운영 체제(64비트 커널)

- OS X Mavericks 10.9.5
- OS X Yosemite 10.10.5
- OS X El Capitan 10.11.4 및 10.11.5

SED 클라이언트

- SED Management를 성공적으로 설치하려면 컴퓨터가 유선 네트워크에 연결되어 있어야 합니다.
- IPv6는 지원되지 않습니다.
- 정책을 적용한 다음 실행 준비를 마친 후에 컴퓨터를 종료하고 다시 시작할 준비를 하십시오.
- 자체 암호화 드라이브가 장착된 컴퓨터에는 HCA 카드를 사용할 수 없습니다. HCA의 프로비저닝을 방지하는 비호환성이 있습니다. Dell은 자체 암호화 드라이브가 설치되어 HCA 모듈까지 지원하는 컴퓨터는 판매하지 않습니다. 이 지원되지 않는 구성은 애프터마켓 구성입니다.
- 암호화 대상으로 지정된 컴퓨터에 자체 암호화 드라이브가 장착된 경우 Active Directory 옵션인 *다음 로그인할 때 반드시 암호 변경*이 비활성화되어 있는지 확인하십시오. Preboot Authentication이 이 Active Directory 옵션을 지원하지 않습니다.
- PBA가 활성화된 후에는 인증 방법을 변경하지 않을 것을 권장합니다. 인증 방법을 전환해야 할 경우
 - PBA에서 모든 사용자를 제거합니다.

또는

- PBA를 비활성화하고 인증 방법을 변경한 후 PBA를 다시 활성화합니다.

① 중요: RAID 및 SED 특성 상, SED 관리에서 RAID가 지원되지 않습니다. SED의 **RAID=On** 문제는 잠긴 SED에서 사용할 수 없는 높은 수준의 섹터에서 RAID 관련 데이터를 읽고 쓰려면 RAID에서 처음부터 디스크에 액세스할 수 있어야 하며 이 데이터를 읽기 위해 사용자가 로그인할 때까지 기다릴 수 없다는 것입니다. 이 문제를 해결하려면 BIOS에서 SATA 작동을 RAID=On에서 AHCI로 변경합니다. 운영 체제에 AHCI 컨트롤러 드라이브가 사전 설치되어 있지 않은 경우 RAID=On에서 AHCI로 전환할 때 파란색 화면이 표시됩니다.

- SED Management는 Server Encryption과 함께 사용할 경우에 지원되지 않습니다.

OPAL 드라이버

- 지원되는 OPAL 호환 SED에서는 <http://www.dell.com/support>에 있는 업데이트된 Intel Rapid Storage Technology 드라이버가 필요합니다.

SED 클라이언트 필수 구성 요소

- 마스터 설치 프로그램에서 Microsoft Visual C++ 2010 SP1 및 Microsoft Visual C++ 2012 업데이트 4를 설치합니다(컴퓨터에 이미 설치되어 있지 않은 경우). **하위 설치 프로그램을 사용할 때는** SED Management 설치에 앞서 이 구성 요소를 먼저 설치해야 합니다.

전제조건

- Visual C++ 2010 SP1 이상 재배포 가능 패키지(x86 및 x64)
- Visual C++ 2012 업데이트 4 이상의 재배포 가능 패키지(x86 및 x64)

OPAL 호환 SED

- SED Management와 함께 지원되는 Opal 호환 SED의 최신 목록은 다음 KB 문서(<http://www.dell.com/support/article/us/en/19/SLN296720>)를 참조하십시오.

SED 클라이언트 운영 체제

- 다음 표에 지원되는 운영 체제가 나와 있습니다.



Windows 운영 체제(32 및 64비트)

- Windows 7 SP0-SP1: Enterprise, Professional(UEFI를 제외한 레거시 부팅 모드에서 지원됨)

① | 노트: 레거시 부팅 모드는 **Windows 7**에서 지원됩니다. UEFI는 **Windows 7**에서 지원되지 않습니다.

- Windows 8: Enterprise, Pro,
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

국제 키보드

- 다음 표에는 Preboot Authentication과 함께 지원되는 국제 키보드가 나열되어 있습니다.

① | 노트: 이러한 키보드는 **UEFI**에서만 지원됩니다.

국제 키보드 지원 - UEFI

- DE-CH - 독일어(스위스)
- DE-FR - 프랑스어(스위스)

Advanced Authentication 클라이언트

- Advanced Authentication을 통해 Dell Data Protection | Security Tools를 사용하여 관리 및 등록하는 고급 인증 자격 증명을 사용하여 이 컴퓨터에 사용자가 안전하게 액세스할 수 있습니다. Security Tools는 Windows 암호, 지문, 스마트 카드를 포함한 Windows 로그인에 대한 인증 자격 증명의 기본 관리자가 됩니다. Microsoft 운영 체제를 사용하여 등록된 사진 암호, PIN, 지문 자격 증명은 Windows 로그인 시 인식되지 않습니다.

계속해서 Microsoft 운영 체제를 사용하여 사용자의 자격 증명을 관리하려면 Security Tools를 설치하거나 설치 제거하지 마십시오.

- OTP(일회용 암호) 기능을 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. OTP는 TPM 2.0에서 지원되지 않습니다. TPM의 소유권을 제거한 후 설정하려면 <https://technet.microsoft.com>을 참조하십시오.
- SED는 Advanced Authentication이나 암호화를 제공하기 위해 TPM이 필요하지 않습니다.

Advanced Authentication 클라이언트 하드웨어

- 다음 표에는 지원되는 인증 하드웨어가 자세히 설명되어 있습니다.

지문 및 스마트 카드 판독기

- 보안 모드의 Validity VFS495
- Dell ControlVault 스와이프 리더
- UPEK TCS1 FIPS 201 보안 리더 1.6.3.379
- Authentec Eikon 및 Eikon To Go USB 리더

비접촉식 카드

- 지정된 Dell 랩톱에 탑재된 비접촉식 카드 리더기를 이용한 비접촉식 카드

스마트 카드

- [ActivIdentity](#) 클라이언트를 사용하는 PKCS #11 스마트 카드

스마트 카드

노트: ActivIdentity 클라이언트는 사전 로드되어 있지 않으며 별도로 설치해야 합니다.

- CSP 카드
- CAC(Common Access Cards)
- 클래스 B/SIPR Net 카드

다음은 SIPR Net 카드가 지원되는 Dell 컴퓨터 모델을 보여주는 표입니다.

Dell 컴퓨터 모델 - 클래스 B/SIPR Net 카드 지원

- | | | |
|------------------|-------------------|------------------------------|
| · Latitude E6440 | · Precision M2800 | · Latitude 14 Rugged Extreme |
| · Latitude E6540 | · Precision M4800 | · Latitude 12 Rugged Extreme |
| | · Precision M6800 | · Latitude 14 Rugged |

다음은 UEFI가 지원되는 Dell 컴퓨터 모델을 나타낸 표입니다.

Dell 컴퓨터 모델 - UEFI 지원

- | | | | |
|--------------------------------------|-------------------|--|------------------------------|
| · Latitude 7370 | · Precision M3510 | · Optiplex 3040 Micro, Mini Tower, Small Form Factor | · Venue Pro 11(모델 5175/5179) |
| · Latitude E5270 | · Precision M4800 | · Optiplex 3046 | · Venue Pro 11 (모델 7139) |
| · Latitude E5470 | · Precision M5510 | · Optiplex 5040 Mini Tower, Small Form Factor | |
| · Latitude E5570 | · Precision M6800 | · OptiPlex 7020 | |
| · Latitude E7240 | · Precision M7510 | · Optiplex 7040 Micro, Mini Tower, Small Form Factor | |
| · Latitude E7250 | · Precision M7710 | · Optiplex 3240 All-In-One | |
| · Latitude E7270 | · Precision T3420 | · Optiplex 7440 All-In-One | |
| · Latitude E7275 | · Precision T3620 | · OptiPlex 9020 Micro | |
| · Latitude E7350 | · Precision T7810 | | |
| · Latitude E7440 | | | |
| · Latitude E7450 | | | |
| · Latitude E7470 | | | |
| · Latitude 12 Rugged Extreme | | | |
| · Latitude 12 Rugged Tablet(모델 7202) | | | |
| · Latitude 14 Rugged Extreme | | | |
| · Latitude 14 Rugged | | | |

노트: 적격된 **OPAL 호환 SED**와 함께 **Windows 8, Windows 8.1** 및 **Windows 10**을 실행하는 이들 컴퓨터에서 인증 기능들은 **UEFI** 모드를 통해 지원됩니다. 그 밖에 **Windows 7, Windows 8, Windows 8.1, Windows 10**을 실행하는 컴퓨터에서는 레거시 부팅 모드를 지원합니다.

Advanced Authentication 클라이언트 운영 체제

Windows 운영 체제

다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제(32 및 64비트)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

노트: UEFI 모드는 **Windows 7**에서 지원되지 않습니다.



모바일 장치 운영 체제

- 다음 모바일 운영 체제들은 Security Tools 일회용 암호 기능을 지원합니다.

Android 운영 체제

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

iOS 운영 체제

- iOS 7.x
- iOS 8.x

Windows Phone 운영 체제

- Windows Phone 8.1
- Windows 10 Mobile

BitLocker Manager 클라이언트

- 해당 환경에 BitLocker가 배포되어 있지 않으면 [Microsoft BitLocker 요구 사항](#)을 검토하시기 바랍니다.
- PBA 파티션이 설정되었는지 확인하십시오. PBA 파티션이 설정되기 전에 BitLocker Manager를 설치한 경우 BitLocker를 사용할 수 없으며 BitLocker Manager가 작동하지 않습니다. [BitLocker PBA 파티션 설정을 위한 사전 설치 구성](#)을 참조하십시오.
- 키보드, 마우스, 비디오 구성 요소를 컴퓨터에 직접 연결해야 합니다. KVM 스위치는 컴퓨터가 하드웨어를 올바르게 식별하는 데 방해될 수 있으므로 KVM 스위치를 사용하여 주변 장치를 관리하지 마십시오.
- TPM을 켜고 활성화합니다. BitLocker Manager에서 TPM을 소유하며 재부팅은 필요하지 않습니다. 단, TPM 소유권이 이미 있는 경우 BitLocker Manager에서 암호화 설정 프로세스를 시작합니다(재시작이 필요하지 않음). 중요한 점은 TPM을 "소유" 및 활성화해야 한다는 것입니다.
- 해당 장치에서 GPO 보안 설정인 "시스템 암호기법: 암호화, 해싱 및 서명을 위한 FIPS 호환 알고리즘 사용"에 대해 FIPS 모드가 활성화되어 있으며 당사의 제품을 통해 해당 장치를 관리할 경우, BitLocker Manager 클라이언트는 승인된 AES FIPS 유효성 검사 알고리즘을 사용합니다. Microsoft가 응용 프로그램 호환성, 복구 및 미디어 암호화로 인해 고객에게 FIPS 유효성 검사 암호화를 사용하지 않도록 권하기 때문에 우리는 이 모드를 BitLocker 암호화 클라이언트에 대한 기본 설정으로 강제 실행하지는 않습니다. <http://blogs.technet.com>을 참조하십시오.
- BitLocker Manager는 Server Encryption과 함께 사용할 경우에 지원되지 않습니다.

BitLocker Manager 클라이언트 필수 구성 요소

- 마스터 설치 프로그램에서 Microsoft Visual C++ 2010 SP1 및 Microsoft Visual C++ 2012 업데이트 4를 설치합니다(컴퓨터에 이미 설치되어 있지 않은 경우). **하위 설치 프로그램을 사용할 때는** BitLocker Manager를 설치하기 전에 이 구성 요소를 설치해야 합니다.

전제조건

- Visual C++ 2010 SP1 이상 재배포 가능 패키지(x86 및 x64)
- Visual C++ 2012 업데이트 4 이상의 재배포 가능 패키지(x86 및 x64)

BitLocker Manager 클라이언트 운영 체제

- 다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제

- Windows 7 SP0-SP1: Enterprise, Ultimate(32비트 및 64비트)
- Windows 8: Enterprise(64비트)
- Windows 8.1: Enterprise Edition, Pro Edition(64비트)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition(64비트)

Cloud Edition 클라이언트

- Cloud Edition은 Microsoft Office 365에서 지원되지 않습니다.
- 컴퓨터에 할당 가능한 디스크 드라이브 하나(문자 값)가 있어야 합니다.
- 대상 장치가 <https://yoursecurityservername.domain.com:8443/cloudweb/register> 및 <https://yoursecurityservername.domain.com:8443/cloudweb>에 연결되어 있는지 확인하십시오.
- Cloud Edition을 배포하기 전에 대상 장치에 클라우드 스토리지 계정이 아직 설정되지 않은 상태가 가장 좋습니다.

해당 기존 계정을 유지하기로 결정할 경우, 사용자는 경우,은 암호화되지 않은 상태로 유지하려면 이는 모든 파일이 동기화 클라이언트에서 빼냅니다 클라우드 Edition을 설치하기 전에 이동하도록 합니다.

- 클라이언트가 설치된 후 사용자는 컴퓨터를 다시 시작할 준비를 해야 합니다.
- Cloud Edition은 동기화 클라이언트의 동작을 방해하지 않습니다. 그러므로 관리자 및 최종 사용자는 Cloud Edition을 배포하기 전에 이러한 응용 프로그램의 작동 방식을 잘 알아야 합니다. 자세한 내용은 <http://technet.microsoft.com/en-us/library/cc> 상자 지원 참조 <https://support.box.com/home>, dropbox 지원 <https://www.dropbox.com/help>, 또는 onedrive <http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>를 동시에 지원.
- IPv6는 지원되지 않습니다.

Cloud Edition 클라이언트 23

- 마스터 설치 프로그램 및되지 않을 경우 Visual C++ 2010 SP1가 이미 컴퓨터에 설치되어 있는 Microsoft 프로파일 Microsoft .net Framework 4.0 클라이언트를 설치합니다. 하위 설치 프로그램을 사용할 때는 Cloud Edition을 설치하기 전에 이 구성 요소를 설치해야 합니다.

전제조건

- .Net Framework 4.0 Client Profile
- Visual C++ 2010 SP1 재배포 가능 패키지(x86 및 x64)

클라우드 동기화 클라이언트

- 다음은 Cloud Edition에 지원되는 클라우드 동기화 클라이언트를 보여주는 표입니다. 동기화 클라이언트 공급자는 업데이트를 자주 릴리스하므로, 새 동기화 클라이언트 버전을 프로덕션 환경에 도입하기 전에 Cloud Edition에서 테스트할 것을 권장합니다.

클라우드 동기화 클라이언트

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business



① **노트:**

Dropbox for Business를 사용하려면 Dropbox v2.8 이상과 VE Server v8.4 이상 또는 EE Server v8.5 이상이 필요합니다.

v8.4 이전 버전의 VE Server 또는 v8.5 이전 버전의 EE Server를 사용하는 Dropbox for Business의 경우 클라이언트가 모든 파일과 폴더를 보호합니다. VE v8.4 이상 또는 EE Server v8.5 이상을 사용할 경우 사용자가 개인 Dropbox 계정에 파일을 업로드할 수 있습니다. 정책에 따라 해당 파일은 보호되지 않은 상태로 유지됩니다.

Google Drive 또는 OneDrive for Business와 함께 Cloud Edition을 사용하려면 EE Server/VE Server v9.1 이상이 필요합니다.

웹 브라우저

- 지원되는 브라우저에는 Internet Explorer, Mozilla Firefox, Google Chrome이 있습니다. Cloud Edition은 Microsoft Edge 브라우저를 지원하지 않습니다.

클라이언트 운영 체제를 클라우드 Edition

- 다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제(32비트 및 64비트)

- Windows 7 SP0-SP1
- Windows 8
- Windows 8.1
- Windows 10

Android 운영 체제

- 4.0 Ice Cream Sandwich
- 4.1 - 4.3 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

iOS 운영 체제

- iOS 7.x
- iOS 8.x
- iOS 9.x

인증 옵션

- 다음 인증 옵션은 특정 하드웨어를 필요로 합니다. 지문, 스마트 카드, 비접촉식 카드, 클래스 B/SIPR 넷 카드 및 UEFI 컴퓨터에서 인증 Windows 인증을 사용하는 스마트 카드, PBA(부팅 전 인증)를 사용하는 스마트 카드 및 일회용 암호옵션에는 구성이 필요합니다. 다음 표는 하드웨어 및 구성 요구 사항이 충족될 때 사용 가능한 인증 옵션을 운영 체제별로 보여줍니다.

Encryption 클라이언트

비 UEFI

	PBA					Windows 인증				
	암호	지문	접촉식 스마트 카드	OTP	SIPR 카드	암호	지문	스마트 카드	OTP	SIPR 카드
Windows 7 SP0-SP1						X	X ²	X ²	X ¹	X ²
Windows 8						X	X ²	X ²	X ¹	X ²
Windows 8.1 업데이트 0-1						X	X ²	X ²	X ¹	X ²
Windows 10						X	X ²	X ²	X ¹	X ²

1. 마스터 설치 프로그램 또는 Advanced Authentication 패키지(하위 설치 프로그램을 사용하는 경우)와 함께 설치하는 경우 사용할 수 있습니다.

2. support.dell.com에서 인증 드라이브를 다운로드할 때 사용할 수 있습니다.

UEFI

	PBA - 지원되는 Dell 컴퓨터에서					Windows 인증				
	암호	지문	접촉식 스마트 카드	OTP	SIPR 카드	암호	지문	스마트 카드	OTP	SIPR 카드
Windows 7 SP0-SP1										
Windows 8						X	X ²	X ²	X ¹	X ²
Windows 8.1 업데이트 0-1						X	X ²	X ²	X ¹	X ²
Windows 10						X	X ²	X ²	X ¹	X ²

1. 마스터 설치 프로그램 또는 Advanced Authentication 패키지(하위 설치 프로그램을 사용하는 경우)와 함께 설치하는 경우 사용할 수 있습니다.

2. support.dell.com에서 인증 드라이브를 다운로드할 때 사용할 수 있습니다.

SED 클라이언트

비 UEFI

	PBA					Windows 인증				
	암호	지문	접촉식 스마트 카드	OTP	SIPR 카드	암호	지문	스마트 카드	OTP	SIPR 카드
Windows 7 SP0-SP1	X ²		X ^{2 3}		X ^{2 3}	X	X ³	X ³	X ¹	X ³
Windows 8	X ²		X ^{2 3}		X ^{2 3}	X	X ³	X ³	X ¹	X ³



비 UEFI

	PBA					Windows 인증				
	암호	지문	접촉식 스마트 카드	OTP	SIPR 카드	암호	지문	스마트 카드	OTP	SIPR 카드
Windows 8.1	X ²		X ^{2,3}		X ^{2,3}	X	X ³	X ³	X ¹	X ³
Windows 10	X ²		X ^{2,3}			X	X ³	X ³	X ¹	X ³

1. 마스터 설치 프로그램 또는 Advanced Authentication 패키지(하위 설치 프로그램을 사용하는 경우)와 함께 설치하는 경우 사용할 수 있습니다.

2. support.dell.com에서 인증 드라이브를 다운로드할 때 사용할 수 있습니다.

3. 지원되는 OPAL SED에서 사용할 수 있습니다.

UEFI

	PBA - 지원되는 Dell 컴퓨터에서					Windows 인증				
	암호	지문	접촉식 스마트 카드	OTP	SIPR 카드	암호	지문	스마트 카드	OTP	SIPR 카드
Windows 7										
Windows 8	X ⁴					X	X ²	X ²	X ¹	X ²
Windows 8.1	X ⁴					X	X ²	X ²	X ¹	X ²
Windows 10	X ⁴					X	X ²	X ²	X ¹	X ²

1. 마스터 설치 프로그램 또는 Advanced Authentication 패키지(하위 설치 프로그램을 사용하는 경우)와 함께 설치하는 경우 사용할 수 있습니다.

2. support.dell.com에서 인증 드라이브를 다운로드할 때 사용할 수 있습니다.

4. 지원되는 UEFI 컴퓨터에서 지원되는 OPAL SED에 사용할 수 있습니다.

BitLocker Manager

비 UEFI

	PBA ⁵					Windows 인증				
	암호	지문	접촉식 스마트 카드	OTP	SIPR 카드	암호	지문	스마트 카드	OTP	SIPR 카드
Windows 7						X	X ²	X ²	X ¹	X ²
Windows 8						X	X ²	X ²	X ¹	X ²
Windows 8.1						X	X ²	X ²	X ¹	X ²
Windows 10						X	X ²	X ²	X ¹	X ²
Windows Server 2008 R2(64비트)						X		X ²		

1. 마스터 설치 프로그램 또는 Advanced Authentication 패키지(하위 설치 프로그램을 사용하는 경우)와 함께 설치하는 경우 사용할 수 있습니다.



비 UEFI

PBA ⁵					Windows 인증				
암호	지문	접촉식 스마트카드	OTP	SIPR 카드	암호	지문	스마트카드	OTP	SIPR 카드

2. support.dell.com에서 인증 드라이브를 다운로드할 때 사용할 수 있습니다.

5. BitLocker Preboot PIN은 Microsoft 기능을 통해 관리됩니다.

UEFI

PBA ⁵ - 지원되는 Dell 컴퓨터에서					Windows 인증				
암호	지문	접촉식 스마트카드	OTP	SIPR 카드	암호	지문	스마트카드	OTP	SIPR 카드

Windows 7

Windows 8 X X² X² X¹ X²

Windows 8.1 X X² X² X¹ X²

Windows 10 X X² X² X¹ X²

Windows Server 2008 R2(64비트) X X²

1. 마스터 설치 프로그램 또는 Advanced Authentication 패키지(하위 설치 프로그램을 사용하는 경우)와 함께 설치하는 경우 사용할 수 있습니다.

2. support.dell.com에서 인증 드라이브를 다운로드할 때 사용할 수 있습니다.

5. BitLocker Preboot PIN은 Microsoft 기능을 통해 관리됩니다.



레지스트리 설정

- 이 섹션에서는 레지스트리 설정 이유와 관계 없이 로컬 **클라이언트** 컴퓨터에 대해 Dell ProSupport에서 승인한 모든 레지스트리 설정에 대해 자세히 설명합니다. 레지스트리 설정에 두 제품이 겹치면 각 범주에 해당 설정이 나열됩니다.
- 이러한 레지스트리 변경 작업은 관리자만 수행할 수 있으며 일부 시나리오에서는 적절하지 않거나 작업하지 못할 수도 있습니다.

Encryption 클라이언트 레지스트리 설정

- EE Server/VE Server에서 Windows용 EE에 자체 서명된 인증서를 사용하는 경우 클라이언트 컴퓨터에서 인증서 신뢰 유효성 검사는 비활성 상태로 유지해야 합니다(Windows용 EE에서 신뢰 유효성 검사는 기본적으로 *비활성화*됨). 클라이언트 컴퓨터에서 신뢰 유효성 검사를 *활성화*하기 전에 다음 조건을 충족시켜야 합니다.

- EnTrust 또는 Verisign 등 루트 인증 기관이 서명한 인증서를 EE Server/VE Server로 가져와야 합니다.
- 인증서의 전체 신뢰 체인은 클라이언트 컴퓨터의 KeyStore에 저장되어야 합니다.
- Windows용 EE에서 신뢰 유효성 검사를 *활성화*하려면 클라이언트 컴퓨터에서 다음 레지스트리 항목의 값을 0으로 변경하십시오.

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"IgnoreCertErrors"=dword:00000000

0 = 인증서 오류가 발생할 경우 실패

1= 오류 무시

- Windows 인증과 함께 스마트 카드를 사용하려면 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정해야 합니다.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

- Encryption Removal Agent 로그 파일을 만들려면 다음과 같이 암호 해독 대상 컴퓨터에서 레지스트리 항목을 만드십시오. ([선택 사항](#)) [Encryption Removal Agent 로그 파일 생성](#)을 참조하십시오.

[HKLM\Software\Credant\DecryptionAgent]

"LogVerbosity"=dword:2

0: 로깅하지 않음

1: 서비스가 실행되지 않는 오류 로깅

2: 전체 데이터 암호 해독이 안 되는 오류 로깅(권장 수준)

3: 모든 암호 해독 볼륨 및 파일에 대한 정보 로깅

5: 디버깅 정보 로깅

- 기본적으로, 설치 중에 시스템 트레이 아이콘이 표시됩니다. 최초 설치 후에 컴퓨터에서 모든 관리되는 사용자에게 대해 시스템 트레이 아이콘을 숨기려면 다음 레지스트리 설정을 사용하십시오. 다음의 레지스트리 설정을 생성하거나 수정합니다.

[HKLM\Software\CREDANT\CMGShield]

"HIDESYSTRAYICON"=dword:1

- 기본적으로, 설치 중에 c:\windows\temp 디렉터리의 모든 임시 파일이 자동으로 삭제됩니다. 임시 파일이 삭제되면 초기 암호화가 신속하게 진행되며 삭제 작업은 초기 암호화 스윙이 수행되기 전에 발생합니다.

하지만 조직에서 \temp 디렉터리 내에 파일 구조를 유지해야 하는 타사 응용 프로그램을 사용하는 경우에는 이러한 삭제를 방지해야 합니다.

임시 파일 삭제를 사용하지 않으려면 다음과 같이 레지스트리 설정을 만들거나 수정하십시오.

[HKLM\SOFTWARE\CREDANT\CMGShield]

"DeleteTempFiles"=REG_DWORD:0

임시 파일을 삭제하지 않으면 초기 암호화에 시간이 더 걸립니다.

- Encryption 클라이언트는 업데이트가 수행될 때마다 *각 정책 업데이트 시간 연기* 메시지를 5분 동안 표시합니다. 사용자가 메시지에 응답하지 않으면 다음 지연이 시작됩니다. 최종 연기 메시지에 카운트다운 및 진행률 표시줄이 포함되고, 사용자가 응답하거나 최종 연기가 만료되고 필요한 로그오프/재부팅이 수행될 때까지 해당 메시지가 표시됩니다.

사용자가 메시지에 응답하지 않으면 암호화가 처리되지 않도록 방지하기 위해 암호화를 시작하거나 지연하도록 사용자 메시지의 동작을 변경할 수 있습니다. 이렇게 하려면 레지스트리를 다음 값으로 설정하십시오.

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

0이 아닌 값을 사용하면 기본 동작이 다시 알림으로 변경됩니다. 사용자가 상호 작용하지 않으면 구성 가능한 허용 연기 횟수까지 암호화 처리가 연기됩니다. 마지막 연기 시간이 끝나면 암호화 처리가 시작됩니다.

다음과 같이 최대 연기 시간을 계산합니다(사용자가 5분 동안 표시되는 각 지연 메시지에 응답하지 않을 경우 최대 시간 동안 지연됨).

(허용되는 정책 업데이트 연기 횟수 × 각 정책 업데이트 연기 시간) + (5분 × [허용되는 정책 업데이트 연기 횟수 - 1])

- 정책을 업데이트를 강제 적용하기 위해 Encryption 클라이언트가 EE Server/VE Server를 폴링하도록 하려면 다음 레지스트리 설정을 사용하십시오. 다음의 레지스트리 설정을 생성하거나 수정합니다.

[HKLM\SOFTWARE\Credant\CMGShield\Notify]

"PingProxy"=DWORD value:1

작업이 완료되면 레지스트리 설정이 자동으로 사라집니다.

- Encryption 클라이언트가 최적화된 인벤토리를 EE Server/VE Server에 보내거나, 전체 인벤토리를 EE Server/VE Server에 보내거나, 활성화된 모든 사용자에 대한 전체 인벤토리를 EE Server/VE Server에 보내도록 허용하려면 다음 레지스트리 설정을 사용하십시오.

- 최적화된 인벤토리를 EE Server/VE Server에 보내는 경우:

다음의 레지스트리 설정을 생성하거나 수정합니다.

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"OnlySendInvChanges"=REG_DWORD:1

항목이 없으면 최적화된 인벤토리가 EE Server/VE Server에 전송됩니다.

- 전체 인벤토리를 EE Server/VE Server에 보내는 경우:

다음의 레지스트리 설정을 생성하거나 수정합니다.

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]



"OnlySendInvChanges"=REG_DWORD:0

항목이 없으면 최적화된 인벤토리가 EE Server/VE Server에 전송됩니다.

- 활성화된 모든 사용자에 대한 전체 인벤토리를 보내는 경우:

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"RefreshInventory"=REG_DWORD:1

이 항목은 처리되는 즉시 레지스트리에서 삭제됩니다. 이 값은 자격 증명 모음에 저장되므로 인벤토리 업로드가 발생하기 전에 컴퓨터가 재부팅되더라도 Encryption 클라이언트는 다음에 발생하는 인벤토리 업로드에서 이 요청을 적용합니다.

이 항목은 OnlySendInvChanges 레지스트리 값을 대체합니다.

- 슬롯된 활성화는 대규모 배포 중에 EE Server/VE Server에서 쉽게 로드되도록 설정된 기간 동안 클라이언트 활성화를 분산시킬 수 있는 기능입니다. 알고리즘 방식으로 형성된 시간 슬롯을 기준으로 활성화가 지연되므로 활성화 횟수가 원활하게 분산됩니다.

VPN을 통해 활성화해야 하는 사용자의 경우, VPN 클라이언트가 네트워크 연결을 설정할 수 있을 때까지 초기 활성화를 지연하기 위해 클라이언트에 슬롯된 활성화 구성이 필요할 수 있습니다.

① 중요: 슬롯된 활성화는 Dell ProSupport의 지시에 따라서만 구성해야 합니다. 시간 슬롯을 올바르게 구성하면 EE Server/VE Server에 대해 한 번에 많은 수의 클라이언트가 활성화를 시도하므로 심각한 성능 문제가 발생할 수 있습니다.

다음 레지스트리 항목을 사용할 때는 컴퓨터를 다시 시작하여 업데이트를 적용해야 합니다.

- [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\SlottedActivation]

슬롯된 활성화 사용 또는 사용 해제

사용 해제=0 (기본값)

사용=1

- [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat]

활성화 슬롯 간격이 발생하는 기간(초)입니다. 활성화 슬롯 간격이 발생하는 기간(초)을 재정의하려면 이 설정을 사용합니다. 7시간 동안 활성화 슬롯이 발생되도록 하려면 25200초로 설정할 수 있습니다. 기본 설정은 86400초이며 활성화 슬롯이 매일 반복됩니다.

- [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\SlotIntervals]

모든 활성화 시간 슬롯이 발생할 때 반복되는 간격입니다(ACTIVATION_SLOT_CALREPEAT). 하나의 간격만 허용됩니다. 이 설정은 0(<CalRepeat>)이어야 합니다. 0 이외의 값으로 설정하면 예기치 않은 결과가 발생할 수 있습니다. 기본 설정은 0,86400입니다. 7시간마다 반복되도록 하려면 0,25200으로 설정합니다. CALREPEAT는 사용자가 로그인할 때 활성화됩니다.

- [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\MissThreshold]

활성화가 슬롯된 사용자가 다음에 로그인할 때 컴퓨터가 활성화를 시도하기 전에 생략할 수 있는 활성화 슬롯 개수입니다. 이 시도에서 활성화에 실패하면 클라이언트는 슬롯된 활성화를 다시 시도합니다. 네트워크 장애로 인해 활성화에 실패하면 MISSTHRESHOLD의 값이 초과하지 않았더라도 네트워크가 다시 연결될 때 활성화가 시도됩니다. 활성화 시간 슬롯에 도달하기 전에 사용자가 로그아웃하면, 다음에 로그인할 때 새 슬롯이 지정됩니다.

- [HKCU/Software/CREDANT/ActivationSlot] (사용자 데이터별)

슬롯된 활성화 시도가 지연되는 시간으로서, 슬롯된 활성화가 사용되도록 설정된 후에 사용자가 처음으로 네트워크에 로그인할 때 설정됩니다. 활성화 슬롯은 활성화가 시도될 때마다 다시 계산됩니다.

- [HKCU/Software/CREDANT/SlotAttemptCount] (사용자 데이터별)

시간 슬롯에 도달하여 활성화를 시도했지만 실패할 경우 실패 또는 생략된 시도의 횟수입니다. 이 횟수가 ACTIVATION_SLOT_MISSTHRESHOLD의 값에 도달하면, 컴퓨터가 네트워크에 연결될 때 즉시 활성화가 시도됩니다.

- 클라이언트 컴퓨터의 관리되지 않는 사용자를 검색하려면 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정하십시오.

[HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]



"UnmanagedUserDetected"=DWORD value:1

이 컴퓨터에서 관리되지 않는 사용자를 검색하려면 값을 1로 설정합니다.

이 컴퓨터에서 관리되지 않는 사용자를 검색하지 않으려면 값을 0으로 설정합니다.

- 미디어가 암호화된 암호화 키를 생성한 EE Server/VE Server에 대한 액세스 권한이 있는 컴퓨터에 대해 External Media Edition으로 암호화된 외부 미디어에 대한 액세스를 제한할 수 있습니다.

다음 레지스트리를 설정하여 이 기능을 사용할 수 있습니다.

[HKLM\SYSTEM\CurrentControlSet\Services\EMS]

"EnterpriseUsage"=dword:0

해제(기본값)=0

엔터프라이즈로 파일 액세스 제한=1

외부 미디어의 파일이 암호화된 후 이 값을 변경한 경우 레지스트리 설정이 업데이트된 컴퓨터에 미디어가 연결되면 업데이트된 레지스트리 키 값을 기반으로 파일이 다시 암호화됩니다.

- 사용자가 비활성화되는 드문 경우에서 자동 재활성화를 사용하려면 다음 레지스트리 값을 클라이언트 컴퓨터에서 설정해야 합니다.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

"AutoReactivation"=dword:00000001

0=사용 안 함(기본값)

1=사용

- SDE(System Data Encryption)는 SDE 암호화 규칙에 대한 정책 값에 따라 적용됩니다. 추가 디렉터리는 SDE 암호 기능 활성화 정책이 선택되어 있는 경우 기본적으로 보호됩니다. 자세한 내용은 AdminHelp에서 "SDE 암호화 규칙"을 검색하십시오. Encryption 클라이언트가 활성화 SDE 정책이 포함된 정책 업데이트를 처리하면, SDE 키(장치 키)가 아닌 SDUser 키(사용자 키)로 현재 사용자 프로필 디렉터리가 기본적으로 암호화됩니다. SDE로 암호화되지 않은 사용자 디렉터리로 복사되는(이동 아님) 파일 또는 폴더를 암호화하는 데에도 이 SDUser 키가 사용됩니다.

SDUser 키를 비활성화하여 SDE 키를 사용해 이러한 사용자 디렉터리를 암호화하려면, 컴퓨터에서 다음 레지스트리 항목을 생성하십시오.

[HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

"EnableSDUserKeyUsage"=dword:00000000

이 레지스트리 키가 없거나 0 이외의 다른 값으로 설정되어 있으면, SDUser 키가 이러한 사용자 디렉터리를 암호화하는 데 사용됩니다.

- 비도메인 활성화 기능을 사용하려면 Dell ProSupport에 연락하여 요청하십시오.

SED 클라이언트 레지스트리 설정

- EE Server/VE Server가 SED 클라이언트와 통신할 수 없을 경우 재시도 간격을 설정하려면 다음 레지스트리 값을 추가합니다.

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

"CommErrorSleepSecs"=dword:300

이 값은 EE Server/VE Server가 SED 클라이언트와 통신할 수 없는 경우 SED 클라이언트가 서버에 연결하도록 시도할 때까지 대기하는 시간(초)입니다. 기본값은 300초(5분)입니다.



- EE Server/VE Server에서 SED Management에 자체 서명된 인증서를 사용하는 경우 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사는 비활성 상태로 유지해야 합니다(SED Management에서 SSL/TLS 신뢰 유효성 검사는 기본적으로 *비활성화됨*). 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사를 *활성화*하기 전에 다음 조건을 충족시켜야 합니다.
 - EnTrust 또는 Verisign 등 루트 인증 기관이 서명한 인증서를 EE Server/VE Server로 가져와야 합니다.
 - 인증서의 전체 신뢰 체인은 클라이언트 컴퓨터의 KeyStore에 저장되어야 합니다.
 - SED Management에서 SSL/TLS 신뢰 유효성 검사를 *활성화*하려면 클라이언트 컴퓨터에서 다음 레지스트리 항목의 값을 0으로 변경하십시오.


```
[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]
```

```
"DisableSSLCertTrust"=DWORD:0
```

0 = 활성화

1 = 비활성화
- Windows 인증과 함께 스마트 카드를 사용하려면 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정해야 합니다.


```
[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]
```

```
"MSSmartcardSupport"=dword:1
```
- PBA(부팅 전 인증)와 함께 스마트 카드를 사용하려면 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정해야 합니다. Remote Management Console에서 인증 방법 정책을 스마트 카드로 설정하고 변경을 커밋합니다.


```
[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]
```

```
"MSSmartcardSupport"=dword:1
```
- PBA가 활성화되어 있는지 확인하려면 다음 값이 설정되어 있어야 합니다.


```
[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]
```

```
"PBAIsActivated"=DWORD (32-bit):1
```

값이 1이면 PBA가 활성화되어 있는 것입니다. 값이 0이면 PBA가 비활성화되어 있는 것입니다.
- EE Server/VE Server가 SED 클라이언트와 통신할 수 없을 때 SED 클라이언트가 EE Server/VE Server에 연결을 시도하는 간격을 설정하려면 클라이언트 컴퓨터에 다음 값을 설정합니다.


```
[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]
```

```
"CommErrorSleepSecs"=DWORD Value:300
```

이 값은 EE Server/VE Server가 SED 클라이언트와 통신할 수 없는 경우 SED 클라이언트가 서버에 연결하도록 시도할 때까지 대기하는 시간(초)입니다. 기본값은 300초(5분)입니다.
- 필요에 따라 Security Server 호스트는 원래 설치 위치에서 변경될 수 있습니다. 호스트 정보는 정책 폴링이 발생할 때마다 클라이언트 컴퓨터에서 판독합니다. 클라이언트 컴퓨터에서 다음 레지스트리 값을 변경하십시오.


```
[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]
```

```
"ServerHost"=REG_SZ:<newname>.<organization>.com
```
- 필요에 따라 Security Server 포트는 원래 설치 위치에서 변경될 수 있습니다. 이 값은 정책 폴링이 발생할 때마다 클라이언트 컴퓨터에서 판독합니다. 클라이언트 컴퓨터에서 다음 레지스트리 값을 변경하십시오.


```
[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]
```

```
ServerPort=REG_SZ:8888
```
- 필요에 따라 Security Server URL은 원래 설치 위치에서 변경될 수 있습니다. 이 값은 정책 폴링이 발생할 때마다 클라이언트 컴퓨터에서 판독합니다. 클라이언트 컴퓨터에서 다음 레지스트리 값을 변경하십시오.



[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

"ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

Advanced Authentication 클라이언트 레지스트리 상태

- Advanced Authentication 클라이언트(Security Tools)가 스마트 카드 및 생체 인식 장치와 관련된 서비스의 시작 유형을 "자동"으로 변경하지 **않도록** 서비스 시작 기능을 비활성화할 수 있습니다. 이 기능을 비활성화하면 실행해야 하는 필요한 서비스와 관련된 경고도 표시되지 않습니다.

이 기능을 **비활성화**하면 Security Tools가 다음 서비스를 시작하지 않습니다.

- SCardSvr - 컴퓨터가 판독하는 스마트 카드에 대한 액세스를 관리합니다. 이 서비스가 중지되면 컴퓨터에서 스마트 카드를 판독할 수 없습니다. 이 서비스가 비활성화되면 서비스에 명시적으로 의존된 모든 서비스가 시작되지 않습니다.
- SCPolicSvc - 스마트 카드가 제거되면 사용자의 데스크톱이 잠기도록 시스템을 구성할 수 있습니다.
- WbioSvc - Windows 생체 인식 서비스를 통해 클라이언트 응용 프로그램은 생체 인식 하드웨어 또는 샘플에 직접 액세스하지 않고도 생체 인식 데이터를 캡처, 비교, 조종, 저장할 수 있습니다. 이 서비스는 권한이 부여된 SVCHOST 프로세스에서 호스팅됩니다.

기본적으로 레지스트리 키가 없거나 값이 0으로 설정되어 있는 경우 이 기능이 사용됩니다.

[HKLM\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

0 = 활성화

1 = 비활성화

- Windows 인증과 함께 스마트 카드를 사용하려면 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정해야 합니다.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

- SED PBA(부팅 전 인증)와 함께 스마트 카드를 사용하려면 SED가 장착된 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정해야 합니다.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

Remote Management Console에서 인증 방법 정책을 스마트 카드로 설정하고 변경을 커밋합니다.

BitLocker Manager 클라이언트 레지스트리 설정

- EE Server/VE Server에서 BitLocker Manager에 자체 서명된 인증서를 사용하는 경우 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사는 비활성 상태로 유지해야 합니다(BitLocker Manager에서 SSL/TLS 신뢰 유효성 검사는 기본적으로 *비활성화됨*). 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사를 *활성화*하기 전에 다음 조건을 충족시켜야 합니다.

- EnTrust 또는 Verisign 등 루트 인증 기관이 서명한 인증서를 EE Server/VE Server로 가져와야 합니다.
- 인증서의 전체 신뢰 체인은 클라이언트 컴퓨터의 KeyStore에 저장되어야 합니다.
- BitLocker Manager에서 SSL/TLS 신뢰 유효성 검사를 *활성화*하려면 클라이언트 컴퓨터에서 다음 레지스트리 항목의 값을 0으로 변경하십시오.

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

"DisableSSLCertTrust"=DWORD:0



0 = 활성화

1 = 비활성화

Cloud Edition 클라이언트 레지스트리 설정

- 로깅 수준을 높이면 문제 해결에 도움이 될 수 있습니다. 다음 레지스트리 설정을 생성하거나 수정합니다.

[HKLM\SOFTWARE\Dell\Dell Data Protection\Cloud Edition]

"LogVerbosity"=dword:0x1f (31)

기본적으로 로그인 수준은 0xf (15)로 설정되어 있습니다.

해제=0x0 (0)

위험=0x1 (1)

오류=0x3 (3)

경고=0x7 (7)

정보=0xf (15)

디버그=0x1f (31)



마스터 설치 프로그램을 사용하여 설치

- 명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.
 - 기본이 아닌 포트를 사용하여 설치하려면 마스터 설치 프로그램 대신 하위 설치 프로그램을 사용합니다.
 - 마스터 설치 프로그램 로그 파일은 **C:\ProgramData\Dell\Dell Data Protection\Installer**에 있습니다.
 - 응용 프로그램에 대한 도움이 필요한 사용자에게는 다음과 같은 문서 및 도움말 파일을 참조하도록 안내하십시오.
 - Encryption 클라이언트의 기능 사용 방법에 대해서는 *Dell 암호화 도움말*을 참조하십시오. <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help에 있는 도움말에 액세스하십시오.
 - External Media Shield의 기능 사용 방법에 대해서는 *EMS 도움말*을 참조하십시오. <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS에 있는 도움말에 액세스하십시오.
 - Advanced Authentication의 기능 사용 방법에 대해서는 *Security Tools 도움말*을 참조하십시오. <Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools\Help에서 도움말에 액세스하십시오.
 - Cloud Edition의 기능 사용 방법에 대해서는 *Cloud Edition 사용 설명서*를 참조하십시오. support.dell.com에서 문서를 가져오십시오.
 - 설치 후, 사용자가 시스템 트레이에서 Dell Data Protection 아이콘을 마우스 오른쪽 단추로 클릭하고 **정책 업데이트 확인**을 선택하여 정책을 업데이트해야 합니다.
 - 마스터 설치 프로그램은 전체 제품군을 설치합니다. 마스터 설치 프로그램을 사용하여 설치하는 방법은 두 가지입니다. 다음 중 하나를 선택하십시오.
 - [마스터 설치 프로그램을 사용하여 대화형으로 설치](#)
- 또는
- [마스터 설치 프로그램을 사용하여 명령줄을 통해 설치](#)

마스터 설치 프로그램을 사용하여 대화형으로 설치

- 마스터 설치 프로그램의 위치는 다음과 같습니다.
 - **support.dell.com** - 필요한 경우 support.dell.com에서 **소프트웨어를 다운로드**하고 **마스터 설치 프로그램**에서 **하위 설치 프로그램**을 추출합니다. 추출한 후에 다음 위치에서 해당 파일을 찾습니다.
 - **Dell FTP 계정** - DDP-Enterprise-Edition-8.x.x.xxx.zip에서 설치 번들을 찾습니다.
- 지침에 따라 마스터 설치 프로그램을 사용하여 Dell Data Protection | Endpoint Security Suite Enterprise을 대화형으로 설치합니다. 이 방법을 사용하면 제품군을 한 번에 한 대의 컴퓨터에 설치할 수 있습니다.
 - 1 Dell 설치 미디어에서 **DDPSetup.exe**를 찾습니다. 로컬 컴퓨터로 복사합니다.
 - 2 설치 프로그램을 실행하려면 **l**를 두 번 클릭합니다. 몇 분 정도 걸릴 수 있습니다.
 - 3 시작 대화 상자에서 **Next(다음)**를 클릭합니다.
 - 4 라이선스 계약서를 읽고 조건을 수락한 후 **Next(다음)**를 클릭합니다.
 - 5 **Enterprise Edition**을 선택하고 **Next(다음)**를 클릭합니다.
External Media Edition만 설치하려는 경우 External Media Edition만 확인란을 선택합니다
 - 6 **Dell Enterprise Server 이름** 필드에 대상 사용자를 관리할 EE Server/VE Server의 정규화된 호스트 이름(예: server.organization.com)을 입력합니다.
Dell Device Server URL 필드에 클라이언트가 통신할 Device Server(Security Server)의 URL을 입력합니다.
EE Server가 v7.7 이전 버전인 경우 형식은 <https://server.organization.com:8081/xapi>입니다.

EE Server가 v7.7 이상일 경우 형식은 <https://server.organization.com:8443/xapi/>(맨 끝의 슬래시 포함)입니다.

Next(다음)를 클릭합니다.

7 **Next(다음)**를 클릭하여 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 제품을 설치합니다. 다른 위치에 설치하면 문제가 발생할 수도 있으므로 **Dell recommends installing in the default location only.**

8 설치할 구성 요소를 선택합니다.

*Security Framework*는 근본적인 보안 구조와, 지문과 암호 등의 자격 증명 및 PBA 등을 비롯한 여러 가지 인증 방법을 관리하는 고급 인증 클라이언트인 *Security Tools*를 설치합니다.

*Drivers*에는 DDP 응용 프로그램에 필요한 드라이버가 포함되어 있습니다.

*Encryption*은 끝점이 네트워크에 연결, 네트워크에서 분리, 분실 또는 도난 여부에 따라 보안 정책을 시행하는 구성 요소인 *Encryption 클라이언트*를 설치합니다.

*Cloud Edition*은 Dropbox, Dropbox for Business, Box, OneDrive 등과 같은 공용 클라우드 서비스에 저장된 데이터를 보호하는 구성 요소인 *Cloud Edition*을 설치합니다. 데이터는 파일이 클라우드 내부 및 외부로 이동될 때 완벽하게 암호화됩니다.

*BitLocker Manager*는 BitLocker 암호화 정책을 중앙에서 관리하여 소유 비용을 간소화하고 절감함으로써 BitLocker 배포의 보안을 강화하도록 설계된 *BitLocker Manager 클라이언트*를 설치합니다.

선택이 완료되면 **Next(다음)**를 클릭합니다.

9 **Install(설치)**을 클릭하여 설치를 시작합니다. 설치에 몇 분 정도 걸릴 수 있습니다.

10 **예, 컴퓨터를 지금 다시 시작합니다**를 선택하고 **Finish(마침)**를 클릭합니다.
설치가 완료됩니다.

마스터 설치 프로그램을 사용하여 명령줄을 통해 설치

· 명령줄 설치에 스위치를 먼저 지정해야 합니다. 다른 매개 변수는 인수 안에 포함되어 /v 스위치로 전달됩니다.

스위치

· 다음 표에 마스터 설치 프로그램과 함께 사용할 수 있는 스위치에 대한 설명이 나와 있습니다.

스위치	설명
-y -gm2	마스터 설치 프로그램의 사전 추출. -y 및 -gm2 스위치는 함께 사용해야 합니다. 두 스위치를 각각 사용하지 마십시오.
/S	자동 설치
/z	변수를 DDPSetup.exe 내 .msi로 전달

매개 변수

· 다음 표에 마스터 설치 프로그램과 함께 사용할 수 있는 매개 변수에 대한 설명이 나와 있습니다.

매개 변수	설명
SUPPRESSREBOOT	설치가 완료된 후 자동 재부팅을 하지 않습니다. 자동 모드에서 사용할 수 있습니다.
서버	EE Server/VE Server의 URL을 지정합니다.
InstallPath	설치 경로를 지정합니다. 자동 모드에서 사용할 수 있습니다.
기능	자동 모드로 설치할 수 있는 구성 요소를 지정합니다. DE = Drive Encryption(Encryption 클라이언트)



매개변수	설명
	EME = External Media Edition만
	BLM = BitLocker Manager
	SED = 자체 암호화 드라이브 관리(EMAgent/Manager, PBA/GPE 드라이버)
	CE = Cloud Edition
BLM_ONLY=1	명령줄에서 FEATURES=BLM을 사용하여 SED Management 플러그인을 제외할 때 사용해야 합니다.

명령줄의 예

- 명령줄 매개 변수는 대/소문자를 구분합니다.
- 이 예에서는 마스터 설치 프로그램을 사용하여 표준 포트에서 모든 구성 요소를 설치합니다(자동 설치, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).


```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com\""
```
- 이 예에서는 마스터 설치 프로그램을 사용하여 표준 포트에서 SED Management 및 External Media Edition을 설치합니다(자동 설치, 재부팅 안 함, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).


```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=EME-SED, SUPPRESSREBOOT=1\""
```
- 이 예에서는 마스터 설치 프로그램을 사용하여 표준 포트에서 SED Management를 설치합니다(자동 설치, 재부팅 안 함, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).


```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=SED, SUPPRESSREBOOT=1\""
```
- 이 예에서는 마스터 설치 프로그램을 사용하여 표준 포트에서 SED Management를 설치합니다(자동 설치, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).


```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=SED\""
```
- 이 예에서는 마스터 설치 프로그램을 사용하여 표준 포트에서 Encryption 클라이언트 및 BitLocker Manager(SED Management 플러그인 사용하지 않음)를 설치합니다(자동 설치, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).


```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
```
- 이 예에서는 마스터 설치 프로그램을 사용하여 표준 포트에서 BitLocker Manager(SED Management 플러그인 사용) 및 External Media Edition을 설치합니다(자동 설치, 재부팅 안 함, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).


```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=BLM-EME, SUPPRESSREBOOT=1\""
```
- 이 예에서는 마스터 설치 프로그램을 사용하여 표준 포트에서 BitLocker Manager(SED Management 플러그인 사용하지 않음) 및 External Media Edition을 설치합니다(자동 설치, 재부팅 안 함, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).


```
"DDPSetup.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1, SUPPRESSREBOOT=1\""
```



마스터 설치 프로그램을 사용하여 설치 제거

- 각 구성 요소를 별도로 설치 제거한 후에 마스터 설치 프로그램을 설치 제거해야 합니다. 설치 제거 장애를 방지하려면 특정 순서대로 클라이언트를 설치 제거해야 합니다.
- 하위 설치 프로그램을 가져오려면 마스터 설치 프로그램에서 하위 설치 프로그램 추출의 지침을 따릅니다.
- 설치 작업과 설치 제거 작업에 동일한 버전의 마스터 설치 프로그램(및 해당 클라이언트)을 사용해야 합니다.
- 이 장에서는 하위 설치 프로그램 사용 방법에 대한 자세한 지침이 있는 다른 장에 대해 설명합니다. 이 장에서는 마지막 단계인 마스터 설치 프로그램 설치 제거에 대해서만 설명합니다.
- 클라이언트를 다음 순서로 설치 제거합니다.
 - a Encryption 클라이언트 설치 제거.
 - b SED 및 Advanced Authentication 클라이언트 설치 제거
 - c BitLocker Manager 클라이언트 설치 제거
 - d Cloud Edition 설치 제거
- 드라이버 패키지는 설치 제거할 필요가 없습니다.
- 마스터 설치 프로그램 설치 제거를 계속 진행합니다.

마스터 설치 프로그램 설치 제거

개별 클라이언트가 모두 제거되었으면 마스터 설치 프로그램을 설치 제거할 수 있습니다.

명령줄 설치 제거

- 다음 예에서는 마스터 설치 프로그램을 자동으로 설치 제거합니다.

```
"DDPSetup.exe" -y -gm2 /S /x
```

완료되면 컴퓨터를 다시 부팅합니다.

하위 설치 프로그램을 사용하여 설치

- 각 클라이언트 개별적으로 설치하려면 **마스터 설치 프로그램에서 하위 설치 프로그램 추출**에 나와 있는 대로 먼저 마스터 설치 프로그램에서 하위 실행 파일을 추출해야 합니다.
- 명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.
- 명령줄에서 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표로 묶어야 합니다.
- 이러한 설치 프로그램을 사용하여 스크립팅된 설치, 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 통해 클라이언트를 설치합니다.
- 명령줄 예에서는 재부팅을 수행하지 않았습니니다. 하지만 실제 상황에서는 재부팅이 필요합니다. 컴퓨터를 재부팅해야만 암호화가 시작됩니다.
- 로그 파일 - Windows는 로그인된 사용자에게 대해 고유한 하위 설치 프로그램 설치 로그 파일을 `C:\Users\\AppData\Local\Temp\`의 `%temp%`에 생성합니다.

설치 프로그램을 실행할 때 별도의 로그 파일을 추가하려는 경우, 하위 설치 프로그램이 첨부되지 않으므로 해당 로그 파일의 이름은 고유해야 합니다. 표준 .msi 명령을 통해 `/i*C:\<any directory>\<any log file name>.log`를 사용하여 로그 파일을 생성할 수 있습니다.

- 별도로 표시된 경우를 제외하고, 모든 하위 설치 프로그램은 명령줄 설치에 동일한 기본 .msi 스위치와 표시 옵션을 사용합니다. 스위치를 먼저 지정해야 합니다. /v 스위치가 필요하며 인수를 사용합니다. 다른 매개 변수는 인수 안에 포함되어 /v 스위치로 전달됩니다.

표시 옵션은 예상 동작을 수행하도록 /v 스위치에 전달된 인수 끝에 지정할 수 있습니다. 동일한 명령줄에 /q와 /qn을 동시에 사용하지 마십시오. /qb 이후에 ! 및 - 만 사용합니다.

스위치	의미
/v	변수를 *.exe 내의 .msi로 전달
/s	자동 모드
/i	설치 모드
옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	Cancel(취소) 버튼이 있는 진행률 대화 상자, 다시 시작할 것인지 묻습니다.
/qb-	Cancel(취소) 버튼이 있는 진행률 대화 상자, 프로세스 완료 후 자동으로 다시 시작합니다.
/qb!	Cancel(취소) 버튼이 없는 진행률 대화 상자, 다시 시작할 것인지 묻습니다.
/qb!-	Cancel(취소) 버튼이 없는 진행률 대화 상자, 프로세스 완료 후 자동으로 다시 시작합니다.
/qn	사용자 인터페이스 없음

- 응용 프로그램에 대한 도움이 필요한 사용자에게는 다음과 같은 문서 및 도움말 파일을 참조하도록 안내하십시오.
 - Encryption 클라이언트의 기능 사용 방법에 대해서는 *Dell 암호화 도움말*을 참조하십시오. `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`에 있는 도움말에 액세스하십시오.



- External Media Shield의 기능 사용 방법에 대해서는 *EMS 도움말*을 참조하십시오. <Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS에 있는 도움말에 액세스하십시오.
- Advanced Authentication의 기능 사용 방법에 대해서는 *Security Tools 도움말*을 참조하십시오. <Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help에서 도움말에 액세스하십시오.
- Cloud Edition의 기능 사용 방법에 대해서는 *Cloud Edition 사용 설명서*를 참조하십시오. support.dell.com에서 문서를 가져오십시오.

드라이버 클라이언트 설치

- Dell ControlVault용 드라이버 및 펌웨어, 지문 판독기 및 스마트 카드는 마스터 설치 프로그램 또는 하위 설치 프로그램 실행 파일에 포함되어 있지 않습니다. 드라이버 및 펌웨어는 최신 상태로 유지해야 하며 <http://www.dell.com/support>에서 해당 컴퓨터 모델을 선택하여 다운로드할 수 있습니다. 인증 하드웨어에 따라 적절한 드라이버 및 펌웨어를 다운로드하십시오.

- Dell ControlVault
- NEXT 생체 인식 지문 드라이버
- 유효 지문 판독기 495 드라이버
- O2Micro 스마트 카드 드라이버

Dell 이외의 하드웨어에 설치하는 경우 해당 벤더의 웹 사이트에서 업데이트된 드라이버 및 펌웨어를 다운로드하십시오.

- 설치 프로그램은 TPM의 TSS(신뢰할 수 있는 소프트웨어 스택), Microsoft 핫픽스용 드라이버를 설치합니다.
- 이러한 드라이버는 Encryption 클라이언트 설치 시 설치되어야 합니다.
- 드라이버 설치 프로그램의 위치는 다음과 같습니다.
 - support.dell.com** - 필요한 경우 support.dell.com에서 소프트웨어를 다운로드하고 마스터 설치 프로그램에서 하위 설치 프로그램을 추출합니다. 추출한 후에 **C:\extracted\Drivers**에서 해당 파일을 찾습니다.
 - Dell FTP 계정** - DDP-Enterprise-Edition-8.x.x.xxx.zip에서 설치 번들을 찾은 다음 마스터 설치 프로그램에서 하위 설치 프로그램을 추출합니다. 추출한 후에 **C:\extracted\Drivers**에서 해당 파일을 찾습니다.

명령줄 설치

- 다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다.

매개 변수

SUPPRESSREBOOT=1

INSTALLPATH=<설치 대상 변경>

ARPSYSTEMCOMPONENT=1 <제어판 프로그램 목록에 항목이 표시되지 않음>

명령줄에서 사용할 수 있는 기본 .msi 스위치 및 표시 옵션의 목록은 [하위 설치 프로그램을 사용하여 설치를 참조하십시오](#).

명령줄의 예

- 다음 예에서는 TPM의 TSS(신뢰할 수 있는 소프트웨어 스택), Microsoft 핫픽스용 드라이버를 지정된 위치에 설치하며, 제어판 프로그램 목록에 항목을 생성하지 않으며, 재부팅하지 않습니다.

```
setup.exe /S /z""InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
```

Encryption 클라이언트 설치

- Encryption 클라이언트를 설치하는 경우에는 드라이버가 필요합니다. 설치 지침을 보려면 [드라이버 클라이언트 설치](#)로 이동하십시오. 이러한 드라이버는 TPM의 TSS(신뢰할 수 있는 소프트웨어 스택), Microsoft 핫픽스용으로 사용됩니다. 이러한 드라이버는 Encryption 클라이언트 설치 시 설치되어야 합니다. 드라이버 설치를 마친 후에는 이 섹션으로 돌아오십시오.



- 조직에서 EnTrust 또는 Verisign 등과 같은 루트 인증 기관이 서명한 인증서를 사용하는 경우 [Encryption 클라이언트 요구 사항](#)을 검토하십시오. 인증서 유효성 검사를 사용하려면 클라이언트 컴퓨터에서 레지스트리 설정을 변경해야 합니다.
- 설치 후, 사용자가 시스템 트레이에서 Dell Data Protection 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **정책 업데이트 확인**을 선택하여 정책을 업데이트해야 합니다.
- Encryption 클라이언트 설치 프로그램의 위치는 다음과 같습니다.
 - **support.dell.com** - 필요한 경우 [support.dell.com](#)에서 [소프트웨어를 다운로드](#)하고 **마스터 설치 프로그램**에서 하위 설치 프로그램을 추출합니다. 추출한 후에 **C:\extracted\Encryption**에서 해당 파일을 찾습니다.
 - **Dell FTP 계정** - DDP-Enterprise-Edition-8.x.x.xxx.zip에서 설치 번들을 찾은 다음 **마스터 설치 프로그램**에서 하위 설치 프로그램을 추출합니다. 추출한 후에 **C:\extracted\Encryption**에서 해당 파일을 찾습니다.

명령줄 설치

- 다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다.

매개 변수

SERVERHOSTNAME=<ServerName>

POLICYPROXYHOSTNAME=<RGKName>

MANAGEDDOMAIN=<MyDomain>

DEVICESTRVERURL=<DeviceServerName/SecurityServerName>

GKPORT=<NewGKPort>

MACHINEID=<MachineName>

RECOVERYID=<RecoveryID>

REBOOT=ReallySuppress

HIDEOVERLAYICONS=1

HIDESYSTRAYICON=1

EME=1

명령줄에서 사용할 수 있는 기본 .msi 스위치 및 표시 옵션의 목록은 [하위 설치 프로그램을 사용하여 설치](#)를 참조하십시오.

명령줄의 예

- 다음 예에서는 기본 매개 변수로 클라이언트를 설치합니다(Encryption 클라이언트, 공유를 위한 암호화, 대화 상자 표시되지 않음, 진행률 표시줄 표시되지 않음, 자동 다시 시작, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESTRVERURL=https://
server.organization.com:8443/xapi /qn"
```

- v7.7 이전 버전의 EE Server일 경우 DEVICESTRVERURL=https://server.organization.com:**8081/xapi**(맨 끝의 슬래시 제외)를 바꿉니다.

- 다음 예에서는 Encryption 클라이언트 및 공유를 위한 암호화를 설치합니다(DDP 시스템 트레이 아이콘 숨김, 오버레이 아이콘 숨김, 대화 상자 표시하지 않음, 진행률 표시줄 표시하지 않음, 다시 시작하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESTRVERURL=https://
server.organization.com:8443/xapi/ HIDESYSTRAYICON=1 HIDEOVERLAYICONS=1
REBOOT=ReallySuppress /qn"
```



- v7.7 이전 버전의 EE Server일 경우 DEVICESTRURL=https://server.organization.com:8081/xapi(맨 끝의 슬래시 제외)를 바꿉니다.

EME(External Media Edition)만 설치하는 명령줄의 예

- 자동 설치, 진행률 표시줄 표시하지 않음, 자동 다시 시작, 기본 위치인 C:\Program Files\Dell\Dell Data Protection.에 설치합니다.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESTRURL=https://
server.organization.com:8443/xapi/ EME=1 /qn"
```

- v7.7 이전 버전의 EE Server일 경우 DEVICESTRURL=https://server.organization.com:8081/xapi(맨 끝의 슬래시 제외)를 바꿉니다.
- 자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치합니다.

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTRURL=https://server.organization.com:8443/
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

- v7.7 이전 버전의 EE Server일 경우 DEVICESTRURL=https://server.organization.com:8081/xapi(맨 끝의 슬래시 제외)를 바꿉니다.

① 노트:

클라이언트의 정보 상자에 소프트웨어 버전 번호 정보가 표시되지만 전체 클라이언트가 설치되었는지 또는 EME만 설치되었는지는 표시되지 않습니다. 이 정보를 찾으려면 C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log로 이동하여 다음 항목을 찾으십시오.

```
[<date/timestamp> DeviceInfo: <>] Shield Information - SM=External Media Only, SB=DELL, UNF=FQUN, last sweep={0, 0}
```

External Media Edition을 전체 버전의 Shield로 변환하는 명령줄의 예

- External Media Edition을 전체 버전의 Shield로 변환할 때 암호 해독은 필요하지 않습니다.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESTRURL=https://
server.organization.com:8443/xapi/ REINSTALL=ALL EME=0 REINSTALLMODE=vemus /qn"
```

- v7.7 이전 버전의 EE Server일 경우 DEVICESTRURL=https://server.organization.com:8081/xapi(맨 끝의 슬래시 제외)를 바꿉니다.

Server Encryption 클라이언트 설치

Server Encryption을 설치하는 방법에는 두 가지가 있습니다. 다음 중 한 가지 방법을 선택하십시오.

- Server Encryption 대화형 설치

① **노트:** Server Encryption은 서버 운영 체제를 실행 중인 컴퓨터에만 대화형으로 설치할 수 있습니다. 비서버 운영 체제에서 실행되는 컴퓨터에 설치하는 경우에는 SERVERMODE=1 매개 변수를 지정해 명령줄을 통해 수행해야 합니다.

- 명령줄을 사용하여 Server Encryption 설치

가상 사용자 계정

- 설치 중에 Server Encryption 전용으로 가상 서버 사용자 계정이 생성됩니다. 암호 및 DPAPI 인증은 사용되지 않으므로 가상 서버 사용자만 컴퓨터의 암호화 키에 액세스할 수 있습니다.

시작하기 전에

- 설치를 수행하는 사용자 계정은 관리자 수준의 권한이 있는 로컬 또는 도메인 사용자여야 합니다.
- 도메인 관리자가 Server Encryption을 활성화하거나 비도메인 또는 다중 도메인 서버에 Server Encryption을 실행해야 하는 요구 사항을 재정의하려면 application.properties 파일에서 ssos.domainadmin.verify 속성을 false로 설정하십시오. 파일은 사용 중인 DDP Server에 따라 다음 파일 경로에 저장됩니다.

Dell Enterprise Server - <설치 폴더>/Security Server/conf/application.properties



- 서버에서 포트 제어를 지원해야 합니다.

서버 포트 제어 시스템 정책은 보호되는 서버의 이동식 미디어에 영향을 줍니다(예: USB 장치별로 서버의 USB 포트의 액세스 및 사용 제어). USB 포트 정책은 외장형 USB 포트에 적용됩니다. 내장형 USB 포트 기능은 USB 포트 정책의 영향을 받지 않습니다. USB 포트 정책이 비활성화되어 있으면 클라이언트 USB 키보드 및 마우스가 작동되지 않으며, 이 정책이 적용되기 전에 Remote Desktop Connection이 설정된 경우가 아니라면 사용자가 컴퓨터를 사용할 수 없게 됩니다.

- Server Encryption을 성공적으로 활성화하려면 컴퓨터가 네트워크에 연결되어 있어야 합니다.
- TPM(Trusted Platform Module)을 사용할 수 있는 경우 Dell 하드웨어의 GPK 봉인에 사용됩니다. TPM을 사용할 수 없는 경우에는 Server Encryption이 Microsoft의 DPAPI(Data Protection API)를 사용하여 범용 키를 보호합니다.

① 노트: Server Encryption을 실행 중인 TPM이 있는 Dell 컴퓨터에 새 운영 체제를 설치하는 경우 BIOS에서 TPM을 지우십시오. 지침은 https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2를 참조하십시오.

하위 설치 프로그램 추출

- Server Encryption에는 마스터 설치 프로그램에 있는 설치 프로그램 중 하나만 필요합니다. Server Encryption을 설치하려면 먼저 마스터 설치 프로그램에서 Encryption 클라이언트의 하위 설치 프로그램, **DDPE_xxbit_setup.exe**를 추출해야 합니다. **마스터 설치 프로그램에서 하위 설치 프로그램 추출**을 참조합니다.

Server Encryption 대화형 설치

- 다음 지침에 따라 Server Encryption을 대화형으로 설치하십시오. 이 설치 프로그램에는 소프트웨어 암호화에 필요한 구성 요소가 포함되어 있습니다.

- 1 C:\extracted\Encryption 폴더에서 **DDPE_XXbit_setup.exe**를 찾습니다. 로컬 컴퓨터로 복사합니다.
- 2 서버에 Server Encryption을 설치하는 경우 **DDPE_XXbit_setup.exe** 파일을 두 번 클릭하여 설치 프로그램을 시작합니다.
 - ① 노트:** 서버 운영 체제(예: Windows Server 2012 R2)가 실행 중인 컴퓨터에 Server Encryption이 설치되면 설치 프로그램이 기본적으로 서버 모드로 암호화를 설치합니다.
- 3 시작 대화상자에서 **Next(다음)**를 클릭합니다.
- 4 라이선스 계약서 화면에서 라이선스 계약서를 읽고 조건을 수락한 후 **Next(다음)**를 클릭합니다.
- 5 **Next(다음)**를 클릭하여 기본 위치에 Server Encryption을 설치합니다.
 - ① 노트:** 기본 위치에 설치하는 것이 좋습니다. 다른 디렉터리, D 드라이브 또는 USB 드라이브 등과 같이 기본 위치가 아닌 위치에 설치하는 것은 권장되지 않습니다.
- 6 **Next(다음)**를 클릭하여 **Management Type(관리 유형)** 대화 상자를 건너뛵니다.
- 7 Dell Enterprise Server Name(Dell Enterprise Server 이름) 필드에 대상 사용자를 관리할 Dell Enterprise Server 또는 Virtual Edition의 정규화된 호스트 이름(예: server.organization.com)을 입력합니다.
- 8 **Managed Domain(관리되는 도메인)** 필드에 도메인 이름을 입력하고(예: 조직) **Next(다음)**를 클릭합니다.
- 9 **Next(다음)**를 클릭하여 자동으로 채워진 **Dell Policy Proxy Information(Dell 정책 프록시 정보)** 대화 상자를 건너뛵니다.
- 10 **Next(다음)**를 클릭하여 자동으로 채워진 **Dell Device Server Information(Dell 장치 서버 정보)** 대화 상자를 건너뛵니다.
- 11 **Install(설치)**를 클릭하여 설치를 시작합니다.

설치는 몇 분 정도 걸릴 수 있습니다.
- 12 **Configuration Completed(구성 완료)** 대화상자에서 Finish(마침)를 클릭합니다.

설치가 완료됩니다.

 - ① 노트:** 설치를 위한 로그 파일은 C:\Users\\AppData\Local\Temp에 있는 계정의 %temp% 디렉터리에 있습니다. 설치 프로그램의 로그 파일을 찾으려면 MSI로 시작하고 .log 확장자로 끝나는 파일 이름을 찾아보십시오. 이 파일에는 설치 프로그램을 실행한 시간과 일치하는 날짜/시간 스탬프가 있어야 합니다.
 - ① 노트:** 설치 중에 Server Encryption 전용으로 가상 서버 사용자 계정이 생성됩니다. 암호 및 DPAPI 인증은 사용되지 않으므로 가상 서버 사용자만 컴퓨터의 암호화 키에 액세스할 수 있습니다.
- 13 컴퓨터를 다시 시작합니다.



① **중요:** 작업을 저장하고 열려 있는 모든 응용 프로그램을 닫기 위해 시간이 필요한 경우에만 재부팅 다시 알림을 선택합니다.

명령줄을 사용하여 Server Encryption 설치

Server Encryption 클라이언트 - C:\extracted\Encryption에서 설치 프로그램 찾기

- **DDPE_xxbit_setup.exe**를 사용하여 스크립팅된 설치, 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 통해 설치 또는 업그레이드합니다.

스위치

다음 표에 설치 시 사용할 수 있는 스위치 정보가 나와 있습니다.

스위치	의미
/v	변수를 DDPE_XXbit_setup.exe 안의 .msi로 전달합니다.
/a	관리 설치
/s	자동 모드

매개 변수

다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다.

Component(구성 요소)	로그 파일	명령줄 매개 변수
모두	/i*v [fullpath][filename].log *	SERVERHOSTNAME=<관리 서버 이름> SERVERMODE=1 POLICYPROXYHOSTNAME=<RGK 이름> MANAGEDDOMAIN=<내 도메인> DEVICESERVERURL=<Activation Server 이름> GKPORT=<새 GK 포트> MACHINEID=<컴퓨터 이름> RECOVERYID=<복구 ID> REBOOT=ReallySuppress HIDEOVERLAYICONS=1 HIDESYSTRAYICON=1 EME=1

① **노트:** 여기에서는 재부팅을 하지 않지만 실제로는 재부팅이 필요합니다. 컴퓨터를 재부팅해야만 암호화가 시작됩니다.

옵션

다음 표에는 /v 스위치에 전달하는 인수 끝에 지정할 수 있는 표시 옵션이 나와 있습니다.



옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	Cancel(취소) 단추가 있는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb-	Cancel(취소) 단추가 있는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qb!	Cancel(취소) 단추가 없는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb!-	Cancel(취소) 단추가 없는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qn	사용자 인터페이스 없음

❗ | 노트: 동일한 명령줄에 /q와 /qn을 동시에 사용하지 마십시오. /qb 이후에 ! 및 - 만 사용합니다.

- 명령줄 매개 변수인 SERVERMODE=1은 새 설치 중에만 처리되며 설치 제거 시에는 무시됩니다.
- 다른 디렉터리, C: 외에 다른 드라이브나 USB 드라이브 등과 같이 기본 위치가 아닌 위치에 설치하는 것은 권장되지 않으며 기본 위치에 설치하는 것이 좋습니다.
- 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표 안에 포함합니다.
- Dell Activation Server URL(DEVICESERVERURL)은 대/소문자를 구분합니다.

명령줄 설치 예

- 다음 예에서는 기본 매개 변수로 Server Encryption 클라이언트를 설치합니다(Server Encryption 클라이언트, 공유를 위한 암호화, 대화상자 없음, 진행률 표시줄 없음, 자동 재시작, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/qn"
```

- 다음 예에서는 로그 파일 및 기본 매개 변수로 Server Encryption 클라이언트를 설치하고(Server Encryption 클라이언트, 자동 설치, Encrypt for Sharing, 대화 상자 없음, 진행률 표시줄 없음, 다시 시작하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection\Encryption에 설치), 숫자로 끝나는 사용자 지정 로그 파일 이름(DDP_ssos-090.log)을 지정합니다. 이 숫자는 명령줄이 같은 서버에서 두 번 이상 실행될 경우 증가되어야 합니다.

```
DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/ /1*v DDP_ssos-090.log /norestart/qn"
```

실행 파일이 있는 기본 위치와 다른 로그 위치를 지정하려면 명령에 전체 경로를 입력합니다. 예를 들어 /1*v C:\Logs \DDP_ssos-090.log를 입력하면 C:\Logs 폴더에 설치 로그가 생성됩니다.

컴퓨터 다시 시작

설치 후에 컴퓨터를 다시 시작하십시오. 가능하면 빨리 컴퓨터를 다시 시작해야 합니다.

❗ | 중요: 작업을 저장하고 열려 있는 모든 응용 프로그램을 닫기 위해 시간이 필요한 경우에만 재부팅 다시 알림을 선택합니다.

Server Encryption 활성화

- 서버가 조직의 네트워크에 연결되어 있어야 합니다.
- 서버의 컴퓨터 이름이 Remote Management Console에 표시할 끝점 이름인지 확인합니다.
- 도메인 관리자 자격 증명이 있는 라이브 대화형 사용자는 초기 활성화를 위해 서버에 한 번 이상 로그인해야 합니다. 로그인된 사용자가 서버에서 도메인 또는 비도메인, 원격 데스크톱 연결 또는 대화형 사용자 유형 중 하나가 될 수 있지만 활성화를 위해서는 도메인 관리자 자격 증명이 필요합니다.




- 설치 후에 다시 시작하면 Activation(활성화) 대화 상자가 표시됩니다. 관리자는 UPN(사용자 이름) 형식의 사용자 이름과 함께 도메인 관리자 자격 증명을 입력해야 합니다. Server Encryption 클라이언트는 자동으로 활성화되지 않습니다.
- 초기 활성화 중에는 가상 서버 사용자 계정이 생성됩니다. 초기 활성화 이후에 장치 활성화가 시작할 수 있도록 컴퓨터가 다시 시작됩니다.
- 활성화 및 장치 활성화 단계 중에 컴퓨터에 고유한 컴퓨터 ID가 할당되고 암호화 키가 생성되어 번들로 묶이며 암호화 키 번들과 가상 서버 사용자 간에 관계가 설정됩니다. 암호화 키 번들은 암호화 키와 정책을 새로운 가상 서버 사용자와 연결하여 암호화된 데이터, 특정 컴퓨터, 가상 서버 사용자 간에 안정적인 관계를 만듭니다. 장치 활성화 후에는 가상 서버 사용자가 Remote Management Console에 SERVER-USER@<정규화된 서버 이름>으로 나타납니다. 활성화에 대한 자세한 내용은 [서버 운영 체제의 활성화](#)를 참조하십시오.

① 노트:

활성화 후에 서버의 이름을 변경하면 Remote Management Console에서 표시 이름이 변경되지 않습니다. 그러나 서버 이름이 변경된 후에 Server Encryption 클라이언트가 다시 활성화되면 Remote Management Console에 새 서버 이름이 나타납니다.

다시 시작할 때마다 Activation(활성화) 대화상자에 Server Encryption을 활성화하라는 메시지가 사용자에게 표시됩니다. 활성화가 완료되지 않은 경우에는 다음 단계를 따르십시오.

- 1 서버에서나 Remote Desktop Connection을 통해 서버에 로그인합니다.
- 2 시스템 트레이에서 Encryption 아이콘 을 마우스 오른쪽 단추로 클릭하고 **About(정보)**을 클릭합니다.
- 3 서버 모드에서 Encryption이 실행되고 있는지 확인합니다.
- 4 메뉴에서 **Activate Dell Data Protection | Encryption(Dell Data Protection | Encryption 활성화)**을 선택합니다.
- 5 UPN 형식으로 도메인 관리자의 사용자 이름과 암호를 입력하고 **Activate(활성화)**를 클릭합니다. 표시되는 대화상자는 활성화되지 않은 시스템이 다시 시작될 때마다 나타나는 "활성화" 대화상자와 동일합니다.

DDP Server가 컴퓨터 ID용 암호화 키를 발급하고, 가상 서버 사용자 계정을 만들고, 사용자 계정용 암호화 키를 만들고, 암호화 키를 번들로 묶고, 암호화 번들과 가상 서버 사용자 계정 간에 관계를 만듭니다.

- 6 **Close(닫기)**를 클릭합니다.

활성화 후 암호화가 시작됩니다.

- 7 암호화 스윙이 완료되면 컴퓨터를 다시 시작해 이전에 사용 중이던 파일을 처리합니다. 이는 보안을 위한 중요한 단계입니다.

① 노트: 보안 *Windows* 자격 증명 정책이 "참"으로 설정되면 Server Encryption이 Windows 자격 증명을 비롯하여 `\Windows\system32\config` 파일을 암호화합니다. `\Windows\system32\config`의 파일은 *SDE Encryption Enabled* 정책이 **Not Selected**(선택되지 않음)로 설정된 경우에도 암호화됩니다. 기본적으로 *Secure Windows Credentials* 정책은 **Selected**(선택됨)입니다.

① 노트:

컴퓨터를 다시 시작한 후에 일반 키 자료를 인증하려면 보호되는 서버의 컴퓨터 키가 항상 필요합니다. DDP Server가 잠금 해제된 키를 반환하여 자격 증명 모음에 있는 암호화 키 및 정책에 액세스합니다. (해당 키와 정책은 사용자용이 아닌 서버용입니다.) 서버의 컴퓨터 키가 없으면 일반 파일 암호화 키를 잠금 해제할 수 없으며 컴퓨터가 정책 업데이트를 수신할 수 없습니다.

활성화 확인

로컬 콘솔에서 **About(정보)** 대화상자를 열어 Server Encryption이 설치되고, 인증되었으며, 서버 모드임을 확인합니다. Shield ID가 **빨간색**이면 암호화가 아직 활성화되지 않은 것입니다.

가상 서버 사용자

- Remote Management Console에서, 보호되는 서버는 해당 컴퓨터 이름 아래에서 볼 수 있습니다. 또한 보호되는 서버마다 고유한 가상 서버 사용자 계정이 있습니다. 각 계정에는 고유한 고정 사용자 이름과 고유한 컴퓨터 이름이 있습니다.
- 가상 서버 사용자 계정은 Server Encryption에서만 사용되며, 그렇지 않으면 보호되는 서버 작업에 투명하게 사용됩니다. 가상 서버 사용자는 암호화 키 번들 및 정책 프록시와 연결되어 있습니다.



- 활성화 이후에 가상 서버 사용자 계정은 활성화되고 서버와 연결된 사용자 계정입니다.
- 가상 서버 사용자 계정이 활성화되면 모든 로그인/로그오프 알림이 무시됩니다. 대신 시작되는 동안 컴퓨터가 가상 서버 사용자를 통해 인증한 후 Dell Data Protection Server에서 컴퓨터 키를 다운로드합니다.

SED Management 및 Advanced Authentication 클라이언트 설치

- v8.x의 Advanced Authentication에는 SED 클라이언트가 필요합니다.
- 조직에서 EnTrust 또는 Verisign 등과 같은 루트 인증 기관이 서명한 인증서를 사용하는 경우 **SED 클라이언트 요구 사항**을 검토하십시오. SSL/TLS 신뢰 유효성 검사를 사용하려면 클라이언트 컴퓨터에서 레지스트리 설정을 변경해야 합니다.
- 사용자가 Windows 인증서를 사용하여 PBA에 로그인합니다.
- SED 및 Advanced Authentication 클라이언트 설치 프로그램의 위치는 다음과 같습니다.
 - **support.dell.com** - 필요한 경우 **support.dell.com**에서 **소프트웨어를 다운로드**하고 **마스터 설치 프로그램에서 하위 설치 프로그램을 추출**합니다. 추출한 후에 **C:\extracted\Security Tools** 및 **C:\extracted\Security Tools\Authentication**에서 해당 파일을 찾습니다.
 - **Dell FTP 계정** - DDP-Enterprise-Edition-8.x.x.xxx.zip에서 설치 번들을 찾은 다음 **마스터 설치 프로그램에서 하위 설치 프로그램을 추출**합니다. 추출한 후에 **C:\extracted\Security Tools** 및 **C:\extracted\Security Tools\Authentication**에서 해당 파일을 찾습니다.

명령줄 설치

- 다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다.

매개 변수

CM_EDITION=1 <원격 관리>

INSTALLDIR=<설치 대상 변경>

SERVERHOST=<securityserver.organization.com>

SERVERPORT=8888

SECURITYSERVERHOST=<securityserver.organization.com>

SECURITYSERVERPORT=8443

ARPSYSTEMCOMPONENT=1 <제어판 프로그램 목록에 항목이 표시되지 않음>

명령줄에서 사용할 수 있는 기본 .msi 스위치 및 표시 옵션의 목록은 **하위 설치 프로그램을 사용하여 설치**를 참조하십시오.

명령줄의 예

\Security Tools

- 다음 예에서는 원격으로 관리되는 SED를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

다음 작업:

\Security Tools\Authentication

- 다음 예에서는 Advanced Authentication을 설치합니다(자동 설치, 재부팅하지 않음).



```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

Cloud Edition 설치

- **Cloud Edition을 설치하기 전에** EE Server/VE Server에서 몇 가지 작업을 수행해야 합니다. **Cloud Edition을 위한 서버 구성**을 참조하십시오.
- 조직에서 Dropbox for Business를 사용하는 경우 **Dropbox for Business에서 Cloud Edition 사용**을 참조하십시오.
- Cloud Edition 사용자가 다음 작업을 수행해야만 클라우드 동기화 클라이언트에서 파일 및 폴더가 보호됩니다. 클라우드 클라이언트를 설치한 후에는 사용자가 다음을 수행해야 합니다.
 - Cloud Edition을 활성화합니다.
 - 클라우드 스토리지 서비스를 다운로드합니다.
 - 관리자는 조직에서 선호하는 클라우드 동기화 공급자를 지정해야 합니다.
 - 또는
 - 조직에서 Dropbox for Business 또는 OneDrive for Business 공급자 중 하나를 사용하는 경우에는 이를 다운로드하여 설치할 수 있는 링크를 제공합니다. Dropbox for Business 사용자는 Cloud Edition을 통해 Dropbox for Business에 연결해야 합니다.
- *Cloud Edition 사용 설명서*에서 활성화 및 기타 Cloud Edition 사용자 작업에 대한 정보를 볼 수 있습니다.
- Cloud Edition 클라이언트 설치 프로그램의 위치는 다음과 같습니다.
 - **support.dell.com** - 필요한 경우 **support.dell.com**에서 **소프트웨어를 다운로드**하고 **마스터 설치 프로그램에서 하위 설치 프로그램**을 추출합니다. 추출한 후에 **C:\extracted\Cloud**에서 해당 파일을 찾습니다.
 - **Dell FTP 계정** - DDP-Enterprise-Edition-8.x.x.xxx.zip에서 설치 번들을 찾은 다음 **마스터 설치 프로그램에서 하위 설치 프로그램**을 추출합니다. 추출한 후에 **C:\extracted\Cloud**에서 해당 파일을 찾습니다.

명령줄 설치

- 다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다.

매개변수

SERVER=<ServerName>

명령줄의 예

- 다음 예에서는 Cloud Edition을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /qn"
```

BitLocker Manager 클라이언트 설치

- 조직에서 EnTrust 또는 Verisign 등과 같은 루트 인증 기관이 서명한 인증서를 사용하는 경우 **BitLocker Manager 클라이언트 요구 사항**을 검토하십시오. SSL/TLS 신뢰 유효성 검사를 사용하려면 클라이언트 컴퓨터에서 레지스트리 설정을 변경해야 합니다.
- BitLocker Manager 클라이언트 설치 프로그램의 위치는 다음과 같습니다.
 - **support.dell.com** - 필요한 경우 **support.dell.com**에서 **소프트웨어를 다운로드**하고 **마스터 설치 프로그램에서 하위 설치 프로그램**을 추출합니다. 추출한 후에 **C:\extracted\Security Tools**에서 해당 파일을 찾습니다.
 - **Dell FTP 계정** - DDP-Enterprise-Edition-8.x.x.xxx.zip에서 설치 번들을 찾은 다음 **마스터 설치 프로그램에서 하위 설치 프로그램**을 추출합니다. 추출한 후에 **C:\extracted\Security Tools**에서 해당 파일을 찾습니다.



명령줄 설치

- 다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다.

매개 변수

CM_EDITION=1 <원격 관리>

INSTALLDIR=<설치 대상 변경>

SERVERHOST=<securityserver.organization.com>

SERVERPORT=8888

SECURITYSERVERHOST=<securityserver.organization.com>

SECURITYSERVERPORT=8443

FEATURE=BLM <BitLocker Manager만 설치>

FEATURE=BLM,SED <SED와 함께 BitLocker Manager 설치>

ARPSYSTEMCOMPONENT=1 <제어판 프로그램 목록에 항목이 표시되지 않음>

명령줄에서 사용할 수 있는 기본 .msi 스위치 및 표시 옵션의 목록은 [하위 설치 프로그램을 사용하여 설치](#)를 참조하십시오.

명령줄의 예

- 다음 예에서는 BitLocker Manager만 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

- 다음 예에서는 SED와 함께 BitLocker Manager를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM,SED /norestart /qn"
```



하위 설치 프로그램을 사용하여 설치 제거

- 각 클라이언트 개별적으로 설치하려면 **마스터 설치 프로그램**에서 **하위 설치 프로그램 추출**에 나와 있는 대로 먼저 마스터 설치 프로그램에서 하위 실행 파일을 추출해야 합니다.
- 설치 작업과 설치 제거 작업에 동일한 버전의 클라이언트를 사용해야 합니다.
- 명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.
- 명령줄에서 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표로 묶어야 합니다. 명령줄 매개 변수는 대/소문자를 구분합니다.
- 이러한 설치 프로그램을 사용하여 스크립팅된 설치, 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 통해 클라이언트를 설치 제거합니다.
- 로그 파일 - Windows는 로그인된 사용자에게 대해 고유한 하위 설치 프로그램 설치 로그 파일을 **C:\Users\\AppData\Local\Temp**의 %temp%에 생성합니다.

설치 프로그램을 실행할 때 별도의 로그 파일을 추가하려는 경우, 하위 설치 프로그램이 첨부되지 않으므로 해당 로그 파일의 이름은 고유해야 합니다. 표준 .msi 명령을 통해 **/C:\<any directory>\<any log file name>.log**를 사용하여 로그 파일을 생성할 수 있습니다. 명령줄 설치 제거에서는 사용자 이름/암호가 로그 파일에 기록되므로 **"/!*v"**(자세한 로깅)를 사용하지 않는 것이 좋습니다.

- 별도로 표시된 경우를 제외하고, 모든 하위 설치 프로그램은 명령줄 설치 제거에 동일한 기본 .msi 스위치와 표시 옵션을 사용합니다. 스위치를 먼저 지정해야 합니다. /v 스위치가 필요하며 인수를 사용합니다. 다른 매개 변수는 인수 안에 포함되어 /v 스위치로 전달됩니다.

표시 옵션은 예상 동작을 수행하도록 /v 스위치에 전달된 인수 끝에 지정할 수 있습니다. 동일한 명령줄에 /q와 /qn을 동시에 사용하지 마십시오. /qb 이후에 ! 및 - 만 사용합니다.

스위치	의미
/v	변수를 setup.exe 안의 .msi로 전달
/s	자동 모드
/x	설치 제거 모드
옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	Cancel(취소) 단추가 있는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb-	Cancel(취소) 단추가 있는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qb!	Cancel(취소) 단추가 없는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb!-	Cancel(취소) 단추가 없는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qn	사용자 인터페이스 없음

Encryption 및 Server Encryption 클라이언트 설치 제거

- 암호 해독 시간을 줄이려면 Windows 디스크 정리 마법사를 실행하여 임시 파일 및 기타 불필요한 데이터를 제거합니다.
- 가능하면 야간에 암호 해독을 실행할 수 있도록 계획하십시오.
- 사용자가 없는 시간에 컴퓨터가 절전 모드로 전환되지 않도록 절전 모드를 해제하십시오. 절전 중인 컴퓨터에서는 암호 해독이 실행되지 않습니다.
- 잠긴 파일로 인한 암호 해독 실패를 최소화하기 위해 모든 프로세스와 응용 프로그램을 종료합니다.
- 설치 제거가 완료되고 암호 해독이 진행 중이면 네트워크 연결을 모두 비활성화합니다. 그렇게 하지 않으면 새 정책이 적용되어 암호화가 다시 실행될 수 있습니다.
- 정책 업데이트 실행 등의 기존 데이터 암호 해독 프로세스를 따릅니다.
- Windows 및 EME Shield가 EE Server/VE Server를 업데이트하여 Shield 설치 제거 프로세스가 시작될 때 상태를 *보호되지 않음*으로 변경합니다. 단, 클라이언트에서 EE Server/VE Server에 연결할 수 없으면 이유와 상관없이 상태가 업데이트되지 않습니다. 이 경우 Remote Management Console에서 *끝점 제거*를 수동으로 수행해야 합니다. 조직에서 규정 준수를 위해 이 워크플로를 사용하는 경우 Dell에서는 Remote Management Console 또는 Compliance Reporter에서 *보호되지 않음*이 예상대로 설정되어 있는지 확인할 것을 권장합니다.

프로세스

- **설치 제거 프로세스를 시작하기 전에 (선택 사항) Encryption Removal Agent 로그 파일을 생성**할 수 있습니다. 이 로그 파일은 설치 제거/암호 해독 작업의 문제를 해결하는 데 유용합니다. 설치 제거 프로세스 중 파일을 암호 해독하지 않으려면 Encryption Removal Agent 로그 파일을 만들지 않아도 됩니다.
- **Encryption Removal Agent - 서버에서 키 다운로드** 옵션을 사용하는 경우 설치 제거 전에 Key Server(및 EE Server)를 구성해야 합니다. 지침을 보려면 [EE Server에 대해 활성화된 Encryption 클라이언트 설치 제거를 위한 Key Server 구성](#)을 참조하십시오. VE Server는 Key Server를 사용하지 않기 때문에 설치 제거할 클라이언트가 VE Server에 대해 활성화되어 있으면 사전 작업을 수행할 필요가 없습니다.
- **Encryption Removal Agent - 파일에서 키 가져오기** 옵션을 사용하는 경우에는 Encryption Removal Agent를 실행하기 전에 Dell Administrative Utility(CMGAd)를 사용해야 합니다. 이 유틸리티는 암호화 키 번들을 가져오는 데 사용됩니다. 지침을 보려면 [Administrative Download Utility 사용\(CMGAd\)](#)을 참조하십시오. 이 유틸리티는 Dell 설치 미디어에서 찾을 수 있습니다.
- 설치 제거가 완료된 후, 컴퓨터를 다시 시작하기 전에 모든 데이터가 암호 해독되도록 하려면 WSScan를 실행하십시오. 지침은 [WSScan 사용](#)을 참조하십시오.
- 정기적으로 [Encryption Removal Agent 상태 확인](#) 서비스 패널에 Encryption Removal Agent 서비스가 여전히 있는 경우에 데이터 암호 해독이 계속 진행 중입니다.

명령줄 설치 제거

- 마스터 설치 프로그램에서 추출된 후에 Encryption 클라이언트 설치 프로그램은 `C:\extracted\Encryption\DDPE_XXbit_setup.exe`에서 찾을 수 있습니다.
- 다음 표에는 설치 제거 시 사용할 수 있는 매개 변수가 나와 있습니다.

매개변수	선택
CMG_DECRYPT	Encryption Removal Agent 설치 유형 선택 속성: 3 - LSARecovery 번들 사용 2 - 이전에 다운로드한 Forensics 키 자료 사용 1 - EE Server/VE Server에서 키 다운로드 0 - Encryption Removal Agent를 설치하지 않음
CMGSILENTMODE	자동 설치 제거 속성:



매개변수

선택

1 - 자동

0 - 수동

필수 속성

DA_SERVER

협상 세션을 호스팅하는 EE Server FQHN.

DA_PORT

요청용 EE Server 포트(기본값 8050).

SVCPN

EE Server에서 Key Server 서비스가 로그인된 사용자 이름(UPN 형식).

DA_RUNAS

키 가져오기 요청을 수행할 컨텍스트의 사용자 이름(SAM 호환 형식). 이 사용자는 EE Server의 Key Server 목록에 있어야 합니다.

DA_RUNASPWD

runas 사용자의 암호.

FORENSIC_ADMIN

VE Server의 Forensic 관리자 계정. 이 계정은 서버가 VE Server 인 경우에만 사용됩니다.

노트: Forensic 관리자 계정은 Remote Management Console 에서 생성됩니다. 서버가 EE Server가 아닌 경우 DA_PORT 및 SVCPN 매개 변수를 사용합니다.

FORENSIC_ADMIN_PWD

Forensic 관리자 계정의 암호. 이 계정은 서버가 VE Server인 경우에만 사용됩니다.

선택 사항 속성

SVCCLOGONUN

Encryption Removal Agent 서비스가 로그인된 사용자 이름(UPN 형식) 매개변수.

SVCCLOGONPWD

로그온한 사용자의 암호.

- 다음 예에서는 Encryption 클라이언트를 설치 제거하고 EE Server에서 암호화 키를 다운로드합니다.

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=
\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\"
DA_RUNAS=\"ORGANIZATION\UserInKeyServerList\" DA_RUNASPWD=\"password\" /qn"
```

완료되면 컴퓨터를 다시 부팅합니다.

- 다음 예에서는 Forensic 관리자 계정을 사용하여 Encryption 클라이언트를 설치 제거하고 VE Server에서 암호화 키를 다운로드합니다.

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" FORENSIC_ADMIN=
\"tempadmin\" FORENSIC_ADMIN_PWD=\"tempchangeit\" /qn"
```

완료되면 컴퓨터를 다시 부팅합니다.

중요:

클라이언트가 VE Server에 대해 활성화되어 있을 때 명령줄에서 Forensic 관리자 암호를 사용하는 경우 다음과 같은 작업을 수행할 것을 권장합니다.

- 1 자동 설치 제거를 수행하기 위해 Remote Management Console에서 Forensic 관리자 계정을 만듭니다.
- 2 해당 계정과 기간에만 사용할 수 있는 임시 계정 암호를 사용합니다.
- 3 자동 설치 제거가 완료되면 관리자 목록에서 임시 계정을 제거하거나 암호를 변경합니다.

External Media Edition 설치 제거

마스터 설치 프로그램에서 추출된 후에 Encryption 클라이언트 설치 프로그램은 C:\extracted\Encryption\DDPE_XXbit_setup.exe에서 찾을 수 있습니다.

명령줄 설치 제거

다음과 유사한 명령줄을 실행합니다.

```
DDPE_XXbit_setup.exe /s /x /v"/qn"
```

완료되면 컴퓨터를 다시 부팅합니다.

SED 및 Advanced Authentication 클라이언트 설치 제거

- PBA를 비활성화하려면 EE Server/VE Server에 네트워크가 연결되어 있어야 합니다.

프로세스

- PBA 비활성화 - 컴퓨터에서 모든 PBA 데이터가 제거되고 SED 키가 잠금 해제됩니다.
- SED 클라이언트 설치 제거.
- Advanced Authentication 클라이언트 설치 제거.

PBA 비활성화

- 1 Dell 관리자 계정으로 Remote Management Console에 로그인합니다.
- 2 왼쪽 창에서 **보호 및 관리** > **끝점**을 클릭합니다.
- 3 적절한 끝점 유형을 선택합니다.
- 4 표시 > **표시됨**, **숨김**, 또는 **모두**를 선택합니다.
- 5 컴퓨터의 호스트 이름을 알고 있는 경우 호스트 이름 필드에 입력합니다(와일드카드 사용 가능). 필드를 빈 상태로 두면 모든 컴퓨터가 표시됩니다. **Search(검색)**를 클릭합니다.

호스트 이름을 모르는 경우 목록을 스크롤하여 컴퓨터를 찾습니다.

검색 필터를 기준으로 하나의 컴퓨터 또는 컴퓨터 목록이 표시됩니다.

- 6 원하는 컴퓨터의 **세부 정보** 아이콘을 선택합니다.
- 7 상단 메뉴에서 **보안 정책**을 클릭합니다.
- 8 **정책** 범주 드롭다운 메뉴에서 **SED(Self-Encrypting Drives)**를 선택합니다.
- 9 **SED 관리** 영역을 확장하고 **SED Management 활성화** 및 **PBA 활성화** 정책을 True에서 False로 변경합니다.
- 10 **저장**을 클릭합니다.
- 11 왼쪽 창에서 **작업** > **정책 커밋**을 클릭합니다.
- 12 **변경 사항 저장**을 클릭합니다.

정책이 EE Server/VE Server에서 비활성화 대상 컴퓨터로 전파될 때까지 기다립니다.

PBA가 비활성화된 후에 SED 및 Authentication 클라이언트를 설치 제거합니다.



SED 클라이언트 및 Advanced Authentication 클라이언트 설치 제거

명령줄 설치 제거

- 마스터 설치 프로그램에서 추출된 후에 SED 클라이언트 설치 프로그램은 C:\extracted\Security Tools\EMAgent_XXbit_setup.exe에서 찾을 수 있습니다.
- 마스터 설치 프로그램에서 추출된 후에 SED 클라이언트 설치 프로그램은 C:\extracted\Security Tools\Authentication\<<x64/x86>\setup.exe에서 찾을 수 있습니다.
- 다음 예에서는 SED 클라이언트를 자동으로 설치 제거합니다.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

완료되면 컴퓨터를 종료하고 다시 시작합니다.

다음 작업:

- 다음 예에서는 Advanced Authentication 클라이언트를 자동으로 설치 제거합니다.

```
setup.exe /x /s /v" /qn"
```

완료되면 컴퓨터를 종료하고 다시 시작합니다.

BitLocker Manager 클라이언트 설치 제거

명령줄 설치 제거

- 마스터 설치 프로그램에서 추출된 후에 BitLocker 클라이언트 설치 프로그램은 C:\extracted\Security Tools\EMAgent_XXbit_setup.exe에서 찾을 수 있습니다.
- 다음 예에서는 BitLocker Manager 클라이언트를 자동으로 설치 제거합니다.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

완료되면 컴퓨터를 다시 부팅합니다.

Cloud Edition 설치 제거

- 최종 사용자에게 로컬 관리자 계정이 있으면 Cloud Edition을 직접 설치 제거할 수 있습니다. 자세한 내용은 *Cloud Edition 사용 설명서*를 참조하십시오. 이 섹션에서는 Cloud Edition 설치 제거를 위한 관리자 프로세스를 설명합니다.

① 중요: Cloud Edition을 설치 제거하기 전에 모든 중요한 파일을 Cloud Edition 가상 드라이브 외부로 이동하십시오. 최종 사용자의 컴퓨터에서 Cloud Edition을 설치 제거하면 해당 클라우드에 있는 폴더와 파일이 암호화되어 읽을 수 없게 됩니다. 이 최종 사용자가 퇴사하고 해당 폴더 또는 파일을 공유하는 사용자가 없는 경우 데이터를 읽을 수 없지만 안전합니다(파일을 보고, Cloud Edition을 다시 설치할 수 있음).

명령줄 설치 제거

- 마스터 설치 프로그램에서 추출된 후에 Cloud Edition 클라이언트 설치 프로그램은 C:\extracted\Cloud\Cloud_XXbit_setup.exe
- 다음 예에서는 Cloud Edition 클라이언트를 자동으로 설치 제거합니다.

```
Cloud_XXbit_setup.exe /x /s /v" /qn"
```

메시지가 표시되면 컴퓨터를 재부팅합니다.



일반적으로 사용되는 시나리오

- 각 클라이언트 개별적으로 설치하려면 **마스터 설치 프로그램에서 하위 설치 프로그램 추출**에 나와 있는 대로 먼저 마스터 설치 프로그램에서 하위 실행 파일을 추출해야 합니다.
- v8.x에서 Advanced Authentication을 사용하려면 SED 클라이언트가 필요하기 때문에 다음 예에서 명령줄에 포함되어 있습니다.
- 명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.
- 명령줄에서 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표로 묶어야 합니다.
- 이러한 설치 프로그램을 사용하여 스크립팅된 설치, 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 통해 클라이언트를 설치합니다.
- 명령줄 예에서는 재부팅을 수행하지 않았습니니다. 하지만 실제 상황에서는 재부팅이 필요합니다. 컴퓨터를 재부팅해야만 암호화가 시작됩니다.
- 로그 파일 - Windows는 로그인된 사용자에게 고유한 하위 설치 프로그램 설치 로그 파일을 `C:\Users\\AppData\Local\Temp\%temp%`에 생성합니다.

설치 프로그램을 실행할 때 별도의 로그 파일을 추가하려는 경우, 하위 설치 프로그램이 첨부되지 않으므로 해당 로그 파일의 이름은 고유해야 합니다. 표준 .msi 명령을 통해 `/i*v C:\<any directory>\<any log file name>.log`를 사용하여 로그 파일을 생성할 수 있습니다.

- 별도로 표시된 경우를 제외하고, 모든 하위 설치 프로그램은 명령줄 설치에 동일한 기본 .msi 스위치와 표시 옵션을 사용합니다. 스위치를 먼저 지정해야 합니다. /v 스위치가 필요하며 인수를 사용합니다. 다른 매개 변수는 인수 안에 포함되어 /v 스위치로 전달됩니다.

표시 옵션은 예상 동작을 수행하도록 /v 스위치에 전달된 인수 끝에 지정할 수 있습니다. 동일한 명령줄에 /q와 /qn을 동시에 사용하지 마십시오. /qb 이후에 ! 및 - 만 사용합니다.

스위치	의미
/v	변수를 *.exe 내의 .msi로 전달
/s	자동 모드
/i	설치 모드
옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	Cancel(취소) 버튼이 있는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb-	Cancel(취소) 버튼이 있는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qb!	Cancel(취소) 버튼이 없는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb!-	Cancel(취소) 버튼이 없는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qn	사용자 인터페이스 없음

- 응용 프로그램에 대한 도움이 필요한 사용자에게는 다음과 같은 문서 및 도움말 파일을 참조하도록 안내하십시오.
 - Encryption 클라이언트의 기능 사용 방법에 대해서는 *Dell 암호화 도움말*을 참조하십시오. `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`에 있는 도움말에 액세스하십시오.



- External Media Shield의 기능 사용 방법에 대해서는 *EMS 도움말*을 참조하십시오. <Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS에 있는 도움말에 액세스하십시오.
- Advanced Authentication의 기능 사용 방법에 대해서는 *Security Tools 도움말*을 참조하십시오. <Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help에서 도움말에 액세스하십시오.

Encryption 클라이언트 및 Advanced Authentication

- 다음 예에서는 TPM의 TSS(실행할 수 있는 소프트웨어 스택), Microsoft 핫픽스용 드라이버를 지정된 위치에 설치하며, 제어판 프로그램 목록에 항목을 생성하지 않으며, 재부팅하지 않습니다.

이러한 드라이버는 Encryption 클라이언트 설치 시 설치되어야 합니다.

```
setup.exe /s /z""InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1""
```

다음 작업:

- 다음 예에서는 원격으로 관리되는 SED를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

다음 작업:

- 다음 예에서는 Advanced Authentication을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection\Authentication에 설치됨).

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

다음 작업:

- 다음 예에서는 기본 매개 변수로 Encryption 클라이언트를 설치합니다(Encryption 클라이언트, 공유를 위한 암호화, 대화 상자 표시되지 않음, 진행률 표시줄 표시되지 않음, 다시 시작하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
```

v7.7 이전 버전의 EE Server일 경우 DEVICESERVERURL=https://server.organization.com:8081/xapi(맨 끝의 슬래시 제외)를 바꿉니다.

SED 클라이언트(Advanced Authentication 포함) 및 External Media Shield

- 다음 예에서는 원격으로 관리되는 SED를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

다음 작업:

- 다음 예에서는 Advanced Authentication을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection\Authentication에 설치됨).

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

다음 작업:

- 다음 예에서는 EMS만 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).



```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://server.organization.com:8443/  
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

v7.7 이전 버전의 EE Server일 경우 DEVICESERVERURL=https://server.organization.com:**8081/xapi**(맨 끝의 슬래시 제외)를 바꿉니다.

SED 클라이언트(Advanced Authentication 포함), External Media Edition, 및 Cloud Edition

- 다음 예에서는 TPM의 TSS(신뢰할 수 있는 소프트웨어 스택), Microsoft 핫픽스용 드라이버를 지정된 위치에 설치하며, 제어판 프로그램 목록에 항목을 생성하지 않으며, 재부팅하지 않습니다.

이러한 드라이버는 Encryption 클라이언트 설치 시 설치되어야 합니다.

```
setup.exe /S /z\"InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
```

다음 작업:

- 다음 예에서는 원격으로 관리되는 SED를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888  
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /  
norestart /qn"
```

다음 작업:

- 다음 예에서는 Advanced Authentication을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection\Authentication**에 설치됨).

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

다음 작업:

- 다음 예에서는 기본 매개 변수를 사용하여 클라이언트를 설치합니다(Encryption 클라이언트, 공유를 위한 암호화, 대화 상자 표시되지 않음, 진행률 표시줄 표시되지 않음, 다시 시작하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://  
server.organization.com:8443/xapi/ /norestart /qn"
```

v7.7 이전 버전의 EE Server일 경우 DEVICESERVERURL=https://server.organization.com:**8081/xapi**(맨 끝의 슬래시 제외)를 바꿉니다.

다음 작업:

- 다음 예에서는 Cloud Edition을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /qn"
```

Encryption 클라이언트 및 Cloud Edition

- 다음 예에서는 TPM의 TSS(신뢰할 수 있는 소프트웨어 스택), Microsoft 핫픽스용 드라이버를 지정된 위치에 설치하며, 제어판 프로그램 목록에 항목을 생성하지 않으며, 재부팅하지 않습니다.

이러한 드라이버는 Encryption 클라이언트 설치 시 설치되어야 합니다.

```
setup.exe /S /z\"InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
```

다음 작업:

- 다음 예에서는 기본 매개 변수를 사용하여 클라이언트를 설치합니다(Encryption 클라이언트, 공유를 위한 암호화, 대화 상자 표시되지 않음, 진행률 표시줄 표시되지 않음, 다시 시작하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).



```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESTERURL=https://  
server.organization.com:8443/xapi/ /norestart /qn"
```

v7.7 이전 버전의 EE Server일 경우 DEVICESTERURL=https://server.organization.com:**8081/xapi**(맨 끝의 슬래시 제외)를 바꿉니다.

다음 작업:

- 다음 예에서는 Cloud Edition을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /qn"
```

BitLocker Manager 및 External Media Shield

- 다음 예에서는 BitLocker Manager를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888  
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

다음 작업:

- 다음 예에서는 EMS만 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTERURL=https://server.organization.com:8443/  
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

v7.7 이전 버전의 EE Server일 경우 DEVICESTERURL=https://server.organization.com:**8081/xapi**(맨 끝의 슬래시 제외)를 바꿉니다.

BitLocker Manager, External Media Edition 및 Cloud Edition

- 다음 예에서는 BitLocker Manager를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888  
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

다음 작업:

- 다음 예에서는 EME만 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESTERURL=https://server.organization.com:8443/  
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

v7.7 이전 버전의 EE Server일 경우 DEVICESTERURL=https://server.organization.com:**8081/xapi**(맨 끝의 슬래시 제외)를 바꿉니다.

다음 작업:

- 다음 예에서는 Cloud Edition을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /qn"
```



SED 클라이언트(Advanced Authentication 포함), Encryption 클라이언트 및 Cloud Edition

- 다음 예에서는 TPM의 TSS(신뢰할 수 있는 소프트웨어 스택), Microsoft 핫픽스용 드라이버를 지정된 위치에 설치하며, 제어판 프로그램 목록에 항목을 생성하지 않으며, 재부팅하지 않습니다.

이러한 드라이버는 Encryption 클라이언트 설치 시 설치되어야 합니다.

```
setup.exe /S /z "\"InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
```

다음 작업:

- 다음 예에서는 원격으로 관리되는 SED를 설치합니다(자동 설치, 재부팅하지 않음, 제어판 프로그램 목록에 항목 표시되지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

다음 작업:

- 다음 예에서는 Advanced Authentication을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection\Authentication**에 설치됨).

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

다음 작업:

- 다음 예에서는 기본 매개 변수를 사용하여 클라이언트를 설치합니다(Encryption 클라이언트, 공유를 위한 암호화, 대화 상자 표시되지 않음, 진행률 표시줄 표시되지 않음, 다시 시작하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
```

v7.7 이전 버전의 EE Server일 경우 DEVICESERVERURL=https://server.organization.com:**8081/xapi**(맨 끝의 슬래시 제외)를 바꿉니다.

다음 작업:

- 다음 예에서는 Cloud Edition을 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치됨).

```
Cloud_XXbit_setup.exe /s /v"SERVER=securityserver.organization.com /norestart /qn"
```



다운로드할 소프트웨어

이 섹션은 support.dell.com에서 소프트웨어를 얻는 방법에 대해서 다룹니다. 소프트웨어가 이미 있는 경우, 이 섹션을 건너뛸 수 있습니다.

시작하려면 support.dell.com으로 이동합니다.

- 1 Product Support(제품 지원) 페이지에서 제품을 찾습니다.
- 2 **View products(제품 보기)** 드롭다운을 클릭합니다.
- 3 제품의 목록에서 Software & Security(소프트웨어 및 보안)를 선택합니다.
- 4 *Software & Security*(소프트웨어 및 보안) 섹션에서 **Endpoint Security Solutions**(종단점 보안 솔루션)를 선택합니다. 한 번 선택하고 나면 선택 내용이 웹사이트에 기억됩니다.
- 5 Dell Data Protection 제품을 선택합니다.
예:

Dell Data Protection | Encryption

Dell Data Protection | Endpoint Security Suite

Dell Data Protection | Endpoint Security Suite Enterprise

Dell Data Protection | Security Tools

- 6 **Drivers & downloads**(드라이버 및 다운로드)를 선택합니다.
- 7 원하는 클라이언트 운영 체제 유형을 선택합니다.
- 8 일치하는 내용에서 **Dell Data Protection (4 files)**(Dell 데이터 보호(4개 파일))을 선택합니다. 다음은 예일 뿐이므로 실제 모습은 조금 다를 수 있습니다. 예를 들어, 선택 가능한 파일이 4개가 아닐 수 있습니다.
- 9 **파일 다운로드**를 선택하거나 **내 다운로드 목록 #XX**에 추가를 선택합니다.

일회용 암호, SED UEFI, BitLocker의 사전 설치 구성

TPM 초기화

- 로컬 관리자 그룹(또는 이와 동등)의 구성원이어야 합니다.
- 컴퓨터에 호환되는 BIOS 및 TPM이 장착되어 있어야 합니다.

이 작업은 OTP(일회용 암호)를 사용하는 경우에 필요합니다.

- <http://technet.microsoft.com/en-us/library/cc753140.aspx>의 지침을 따릅니다.

UEFI 컴퓨터의 사전 설치 구성

UEFI 부팅 전 인증이 진행되는 동안 네트워크 연결 활성화

UEFI 펌웨어가 설치된 컴퓨터에서 PBA(부팅 전 인증)를 성공적으로 수행하려면 PBA에 네트워크가 연결되어 있어야 합니다. 기본적으로, UEFI 펌웨어가 설치된 컴퓨터는 운영 체제가 로드될 때까지 네트워크에 연결되지 않고 PBA 모드가 끝나야 연결됩니다.

다음 절차에 따라 PBA가 진행되는 동안 UEFI를 사용할 수 있는 컴퓨터의 네트워크 연결을 활성화합니다. 구성 단계는 UEFI 컴퓨터 모델에 따라 다르기 때문에 다음에 제시된 방법은 여러 가지 구성 방법 중 하나의 예입니다.

- 1 UEFI 펌웨어 구성으로 부팅합니다.
- 2 부팅되고 있는 동안 오른쪽 상단 화면에 "일회용 부팅 메뉴 준비 중"과 같은 메시지가 나타날 때까지 F2 키를 계속 누릅니다.
- 3 메시지가 나타나면 BIOS 관리자 암호를 입력합니다.

① **노트:** 새 컴퓨터에는 BIOS 암호가 구성되어 있지 않기 때문에 일반적으로 이 메시지는 표시되지 않습니다.

- 4 시스템 구성을 선택합니다.
- 5 통합 NIC를 선택합니다.
- 6 UEFI 네트워크 스택 활성화 확인란을 선택합니다.
- 7 활성화됨 또는 w/PXE 활성화됨을 선택합니다.
- 8 적용을 선택합니다.

① **노트:**

UEFI 펌웨어가 설치되지 않은 컴퓨터에는 구성이 필요하지 않습니다.

레거시 옵션 ROM 비활성화

BIOS에서 레거시 옵션 ROM 활성화 설정을 비활성화해야 합니다.

- 1 컴퓨터를 다시 시작합니다.
- 2 컴퓨터가 다시 시작되면 **F12** 키를 계속 눌러 UEFI 컴퓨터의 부팅 설정을 표시합니다.
- 3 아래쪽 화살표를 누르고 **BIOS Settings(BIOS 설정)** 옵션을 강조 표시한 후 **Enter**를 누릅니다.



- 4 **Settings(설정) > General(일반) > Advanced Boot Options(고급 부팅 옵션)**를 선택합니다.
- 5 레거시 옵션 **ROM 활성화** 확인란을 선택 해제하고 **적용**을 클릭합니다.

BitLocker PBA 파티션 설정을 위한 사전 설치 구성

- BitLocker Manager를 설치하기 **전에** PBA 파티션을 생성해야 합니다.
- BitLocker Manager를 설치하기 **전에** TPM을 켜고 활성화합니다. BitLocker Manager가 TPM의 소유권을 가져오며 재부팅은 필요하지 않습니다. 단, TPM 소유권이 이미 있는 경우 BitLocker Manager에서 암호화 설정 프로세스를 시작합니다. 중요한 점은 TPM을 "소유"해야 한다는 것입니다.
- 디스크를 수동으로 파티션해야 할 수 있습니다. 자세한 내용은 Microsoft의 BitLocker 드라이브 준비 도구 설명을 참조하십시오.
- BdeHdCfg.exe 명령을 사용하여 PBA 파티션을 만듭니다. 기본 매개 변수는 명령줄 도구가 BitLocker 설정 마법사와 동일한 프로세스를 따름을 나타냅니다.

```
BdeHdCfg -target default
```

① 팁:

BdeHdCfg 명령에 사용할 수 있는 추가 옵션을 보려면 [Microsoft의 BdeHdCfg.exe 매개 변수 참조](#)를 확인하십시오.

권한 부여 활성화를 위해 도메인 컨트롤러에서 GPO 설정

- 클라이언트에 Dell Digital Delivery(DDD) 사용 권한이 부여되는 경우 다음 지침에 따라 도메인 컨트롤러에서 GPO를 설정하여 권한 부여를 사용하도록 설정합니다(EE Server/VE Server를 실행하는 서버와 다를 수 있음).
- 워크스테이션은 GPO가 적용된 OU의 구성원이어야 합니다.

① **노트:** 아웃바운드 포트 443을 사용하여 EE 서버/VE 서버와 통신할 수 있는지 확인하십시오. 어떠한 이유로든 포트 443이 차단된 경우 권한 부여 기능이 작동하지 않습니다.

- 1 클라이언트를 관리할 도메인 컨트롤러에서 **시작 > 관리 도구 > 그룹 정책 관리**를 클릭합니다.
- 2 정책을 적용해야 하는 OU를 마우스 오른쪽 버튼으로 클릭하고 **이 도메인에서 GPO를 만들고 여기에 연결하십시오...**를 선택합니다.
- 3 새 GPO의 이름을 입력하고 원본 스타터 GPO에 대해 (없음)을 선택한 다음 **확인**을 클릭합니다.
- 4 생성된 GPO를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 선택합니다.
- 5 그룹 정책 관리 편집기가 로드됩니다. **컴퓨터 구성 > 환경설정 > Windows 설정 > 레지스트리**에 액세스합니다.
- 6 레지스트리를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 레지스트리 항목**을 선택합니다. 다음 작업을 완료합니다.

작업: 생성

하이브: HKEY_LOCAL_MACHINE

키 경로: SOFTWARE\Dell\Dell Data Protection

값 이름: Server

값 유형: REG_SZ

값 데이터: <EE Server/VE Server의 IP 주소>

- 7 **확인**을 클릭합니다.
- 8 워크스테이션에서 로그아웃했다가 다시 로그인하거나 **gpupdate /force**를 실행하여 그룹 정책을 적용합니다.



마스터 설치 프로그램에서 하위 설치 프로그램 추출

- 각 클라이언트를 개별적으로 설치하려면 설치 프로그램에서 하위 실행 파일을 추출합니다.
 - 마스터 설치 프로그램은 마스터 설치 제거 프로그램이 아닙니다. 각 클라이언트를 별도로 설치 제거한 후에 마스터 설치 프로그램을 설치 제거해야 합니다. 클라이언트를 설치 제거에 사용할 수 있도록 이 프로세스에 따라 마스터 설치 프로그램에서 클라이언트를 추출하십시오.
- 1 Dell 설치 미디어에서 **DDPSetup.exe** 파일을 로컬 컴퓨터로 복사합니다.
 - 2 **DDPSetup.exe** 파일과 동일한 위치에서 명령 프롬프트를 열고 다음을 입력합니다.

```
DDPSetup.exe /z "\"EXTRACT_INSTALLERS=C:\extracted\""
```

추출 경로는 63자를 초과할 수 없습니다.

설치를 시작하기 전에 설치하고자 하는 각 하위 설치 프로그램에 필요한 모든 필수 조건이 충족되었고 필요한 모든 소프트웨어가 설치되었는지 확인하십시오. 자세한 내용은 [요구 사항](#)을 참조하십시오.

추출된 하위 설치 프로그램은 **C:\extracted**에 있습니다.

EE Server에 대해 활성화된 Encryption 클라이언트 설치 제거를 위한 Key Server 구성

- 이 섹션에서는 EE Server를 사용할 경우 Kerberos 인증에 사용할 구성 요소를 구성하는 방법에 대해 설명합니다. VE Server는 Key Server를 사용하지 않습니다.

Key Server는 소켓에 연결할 클라이언트를 수신 대기하는 서비스입니다. 클라이언트가 연결되면 보안 연결이 협상, 인증되고 Kerberos API를 사용하여 암호화됩니다(보안 연결을 협상할 수 없는 경우 클라이언트 연결이 끊어집니다).

그런 다음 Key Server가 Security Server(이전에는 Device Server라고 함)와 함께 클라이언트를 실행하는 사용자가 키에 액세스할 수 있는지 여부를 확인합니다. 이 액세스 권한은 개별 도메인을 통해 원격 관리 콘솔에 부여됩니다.

- Kerberos 인증을 사용하려는 경우 Key Server 구성 요소가 포함된 서버는 영향을 받는 도메인에 포함되어야 합니다.
- VE Server가 Key Server를 사용하지 않기 때문에 일반적인 설치 제거 과정이 적용됩니다. VE Server에 대해 활성화된 Encryption 클라이언트가 제거되면, Key Server의 Kerberos 대신 Security Server를 통한 표준 Forensic 키 검색이 사용됩니다. 자세한 내용은 [명령줄 설치 제거](#)를 참조하십시오.

서비스 패널 - 도메인 계정 사용자 추가

- EE Server에서 서비스 패널로 이동합니다(시작 > 실행...services.msc > OK(확인)).
- Dell Key Server를 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)**를 선택합니다.
- 로그온 탭을 선택한 후 **This account:(이 계정:)** 옵션을 선택합니다.

이 계정: 필드에서 원하는 도메인 사용자를 추가합니다. 이 도메인 사용자는 Key Server 폴더에 대해 로컬 관리자 이상의 권한이 있어야 합니다(Key Server 구성 파일뿐만 아니라 log.txt 파일에도 데이터를 쓸 수 있어야 함).

도메인 사용자에 대한 암호를 입력하고 확인합니다.

OK(확인)를 클릭합니다.

- Key Server 서비스를 다시 시작합니다(추가 작업을 위해 서비스 패널은 열어 둡).
- <Key Server 설치 디렉터리> log.txt를 탐색하여 서비스가 올바르게 시작되었는지 확인합니다.

Key Server 구성 파일 - EE Server 통신에 대한 사용자 추가

- <Key Server 설치 디렉터리>를 탐색합니다.
- 텍스트 편집기를 사용해 **Credant.KeyServer.exe.config**를 엽니다.
- <add key="user" value="superadmin" />으로 이동한 다음 "superadmin" 값을 적절한 사용자 이름으로 변경합니다("superadmin"을 유지할 수도 있음).

"superadmin" 형식으로는 EE Server에 인증할 수 있는 모든 방법이 허용됩니다. SAM 계정 이름, UPN 또는 도메인\사용자 이름이 허용됩니다. Active Directory에 대한 인증을 위해서는 해당 사용자 계정에 대한 유효성 검사가 필요하므로 EE Server에 인증할 수 있는 모든 방법이 허용됩니다.



예를 들어, 다중 도메인 환경에서 "jdoe"와 같은 SAM 계정 이름만 입력하면 EE Server가 "jdoe"를 찾을 수 없어 이를 인증할 수 없으므로 실패할 가능성이 높습니다. 다중 도메인 환경에서는 도메인\사용자 이름 형식이 허용되더라도 UPN을 사용하는 것이 좋습니다. 단일 도메인 환경에서는 SAM 계정 이름이 허용됩니다.

- 4 <add key="epw" value="<encrypted value of the password>" />으로 가서 "epw"를 "password"로 변경합니다. 그런 다음 "<encrypted value of the password>"을 3단계의 사용자 암호로 변경합니다. EE Server가 다시 시작되면 이 암호가 다시 암호화됩니다.

3단계에서 "superadmin"을 사용할 경우 superadmin 암호가 "changeit"이 아니면 여기에서 변경해야 합니다. 파일을 저장하고 닫습니다.

예시 구성 파일:

```
<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="port" value="8050" /> [Key Server가 수신하는 TCP 포트. 기본값은 8050.]

<add key="maxConnections" value="2000" /> [Key Server에서 허용할 활성 소켓 연결 수]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [Security Server(이전에는 Device Server라고 함) URL(v7.7 이전 EE Server의 형식은 8081/xapi)]

<add key="verifyCertificate" value="false" /> [참일 경우 인증서를 검증함/검증하지 않거나 자체 서명 인증서를 사용할 경우 거짓으로 설정함]

<add key="user" value="superadmin" /> [Security Server와 통신하는 데 사용하는 사용자 이름. 이 사용자는 Remote Management Console에서 관리자 역할을 선택한 상태여야 합니다. "superadmin" 형식으로는 EE Server에 인증할 수 있는 모든 방법이 허용됩니다. SAM 계정 이름, UPN 또는 도메인\사용자 이름이 허용됩니다. Active Directory에 대한 인증을 위해서는 해당 사용자 계정에 대한 유효성 검사가 필요하므로 EE Server에 인증할 수 있는 모든 방법이 허용됩니다. 예를 들어, 다중 도메인 환경에서 "jdoe"와 같은 SAM 계정 이름만 입력하면 EE Server가 "jdoe"를 찾을 수 없어 이를 인증할 수 없으므로 실패할 가능성이 높습니다. 다중 도메인 환경에서는 도메인\사용자 이름 형식이 허용되더라도 UPN을 사용하는 것이 좋습니다. 단일 도메인 환경에서는 SAM 계정 이름이 허용됩니다.]

<add key="cacheExpiration" value="30" /> [서비스가 키를 요청할 수 있는 사용자를 확인해야 하는 빈도(초). 서비스는 캐시를 유지하고 경과 시간을 추적합니다. 캐시가 해당 값보다 오래된 경우 새 목록을 가져옵니다. 사용자가 연결되면 Key Server가 Security Server에서 인증된 사용자를 다운로드해야 합니다. 이러한 사용자의 캐시가 없거나 마지막 "x"초 동안 다운로드된 목록이 없을 경우 다시 다운로드됩니다. 폴링은 수행되지 않지만 이 값은 새로 고침이 필요할 경우 새로 고침 전 목록의 기간을 구성합니다.]

<add key="epw" value="encrypted value of the password" /> [Security Server와 통신하는 데 사용하는 암호. superadmin 암호가 변경된 경우 여기에서 변경해야 합니다.]

</appSettings>

</configuration>
```

서비스 패널 - Key Server 서비스 재시작

- 1 서비스 패널로 돌아갑니다(시작 > 실행... > services.msc > 확인).
- 2 Key Server 서비스를 다시 시작합니다.
- 3 <Key Server 설치 디렉터리> log.txt를 탐색하여 서비스가 올바르게 시작되었는지 확인합니다.
- 4 서비스 패널을 닫습니다.



원격 관리 콘솔 - Forensic Administrator 추가

- 1 필요할 경우 원격 관리 콘솔에 로그인합니다.
- 2 **Populations(채우기) > Domains(도메인)**를 클릭합니다.
- 3 적절한 도메인을 선택합니다.
- 4 **Key Server** 탭을 클릭합니다.
- 5 계정 필드에서, 관리자 활동을 수행할 사용자를 추가합니다. 형식은 도메인\사용자 이름입니다. **Add Account(계정 추가)**를 클릭합니다.
- 6 왼쪽 메뉴에서 **Users(사용자)**를 클릭합니다. 검색 상자에서, 5단계에서 추가한 사용자 이름을 검색합니다. **Search(검색)**를 클릭합니다.
- 7 올바른 사용자를 찾았으면 **Admin (관리자)** 탭을 클릭합니다.
- 8 **Forensic Administrator(Forensic 관리자)** 를 선택하고 **Update(업데이트)**를 클릭합니다.
Kerberos 인증을 위한 요소가 구성되었습니다.



Administrative Download Utility 사용 (CMGAd)

- 이 유틸리티를 사용하면 EE Server/VE Server에 연결되지 않은 컴퓨터에 키 자료 번들을 다운로드하여 사용할 수 있습니다.
- 이 유틸리티는 응용 프로그램에 전달되는 명령줄 매개 변수에 따라 다음 방법 중 하나로 키 번들을 다운로드합니다.
 - Forensic 모드: -f가 명령줄에 전달되거나 사용된 명령줄 매개 변수가 없는 경우에 사용됩니다.
 - 관리 모드: -a가 명령줄에 전달되는 경우에 사용됩니다.

로그 파일은 C:\ProgramData\CmgAdmin.log에서 볼 수 있습니다.

Forensic 모드로 Administrative Download Utility 사용

- 1 **cmgad.exe**를 두 번 클릭하여 유틸리티를 실행하거나 CMGAd가 있는 명령 프롬프트를 열고 **cmgad.exe -f**(또는 **cmgad.exe**)를 입력합니다.
- 2 다음 정보를 입력합니다(일부 필드는 미리 채워져 있을 수 있음).
Device Server URL: 정규화된 Security Server(Device Server) URL. <https://securityserver.domain.com:8443/xapi/> 형식으로 입력합니다. EE Server가 v7.7 이전 버전일 경우 <https://deviceserver.domain.com:8081/xapi> 형식으로 입력합니다(뒤에 슬래시 없이 다른 포트 번호 입력).

Dell 관리자: jdoe 등과 같이 Forensic 관리자 자격 증명(원격 관리 콘솔에 활성화됨)을 사용하는 관리자의 이름.

암호: Forensic 관리자 암호.

MCID: machinelD.domain.com과 같은 시스템 ID.

DCID: 16자리 Shield ID의 처음 8개 숫자.

① 팁: 일반적으로 MCID 또는 DCID를 지정하면 됩니다. 하지만 두 ID 모두를 알고 있는 경우에는 둘 다 입력하는 것이 좋습니다. 각 매개 변수에는 각각의 클라이언트 및 클라이언트 컴퓨터에 대한 정보가 포함되어 있습니다.

Next(다음)를 클릭합니다.

- 3 '패스프레이즈' 필드에 다운로드 파일을 보호할 패스프레이즈를 입력합니다. 패스프레이즈는 8자 이상이어야 하며 하나 이상의 영문자 및 숫자가 포함되어야 합니다. 패스프레이즈를 확인합니다.
파일이 저장될 기본 이름과 위치를 수락하거나 ...를 클릭하여 다른 위치를 선택합니다.

다음을 클릭합니다.

키 자료가 성공적으로 잠금 해제되었다는 메시지가 표시됩니다. 이제 파일에 액세스할 수 있습니다.

- 4 완료되면 **마침**을 클릭합니다.

관리 모드로 Administrative Download Utility 사용

VE Server는 Key Server를 사용하지 않으므로 관리 모드로 VE Server에서 키 번들을 가져올 수 없습니다. 클라이언트가 VE Server에 대해 활성화된 경우 Forensic 모드로 키 번들을 가져오십시오.

- 1 CMGAd가 있는 명령 프롬프트를 열고 **cmgad.exe -a**를 입력합니다.
- 2 다음 정보를 입력합니다(일부 필드는 미리 채워져 있을 수 있음).

서버: Key Server의 정규화된 호스트 이름(예: keyserver.domain.com)

포트 번호: 기본 포트는 8050입니다.

서버 계정: Key Server를 실행하고 있는 도메인 사용자로서 형식은 도메인\사용자 이름입니다. 이 유틸리티를 실행하는 도메인 사용자는 Key Server에서 다운로드를 수행할 수 있는 권한이 있어야 합니다.

MCID: machinelD.domain.com과 같은 시스템 ID.

DCID: 16자리 Shield ID의 처음 8개 숫자.

① 팁: 일반적으로 MCID 또는 DCID를 지정하면 됩니다. 하지만 두 ID 모두를 알고 있는 경우에는 둘 다 입력하는 것이 좋습니다. 각 매개 변수에는 각각의 클라이언트 및 클라이언트 컴퓨터에 대한 정보가 포함되어 있습니다.

Next(다음)를 클릭합니다.

- 3 '패스프레이즈' 필드에 다운로드 파일을 보호할 패스프레이즈를 입력합니다. 패스프레이즈는 8자 이상이어야 하며 하나 이상의 영문자 및 숫자가 포함되어야 합니다.

패스프레이즈를 확인합니다.

파일이 저장될 기본 이름과 위치를 수락하거나 ...를 클릭하여 다른 위치를 선택합니다.

다음을 클릭합니다.

키 자료가 성공적으로 잠금 해제되었다는 메시지가 표시됩니다. 이제 파일에 액세스할 수 있습니다.

- 4 완료되면 **마침**을 클릭합니다.



Server Encryption 구성

Server Encryption 사용

① **노트:** Server Encryption은 User 암호화를 Common 암호화로 변환합니다.

- 1 Dell 관리자로 Dell Remote Management Console에 로그인합니다.
- 2 **Endpoint Group(끝점 그룹)**(또는 **Endpoint(끝점)**)을 선택하고, 활성화할 끝점 그룹을 검색하고, **Security Policies(보안 정책)**를 선택한 후에, **Server Encryption** 정책 범주를 선택합니다.
- 3 다음 정책을 설정합니다.
 - Server Encryption - **선택**하여 Server Encryption 및 관련 정책을 활성화합니다.
 - SDE Encryption Enabled - **선택**하여 SDE 암호화를 켭니다.
 - Encryption Enabled - **선택**하여 Common 암호화를 켭니다.
 - Secure Windows Credentials - 이 정책은 기본적으로 **Selected(선택됨)**로 설정됩니다.

Secure Windows Credentials 정책이 **Selected(기본값)**로 설정되면 Windows 자격 증명을 비롯하여 \Windows\system32\config files 폴더의 모든 파일이 암호화됩니다. Windows 자격 증명 암호화되지 않도록 하려면 Secure Windows Credentials 정책을 **Not Selected(선택되지 않음)**로 설정하십시오. Windows 자격 증명 암호화는 SDE Encryption Enabled 정책 설정과 관계가 없습니다.
- 4 정책을 저장하고 커밋합니다.

활성화 로그인 대화 상자 사용자 지정

활성화 대화상자에 표시되는 내용은 다음과 같습니다.

- 관리되지 않는 사용자가 로그인한 시기.
- 사용자가 시스템 트레이에 있는 Encryption 아이콘 메뉴에서 Activate Dell Data Protection | Encryption(Dell Data Protection | Encryption 활성화)을 선택합니다.



Customizable text

Server Encryption EMS 정책 설정

원본 암호화 컴퓨터는 이동식 장치를 원래 암호화하는 컴퓨터입니다. 원본 컴퓨터가 **보호되는 서버**(Server Encryption이 설치되고 활성화된 서버)이고 보호되는 서버가 이동식 장치가 있음을 먼저 감지하는 경우, 이동식 장치를 암호화하라는 메시지가 사용자에게 표시됩니다.

- EMS 정책은 서버, 인증, 암호화 등에 대한 이동식 미디어 액세스를 제어합니다.
- Port Control 정책은 보호되는 서버의 이동식 미디어에 영향을 줍니다(예: USB 장치별로 서버의 USB 포트의 액세스 및 사용 제어).

이동식 미디어 암호화에 대한 정책은 Remote Management Console의 *Server Encryption* 기술 그룹 아래에서 찾을 수 있습니다.

Server Encryption 및 외장형 미디어

보호된 서버의 *EMS Encrypt External Media* 정책이 **선택**되어 있으면 외부 미디어가 암호화됩니다. Server Encryption은 해당 장치를 컴퓨터 키를 사용하여 보호되는 서버에 연결하고, 이동식 장치의 소유자/사용자의 사용자 로밍 키를 사용하여 해당 사용자에게 연결합니다. 그러면 장치가 연결된 컴퓨터와 관계없이 동일한 키를 사용하여 이동식 장치에 추가된 모든 파일이 암호화됩니다.

① 노트:

Server Encryption은 사용자 암호화를 일반 암호화로 변환합니다(이동식 장치에서는 예외). 이동식 장치에서 컴퓨터와 연관된 사용자 로밍 키를 사용하여 암호화가 수행됩니다.

사용자가 이동식 장치 암호화에 동의하지 않으면, 장치가 보호되는 서버에 사용될 경우 이 장치에 대한 사용자 액세스를 **차단됨, 읽기 전용** 또는 **전체 액세스**로 설정할 수 있습니다. 보호되는 서버의 정책에 따라 보호되지 않는 이동식 장치의 액세스 수준이 결정됩니다.

이동식 장치가 원본 보호되는 서버에 다시 삽입되면 정책이 업데이트됩니다.

인증 및 외장형 미디어

보호되는 서버의 정책에 따라 인증 기능이 결정됩니다.

이동식 장치가 암호화된 후에는 장치의 소유자/사용자만 보호되는 서버의 이동식 장치에 액세스할 수 있습니다. 다른 사용자는 이동식 장치에 있는 암호화된 파일에 액세스할 수 없습니다.

로컬 자동 인증은 보호된 이동 가능한 미디어를 보호된 서버에 삽입할 경우 해당 미디어의 소유자가 로그인되어 있을 때 자동으로 인증되도록 허용합니다. 자동 인증이 비활성화되어 있으면 소유자/사용자가 보호된 이동식 장치에 대한 액세스 권한을 인증해야 합니다.

이동식 장치의 원본 암호화 컴퓨터가 보호되는 서버일 경우, 다른 컴퓨터에 정의된 EMS 정책 설정과 관계없이 소유자/사용자가 원본이 아닌 컴퓨터에서 사용할 때 이동식 장치에 항상 로그인해야 합니다.

Server Encryption Port Control 및 EMS 정책에 대한 자세한 내용은 AdminHelp를 참조하십시오.

암호화된 서버 인스턴스 일시 중단

암호화된 서버를 일시 중지하면 다시 시작한 후에 암호화된 데이터에 액세스할 수 없습니다. 가상 서버 사용자는 일시 중단할 수 없습니다. 대신 Server Encryption 컴퓨터 키가 일시 중단됩니다.

- ① **노트:** 서버 끝점을 일시 중단해도 서버가 즉시 일시 중단되지 않습니다. 일시 중단은 다음에 키가 요청될 때(일반적으로 다음에 서버가 다시 시작될 때) 적용됩니다.
- ① **중요:** 이 기능은 주의해서 사용해야 합니다. 정책 설정에 따라 네트워크에서 연결이 끊겨 있는 동안 보호되는 서버가 일시 중단된 경우에는 암호화된 서버 인스턴스를 일시 중단하면 불안정해질 수 있습니다.

전제조건

- Remote Management Console에서 지정된 헬프 데스크 관리자 권한이 있어야만 끝점을 일시 중단할 수 있습니다.
- 관리자가 Remote Management Console에 로그인되어 있어야 합니다.



Remote Management Console의 왼쪽 창에서 **Populations(채우기) > Endpoints(끝점)**를 클릭합니다.

호스트 이름을 검색하거나 선택한 뒤 **Details & Actions(세부 정보 및 조치)** 탭을 클릭합니다.

Server Device Control(서버 장치 제어) 아래에서 **Suspend(일시 중단)**를 클릭한 후 **Yes(예)**를 클릭합니다.

① **노트:** 서버가 다시 시작된 후 **Server Encryption**이 서버에 있는 암호화된 데이터에 액세스하려면 **Reinstate(다시 시작)** 단추를 클릭합니다.

Cloud Edition을 위한 서버 구성

Cloud Edition을 위한 VE Server 구성

Cloud Edition 지원을 위해 VE Server를 구성하려면 원격 관리 콘솔에서 '클라우드 스토리지 보호 사용' 보호 정책을 True(참)로 설정합니다.

Cloud Edition을 위한 EE Server 구성

Cloud Edition을 지원하도록 EE Server를 구성하려면 원격 관리 콘솔에서 클라우드 보호 정책을 ON(켜짐)으로 설정한 후 [클라우드 클라이언트 다운로드를 허용하도록 Security Server 구성](#)을 실행합니다.

클라우드 클라이언트 다운로드를 허용하도록 Security Server 구성

이 섹션에는 최종 사용자가 Security Server에서 Windows 클라우드 클라이언트를 다운로드할 수 있도록 허용하는 데 필요한 단계가 나와 있습니다.

- 1 EE Server에서 <Security Server 설치 디렉터리>\webapps\cloudweb\brand\dell\resources로 이동하고 텍스트 편집기를 사용해 messages.properties 파일을 엽니다.
- 2 항목이 다음과 같은지 확인하십시오.

```
download.deviceWin.mode=remote
```

```
download.deviceWin.local.filename.32=cloud32.exe
```

```
download.deviceWin.local.filename.64=cloud64.exe
```

```
download.deviceWin.remote.link.32=https://<YOUR HOST URL>:<PORT>/cloudweb/download/cloud32.exe
```

```
download.deviceWin.remote.link.64=https://<YOUR HOST URL>:<PORT>/cloudweb/download/cloud64.exe
```

- 3 파일을 저장하고 닫습니다.
- 4 <Security Server 설치 디렉터리>로 이동한 다음 그 아래에 새 폴더를 만들고 이름을 Download로 지정합니다(Security Server \Download).
- 5 Download 폴더 안에 새 폴더를 만들고 이름을 Cloudweb으로 지정합니다(Security Server\Download\Cloudweb).
- 6 Cloud Edition의 64비트 및 32비트 설치 파일을 Cloudweb 폴더에 추가하고 이름을 각각 cloud64.exe 및 cloud32.exe로 바꿉니다.

Windows 클라우드 클라이언트의 자동 다운로드를 위해 EE Server 구성(선택 사항)

- 1 EE Server를 호스팅하는 서버에서 C:\inetpub\wwwroot\로 이동합니다. 이 웹 서버에는 신뢰할 수 있는 인증서가 있어야 합니다.
- 2 wwwroot 아래 CloudUpdate라는 폴더를 만듭니다(C:\inetpub\wwwroot\CloudUpdate).

① | 노트: 이 예에서는 **CloudUpdate**를 사용했지만 사용자가 원하는 대로 다른 이름을 선택할 수 있습니다.

- 3 업데이트된 실행 파일을 CloudUpdate 폴더에 저장합니다.
- 4 CloudUpdate 폴더에 업데이트된 versions.xml 파일을 넣습니다.
- 5 텍스트 편집기를 사용해 versions.xml을 열고 파일 이름 경로가 환경에 맞는 지 확인합니다.

예:



```
<?xml version="1.0"?> <VERSIONS><VERSION channel="release" brand="1" arch="x86"
version="1.0.0.1814" filename="/Cloud32.exe"/><VERSION channel="release" brand="1" arch="x64"
version="1.0.0.1814" filename="/Cloud64.exe"/></VERSIONS>
```

버전: 업데이트된 실행 파일의 파일 버전

파일 이름: 위 URL 끝(/CloudUpdate)에서 실제 실행 파일까지의 경로

- 6 파일을 저장하고 닫습니다.
- 7 IIS를 다시 시작합니다.
- 8 Dell 관리자 자격으로 원격 관리 콘솔에 로그인합니다.
- 9 왼쪽 창에서 **채우기 > 엔터프라이즈**를 클릭합니다.
- 10 상단 메뉴에서 **보안 정책**을 클릭합니다.
- 11 **클라우드 암호화**를 선택합니다.
- 12 **고급 설정 표시**를 클릭합니다.
- 13 **소프트웨어 업데이트 서버 URL** 정책으로 스크롤하고 <https://<YOUR HOST URL>/CloudUpdate>를 입력합니다.

① | 노트: 위 예와 일치하는 예는 **CloudUpdate**뿐입니다.

- 14 **저장**을 클릭하여 대기열에서 커밋할 정책 수정 사항을 저장합니다.
- 15 **관리 > 커밋**을 클릭합니다.

Cloud Storage Protection Provider 프로필 관리

Cloud Edition은 사용자의 파일을 암호화하여 EE Server/VE Server에 감사 이벤트를 보냅니다. 지원되는 각 클라우드 스토리지 공급자에 대한 동작을 변경하려면 각 공급자를 다음 값 중 하나로 설정합니다.

값	설명
보호	공급자/연결을 허용하고, 파일을 암호화하고, 파일/폴더 작업에 관한 감사 이벤트를 보냅니다.
차단	공급자/연결에 대한 모든 액세스를 차단합니다.
허용	공급자/연결에서 암호화는 수행하지 않되 파일/폴더 감사를 수행하고 통과하도록 허용합니다.
무시	암호화나 감사 없이 공급자/연결 보호를 무시합니다. 이 값이 설정되면, 클라우드 스토리지 공급자 폴더는 클라이언트 컴퓨터의 Cloud Edition 가상 드라이브에 표시되지 않습니다.

자세한 내용은 원격 관리 콘솔에 있는 관리자 도움말을 참조하십시오.

허용 목록/거부 목록에서 사용자 허용/거부

내부 사용자가 Cloud Edition으로 보호되는 파일을 외부 사용자와 공유하려는 경우 관리자와 조율해야 합니다.

내부 사용자가 비즈니스에 중요한 파일과 폴더를 외부 사용자와 공유할 수 있는 범위는 회사가 결정합니다. 예:

- 내부 사용자는 Cloud Edition을 등록하고 설치하도록 외부 사용자에게 요청을 보낼 수 있습니다.

또는

- **모범 사례:** 회사는 회사 이메일 도메인 안에 있지 않은 사용자를 거부 목록에 등록합니다. 내부 사용자는 먼저 관리자에게 외부 사용자를 허용 목록에 추가해 달라고 요청해야 합니다.

관리자는 정책 및 허용 목록/거부 목록을 통해 이를 관리하며, EE Server/VE Server에 등록하여 Cloud Edition을 설치할 수 있는 사용자를 결정합니다. 적절한 보안을 위해서는 이 목록을 설정하고 관리할 때 주의해야 합니다.

허용 목록



허용 목록은 특정 사용자나 사용자 그룹이 EE Server/VE Server에 등록하고 Cloud Edition을 사용할 수 있도록 허용합니다.

조직에서 외부 사용자(도메인 이외의 이메일 주소를 갖는 사용자)가 Cloud Edition에 등록하도록 허용할 수 있습니다. 외부 사용자는 허용 목록에 추가되어야 하며, 관리자가 그 외부 사용자에게 등록 이메일을 전송해야 합니다.

거부 목록을 사용하려면 허용 목록의 모든 와일드카드를 제거해야 합니다. 다음 예를 참조하십시오.

`<Allow>*@organization.com</Allow>` 모든 organization.com 이메일 주소에서 EE Server/VE Server에 등록할 수 있습니다.

`<Allow>*</Allow>` 모든 사용자가 EE Server/VE Server에 등록할 수 있습니다.

`<Allow>jdoe@organization.com</Allow>` 이 특정 사용자가 EE Server/VE Server에 등록할 수 있습니다.

`<Allow>*@gmail.com</Allow>` 모든 Gmail 사용자가 EE Server/VE Server에 등록할 수 있습니다.

거부 목록

거부 목록은 특정 사용자 또는 사용자 그룹이 EE Server/VE Server에 등록하고 Cloud Edition을 사용하지 못하도록 합니다.

거부 목록을 사용하여 허용 목록에 승인되어 있는 특정 사용자를 제외할 수 있습니다. 와일드카드 문자(*)를 사용하면 전체 도메인을 거부 목록에 등록할 수 있으므로 해당 도메인에 이메일 주소가 있는 사용자가 등록하지 못합니다.

거부 목록에 등록된 도메인 사용자는 등록은 할 수 있지만 활성화되지는 못합니다. 거부 목록에 등록된 비 도메인 사용자는 등록을 할 수 없으며, 대화 상자가 하나 표시되어 이들 사용자는 등록 허가를 받지 않았음을 알려줍니다.

이미 등록된 사용자의 경우 Cloud Edition 사용을 차단하는 거부 목록의 영향을 받지 않습니다.

다음 예를 참조하십시오.

`<deny>*@organization.com</deny>` 모든 organization.com 이메일 주소가 EE Server/VE Server에 등록하지 못하도록 합니다.

`<deny>jdoe@organization.com</deny>` 특정 사용자가 이 이메일 주소로 EE Server/VE Server에 등록하지 못하도록 합니다.

`<deny>*@gmail.com</deny>` 모든 Gmail 사용자가 EE Server/VE Server에 등록하지 못하도록 합니다.

허용 목록/거부 목록을 수정하려면 다음 지침을 따르십시오.

- 1 `<Security Server 설치 디렉터리>\conf\`로 이동합니다.
- 2 텍스트 편집기로 registration-access.xml을 엽니다.
- 3 위 정보와 다음 예를 기준으로 사용자를 허용 또는 거부합니다.

```
<?xml version="1.0" encoding="UTF-8"?><access><whitelist><allow>user1@organization.com</allow><allow>*@organization.com</allow><allow>*</allow></whitelist><blacklist><!--All addresses not specifically allowed are denied.<deny> </deny--></blacklist></access>
```

- 4 파일을 저장하고 닫습니다.



Dropbox for Business에서 Cloud Edition 사용

Dropbox for Business를 사용하는 Cloud Edition은 기본 Dropbox 외에 추가적인 기능을 제공합니다.

- 팀원 계정 원격 삭제
- VE Server v8.4 이상에서는 업무용 및 개인용 Dropbox 폴더가 보호되는 방법을 제어하는 정책을 설정할 수 있습니다. 회사에서 업무 및 개인 계정을 모두 허용할 경우 최종 사용자는 각 계정 유형의 암호화를 이해해야 합니다. **업무 및 개인 계정을 위한 정책**을 참조하십시오.

업무 및 개인 계정을 위한 정책

회사에 팀원이 업무 및 개인 계정 중 어떤 것을 사용할 수 있는지에 대한 지침이 있을 수 있습니다. 또한 회사에서 특정 사용자가 업무 및 개인 계정을 소유하도록 허용할 수도 있습니다.

① 노트:

회사에서 업무 및 개인 계정을 모두 허용하고 최종 사용자가 둘 다 사용하도록 선택할 경우 사용자는 두 계정 유형의 폴더 관리를 이해하고 있어야 합니다.

다음 표에서는 EE Server/VE Server 유형 및 정책을 기반으로 암호화에 대해 설명합니다.

암호화	서버 유형 및 정책	배포 고려 사항
모든 업무 및 개인 파일과 폴더를 암호화합니다.	VE Server(v8.4 이전) 또는 EE Server 또는 VE Server(v8.4 이상) 방법 정책 > Dropbox 개인 폴더 암호화 > 참 으로 설정 (참이 기본값임)	Cloud Edition이 배포되기 전에 사용자는 클라우드로 동기화 폴더에 있는 기존 업무 파일을 동기화 폴더 외부의 위치로 백업해야 합니다. 암호화되지 않은 상태로 유지해야 하는 개인 파일이 있는 사용자는 파일을 업무 동기화 폴더 외부로 이동하거나 업무 동기화 클라이언트에서 개인 계정의 연결을 해제해야 합니다. Cloud Edition을 배포한 후에 Cloud Edition을 실행하는 컴퓨터나 장치에서만 클라우드 파일과 폴더를 볼 수 있습니다. 개인 폴더가 우발적으로 암호화된 경우에는 Cloud Edition 사용 설명서에서 "개인 계정의 폴더 암호 해독"을 참조하십시오.
모든 업무 계정 파일 및 폴더를 암호화합니다. 개인 계정 파일 및 폴더를 암호화하지 않은 상태로 유지하도록 허용합니다.	VE Server(v8.4 이상) 방법 정책 > Dropbox 개인 폴더 암호화 > 거짓 으로 설정	선택 사항인 Dropbox 개인 폴더 메시지 암호화 정책을 사용하여 사용자에게 개인 계정에 업무 파일을 저장하지 말라 는 사용자 지정된 메시지를 표시합니다. 이러한 파일은 보호되지 않기 때문입니다. 이 메시지는 다음과 같은 경우에 표시됩니다. · 사용자가 로그인할 때 · 사용자가 새 파일 또는 폴더를 생성하거나 개인 Dropbox 계정에 추가할 때 끝점 또는 끝점 그룹에 대해 Dropbox 개인 폴더 암호화 정책을 거짓 으로 설정

정하면 해당 끝점에 있는 모든 사용자의 개인 계정이 암호화되지 않은 상태로 유지됩니다.

업무 및 개인 폴더

회사에 Dropbox for Business가 있고 최종 사용자가 업무 및 개인 폴더를 소유할 수 있도록 허용할 경우 최종 사용자가 보호되지 않은 중요한 파일을 업무 폴더에 복사할 경우에 대비해 보고서를 실행하여 모든 업무 파일에 .xen 파일 확장자가 있는지 확인해야 할 수도 있습니다. [Cloud Edition](#) 문제 해결을 참조하십시오.

팀원 계정 원격 삭제

회사에 Dropbox for Business가 있으면 회사 Dropbox for Business 팀 계정에서 원격으로 팀원을 제거할 수 있습니다(예: 사용자가 퇴사하는 경우). 팀원의 계정과 연결된 파일 및 폴더가 계정에서 사용되는 모든 장치에서 제거됩니다. 이렇게 하면 해당 파일에 대한 사용자의 액세스 권한이 취소됩니다.

전제조건

- 원격 삭제를 수행하기 전에 팀원 계정에서 회사나 기타 Dropbox for Business 팀원에게 필요할 수 있는 파일 또는 폴더를 백업해야 합니다.
- Dropbox for Business 관리자만 Dropbox for Business 계정을 원격 삭제할 수 있습니다.
- 최종 사용자는 미리 Cloud Edition을 활성화하고 Dropbox for Business에 연결해야 합니다.

원격 관리 콘솔에서 등록

Dropbox for Business 관리자 한 명만 등록하면 됩니다.

- 1 원격 관리 콘솔의 왼쪽 창에서 **설정**을 선택합니다.
- 2 **클라우드** 탭을 클릭합니다.
- 3 **등록**을 클릭합니다. Dropbox for Business 사이트로 브라우저가 열립니다.
- 4 메시지가 나타나면 Dropbox for Business 관리자 계정을 사용하여 Dropbox에 로그인합니다.
- 5 **허용**을 클릭하여 Cloud Edition에 대해 액세스를 허용합니다. Dropbox 권한이 VE Server에 부여되었음을 나타내는 확인 페이지가 표시됩니다.
- 6 원격 관리 콘솔에서 **설정 > 클라우드**로 돌아가 페이지를 새로 고칩니다. 관리자 이름이 표시됩니다.

① 노트:

일반적으로 가장 좋은 방법은 등록을 취소하지 않는 것입니다. 그러나 Dropbox for Business 팀에서 팀원을 제거하기 위한 Dropbox for Business 관리자의 권한을 무효화하려면 **등록 해제**를 클릭합니다.

팀원 계정 원격 삭제

원격 삭제 옵션은 등록된 Dropbox for Business 팀원 계정에서만 사용할 수 있습니다. 사용자 계정에 대해 원격 삭제 옵션이 표시되지 않으면 사용자가 Dropbox for Business 계정에 등록하지 않는 것입니다.

- 1 원격 관리 콘솔의 왼쪽 창에서 **채우기 > 사용자**를 선택합니다.
- 2 특정 사용자를 검색합니다.
- 3 **사용자 세부 정보** 페이지에 액세스합니다.
- 4 명령 열에서 **원격 삭제**를 클릭합니다.

① 노트:

팀원 계정을 원격 삭제하기 전에 이 계정에서 회사나 기타 **Dropbox for Business** 팀원에게 필요할 수 있는 파일 또는 폴더를 백업해야 합니다.

- 5 원격 삭제를 확인하는 페이지에서 **예**를 클릭합니다. 사용자 세부 정보 페이지에 원격 삭제가 수행된 날짜가 나열됩니다.



- Dropbox for Business 관리자 콘솔 멤버 페이지에서 팀원 목록을 새로 고칩니다. 목록에서 사용자가 제거됩니다. **제거된 구성원** 탭을 선택하여 어떤 사용자가 제거되었는지 볼 수 있습니다.

보고서 실행

Cloud Edition 환경에 대한 보고서는 Compliance Reporter를 통해 사용할 수 있습니다. 다음과 같은 내용을 설명하는 보고서를 사용할 수 있습니다.

- 사용자 활성화
- 장치에서 적용된 정책
- 암호화된 파일에서 수행한 작업
- Dropbox for Business 파일 암호화 상태

보고서 실행에 대한 자세한 내용은 *Compliance Reporter 도움말*을 참조하십시오.

① 노트:

보안 상의 이유로 모바일 장치의 로그는 사용할 수 없습니다.



모든 클라이언트 - 문제 해결

- 마스터 설치 프로그램 로그 파일은 C:\ProgramData\Dell\Dell Data Protection\Installer에 있습니다.
- Windows는 로그인된 사용자에게 대해 고유한 하위 설치 프로그램 설치 로그 파일을 C:\Users\- Windows는 로그인된 사용자에게 대해 Visual C++ 등과 같은 클라이언트 필수 구성 요소의 로그 파일을 C:\Users\- 설치 대상 컴퓨터에 설치되는 Microsoft .Net 버전을 확인하려면 <http://msdn.microsoft.com>에 있는 지침을 따르십시오.
전체 버전의 Microsoft .Net Framework 4.5를 설치하려면 <https://www.microsoft.com/en-us/download/details.aspx?id=30653>으로 이동하십시오.
- 설치 대상 컴퓨터에 Dell Data Protection | Access가 이전에 설치된 적이 있거나 현재 설치되어 있는 경우 *Dell Data Protection | Security Tools 호환성*을 참조하십시오. DDPIA는 이 제품군과 호환되지 않습니다.

Encryption 및 Server Encryption 클라이언트 문제 해결

Windows 10 Anniversary Update로 업그레이드

Windows 10 Anniversary Update 버전으로 업그레이드하려면 다음 문서의 지침을 따르십시오. <http://www.dell.com/support/article/us/en/19/SLN298382>.

서버 운영 체제에서 활성화

서버 운영 체제에 Encryption이 설치되어 있는 경우 활성화를 위해 두 단계의 활성화가 필요합니다(초기 활성화 및 장치 활성화).

초기 활성화 문제 해결

다음과 같은 경우에 초기 활성화에 실패합니다.

- 제공된 자격 증명을 사용하여 유효한 UPN을 구성할 수 없습니다.
- 엔터프라이즈 자격 증명 모음에서 자격 증명을 찾을 수 없습니다.
- 활성화에 사용되는 자격 증명에 도메인 관리자의 자격 증명입니다.

오류 메시지: 사용자 이름을 알 수 없거나 암호가 잘못되었습니다.

사용자 이름 또는 암호가 일치하지 않습니다.

가능한 해결 방법: 다시 로그인하여 사용자 이름과 암호를 정확히 입력합니다.

오류 메시지: 사용자 계정에 도메인 관리 권한이 없기 때문에 활성화에 실패했습니다.

활성화에 사용된 자격 증명에 도메인 관리자 권한이 없거나 관리자의 사용자 이름이 UPN 형식이 아닙니다.



가능한 해결 방법: "활성화" 대화상자에 도메인 관리자의 자격 증명을 UPN 형식으로 입력합니다.

오류 메시지: 서버와의 연결을 설정할 수 없습니다.

또는

The operation timed out.

Server Encryption이 DDP Security Server에 대한 HTTPS를 통해 포트 8449와 통신할 수 없습니다.

가능한 해결 방법

- 네트워크를 직접 연결하고 다시 활성화해 보십시오.
- VPN에 연결된 경우, 네트워크에 직접 연결하고 다시 활성화해 보십시오.
- DDP Server URL이 관리자가 제공한 URL과 일치하는지 확인합니다. 사용자가 설치 프로그램에 입력한 URL 및 기타 데이터는 레지스트리에 저장됩니다. [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] 및 [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]에서 데이터가 정확한지 확인합니다.
- 서버의 네트워크 연결을 끊습니다. 서버를 다시 시작하고 네트워크에 다시 연결합니다.

오류 메시지: 서버가 이 요청을 지원할 수 없으므로 활성화에 실패했습니다.

가능한 해결 방법

- Server Encryption을 레거시 서버에 대해 활성화할 수 없습니다. DDP Server 버전이 9.1 이상이어야 합니다. 필요한 경우 DDP Server를 9.1 버전 이상으로 업그레이드하십시오.
- DDP Server URL이 관리자가 제공한 URL과 일치하는지 확인합니다. 사용자가 설치 프로그램에 입력한 URL 및 기타 데이터는 레지스트리에 저장됩니다.
- [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] 및 [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]에서 데이터가 정확한지 확인합니다.

초기 활성화 프로세스

다음 다이어그램은 성공적인 초기 활성화를 보여 줍니다.

Server Encryption의 초기 활성화 프로세스를 위해서는 활성 사용자가 서버에 액세스해야 합니다. 로그인된 사용자는 도메인 또는 비도메인, 원격 데스크톱 연결 또는 대화식 사용자 유형 중 하나가 될 수 있지만, 반드시 도메인 관리자 자격 증명에 액세스할 수 있는 권한이 있어야 합니다.

활성화 대화 상자는 다음 두 가지 상황 중 하나가 발생하면 표시됩니다.

- 새(관리되지 않은) 사용자가 컴퓨터에 로그인합니다.
- 새 사용자가 시스템 트레이에서 Encryption 클라이언트 아이콘을 마우스 오른쪽 단추로 클릭하고 Activate Dell Data Protection | Encryption(Dell Data Protection | Encryption 활성화)을 선택합니다.

초기 활성화 프로세스는 다음과 같습니다.

- 1 사용자가 로그인합니다.
- 2 새(관리되지 않은) 사용자가 감지되고 Activate(활성화) 대화 상자가 표시됩니다. 사용자가 **Cancel(취소)**을 클릭합니다.
- 3 사용자가 Server Encryption의 About(정보) 상자를 열어 Server(서버) 모드에서 실행 중인지 확인합니다.
- 4 사용자가 시스템 트레이에서 Encryption 클라이언트 아이콘을 마우스 오른쪽 단추로 클릭하고 **Activate Dell Data Protection | Encryption(Dell Data Protection | Encryption 활성화)**을 선택합니다.
- 5 사용자가 Activate(활성화) 대화 상자에서 도메인 관리자 자격 증명을 입력합니다.

① 노트: 도메인 관리자 자격 증명에 대한 요구 사항은 지원되지 않는 다른 서버 환경으로 Server Encryption이 돌아오되지 않도록 하기 위한 안전 조치입니다. 도메인 관리자 자격 증명에 대한 요구 사항을 비활성화하려면 **시작하기 전에**를 참조하십시오.

- 6 DDP Server는 엔터프라이즈 자격 증명 모음(Active Directory 또는 동급)에 자격 증명이 있는지 확인해 자격 증명에 도메인 관리자 자격 증명인지 확인합니다.
- 7 UPN은 자격 증명을 사용하여 구성됩니다.



- 8 DDP Server는 UPN을 사용하여 가상 서버 사용자를 위한 새 사용자 계정을 생성하고 DDP Server의 자격 증명 모음에 자격 증명을 저장합니다.

가상 서버 사용자 계정은 Encryption 클라이언트에만 독점적으로 사용됩니다. 서버를 인증하고, Common 암호화 키를 처리하고, 정책 업데이트를 수신하는 데 사용됩니다.

① 노트: 암호 및 DPAPI 인증은 이 계정에 사용되지 않으므로 가상 서버 사용자만 컴퓨터의 암호화 키에 액세스할 수 있습니다. 이 계정은 컴퓨터나 도메인의 기타 사용자 계정에 해당되지 않습니다.

- 9 활성화가 성공적으로 완료되고 사용자가 컴퓨터를 다시 시작하면 활성화의 두 번째 부분인 활성화 및 장치 활성화가 시작됩니다.

인증 문제 해결 및 장치 활성화

다음과 같은 경우에 장치 활성화에 실패합니다.

- 초기 활성화가 실패했습니다.
- 서버와의 연결을 설정할 수 없습니다.
- 신뢰 인증서의 유효성을 검사할 수 없습니다.

활성화 후에 컴퓨터가 다시 시작되면 Server Encryption은 가상 서버 사용자로 자동 로그인되며 DDP Enterprise Server의 컴퓨터 키를 요청합니다. 사용자가 로그인하기 전에 이러한 상황이 발생합니다.

- About(정보) 대화상자를 열어 Server Encryption이 인증되었으며 서버 모드임을 확인합니다.
- Shield ID가 빨간색이면 암호화가 아직 활성화되지 않은 것입니다.
- Remote Management Console에서 Server Encryption이 설치된 서버 버전이 *서버용 Shield*로 나열됩니다.
- 네트워크 장애로 인해 컴퓨터 키 검색에 실패할 경우 Server Encryption은 운영 체제에 네트워크 알림을 등록합니다.
- 컴퓨터 키 검색에 실패할 경우:
 - 가상 서버 사용자가 여전히 성공적으로 로그인할 수 있습니다.
 - 지정된 시간 간격으로 키 검색이 시도되도록 *네트워크 장애 시 검색 재시도* 정책을 설정합니다.

네트워크 장애 시 검색 재시도 정책에 대한 자세한 내용은 Remote Management Console의 AdminHelp를 참조하십시오.

인증 및 장치 활성화 프로세스

다음 다이어그램은 성공적인 인증 및 장치 활성화를 보여 줍니다.

- 1 성공적인 초기 활성화 이후에 다시 시작하면 Server Encryption이 있는 컴퓨터가 가상 서버 사용자 계정을 사용하여 자동으로 인증하고 서버 모드에서 Encryption 클라이언트를 실행합니다.
- 2 컴퓨터가 DDP Server와 비교해 장치 활성화 상태를 확인합니다.
 - 컴퓨터가 이전에 장치 활성화되지 않은 경우에는 DDP Server가 컴퓨터에 MCID, DCID 및 신뢰 인증서를 할당하고 DDP Server의 자격 증명 모음에 모든 정보를 저장합니다.
 - 컴퓨터가 이전에 장치 활성화된 경우에는 DDP Server가 신뢰 인증서를 확인합니다.
- 3 DDP Server가 서버에 신뢰 인증서를 할당하고 나면 서버가 해당 암호화 키에 액세스할 수 있습니다.
- 4 장치가 성공적으로 활성화됩니다.

① 노트: 서버 모드에서 실행할 경우 Encryption 클라이언트가 장치 활성화에 사용된 것과 동일한 인증서에 액세스하여 암호화 키에 액세스해야 합니다.

(선택 사항) Encryption Removal Agent 로그 파일 생성

- 설치 제거 프로세스를 시작하기 전에 선택적으로 Encryption Removal Agent 로그 파일을 생성할 수 있습니다. 이 로그 파일은 설치 제거/암호 해독 작업의 문제를 해결하는 데 유용합니다. 설치 제거 프로세스 중 파일을 암호 해독하지 않으려면 이 로그 파일을 만들지 않아도 됩니다.



- Encryption Removal Agent 로그 파일은 Encryption Removal Agent 서비스가 실행될 때까지 생성되지 않으며, 이 서비스는 컴퓨터를 다시 시작해야 실행됩니다. 클라이언트가 성공적으로 설치 제거되고 컴퓨터가 완전히 암호 해독되면 로그 파일이 영구적으로 삭제됩니다.
- 로그 파일 경로는 **C:\ProgramData\Dell\Dell Data Protection\Encryption**입니다.
- 암호 해독 대상 컴퓨터에 다음과 같은 레지스트리 항목을 만듭니다.

[HKLM\Software\Credant\DecryptionAgent]

"LogVerbosity"=dword:2

- 0: 로깅하지 않음
- 1: 서비스가 실행되지 않는 오류 로깅
- 2: 전체 데이터 암호 해독이 안 되는 오류 로깅(권장 수준)
- 3: 모든 암호 해독 불륨 및 파일에 대한 정보 로깅
- 5: 디버깅 정보 로깅

TSS 버전 찾기

- TSS는 TPM과 상호 작용하는 요소입니다. TSS 버전을 찾으려면 **C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcstd_win32.exe**(기본 위치)로 이동합니다. 파일을 마우스 오른쪽 단추로 클릭하고 **Properties(속성)**를 선택합니다. **Details(세부 정보)** 탭에서 파일 버전을 확인합니다.

EMS와 PCS 상호 작용

미디어가 읽기 전용이 아니고 포트가 차단되지 않았는지 확인하려면

포트 제어 시스템과 상호 작용하는 EMS Shield로 보호되지 않은 미디어에 대한 액세스 정책- 저장소 클래스: 외부 드라이브 제어 정책. 보호되지 않은 미디어 정책에 EMS 액세스를 **전체 액세스**로 설정하려는 경우, 스토리지 클래스: 외부 드라이브 제어 정책 또한 **전체 액세스**로 설정되어 미디어가 읽기 전용으로 설정되지 않고 포트가 차단되지 않았는지 확인합니다.

CD/DVD에 쓴 데이터를 암호화하려면

- EMS 외부 미디어 암호화 = 참을 설정합니다.
- EMS CD/DVD 암호화 제외 = 거짓을 설정합니다.
- 하위 클래스 스토리지: 광학 드라이브 제어 = UDF 전용으로 설정합니다.

WSScan 사용

- WSScan을 사용하면 Encryption 클라이언트를 설치 제거할 때 모든 데이터가 해독되는지 확인할 수 있을 뿐 아니라 암호화 상태를 보고 암호화해야 하는 암호화되지 않은 파일을 식별할 수 있습니다.
- 이 유틸리티를 실행하려면 관리자 권한이 필요합니다.

WSScan

- 1 Dell 설치 미디어에서 스캔할 Windows 컴퓨터로 WSScan.exe를 복사합니다.
- 2 해당 위치에서 명령줄을 실행하고 프롬프트가 표시되면 **wsscan.exe**를 입력합니다. WSScan이 실행됩니다.
- 3 **Advanced(고급)**를 클릭합니다.
- 4 드롭다운 메뉴에서 스캔할 드라이브의 유형을 선택합니다(**모든 드라이브, 고정 드라이브, 이동식 드라이브 또는 CDROM/DVDROM**).
- 5 드롭다운 메뉴에서 원하는 암호화 보고서 유형을 선택합니다(**암호화된 파일, 암호화되지 않은 파일, 모든 파일 또는 위반되는 암호화되지 않은 파일**).



- **암호화된 파일** - Encryption 클라이언트를 설치 제거할 때 모든 데이터가 해독되는지 확인합니다. 암호 해독 정책 업데이트 실행 등의 기존 데이터 암호 해독 프로세스를 따릅니다. 데이터를 암호 해독한 후에는 설치 제거를 준비하는 단계에서 재시작을 수행하기 전에 WSScan를 실행하여 모든 데이터가 암호 해독되었는지 확인합니다.
- **암호화되지 않은 파일** - 암호화되지 않은 파일을 식별합니다. 파일을 암호화해야 하는지 여부(Y/N)가 함께 표시됩니다.
- **모든 파일** - 암호화된 파일과 그렇지 않은 모든 파일을 나열합니다. 파일을 암호화해야 하는지 여부(Y/N)가 함께 표시됩니다.
- **위반되는 암호화되지 않은 파일** - 암호화해야 하지만 암호화되지 않은 파일을 식별합니다.

6 **Search(검색)**를 클릭합니다.

또는

- 1 **Advanced(고급)**를 클릭하여 보기 모드를 **Simple(간단히)**로 전환하여 특정 폴더를 스캔합니다.
- 2 검색 설정으로 이동하고 **Search Path(경로 검색)** 필드에 폴더 경로를 입력합니다. 이 필드를 사용할 경우 드롭다운 상자에 선택한 사항이 무시됩니다.
- 3 WSScan 출력을 파일에 쓰지 않으려는 경우 **Output to File(파일로 출력)** 확인란의 선택을 취소합니다.
- 4 필요할 경우 경로에서 기본 경로와 파일 이름을 변경합니다.
- 5 기존 WSScan 출력 파일을 덮어쓰지 않으려는 경우 **Add to Existing File(기존 파일에 추가)**을 선택합니다.
- 6 다음과 같이 출력 형식을 선택합니다.
 - 스캔된 출력을 보고서 형식의 목록으로 표시하려면 "보고서 형식"을 선택합니다. 이 모드가 기본 형식입니다.
 - 스프레드시트 응용 프로그램으로 가져올 수 있는 출력을 사용하려면 "값 구분 파일"을 선택합니다. 기본 구분 기호는 "|"이며, 최대 9자의 영숫자, 공백 또는 키보드 문자 부호 문자로 변경할 수 있습니다.
 - 각 값을 큰따옴표 표시 안에 포함하려면 "따옴표 붙은 값"을 선택합니다.
 - 암호화된 각 파일에 대해 고정 길이의 정보 행이 연속적으로 포함되어 있고 구분 기호로 구분되지 않은 출력을 사용하려면 "고정 너비 파일"을 선택합니다.

7 **Search(검색)**를 클릭합니다.

검색을 중지하려면 **Stop Searching(검색 중지)**을 클릭합니다. 표시된 메시지를 지우려면 **Clear(지우기)**를 클릭합니다.

WSScan 명령줄 사용법

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r] [-u[a] [-l[v]]] [-d<delimiter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

스위치	의미
드라이브	스캔할 드라이브입니다. 지정되지 않으면, 모든 고정된 로컬 하드 드라이브가 기본적으로 스캔됩니다. 매핑된 네트워크 드라이브일 수 있습니다.
-ta	모든 드라이브 스캔
-tf	고정 드라이브 스캔(기본값)
-tr	이동식 드라이브 스캔
-tc	CDROM/DVDROM 스캔
-s	자동 작업
-o	출력 파일 경로
-A	출력 파일에 첨부합니다. 기본적으로 출력 파일이 잘립니다.
-f	보고서 형식 지정자(보고서, 고정, 구분)
-r	관리자 권한 없이 WSScan을 실행합니다. 이 모드를 사용하는 경우 일부 파일이 표시되지 않을 수 있습니다.



스위치	의미
-u	암호화되지 않은 파일을 출력 파일에 포함합니다. 이 스위치에서는 순서가 중요합니다. "u"가 첫 번째, "a"가 두 번째(또는 생략) 순서여야 합니다. "-" 또는 "v"가 마지막으로 와야 합니다.
-u-	암호화되지 않은 파일만 출력 파일에 포함합니다.
-ua	암호화되지 않은 파일도 보고하지만 모든 사용자 정책을 사용하여 "should" 필드를 표시합니다.
-ua-	암호화되지 않은 파일만 보고하지만 모든 사용자 정책을 사용하여 "should" 필드를 표시합니다.
-uv	정책을 위반하는 암호화되지 않은 파일만 보고합니다(Is=No / Should=Y).
-uav	모든 사용자 정책을 사용하여 정책을 위반하는 암호화되지 않은 파일만 보고합니다(Is=No / Should=Y).
-d	구분된 출력의 값 구분 기호로 사용할 항목을 지정합니다.
-q	구분된 출력에서 따옴표로 묶어야 하는 값을 지정합니다.
-e	구분된 출력에 확장된 암호화 필드를 포함합니다.
-x	디렉토리를 스캔에서 제외합니다. 여러 개의 항목을 제외할 수 있습니다.
-y	디렉터리 간 절전 모드(초)입니다. 이 스위치를 사용하면 스캔 속도가 느려지지만 CPU의 응답 기능이 향상될 수 있습니다.

WSScan 출력

암호화된 파일에 대한 WSScan 정보에는 다음 정보가 포함되어 있습니다.

출력 예제:

```
[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" is still AES256 encrypted
```

출력	의미
날짜/시간 스탬프	파일을 스캔한 날짜와 시간입니다.
암호화 유형	파일 암호화에 사용한 암호화 유형입니다. SysData: SDE 암호화 키입니다. User: 사용자 암호화 키입니다. Common: 일반적인 암호화 키입니다. WSScan은 공유를 위한 암호화를 사용하여 암호화된 파일을 보고하지 않습니다.
DCID	장치 ID입니다. 위의 예에서와 같이, " 7vdlxrsb "입니다. 매핑된 네트워크 드라이브를 스캔하는 경우 스캔 보고서가 DCID를 반환하지 않습니다.
UCID	사용자 ID입니다. 위의 예에서와 같이, " _SDENCR_ "입니다.

출력	의미
	UCID는 해당 컴퓨터의 모든 사용자가 공유합니다.
파일	암호화된 파일의 경로입니다. 위의 예에서와 같이, " c:\temp\Dell - test.log "입니다.
알고리즘	파일을 암호화하는 데 사용하는 암호화 알고리즘입니다. 위의 예에서와 같이, " is still AES256 encrypted "입니다. Rijndael 128 Rijndael 256 AES 128 AES 256 3DES

WSProbe 사용

이 검색 유틸리티는 EMS 정책을 제외하고 모든 버전의 Encryption 클라이언트에서 사용할 수 있습니다. 이 검색 유틸리티의 기능은 다음과 같습니다.

- 암호화된 컴퓨터를 스캔하거나 스캔 일정을 예약합니다. 검색 유틸리티는 워크스테이션 스캔 우선순위 정책을 준수합니다.
- 현재 사용자의 Application Data Encryption 목록을 임시로 비활성화하거나 재활성화합니다.
- 권한 부여된 목록에서 프로세스 이름을 추가하거나 제거합니다.
- Dell ProSupport의 지시에 따라 문제를 해결합니다.

Data Encryption 접근 방식

Windows 장치에서 데이터를 암호화하는 정책을 지정하는 경우 다음과 같은 방법을 이용할 수 있습니다.

- 첫 번째 방법은 클라이언트의 기본 동작을 수락하는 것입니다. 일반 암호화된 폴더 또는 사용자 암호화된 폴더에 폴더를 지정하거나 "내 문서" 암호화, Outlook 개인 폴더 암호화, 임시 파일 암호화, 임시 인터넷 파일 암호화 또는 Windows 페이징 파일 암호화를 선택됨으로 설정하는 경우 영향을 받는 해당 파일은 생성될 때 또는 관리되지 않는 사용자가 파일을 생성한 후에 관리되는 사용자가 로그인할 때 암호화됩니다. 또한 클라이언트는 폴더 이름이 바뀌거나 정책 변경 내용을 수신하면 이러한 정책과 관련되었거나 지정된 폴더를 암호화 또는 암호 해독할 수 있는지 스캔합니다.
- 로그인 시 워크스테이션 스캔을 True(참)로 설정할 수도 있습니다. 로그인 시 워크스테이션 스캔을 True(참)로 설정하면, 클라이언트는 사용자가 로그인할 때 현재와 이전에 암호화된 폴더에서 파일이 사용자 정책으로 암호화되어 있는 방식을 비교하여 필요에 따라 변경합니다.
- 암호화 조건은 충족하지만 암호화 정책이 적용되기 전에 생성된 파일을 암호화하되 스캔 성능에는 영향을 주지 않으려면 이 유틸리티를 사용하여 컴퓨터를 스캔하거나 스캔 일정을 예약할 수 있습니다.

전제조건

- 작업할 Windows 장치가 암호화되어 있어야 합니다.
- 작업할 사용자가 로그인되어 있어야 합니다.

검색 유틸리티 사용

WSProbe.exe는 설치 미디어에 있습니다.

구문

wsprobe [path]



wsprobe [-h]

wsprobe [-f path]

wsprobe [-u n] [-x process_names] [-i process_names]

매개 변수

매개변수	해당
경로	(선택사항) 암호화/암호 해독할 수 있는지 스캔할 장치에서 특정 경로를 지정할 수 있습니다. 경로를 지정하지 않으면 이 유틸리티는 암호화 정책과 관련된 모든 폴더를 스캔합니다.
-h	명령줄 도움말을 봅니다.
-f	Dell ProSupport의 지시에 따라 문제를 해결합니다.
-u	사용자의 Application Data Encryption 목록을 임시로 비활성화하거나 재활성화합니다. 이 목록은 현재 사용자에게 대해 암호화 활성화됨이 선택되어 있는 경우에만 적용됩니다. 비활성화하려면 0을 지정하고 재활성화하려면 1을 지정하십시오. 해당 사용자에게 적용되는 현재 정책이 다음 로그인 시에 복원됩니다.
-x	권한 부여된 목록에 프로세스 이름을 추가합니다. 이 목록에 있는 컴퓨터 및 설치 프로그램 프로세스 이름과 이 매개변수 또는 HKLM\Software\CREDANT\CMGShield\EUWPrivilegedList를 사용하여 추가한 프로세스 이름(Application Data Encryption 목록에 지정된 경우)은 무시됩니다. 프로세스 이름은 쉼표로 구분합니다. 목록에 하나 이상의 공백이 있는 경우 큰따옴표로 목록을 묶습니다.
-i	권한 부여된 목록에 이전에 추가된 프로세스 이름을 제거합니다(하드 코딩된 프로세스 이름은 제거할 수 없음). 프로세스 이름은 쉼표로 구분합니다. 목록에 하나 이상의 공백이 있는 경우 큰따옴표로 목록을 묶습니다.

Encryption Removal Agent 상태 확인

Encryption Removal Agent에서 다음과 같이 해당 상태가 서비스 패널(시작 > 실행... > services.msc > 확인)의 설명 영역에 표시됩니다. 서비스를 정기적으로 새로 고쳐(서비스 강조 표시 > 마우스 오른쪽 단추 클릭 > 새로 고침) 상태를 업데이트합니다.

- **SDE 비활성화 대기 중** - Encryption 클라이언트가 설치 또는 구성되어 있거나, 둘 다에 해당합니다. Encryption 클라이언트가 제거 될 때까지 암호 해독이 시작되지 않습니다.
- **초기 스윙** - 서비스가 초기 스윙을 실행하면서 암호화된 파일과 바이트 수를 계산합니다. 초기 스윙은 한 번만 실행됩니다.
- **암호 해독 스윙** - 서비스가 파일을 암호 해독하고 있으며 잠겨 있는 파일의 암호 해독을 요청할 수도 있습니다.
- **재부팅 시 암호 해독(부분적)** - 암호 해독 스윙이 완료되었으며 다음에 다시 시작하면 잠겨 있는 파일이 일부만 암호 해독됩니다.
- **재부팅 시 암호 해독** - 암호 해독 스윙이 완료되었으며 다음에 다시 시작하면 잠긴 파일이 모두 암호 해독됩니다.
- **모든 파일을 암호 해독할 수 없음** - 암호 해독 스윙이 완료되었지만 모든 파일을 암호 해독할 수 없습니다. 이 상태는 다음 중 하나가 발생했음을 의미합니다.
 - 잠긴 파일이 너무 크거나 잠금 해제를 요청하는 중 오류가 발생하여 잠긴 파일의 암호 해독을 예약할 수 없습니다.
 - 파일을 암호 해독하는 중 입력/출력 오류가 발생했습니다.
 - 정책으로 파일을 암호 해독할 수 없습니다.
 - 파일을 암호화해야 한다는 내용이 표시되었습니다.
 - 암호 해독 스윙 중 오류가 발생했습니다.
 - LogVerbosity=2(또는 이상)가 설정되어 있으면 항상 로그 파일이 생성됩니다(로그이 구성된 경우). 문제를 해결하려면 로그의 자세한 정도를 2로 설정하고 Encryption Removal Agent 서비스를 다시 시작해서 암호 해독 스윙을 한 번 더 강제 실행합니다. 지침을 보려면 (선택 사항) [Encryption Removal Agent 로그 파일 생성](#)을 참조하십시오.
- **완료** - 암호 해독 스윙이 완료되었습니다. 다음에 다시 시작할 때 서비스, 실행 파일, 드라이버 및 드라이버 실행 파일이 모두 삭제 되도록 예약됩니다.



SED 클라이언트 문제 해결

초기 액세스 코드 정책 사용

- 이 정책은 네트워크 액세스를 사용할 수 없을 경우 컴퓨터에 로그인하기 위해 사용됩니다. 즉, EE Server/VE Server와 AD 둘 다에 액세스할 수 없는 경우입니다. 초기 액세스 코드 정책은 반드시 필요한 경우에만 사용하십시오. Dell에서는 이 방법을 사용하여 로그인하는 것을 권장하지 않습니다. 초기 액세스 코드 정책을 사용할 경우 사용자 이름, 도메인 및 암호를 사용하여 로그인하는 일반적인 로그인 방법과 동일한 보안 수준이 제공되지 않습니다.

최종 사용자가 초기 액세스 코드를 사용하여 활성화된 경우 로그인 방법의 보안이 약화될 뿐 아니라 이 컴퓨터에서 활성화하는 해당 사용자의 EE Server/VE Server에 레코드가 없습니다. 따라서 최종 사용자가 틀린 암호를 입력하거나 자체 질문에 틀린 대답을 입력할 경우 EE Server/VE Server에서 응답 코드를 생성할 방법이 없습니다.

- 초기 액세스 코드는 활성화 이후 즉시 **한** 번만 사용할 수 있습니다. 최종 사용자가 로그인한 후에는 초기 액세스 코드를 다시 사용할 수 없습니다. 초기 액세스 코드를 입력한 후에 발생하는 첫 번째 도메인 로그인도 캐시되며 초기 액세스 코드 입력 필드가 다시 표시되지 않습니다.
- 초기 액세스 코드는 오직 다음과 같은 경우에만 표시됩니다.
 - 사용자가 PBA 내에서 등록한 적이 없는 경우
 - 클라이언트가 네트워크 또는 EE Server/VE Server에 연결되지 않는 경우

초기 액세스 코드 사용

- 원격 관리 콘솔에서 **Initial Access Code(초기 액세스 코드)** 정책에 대한 값을 설정합니다.
- 정책을 저장 및 커밋합니다.
- 로컬 컴퓨터를 시작합니다.
- 액세스 코드 화면이 표시되면 **Initial Access Code(초기 액세스 코드)**를 입력합니다.
- blue arrow(파란색 화살표)**를 클릭합니다.
- 법적 고지 사항 화면이 표시되면 **OK(확인)**을 클릭합니다.
- 이 컴퓨터의 사용자 자격 증명을 사용하여 Windows에 로그인합니다. 이러한 자격 증명은 도메인에 포함되어야 합니다.
- 로그인 후 Security Console을 열고 PBA 사용자가 성공적으로 생성되었는지 확인합니다.

상단 메뉴에서 **Log(로그)**를 클릭하고 프로세스가 성공적이었음을 나타내는 <domain\username>에 대한 PBA 사용자가 생성되었습니다라는 메시지를 찾습니다.

- 컴퓨터를 종료하고 다시 시작합니다.
- 로그인 화면에서 이전에 Windows에 로그인하는 데 사용한 사용자 이름, 도메인 및 암호를 입력합니다.

PBA 사용자를 만들 때 사용한 사용자 이름 형식과 동일한 형식을 사용해야 합니다. 따라서 도메인/사용자 이름 형식을 사용한 경우 사용자 이름으로 도메인/사용자 이름을 입력해야 합니다.

- (Credant Manager에만 해당) 질문 및 대답 메시지가 표시되면 알맞게 입력합니다.

blue arrow(파란색 화살표)를 클릭합니다.

- 법적 고지 사항 화면이 표시되면 **Login(로그인)**을 클릭합니다.

이제 Windows가 시작되고 정상적으로 컴퓨터를 사용할 수 있습니다.

문제 해결을 위해 PBA 로그 파일 생성

- PBA 문제를 해결하는 데 PBA 로그 파일이 필요한 경우는 다음과 같습니다.
 - 네트워크에 연결되어 있는데 네트워크 연결 아이콘이 표시되지 않습니다. 로그 파일에 이 문제를 해결하는 DHCP 정보가 포함되어 있습니다.



- EE 서버/VE 서버 연결 아이콘이 표시되지 않습니다. 로그 파일에 EE Server/VE Server 연결 문제를 진단하는 데 도움이 되는 정보가 포함되어 있습니다.
- 올바른 자격 증명을 입력했는데 인증에 실패했습니다. EE 서버/VE 서버 로그에 사용된 로그 파일이 문제를 진단하는 데 도움이 될 수 있습니다.

PBA(레거시 PBA)로 부팅할 때 로그 캡처

- 1 USB 드라이브의 루트 수준에 폴더를 생성하고 이름을 **\CredantSED**로 지정합니다.
- 2 actions.txt라는 파일을 생성하여 **\CredantSED** 폴더에 넣습니다.
- 3 actions.txt에 다음 행을 추가합니다.

get environment

- 4 파일을 저장하고 닫습니다.

컴퓨터 전원이 꺼졌을 때 USB 드라이브를 삽입하지 마십시오. 종료 상태에서 이미 USB 드라이브가 삽입된 경우 USB 드라이브를 제거하십시오.

- 5 컴퓨터를 켜고 PBA에 로그인합니다. 이 단계에서 로그를 수집할 컴퓨터에 USB 드라이브를 삽입합니다.
- 6 USB 드라이브를 삽입하고 5~10초 후 드라이브를 제거합니다.

필요한 로그 파일들이 포함된 **\CredantSED** 폴더에 credpbaenv.tgz 파일이 생성됩니다.

PBA(UEFI PBA)로 부팅할 때 로그 캡처

- 1 USB 드라이브 루트 수준에서 **PBAErr.log**라는 파일을 생성합니다.
- 2 컴퓨터의 전원을 켜기 **전에** USB 드라이브를 삽입합니다.
- 3 로그가 필요한 문제를 재현한 **후에** USB 드라이브를 분리합니다.

PBAErr.log 파일이 업데이트되고 실시간 기록됩니다.

Dell ControlVault 드라이버

Dell ControlVault 드라이버 및 펌웨어 업데이트

출하 시 Dell 컴퓨터에 설치된 Dell ControlVault 드라이버 및 펌웨어는 오래되었으며 다음 절차에 따라 다음 순서대로 업데이트해야 합니다.

클라이언트를 설치하는 동안 Dell ControlVault 드라이버를 업데이트하기 위해 설치 프로그램을 종료하라는 오류 메시지가 표시되면, 이 메시지를 안전하게 해제하여 클라이언트 설치를 계속할 수 있습니다. Dell ControlVault 드라이버 (및 펌웨어)는 클라이언트 설치를 완료한 후에 업데이트할 수 있습니다.

최신 드라이버 다운로드

- 1 support.dell.com으로 이동합니다.
- 2 컴퓨터 모델을 선택합니다.
- 3 **Drivers & Downloads(드라이버 및 다운로드)**를 선택합니다.
- 4 대상 컴퓨터의 **Operating System(운영 체제)**을 선택합니다.
- 5 **Security(보안)** 범주를 확장합니다.
- 6 Dell ControlVault 드라이버를 다운로드하고 저장합니다.
- 7 Dell ControlVault 펌웨어를 다운로드하고 저장합니다.
- 8 필요한 경우, 드라이버와 펌웨어를 대상 컴퓨터에 복사합니다.

Dell ControlVault 드라이버 설치

드라이버 설치 파일을 다운로드한 폴더로 이동합니다.

Dell ControlVault 드라이버를 더블 클릭하여 자동 압축 해제 실행 파일을 시작합니다.





: 반드시 드라이버부터 설치하십시오. 이 문서 생성 시 드라이버의 파일 이름은 **ControlVault_Setup_2MYJC_A37_ZPE.exe**입니다.

Continue(계속)를 클릭하여 시작합니다.

Ok(확인)를 클릭하여 기본 위치인 C:\Dell\Drivers\

Yes(예)를 클릭하여 새 폴더 생성을 허용합니다.

성공적으로 압축 해제했다는 메시지가 표시되면 **Ok(확인)**를 클릭합니다.

압축 해제가 끝나면 파일들이 들어 있는 폴더가 표시될 것입니다. 그렇지 않다면, 파일들을 추출한 폴더로 이동하십시오. 이 경우, 폴더는 **JW22F**입니다.

CVHCI64.MSI를 더블 클릭하여 드라이버 설치 프로그램을 시작합니다. [이 예에서는 **CVHCI64.MSI**가 보기로 나옵니다.(32비트 컴퓨터에서는 CVHCI)]

시작 화면에서 **Next(다음)**를 클릭합니다.

Next(다음)를 클릭하여 기본 위치인 C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\에 드라이버를 설치합니다.

Complete(완료) 옵션을 선택하고 **Next(다음)**를 클릭합니다.

Install(설치)를 클릭하여 드라이버 설치를 시작합니다.

필요에 따라, 설치 프로그램 로그 파일을 표시하기 위해 확인란을 선택합니다. **Finish(마침)**를 클릭하여 마법사를 종료합니다.

드라이버 설치 확인

운영 체제 및 하드웨어 구성에 따라 장치 관리자에 Dell ControlVault 장치 (및 기타 장치)가 있을 것입니다.

Dell ControlVault 펌웨어 설치

- 1 펌웨어 설치 파일을 다운로드한 폴더로 이동합니다.
- 2 Dell ControlVault 펌웨어를 더블 클릭하여 자동 압축 해제 실행 파일을 시작합니다.
- 3 **Continue(계속)**를 클릭하여 시작합니다.
- 4 **Ok(확인)**를 클릭하여 기본 위치인 C:\Dell\Drivers\- 5 **Yes(예)**를 클릭하여 새 폴더 생성을 허용합니다.
- 6 성공적으로 압축 해제했다는 메시지가 표시되면 **Ok(확인)**를 클릭합니다.
- 7 압축 해제가 끝나면 파일들이 들어 있는 폴더가 표시될 것입니다. 그렇지 않다면, 파일들을 추출한 폴더로 이동하십시오. **firmware(펌웨어)** 폴더를 선택합니다.
- 8 **ushupgrade.exe**를 더블 클릭하여 펌웨어 설치 프로그램을 시작합니다.
- 9 **Start(시작)**를 클릭하여 펌웨어 업그레이드를 시작합니다.



: 이전 버전 펌웨어를 업그레이드하는 경우, 관리자 암호를 입력하라는 요청을 받을 수 있습니다. 이 대화 상자가 표시되면 암호로 Broadcom을 입력하고 **Enter**를 클릭합니다.

몇 가지 상태 메시지가 표시됩니다.

- 10 **Restart(재시작)**를 클릭하여 펌웨어 업그레이드를 완료합니다.

Dell ControlVault 드라이버 및 펌웨어 업데이트가 완료됩니다.

Cloud Edition v8.x

세부 정보 화면 사용

세부 정보 화면은 문제 해결이나 지원을 위해 사용할 수 있습니다. 예:

- 경우 사용자지만 해당 폴더를 생성합니다 암호화되지 않는, 상세정보 > 파일 > 폴더를 선택합니다 상태를 확인을 상태.
- 최종 사용자가 지원을 요청할 경우, 고급 세부 정보 화면을 설정하고 이 탭에는 어떤 정책들이 시행되고 있는지 나열되어 있습니다.
- 문제 해결을 위한 로그를 봅니다.

고급 세부 정보 화면 사용

- 를 누른 상태에서 시스템 트레이 아이콘을 클릭한 후 세부 정보...를 선택합니다.
- 파일 및 폴더 외에도 다음이 표시됩니다.

보안: 키, 키 유형 및 상태를 나열합니다.

감사: 모듈, 사용자 ID 및 이벤트 유형을 나열합니다. 정보가 이 감사 로그에서 대기 상태이다가 지정된 간격으로 EE Server/VE Server에 전송됩니다. 관리자는 Compliance Reporter를 사용하여 감사를 위해 보고서를 생성할 수 있습니다.

정책 이름과 값을 나열합니다.

로그 파일 보기

- 세부 정보 화면의 왼쪽 하단에서 로그 보기를 클릭합니다.

로그 파일은 C:\ProgramData\Dell\Dell Data Protection\Cloud Edition에도 있습니다.

임시 폴더 관리 권한 제공

사용자가 Cloud Edition을 설치하기 전에 파일을 업로드한 경우 일부 사용자에게 임시 폴더 관리 권한을 제공할 수 있습니다.

- 1 특정 끝점에 대한 폴더 관리 활성화된 정책을 참으로 설정합니다.
- 2 사용자에게 기존의 폴더에 대해 암호화를 수동으로 설정하도록 지시합니다. 파일이 클라우드로 동기화되면 파일이 암호화됩니다.
- 3 폴더가 암호화되면 이 끝점에 대한 폴더 관리 활성화된 정책을 거짓으로 설정합니다.

자주 묻는 질문

질문

- 파일 이름 단독화 정책을 GUID에서 확장자만으로 변경했습니다. 그런데 이전에 동기화하던 폴더가 여전히 이러한 파일을 GUID 파일 이름의 다른 형식으로 암호화하고 있습니다. 그 이유는 무엇입니까?

답변

- EE Server/VE Server에서 정책이 변경되어도 Cloud Edition은 여전히 해당 폴더에 이전 정책을 유지합니다. 생성된 새 폴더에 새 정책이 적용되며 이 폴더는 확장자만 형식으로 암호화됩니다.



해결 방법

- 확장자만 형식을 이전 파일에 다시 적용하려면 이전 파일을 잘라내고 새 정책이 적용된 새 폴더에 붙여넣으십시오.

질문

- Cloud Edition을 설치하고 활성화했는데 새 도메인이 생성되었습니다. 기존 도메인에서 연결을 끊고 새 도메인으로 연결했습니다. Cloud Edition은 활성화 상태로 표시되지만 정책이 업데이트되지 않고 암호화도 실행되지 않습니다. 그 이유는 무엇입니까?

답변

- EE Server/VE Server는 사용자가 원래 활성화된 끝점만 인식합니다. 끝점 이름을 변경하면 EE Server/VE Server가 정책을 보내기 위해 끝점을 인식할 수 없으며 Cloud Edition이 예상대로 수행되지 않습니다.

해결 방법

- 1 Cloud Edition을 설치 제거한 다음 다시 설치합니다.
- 2 동일한 사용자를 다시 활성화합니다.

① 노트:

그 전에 로컬 컴퓨터로 파일을 동기화하는 작업을 중지하십시오. 그렇지 않으면 클라우드에서 데이터가 보호되지 않거나 삭제될 수 있습니다.

질문

- Cloud Edition이 관리되는 세션에서 난독화되지 않은 파일을 다운로드하지 않는 이유는 무엇입니까?

답변

- Cloud Edition은 브라우저에 표시되는 모든 파일을 .xen 파일로 변환합니다. 파일이 생성된 후 암호화되지 않은 텍스트 다운로드도 여기에 해당합니다. 최종 사용자에게 관리되는 클라우드 웹 사이트에서 모든 파일을 보호하도록 권장해야 합니다.

UEFI 컴퓨터

네트워크 연결 문제 해결

- UEFI 펌웨어가 설치된 컴퓨터에서 부팅 전 인증(PBA)을 성공적으로 수행하려면 PBA 모드에 네트워크가 연결되어 있어야 합니다. 기본적으로, UEFI 펌웨어가 설치된 컴퓨터는 운영 체제가 로드될 때까지 네트워크에 연결되지 않고 PBA 모드가 끝나야 연결됩니다. [UEFI 컴퓨터의 사전 설치 구성](#)에 설명된 컴퓨터 절차를 성공적으로 완료하여 올바르게 구성하면, 컴퓨터가 네트워크에 연결될 때 PBA(부팅 전 인증) 화면에 네트워크 연결 아이콘이 나타납니다.



- 부팅 전 인증이 진행되는 동안에도 네트워크 연결 아이콘이 나타나지 않으면 네트워크 케이블이 컴퓨터에 연결되어 있는지 확인하십시오. 네트워크 케이블이 컴퓨터에 연결되어 있지 않거나 느슨하면 컴퓨터를 다시 시작하여 PBA 모드를 다시 시작하십시오.

TPM 및 BitLocker

TPM 및 BitLocker 오류 코드

상수/값	설명
TPM_E_ERROR_MASK 0x80280000	TPM 하드웨어 오류를 win 오류로 변환하는 오류 마스크입니다.
TPM_E_AUTHFAIL 0x80280001	인증에 실패했습니다.
TPM_E_BADINDEX 0x80280002	PCR, DIR 또는 다른 등록에 대한 인덱스가 잘못되었습니다.
TPM_E_BAD_PARAMETER 0x80280003	하나 이상의 매개 변수가 잘못되었습니다.
TPM_E_AUDITFAILURE 0x80280004	작업이 성공적으로 완료되었지만 해당 작업의 감사가 실패했습니다.
TPM_E_CLEAR_DISABLED 0x80280005	clear disable 플래그가 설정되어 있으며 모든 지우기 작업에 실제 액세스가 필요합니다.
TPM_E_DEACTIVATED 0x80280006	TPM을 활성화합니다.
TPM_E_DISABLED 0x80280007	TPM을 사용할 수 있게 합니다.
TPM_E_DISABLED_CMD 0x80280008	대상 명령을 사용할 수 없도록 설정했습니다.
TPM_E_FAIL 0x80280009	작업이 실패했습니다.
TPM_E_BAD_ORDINAL 0x8028000A	서수를 알 수 없거나 일치하지 않습니다.
TPM_E_INSTALL_DISABLED 0x8028000B	소유자 설치 기능을 사용할 수 없습니다.
TPM_E_INVALID_KEYHANDLE 0x8028000C	키 핸들을 해석할 수 없습니다.



상수/값	설명
TPM_E_KEYNOTFOUND 0x8028000D	키 핸들이 잘못된 키를 가리킵니다.
TPM_E_INAPPROPRIATE_ENC 0x8028000E	허용되지 않는 암호화 구성표입니다.
TPM_E_MIGRATEFAIL 0x8028000F	마이그레이션 인증에 실패했습니다.
TPM_E_INVALID_PCR_INFO 0x80280010	PCR 정보를 해석할 수 없습니다.
TPM_E_NOSPACE 0x80280011	키를 로드할 공간이 없습니다.
TPM_E_NOSRK 0x80280012	SRK(저장소 루트 키) 집합이 없습니다.
TPM_E_NOTSEALED_BLOB 0x80280013	암호화된 blob이 잘못되었거나 이 TPM에서 생성되지 않았습니다.
TPM_E_OWNER_SET 0x80280014	TPM에는 이미 소유자가 있습니다.
TPM_E_RESOURCES 0x80280015	TPM에 내부 리소스가 부족하여 요청한 동작을 수행할 수 없습니다.
TPM_E_SHORTRANDOM 0x80280016	임의 문자열이 너무 짧습니다.
TPM_E_SIZE 0x80280017	TPM에 작업을 수행할 공간이 없습니다.
TPM_E_WRONGPCRVAL 0x80280018	명명된 PCR 값이 현재 PCR 값과 일치하지 않습니다.
TPM_E_BAD_PARAM_SIZE 0x80280019	명령에 대한 paramSize 인수 값이 잘못되었습니다.
TPM_E_SHA_THREAD 0x8028001A	기존 SHA-1 스레드가 없습니다.
TPM_E_SHA_ERROR 0x8028001B	기존 SHA-1 스레드에서 이미 오류가 발생하여 계산을 진행할 수 없습니다.



상수/값	설명
TPM_E_FAILEDSELFTEST 0x8028001C	TPM 하드웨어 장치가 내부 자체 테스트를 진행하는 동안 오류를 보고했습니다. 문제를 해결하려면 컴퓨터를 다시 시작해 보십시오. 문제가 계속되면 TPM 하드웨어 또는 마더보드를 교체해야 합니다.
TPM_E_AUTH2FAIL 0x8028001D	2 키 함수의 두 번째 키에 대한 인증이 실패했습니다.
TPM_E_BADTAG 0x8028001E	명령에 대해 보낸 태그 값이 잘못되었습니다.
TPM_E_IOERROR 0x8028001F	TPM으로 정보를 전송하는 동안 IO 오류가 발생했습니다.
TPM_E_ENCRYPT_ERROR 0x80280020	암호화 프로세스에 문제가 있습니다.
TPM_E_DECRYPT_ERROR 0x80280021	암호 해독 프로세스가 완료되지 않았습니다.
TPM_E_INVALID_AUTHHANDLE 0x80280022	잘못된 핸들이 사용되었습니다.
TPM_E_NO_ENDORSEMENT 0x80280023	TPM에 EK(인증 키)가 설치되어 있지 않습니다.
TPM_E_INVALID_KEYUSAGE 0x80280024	키를 사용할 수 없습니다.
TPM_E_WRONG_ENTITYTYPE 0x80280025	전송한 엔터티 유형이 허용되지 않습니다.
TPM_E_INVALID_POSTINIT 0x80280026	TPM_Init 및 후속 TPM_Startup과 관련하여 잘못된 순서로 명령을 받았습니다.
TPM_E_INAPPROPRIATE_SIG 0x80280027	서명한 데이터에 추가 DER 정보를 포함할 수 없습니다.
TPM_E_BAD_KEY_PROPERTY 0x80280028	이 TPM에서는 TPM_KEY_PARM의 키 속성이 지원되지 않습니다.
TPM_E_BAD_MIGRATION 0x80280029	이 키의 마이그레이션 속성이 잘못되었습니다.
TPM_E_BAD_SCHEME 0x8028002A	이 키의 서명 또는 암호화 구성표가 잘못되었거나 이 상황에서 허용되지 않습니다.



상수/값	설명
TPM_E_BAD_DATASIZE 0x8028002B	데이터 또는 blob 매개 변수의 크기가 잘못되었거나 참조되는 키와 일치하지 않습니다.
TPM_E_BAD_MODE 0x8028002C	TPM_GetCapability의 capArea나 subCapArea, TPM_PhysicalPresence의 physicalPresence 매개 변수 또는 TPM_CreateMigrationBlob의 migrationType과 같은 모드 매개 변수가 잘못되었습니다.
TPM_E_BAD_PRESENCE 0x8028002D	physicalPresence 또는 physicalPresenceLock 비트에 잘못된 값이 있습니다.
TPM_E_BAD_VERSION 0x8028002E	TPM에서 이 버전의 기능을 수행할 수 없습니다.
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	TPM에는 래핑한 전송 세션을 사용할 수 없습니다.
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	TPM 감사 생성이 실패하고 원본으로 사용하는 명령이 오류 코드로 반환했습니다.
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	TPM 감사 생성이 실패하고 원본으로 사용하는 명령이 성공을 반환했습니다.
TPM_E_NOTRESETABLE 0x80280032	다시 설정할 수 있는 특성이 없는 PCR 등록을 다시 설정하려고 합니다.
TPM_E_NOTLOCAL 0x80280033	명령 전송의 일부가 아닌 위치 및 위치 한정자를 필요로 하는 PCR 등록을 다시 설정하려고 합니다.
TPM_E_BAD_TYPE 0x80280034	ID 만들기 blob이 제대로 입력되지 않았습니다.
TPM_E_INVALID_RESOURCE 0x80280035	컨텍스트를 저장할 때 식별된 리소스 종류가 실제 리소스와 일치하지 않습니다.
TPM_E_NOTFIPS 0x80280036	TPM이 FIPS 모드에서만 사용 가능한 명령을 실행하려고 합니다.
TPM_E_INVALID_FAMILY 0x80280037	명령이 잘못된 패밀리 ID를 사용하려고 합니다.
TPM_E_NO_NV_PERMISSION 0x80280038	NV 저장소를 조작하는 권한을 사용할 수 없습니다.
TPM_E_REQUIRES_SIGN 0x80280039	작업을 수행하려면 서명된 명령이 필요합니다.



상수/값	설명
TPM_E_KEY_NOTSUPPORTED 0x8028003A	작업이 잘못되어 NV 키를 로드할 수 없습니다.
TPM_E_AUTH_CONFLICT 0x8028003B	NV_LoadKey blob에 소유자 및 blob 인증이 모두 필요합니다.
TPM_E_AREA_LOCKED 0x8028003C	NV 영역이 잠겨 있으므로 이 영역에 쓸 수 없습니다.
TPM_E_BAD_LOCALITY 0x8028003D	시도한 작업의 위치가 잘못되었습니다.
TPM_E_READ_ONLY 0x8028003E	NV 영역이 읽기 전용이므로 이 영역에 쓸 수 없습니다.
TPM_E_PER_NOWRITE 0x8028003F	NV 영역에 쓰기 금지가 설정되어 있지 않습니다.
TPM_E_FAMILYCOUNT 0x80280040	패밀리 수 값이 일치하지 않습니다.
TPM_E_WRITE_LOCKED 0x80280041	NV 영역에 이미 썼습니다.
TPM_E_BAD_ATTRIBUTES 0x80280042	NV 영역 특성이 충돌합니다.
TPM_E_INVALID_STRUCTURE 0x80280043	구조 태그와 버전이 잘못되었거나 일치하지 않습니다.
TPM_E_KEY_OWNER_CONTROL 0x80280044	TPM 소유자가 제어하는 키이며 TPM 소유자만이 이 키를 제거할 수 있습니다.
TPM_E_BAD_COUNTER 0x80280045	카운터 핸들이 잘못되었습니다.
TPM_E_NOT_FULLWRITE 0x80280046	쓰기가 영역의 전체 쓰기가 아닙니다.
TPM_E_CONTEXT_GAP 0x80280047	저장된 컨텍스트 수의 차이가 너무 큼니다.
TPM_E_MAXNVWRITES 0x80280048	소유자 없이 가능한 최대 NV 쓰기 수를 초과했습니다.



상수/값	설명
TPM_E_NOOPERATOR 0x80280049	연산자 AuthData 값이 설정되지 않았습니다.
TPM_E_RESOURCEMISSING 0x8028004A	컨텍스트에서 가리키는 리소스가 로드되지 않습니다.
TPM_E_DELEGATE_LOCK 0x8028004B	관리 위임이 잠겨 있습니다.
TPM_E_DELEGATE_FAMILY 0x8028004C	위임된 패밀리가 아닌 다른 패밀리를 관리하려고 합니다.
TPM_E_DELEGATE_ADMIN 0x8028004D	위임 테이블 관리를 사용할 수 없습니다.
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	단독 전송 세션 밖에서 실행된 명령이 있습니다.
TPM_E_OWNER_CONTROL 0x8028004F	소유자 제어 키를 저장하려고 합니다.
TPM_E_DAA_RESOURCES 0x80280050	명령 실행에 사용할 수 있는 리소스가 DAA 명령에 없습니다.
TPM_E_DAA_INPUT_DATA0 0x80280051	DAA 매개 변수 inputData0의 일관성을 확인하지 못했습니다.
TPM_E_DAA_INPUT_DATA1 0x80280052	DAA 매개 변수 inputData1의 일관성을 확인하지 못했습니다.
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	DAA_issuerSettings의 일관성을 확인하지 못했습니다.
TPM_E_DAA_TPM_SETTINGS 0x80280054	DAA_tpmSpecific의 일관성을 확인하지 못했습니다.
TPM_E_DAA_STAGE 0x80280055	전송한 DAA 명령이 나타내는 소규모 프로세스는 예상 프로세스가 아닙니다.
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	발급자의 유효성 검사에서 불일치가 발견되었습니다.
TPM_E_DAA_WRONG_W 0x80280057	w의 일관성을 확인하지 못했습니다.



상수/값	설명
TPM_E_BAD_HANDLE 0x80280058	핸들이 잘못되었습니다.
TPM_E_BAD_DELEGATE 0x80280059	위임이 잘못되었습니다.
TPM_E_BADCONTEXT 0x8028005A	컨텍스트 blob이 잘못되었습니다.
TPM_E_TOOMANYCONTEXTS 0x8028005B	TPM에 컨텍스트가 너무 많습니다.
TPM_E_MA_TICKET_SIGNATURE 0x8028005C	마이그레이션 권한 서명의 유효성을 검사하지 못했습니다.
TPM_E_MA_DESTINATION 0x8028005D	마이그레이션 대상이 인증되지 않았습니다.
TPM_E_MA_SOURCE 0x8028005E	마이그레이션 원본이 잘못되었습니다.
TPM_E_MA_AUTHORITY 0x8028005F	마이그레이션 권한이 잘못되었습니다.
TPM_E_PERMANENTEK 0x80280061	EK를 해지하려고 하지만 EK를 해지할 수 없습니다.
TPM_E_BAD_SIGNATURE 0x80280062	CMK 티켓의 서명이 잘못되었습니다.
TPM_E_NOCONTEXTSPACE 0x80280063	컨텍스트 목록에 컨텍스트를 추가할 공간이 없습니다.
TPM_E_COMMAND_BLOCKED 0x80280400	명령이 차단되었습니다.
TPM_E_INVALID_HANDLE 0x80280401	지정한 핸들을 찾을 수 없습니다.
TPM_E_DUPLICATE_VHANDLE 0x80280402	TPM에서 중복 핸들을 반환했으며 명령을 다시 전송해야 합니다.
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	전송 내의 명령이 차단되었습니다.



상수/값	설명
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	전송 내의 명령이 지원되지 않습니다.
TPM_E_RETRY 0x80280800	TPM 사용량이 많아 명령에 바로 응답할 수 없지만 나중에 명령을 다시 전송할 수 있습니다.
TPM_E_NEEDS_SELFTEST 0x80280801	SelfTestFull을 실행하지 않았습니다.
TPM_E_DOING_SELFTEST 0x80280802	TPM에서 현재 전체 자체 테스트를 실행하고 있습니다.
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	TPM이 사전 공격을 방어하고 있으며 제한 기간이 지나지 않았습니다.
TBS_E_INTERNAL_ERROR 0x80284001	내부 소프트웨어 오류가 발생했습니다.
TBS_E_BAD_PARAMETER 0x80284002	하나 이상의 입력 매개 변수가 잘못되었습니다.
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	지정한 출력 포인터가 잘못되었습니다.
TBS_E_INVALID_CONTEXT 0x80284004	지정한 컨텍스트 핸들이 올바른 컨텍스트를 참조하지 않습니다.
TBS_E_INSUFFICIENT_BUFFER 0x80284005	지정한 출력 버퍼가 너무 작습니다.
TBS_E_IOERROR 0x80284006	TPM과 통신하는 동안 오류가 발생했습니다.
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	하나 이상의 컨텍스트 매개 변수가 잘못되었습니다.
TBS_E_SERVICE_NOT_RUNNING 0x80284008	TBS 서비스를 실행하고 있지 않으며 시작할 수 없습니다.
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	열린 컨텍스트가 너무 많으므로 새 컨텍스트를 만들 수 없습니다.
TBS_E_TOO_MANY_RESOURCES 0x8028400A	열린 가상 리소스가 너무 많아 새 가상 리소스를 만들 수 없습니다.



상수/값	설명
TBS_E_SERVICE_START_PENDING 0x8028400B	TBS 서비스가 시작되었지만 아직 실행되고 있지 않습니다.
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	실제 존재 인터페이스가 지원되지 않습니다.
TBS_E_COMMAND_CANCELED 0x8028400D	명령이 취소되었습니다.
TBS_E_BUFFER_TOO_LARGE 0x8028400E	입력 또는 출력 버퍼가 너무 큼니다.
TBS_E_TPM_NOT_FOUND 0x8028400F	이 컴퓨터에 호환 가능한 TPM 보안 장치가 없습니다.
TBS_E_SERVICE_DISABLED 0x80284010	TBS 서비스를 사용할 수 없습니다.
TBS_E_NO_EVENT_LOG 0x80284011	TCG 이벤트 로그를 사용할 수 없습니다.
TBS_E_ACCESS_DENIED 0x80284012	호출자에게 요청한 작업을 수행할 적절한 권한이 없습니다.
TBS_E_PROVISIONING_NOT_ALLOWED 0x80284013	TPM 프로비저닝 작업이 지정한 플래그에서 허용되지 않습니다. 프로비저닝에 성공하려면 몇 가지 작업 중 하나가 필요합니다. TPM을 사용 준비되도록 하는 TPM 관리 콘솔(tpm.msc)이 도움이 될 수 있습니다. 자세한 내용은 Win32_Tpm WMI 메서드 'Provision'의 설명서를 참조하십시오. (필요한 작업에는 TPM 소유자 인증 값을 시스템에 가져오기, TPM 프로비저닝을 위한 Win32_Tpm WMI 메서드 호출, 'ForceClear_Allowed' 또는 'PhysicalPresencePrompts_Allowed'를 TRUE(참)로 지정(추가 정보에서 반환된 값으로 표시됨), 또는 시스템 BIOS에서 TPM 사용이 포함될 수 있습니다.)
TBS_E_PPI_FUNCTION_UNSUPPORTED 0x80284014	이 펌웨어의 실제 존재 인터페이스가 요청한 메서드를 지원하지 않습니다.
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	요청한 TPM OwnerAuth 값을 찾을 수 없습니다.
TBS_E_PROVISIONING_INCOMPLETE 0x80284016	TPM 프로비저닝이 완료되지 않았습니다. 프로비저닝 완료에 대한 자세한 내용을 보려면 TPM 프로비저닝을 위한 Win32_Tpm WMI 메서드를 호출하고('Provision') 반환된 정보를 확인하십시오.
TPMAPI_E_INVALID_STATE 0x80290100	명령 버퍼 상태가 올바르지 않습니다.
TPMAPI_E_NOT_ENOUGH_DATA	명령 버퍼에 데이터가 부족하여 요청을 만족할 수 없습니다.



상수/값**설명**

0x80290101	
TPMAPI_E_TOO_MUCH_DATA	명령 버퍼에 데이터를 추가할 수 없습니다.
0x80290102	
TPMAPI_E_INVALID_OUTPUT_POINTER	하나 이상의 출력 매개 변수가 NULL이거나 잘못되었습니다.
0x80290103	
TPMAPI_E_INVALID_PARAMETER	하나 이상의 입력 매개 변수가 잘못되었습니다.
0x80290104	
TPMAPI_E_OUT_OF_MEMORY	메모리가 부족하여 요청을 만족할 수 없습니다.
0x80290105	
TPMAPI_E_BUFFER_TOO_SMALL	지정한 버퍼가 너무 작습니다.
0x80290106	
TPMAPI_E_INTERNAL_ERROR	내부 오류가 발생했습니다.
0x80290107	
TPMAPI_E_ACCESS_DENIED	호출자에게 요청한 작업을 수행할 적절한 권한이 없습니다.
0x80290108	
TPMAPI_E_AUTHORIZATION_FAILED	지정한 인증 정보가 잘못되었습니다.
0x80290109	
TPMAPI_E_INVALID_CONTEXT_HANDLE	지정한 컨텍스트 핸들이 잘못되었습니다.
0x8029010A	
TPMAPI_E_TBS_COMMUNICATION_ERROR	TBS와 통신하는 동안 오류가 발생했습니다.
0x8029010B	
TPMAPI_E_TPM_COMMAND_ERROR	TPM에서 예기치 않은 결과를 반환했습니다.
0x8029010C	
TPMAPI_E_MESSAGE_TOO_LARGE	인코딩 구성표에 대해 메시지가 너무 큼니다.
0x8029010D	
TPMAPI_E_INVALID_ENCODING	blob의 인코딩이 인식되지 않았습니다.
0x8029010E	
TPMAPI_E_INVALID_KEY_SIZE	키 크기가 잘못되었습니다.
0x8029010F	
TPMAPI_E_ENCRYPTION_FAILED	암호화 작업이 실패했습니다.



상수/값	설명
0x80290110	
TPMAPI_E_INVALID_KEY_PARAMS	키 매개 변수 구조가 잘못되었습니다.
0x80290111	
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB	요청한 제공 데이터가 올바른 마이그레이션 인증 blob이 아닌 것 같습니다.
0x80290112	
TPMAPI_E_INVALID_PCR_INDEX	지정한 PCR 색인이 잘못되었습니다.
0x80290113	
TPMAPI_E_INVALID_DELEGATE_BLOB	지정한 데이터가 올바른 위임 blob이 아닌 것 같습니다.
0x80290114	
TPMAPI_E_INVALID_CONTEXT_PARAMS	지정한 컨텍스트 매개 변수 하나 이상이 잘못되었습니다.
0x80290115	
TPMAPI_E_INVALID_KEY_BLOB	지정한 데이터가 올바른 키 blob이 아닌 것 같습니다.
0x80290116	
TPMAPI_E_INVALID_PCR_DATA	지정한 PCR 데이터가 잘못되었습니다.
0x80290117	
TPMAPI_E_INVALID_OWNER_AUTH	소유자 인증 데이터의 형식이 잘못되었습니다.
0x80290118	
TPMAPI_E_FIPS_RNG_CHECK_FAILED	생성된 난수가 FIPS RNG 검사를 통과하지 못했습니다.
0x80290119	
TPMAPI_E_EMPTY_TCG_LOG	TCG 이벤트 로그에 데이터가 없습니다.
0x8029011A	
TPMAPI_E_INVALID_TCG_LOG_ENTRY	TCG 이벤트 로그의 항목이 잘못되었습니다.
0x8029011B	
TPMAPI_E_TCG_SEPARATOR_ABSENT	TCG 구분 기호가 없습니다.
0x8029011C	
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY	TCG 로그 항목의 다이제스트 값이 해시된 데이터와 일치하지 않습니다.
0x8029011D	
TPMAPI_E_POLICY_DENIES_OPERATION	요청한 작업이 현재 TPM 정책에 의해 차단되었습니다. 도움이 필요하면 시스템 관리자에게 문의하십시오.
0x8029011E	
TBSIMP_E_BUFFER_TOO_SMALL	지정한 버퍼가 너무 작습니다.



상수/값**설명**

0x80290200	
TBSIMP_E_CLEANUP_FAILED	컨텍스트를 정리할 수 없습니다.
0x80290201	
TBSIMP_E_INVALID_CONTEXT_HANDLE	지정한 컨텍스트 핸들이 잘못되었습니다.
0x80290202	
TBSIMP_E_INVALID_CONTEXT_PARAM	잘못된 컨텍스트 매개 변수가 지정되었습니다.
0x80290203	
TBSIMP_E_TPM_ERROR	TPM과 통신하는 동안 오류가 발생했습니다.
0x80290204	
TBSIMP_E_HASH_BAD_KEY	지정한 키를 가진 항목을 찾을 수 없습니다.
0x80290205	
TBSIMP_E_DUPLICATE_VHANDLE	지정한 가상 핸들이 이미 사용 중인 가상 핸들과 일치합니다.
0x80290206	
TBSIMP_E_INVALID_OUTPUT_POINTER	반환된 핸들 위치의 포인터가 NULL이거나 잘못되었습니다.
0x80290207	
TBSIMP_E_INVALID_PARAMETER	하나 이상의 매개 변수가 잘못되었습니다.
0x80290208	
TBSIMP_E_RPC_INIT_FAILED	RPC 하위 시스템을 초기화할 수 없습니다.
0x80290209	
TBSIMP_E_SCHEDULER_NOT_RUNNING	TBS 스케줄러가 실행되고 있지 않습니다.
0x8029020A	
TBSIMP_E_COMMAND_CANCELED	명령이 취소되었습니다.
0x8029020B	
TBSIMP_E_OUT_OF_MEMORY	메모리가 부족하여 요청을 수행하지 못했습니다.
0x8029020C	
TBSIMP_E_LIST_NO_MORE_ITEMS	선택한 목록이 비어 있거나 목록 끝까지 반복되었습니다.
0x8029020D	
TBSIMP_E_LIST_NOT_FOUND	지정한 항목을 목록에서 찾을 수 없습니다.
0x8029020E	
TBSIMP_E_NOT_ENOUGH_SPACE	TPM에 공간이 부족하여 요청한 리소스를 로드할 수 없습니다.



상수/값	설명
0x8029020F	
TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS	사용 중인 TPM 컨텍스트가 너무 많습니다.
0x80290210	
TBSIMP_E_COMMAND_FAILED	TPM 명령이 실패했습니다.
0x80290211	
TBSIMP_E_UNKNOWN_ORDINAL	TBS에서 지정한 서수가 인식되지 않습니다.
0x80290212	
TBSIMP_E_RESOURCE_EXPIRED	요청한 리소스를 더 이상 사용할 수 없습니다.
0x80290213	
TBSIMP_E_INVALID_RESOURCE	리소스 종류가 일치하지 않습니다.
0x80290214	
TBSIMP_E_NOTHING_TO_UNLOAD	리소스를 언로드할 수 없습니다.
0x80290215	
TBSIMP_E_HASH_TABLE_FULL	해시 테이블에 새 항목을 추가할 수 없습니다.
0x80290216	
TBSIMP_E_TOO_MANY_TBS_CONTEXTS	열린 컨텍스트가 너무 많아 새 TBS 컨텍스트를 만들 수 없습니다.
0x80290217	
TBSIMP_E_TOO_MANY_RESOURCES	열린 가상 리소스가 너무 많아 새 가상 리소스를 만들 수 없습니다.
0x80290218	
TBSIMP_E_PPI_NOT_SUPPORTED	실제 존재 인터페이스가 지원되지 않습니다.
0x80290219	
TBSIMP_E_TPM_INCOMPATIBLE	TBS가 시스템에서 발견된 TPM 버전과 호환되지 않습니다.
0x8029021A	
TBSIMP_E_NO_EVENT_LOG	TCG 이벤트 로그를 사용할 수 없습니다.
0x8029021B	
TPM_E_PPI_ACPI_FAILURE	실제 존재 명령에 대한 BIOS의 응답을 가져오는 동안 일반 오류가 발생했습니다.
0x80290300	
TPM_E_PPI_USER_ABORT	사용자가 TPM 작업을 확인하지 못했습니다.
0x80290301	
TPM_E_PPI_BIOS_FAILURE	잘못된 TPM 작업 요청, TPM과의 BIOS 통신 오류 등의 BIOS 오류가 발생하여 요청한 TPM 작업을 실행하지 못했습니다.



상수/값**설명**

0x80290302	
TPM_E_PPI_NOT_SUPPORTED	BIOS에서 실제 존재 인터페이스를 지원하지 않습니다.
0x80290303	
TPM_E_PPI_BLOCKED_IN_BIOS	실제 존재 명령이 현재 BIOS 설정에 의해 차단되었습니다. 시스템 소유자가 BIOS 설정을 다시 구성하여 이 명령을 허용할 수 있습니다.
0x80290304	
TPM_E_PCP_ERROR_MASK	플랫폼 암호화 공급자 오류를 win 오류로 변환하는 오류 마스크입니다.
0x80290400	
TPM_E_PCP_DEVICE_NOT_READY	플랫폼 암호화 공급자가 현재 준비되지 않았습니다. 이 공급자가 완전히 프로비저닝되어야 작동됩니다.
0x80290401	
TPM_E_PCP_INVALID_HANDLE	플랫폼 암호화 공급자에 제공된 핸들이 잘못되었습니다.
0x80290402	
TPM_E_PCP_INVALID_PARAMETER	플랫폼 암호화 공급자에 제공된 매개 변수가 잘못되었습니다.
0x80290403	
TPM_E_PCP_FLAG_NOT_SUPPORTED	플랫폼 암호화 공급자에 제공된 플래그가 지원되지 않습니다.
0x80290404	
TPM_E_PCP_NOT_SUPPORTED	요청한 작업은 이 플랫폼 암호화 공급자에서 지원되지 않습니다.
0x80290405	
TPM_E_PCP_BUFFER_TOO_SMALL	버퍼가 너무 작기 때문에 모든 데이터를 포함할 수 없습니다. 버퍼에 기록된 정보가 없습니다.
0x80290406	
TPM_E_PCP_INTERNAL_ERROR	플랫폼 암호화 공급자에 예기치 않은 내부 오류가 발생했습니다.
0x80290407	
TPM_E_PCP_AUTHENTICATION_FAILED	공급자 개체를 사용할 권한이 실패했습니다.
0x80290408	
TPM_E_PCP_AUTHENTICATION_IGNORED	플랫폼 암호화 장치가 사전 공격을 방지하기 위해 공급자 개체에 대한 권한을 무시했습니다.
0x80290409	
TPM_E_PCP_POLICY_NOT_FOUND	참조된 정책을 찾을 수 없습니다.
0x8029040A	
TPM_E_PCP_PROFILE_NOT_FOUND	참조된 프로필을 찾을 수 없습니다.
0x8029040B	
TPM_E_PCP_VALIDATION_FAILED	유효성 검사에 실패했습니다.



상수/값	설명
0x8029040C	
PLA_E_DCS_NOT_FOUND	데이터 수집기 세트를 찾을 수 없습니다.
0x80300002	
PLA_E_DCS_IN_USE	데이터 수집기 세트 또는 해당 종속 항목 중 하나가 이미 사용 중입니다.
0x803000AA	
PLA_E_TOO_MANY_FOLDERS	폴더가 너무 많아 데이터 수집기 세트를 시작할 수 없습니다.
0x80300045	
PLA_E_NO_MIN_DISK	사용 가능한 디스크 공간이 부족하여 데이터 수집기 세트를 시작할 수 없습니다.
0x80300070	
PLA_E_DCS_ALREADY_EXISTS	데이터 수집기 세트가 이미 있습니다.
0x803000B7	
PLA_S_PROPERTY_IGNORED	속성 값이 무시됩니다.
0x00300100	
PLA_E_PROPERTY_CONFLICT	속성 값이 충돌합니다.
0x80300101	
PLA_E_DCS_SINGLETON_REQUIRED	현재 이 데이터 수집기 세트는 데이터 수집기를 하나만 포함하도록 구성되어 있습니다.
0x80300102	
PLA_E_CREDENTIALS_REQUIRED	데이터 수집기 세트 속성을 커밋하려면 사용자 계정이 필요합니다.
0x80300103	
PLA_E_DCS_NOT_RUNNING	데이터 수집기 세트가 실행되고 있지 않습니다.
0x80300104	
PLA_E_CONFLICT_INCL_EXCL_API	API 포함/제외 목록에서 충돌이 감지되었습니다. 포함 목록과 제외 목록에 같은 API를 지정하지 마십시오.
0x80300105	
PLA_E_NETWORK_EXE_NOT_VALID	지정한 실행 파일 경로가 네트워크 공유나 UNC 경로를 참조합니다.
0x80300106	
PLA_E_EXE_ALREADY_CONFIGURED	지정한 실행 파일 경로가 이미 API 추적용으로 구성되어 있습니다.
0x80300107	
PLA_E_EXE_PATH_NOT_VALID	지정한 실행 파일 경로가 없습니다. 올바른 경로를 지정했는지 확인하십시오.
0x80300108	
PLA_E_DC_ALREADY_EXISTS	데이터 수집기가 이미 있습니다.



상수/값	설명
0x80300109	
PLA_E_DCS_START_WAIT_TIMEOUT	데이터 수집기 세트의 알림 시작 대기 시간이 초과되었습니다.
0x8030010A	
PLA_E_DC_START_WAIT_TIMEOUT	데이터 수집기의 시작 대기 시간이 초과되었습니다.
0x8030010B	
PLA_E_REPORT_WAIT_TIMEOUT	보고서 생성 도구의 완료 대기 시간이 초과되었습니다.
0x8030010C	
PLA_E_NO_DUPLICATES	중복 항목을 사용할 수 없습니다.
0x8030010D	
PLA_E_EXE_FULL_PATH_REQUIRED	추적할 실행 파일을 지정할 때 파일 이름뿐 아니라 전체 경로를 지정해야 합니다.
0x8030010E	
PLA_E_INVALID_SESSION_NAME	제공한 세션 이름이 잘못되었습니다.
0x8030010F	
PLA_E_PLA_CHANNEL_NOT_ENABLED	이 작업을 수행하려면 이벤트 로그 채널 Microsoft-Windows-Diagnosis-PLA/Operational을 사용해야 합니다.
0x80300110	
PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED	이 작업을 수행하려면 이벤트 로그 채널 Microsoft-Windows-TaskScheduler를 사용해야 합니다.
0x80300111	
PLA_E_RULES_MANAGER_FAILED	규칙 관리자를 실행하지 못했습니다.
0x80300112	
PLA_E_CABAPI_FAILURE	데이터를 압축하거나 압축을 푸는 동안 오류가 발생했습니다.
0x80300113	
FVE_E_LOCKED_VOLUME	이 드라이브는 BitLocker 드라이브 암호화로 잠겨 있습니다. 제어판에서 이 드라이브의 잠금을 해제해야 합니다.
0x80310000	
FVE_E_NOT_ENCRYPTED	드라이브가 암호화되지 않았습니다.
0x80310001	
FVE_E_NO_TPM_BIOS	BIOS가 TPM과 올바르게 통신하지 못했습니다. 컴퓨터 제조업체에 BIOS 업그레이드 지침에 대해 문의하십시오.
0x80310002	
FVE_E_NO_MBR_METRIC	BIOS가 MBR(마스터 부트 레코드)과 올바르게 통신하지 못했습니다. 컴퓨터 제조업체에 BIOS 업그레이드 지침에 대해 문의하십시오.
0x80310003	
FVE_E_NO_BOOTSECTOR_METRIC	필요한 TPM 측정이 없습니다. 부팅 가능한 CD나 DVD가 컴퓨터에 있는 경우 이를 제거한 후 컴퓨터를 다시 시작하고 BitLocker를



상수/값

설명

0x80310004	다시 켜십시오. 문제가 계속되는 경우 마스터 부트 레코드가 최신 상태인지 확인하십시오.
FVE_E_NO_BOOTMGR_METRIC 0x80310005	이 드라이브의 부팅 섹터가 BitLocker 드라이브 암호화와 호환되지 않습니다. Windows 복구 환경에서 Bootrec.exe 도구를 사용하여 부팅 관리자(BOOTMGR)를 업데이트하거나 복구하십시오.
FVE_E_WRONG_BOOTMGR 0x80310006	이 운영 체제의 부팅 관리자가 BitLocker 드라이브 암호화와 호환되지 않습니다. Windows 복구 환경에서 Bootrec.exe 도구를 사용하여 부팅 관리자(BOOTMGR)를 업데이트하거나 복구하십시오.
FVE_E_SECURE_KEY_REQUIRED 0x80310007	이 작업을 수행하려면 보안 키 보호기가 하나 이상 필요합니다.
FVE_E_NOT_ACTIVATED 0x80310008	이 드라이브에서 BitLocker 드라이브 암호화는 사용할 수 없습니다. BitLocker를 켜십시오.
FVE_E_ACTION_NOT_ALLOWED 0x80310009	BitLocker 드라이브 암호화에서 요청한 작업을 수행할 수 없습니다. 두 개의 요청이 동시에 있을 때 이런 문제가 발생할 수 있습니다. 잠시 기다린 후 작업을 다시 시도해 보십시오.
FVE_E_AD_SCHEMA_NOT_INSTALLED 0x8031000A	Active Directory 도메인 서비스 포리스트에 BitLocker 드라이브 암호화 또는 TPM 정보를 호스팅하는 데 필요한 특성과 클래스가 없습니다. 도메인 관리자에게 연락하여 필요한 BitLocker Active Directory 스키마 확장이 설치되었는지 확인하십시오.
FVE_E_AD_INVALID_DATATYPE 0x8031000B	Active Directory에서 가져온 데이터의 형식이 잘못되었습니다. BitLocker 복구 정보가 없거나 손상되었을 수 있습니다.
FVE_E_AD_INVALID_DATASIZE 0x8031000C	Active Directory에서 가져온 데이터의 크기가 잘못되었습니다. BitLocker 복구 정보가 없거나 손상되었을 수 있습니다.
FVE_E_AD_NO_VALUES 0x8031000D	Active Directory에서 읽은 특성에 값이 없습니다. BitLocker 복구 정보가 없거나 손상되었을 수 있습니다.
FVE_E_AD_ATTR_NOT_SET 0x8031000E	특성이 설정되지 않았습니다. Active Directory 개체에 정보를 쓸 수 있는 권한이 있는 도메인 계정으로 로그인했는지 확인하십시오.
FVE_E_AD_GUID_NOT_FOUND 0x8031000F	지정된 특성을 Active Directory 도메인 서비스에서 찾을 수 없습니다. 도메인 관리자에게 연락하여 필요한 BitLocker Active Directory 스키마 확장이 설치되었는지 확인하십시오.
FVE_E_BAD_INFORMATION 0x80310010	암호화된 드라이브의 BitLocker 메타데이터가 잘못되었습니다. 드라이브를 복구하여 액세스를 복원하십시오.
FVE_E_TOO_SMALL 0x80310011	드라이브에 사용 가능한 공간이 부족하여 드라이브를 암호화할 수 없습니다. 드라이브에서 필요 없는 데이터를 삭제하여 사용할 수 있는 공간을 추가로 만들고 다시 시도하십시오.
FVE_E_SYSTEM_VOLUME 0x80310012	드라이브에 시스템 부팅 정보가 있으므로 드라이브를 암호화할 수 없습니다. 부팅 정보를 포함하는 시스템 드라이브로 사용할 별도 파티션과 운영 체제 드라이브로 사용할 보조 파티션을 만든 다음 운영 체제 드라이브를 암호화하십시오.

상수/값	설명
FVE_E_FAILED_WRONG_FS 0x80310013	파일 시스템이 지원되지 않으므로 드라이브를 암호화할 수 없습니다.
FVE_E_BAD_PARTITION_SIZE 0x80310014	파일 시스템 크기가 파티션 테이블의 파티션 크기보다 큼니다. 이 드라이브가 손상되었거나 임의로 변경되었을 수 있습니다. BitLocker를 사용하려면 파티션을 다시 포맷해야 합니다.
FVE_E_NOT_SUPPORTED 0x80310015	이 드라이브를 암호화할 수 없습니다.
FVE_E_BAD_DATA 0x80310016	올바르지 않은 데이터입니다.
FVE_E_VOLUME_NOT_BOUND 0x80310017	지정한 데이터 드라이브가 현재 컴퓨터에서 자동으로 잠금 해제하도록 설정되어 있지 않아 자동으로 잠금 해제할 수 없습니다.
FVE_E_TPM_NOT_OWNED 0x80310018	BitLocker 드라이브 암호화를 사용하려면 TPM을 초기화해야 합니다.
FVE_E_NOT_DATA_VOLUME 0x80310019	운영 체제 드라이브에서 수행할 수 없는 작업을 하려고 했습니다.
FVE_E_AD_INSUFFICIENT_BUFFER 0x8031001A	기능에 제공된 버퍼가 부족하여 반환된 데이터를 포함할 수 없습니다. 버퍼 크기를 늘리고 기능을 다시 실행해 보십시오.
FVE_E_CONV_READ 0x8031001B	드라이브를 변환하는 동안 읽기 작업이 실패했습니다. 드라이브가 변환되지 않았습니다. BitLocker를 사용하도록 다시 설정하십시오.
FVE_E_CONV_WRITE 0x8031001C	드라이브를 변환하는 동안 쓰기 작업이 실패했습니다. 드라이브가 변환되지 않았습니다. BitLocker를 사용하도록 다시 설정하십시오.
FVE_E_KEY_REQUIRED 0x8031001D	BitLocker 키 보호기가 하나 이상 필요합니다. 이 드라이브의 마지막 남은 키는 삭제할 수 없습니다.
FVE_E_CLUSTERING_NOT_SUPPORTED 0x8031001E	BitLocker 드라이브 암호화는 클러스터 구성을 지원하지 않습니다.
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	지정한 드라이브가 현재 컴퓨터에서 자동으로 잠금 해제되도록 이미 구성되어 있습니다.
FVE_E_OS_NOT_PROTECTED 0x80310020	운영 체제 드라이브가 BitLocker 드라이브 암호화로 보호되지 않습니다.
FVE_E_PROTECTION_DISABLED 0x80310021	이 드라이브에서 BitLocker 드라이브 암호화가 일시 중단되었습니다. 이 드라이브에 구성된 모든 BitLocker 키 보호기가 효과적으로 해제되어 있습니다. 드라이브가 암호화되지 않은 일반 키를 사용하여 자동으로 잠금 해제됩니다.



상수/값

설명

FVE_E_RECOVERY_KEY_REQUIRED 0x80310022	BitLocker 보호가 현재 일시 중단되어 잠그려는 드라이브에서 키 보호기를 암호화에 사용할 수 없습니다. 이 드라이브를 잠그려면 BitLocker를 사용하도록 다시 설정하십시오.
FVE_E_FOREIGN_VOLUME 0x80310023	BitLocker에서 TPM을 사용하여 데이터 드라이브를 보호할 수 없습니다. TPM 보호는 운영 체제 드라이브에만 사용할 수 있습니다.
FVE_E_OVERLAPPED_UPDATE 0x80310024	암호화된 드라이브의 BitLocker 메타데이터를 업데이트할 수 없습니다. 다른 프로세스에서 업데이트하도록 잠겨 있습니다. 이 프로세스를 다시 시도하십시오.
FVE_E_TPM_SRK_AUTH_NOT_ZERO 0x80310025	TPM의 SRK(저장소 루트 키)에 대한 인증 데이터가 0이 아니므로 BitLocker와 호환되지 않습니다. TPM을 초기화한 다음 BitLocker에 사용해 보십시오.
FVE_E_FAILED_SECTOR_SIZE 0x80310026	이 섹터 크기에는 드라이브 암호화 알고리즘을 사용할 수 없습니다.
FVE_E_FAILED_AUTHENTICATION 0x80310027	제공된 키로 드라이브를 잠금 해제할 수 없습니다. 올바른 키를 제공했는지 확인하고 다시 시도하십시오.
FVE_E_NOT_OS_VOLUME 0x80310028	지정된 드라이브가 운영 체제 드라이브가 아닙니다.
FVE_E_AUTOUNLOCK_ENABLED 0x80310029	운영 체제 드라이브에서 BitLocker 드라이브 암호화를 끄려면 먼저 이 컴퓨터에 연결된 고정 데이터 드라이브와 이동식 데이터 드라이브의 자동 잠금 해제 기능을 사용하지 않도록 설정해야 합니다.
FVE_E_WRONG_BOOTSECTOR 0x8031002A	시스템 파티션 부팅 섹터에서 TPM 측정을 수행하지 않습니다. Windows 복구 환경에서 Bootrec.exe 도구를 사용하여 부팅 섹터를 업데이트하거나 복구하십시오.
FVE_E_WRONG_SYSTEM_FS 0x8031002B	BitLocker 드라이브 암호화 운영 체제 드라이브를 암호화하려면 NTFS 파일 시스템으로 포맷해야 합니다. 드라이브를 NTFS로 변환하고 BitLocker를 켜십시오.
FVE_E_POLICY_PASSWORD_REQUIRED 0x8031002C	복구 암호를 지정해야 드라이브를 암호화할 수 있도록 그룹 정책이 설정되어 있습니다.
FVE_E_CANNOT_SET_FVEK_ENCRYPTED 0x8031002D	이전에 암호화된 드라이브에는 드라이브 암호화 알고리즘과 키를 설정할 수 없습니다. 이 드라이브를 BitLocker 드라이브 암호화로 암호화하려면 이전 암호화를 제거한 다음 BitLocker를 켜십시오.
FVE_E_CANNOT_ENCRYPT_NO_KEY 0x8031002E	암호화 키를 사용할 수 없기 때문에 BitLocker 드라이브 암호화에서 지정된 드라이브를 암호화할 수 없습니다. 이 드라이브를 암호화하려면 키 보호기를 추가하십시오.
FVE_E_BOOTABLE_CDDVD 0x80310030	BitLocker 드라이브 암호화에서 컴퓨터에 부팅 가능한 미디어(CD 또는 DVD)가 있는 것을 검색했습니다. 해당 미디어를 제거하고 컴퓨터를 다시 시작한 다음 BitLocker를 구성하십시오.
FVE_E_PROTECTOR_EXISTS	키 보호기를 추가할 수 없습니다. 이 드라이브에는 이 유형의 키 보호기 하나만 사용할 수 있습니다.

상수/값

설명

0x80310031	
FVE_E_RELATIVE_PATH	
0x80310032	상대 경로가 지정되어 복구 암호 파일을 찾을 수 없습니다. 복구 암호는 정규화된 경로로 저장해야 합니다. 컴퓨터에 구성된 환경 변수를 경로에 사용할 수 있습니다.
FVE_E_PROTECTOR_NOT_FOUND	
0x80310033	지정한 키 보호기가 드라이브에 없습니다. 다른 키 보호기를 사용해 보십시오.
FVE_E_INVALID_KEY_FORMAT	
0x80310034	제공된 복구 키가 손상되어 드라이브에 액세스하는 데 사용할 수 없습니다. 복구 암호, 데이터 복구 에이전트, 백업 버전의 복구 키 등 다른 복구 방법을 사용하여 드라이브 대한 액세스를 복구해야 합니다.
FVE_E_INVALID_PASSWORD_FORMAT	
0x80310035	제공된 복구 암호의 형식이 잘못되었습니다. BitLocker 복구 암호는 48자릿수입니다. 복구 암호 형식이 올바른지 확인하고 다시 시도하십시오.
FVE_E_FIPS_RNG_CHECK_FAILED	
0x80310036	난수 생성기 검사 테스트에 실패했습니다.
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD	
0x80310037	FIPS를 따라야 하는 그룹 정책 설정 때문에 로컬 복구 암호를 생성하거나 BitLocker 드라이브 암호화에서 사용할 수 없습니다. FIPS 준수 모드로 작동하는 경우 BitLocker 복구 옵션은 USB 드라이브에 저장된 복구 키 또는 데이터 복구 에이전트를 통한 복구가 될 수 있습니다.
FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT	
0x80310038	FIPS를 따라야 하는 그룹 정책 설정 때문에 복구 암호를 Active Directory에 저장할 수 없습니다. FIPS 준수 모드로 작동하는 경우 BitLocker 복구 옵션은 USB 드라이브에 저장된 복구 키 또는 데이터 복구 에이전트를 통한 복구가 될 수 있습니다. 그룹 정책 설정 구성을 확인하십시오.
FVE_E_NOT_DECRYPTED	
0x80310039	이 작업을 완료하려면 드라이브의 암호를 완전히 해독해야 합니다.
FVE_E_INVALID_PROTECTOR_TYPE	
0x8031003A	지정한 키 보호기를 이 작업에 사용할 수 없습니다.
FVE_E_NO_PROTECTORS_TO_TEST	
0x8031003B	하드웨어 테스트를 수행하기 위한 드라이브에 키 보호기가 없습니다.
FVE_E_KEYFILE_NOT_FOUND	
0x8031003C	BitLocker 시작 키나 복구 암호를 USB 장치에서 찾을 수 없습니다. 올바른 USB 장치를 사용하는지, USB 장치가 컴퓨터의 활성 USB 포트에 연결되어 있는지 확인한 다음 컴퓨터를 다시 시작하고 다시 시도하십시오. 문제가 계속되면 BIOS 업그레이드 지침에 대해 컴퓨터 제조업체에 문의하십시오.
FVE_E_KEYFILE_INVALID	
0x8031003D	제공된 BitLocker 시작 키나 복구 암호 파일이 손상되었거나 잘못되었습니다. 올바른 시작 키 또는 복구 암호 파일을 사용하는지 확인하고 다시 시도하십시오.
FVE_E_KEYFILE_NO_VMK	
0x8031003E	BitLocker 암호화 키를 시작 키나 복구 암호에서 얻을 수 없습니다. 올바른 시작 키 또는 복구 암호를 사용하는지 확인하고 다시 시도하십시오.



상수/값

설명

FVE_E_TPM_DISABLED 0x8031003F	TPM이 사용하지 않도록 설정되어 있습니다. BitLocker 드라이브 암호화에 사용하려면 TPM이 사용하도록 설정되고 초기화되어 있으며 올바른 소유권을 가지고 있어야 합니다.
FVE_E_NOT_ALLOWED_IN_SAFE_MODE 0x80310040	이 컴퓨터가 현재 안전 모드로 작동하기 때문에 지정한 드라이브의 BitLocker 구성을 관리할 수 없습니다. 안전 모드에서는 BitLocker 드라이브 암호화를 복구용으로만 사용할 수 있습니다.
FVE_E_TPM_INVALID_PCR 0x80310041	시스템 부팅 정보가 변경되었거나 제공한 PIN이 올바르지 않기 때문에 TPM에서 드라이브의 잠금을 해제할 수 없습니다. 드라이브가 임의로 변경되지 않았는지 확인하고 신뢰할 수 있는 원본에서 시스템 부팅 정보를 변경했는지 확인하십시오. 드라이브가 액세스하기에 안전한지 확인한 후 BitLocker 복구 콘솔을 사용하여 드라이브의 잠금을 해제한 다음 BitLocker를 일시 중단했다가 다시 시작하여 BitLocker에서 이 드라이브에 연결한 시스템 부팅 정보를 업데이트하십시오.
FVE_E_TPM_NO_VMK 0x80310042	BitLocker 암호화 키를 TPM에서 가져올 수 없습니다.
FVE_E_PIN_INVALID 0x80310043	BitLocker 암호화 키를 TPM과 PIN에서 가져올 수 없습니다.
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	BitLocker 드라이브 암호화를 사용하도록 설정한 후 부팅 응용 프로그램이 변경되었습니다.
FVE_E_AUTH_INVALID_CONFIG 0x80310045	BitLocker 드라이브 암호화를 사용하도록 설정한 후 BCD(부팅 구성 데이터) 설정이 변경되었습니다.
FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED 0x80310046	FIPS를 따라야 하는 그룹 정책 설정 때문에 암호화되지 않은 키를 사용할 수 없어 이 드라이브에서 BitLocker를 일시 중단할 수 없습니다. 자세한 내용은 도메인 관리자에게 문의하십시오.
FVE_E_FS_NOT_EXTENDED 0x80310047	파일 시스템이 드라이브 끝까지 확장되지 않기 때문에 이 드라이브를 BitLocker 드라이브 암호화로 암호화할 수 없습니다. 이 드라이브를 다시 분할하고 다시 시도하십시오.
FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED 0x80310048	BitLocker 드라이브 암호화를 운영 체제 드라이브에서 사용하도록 설정할 수 없습니다. 컴퓨터 제조업체에 BIOS 업그레이드 지침에 대해 문의하십시오.
FVE_E_NO_LICENSE 0x80310049	이 버전의 Windows에서는 BitLocker 드라이브 암호화를 지원하지 않습니다. BitLocker 드라이브 암호화를 사용하려면 운영 체제를 업그레이드하십시오.
FVE_E_NOT_ON_STACK 0x8031004A	중요한 BitLocker 시스템 파일이 없거나 손상되어 BitLocker 드라이브 암호화를 사용할 수 없습니다. Windows 시작 복구를 사용하여 해당 파일을 컴퓨터로 복원하십시오.
FVE_E_FS_MOUNTED 0x8031004B	드라이브를 사용하는 동안에는 드라이브를 잠글 수 없습니다.
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	현재 스레드에 연결된 액세스 토큰이 가장된 토큰이 아닙니다.

상수/값

설명

FVE_E_DRY_RUN_FAILED 0x8031004D	BitLocker 암호화 키를 얻을 수 없습니다. TPM이 사용하도록 설정되어 있고 소유권을 가져왔는지 확인하십시오. 컴퓨터에 TPM이 없는 경우 USB 드라이브가 삽입되어 있고 사용 가능한지 확인하십시오.
FVE_E_REBOOT_REQUIRED 0x8031004E	BitLocker 드라이브 암호화를 계속하기 전에 시스템을 다시 시작해야 합니다.
FVE_E_DEBUGGER_ENABLED 0x8031004F	부팅 디버깅이 사용하도록 설정되어 있으면 드라이브 암호화를 수행할 수 없습니다. bcdedit 명령줄 도구를 사용하여 부팅 디버깅을 해제하십시오.
FVE_E_RAW_ACCESS 0x80310050	BitLocker 드라이브 암호화가 원시 액세스 모드이기 때문에 수행된 작업이 없습니다.
FVE_E_RAW_BLOCKED 0x80310051	드라이브가 현재 사용 중이기 때문에 BitLocker 드라이브 암호화가 이 드라이브에 대해 원시 액세스 모드로 전환할 수 없습니다.
FVE_E_BCD_APPLICATIONS_PATH_INCORRECT 0x80310052	BitLocker 드라이브 암호화 무결성이 보호된 응용 프로그램의 BCD(부팅 구성 데이터)에 지정된 경로가 잘못되었습니다. BCD 설정을 확인하고 수정한 다음 다시 시도하십시오.
FVE_E_NOT_ALLOWED_IN_VERSION 0x80310053	컴퓨터 사전 설치 또는 복구 환경이 실행되고 있는 경우 BitLocker 드라이브 암호화는 제한된 프로비저닝 또는 복구 용도로만 사용할 수 있습니다.
FVE_E_NO_AUTO_UNLOCK_MASTER_KEY 0x80310054	운영 체제 드라이브에서 자동 잠금 해제 마스터 키를 사용할 수 없습니다.
FVE_E_MOR_FAILED 0x80310055	시스템 펌웨어가 컴퓨터를 다시 시작할 때 시스템 메모리를 지우도록 설정하지 못했습니다.
FVE_E_HIDDEN_VOLUME 0x80310056	숨겨진 드라이브는 암호화할 수 없습니다.
FVE_E_TRANSIENT_STATE 0x80310057	드라이브가 일시적인 상태이므로 BitLocker 암호화 키가 무시되었습니다.
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	이 드라이브에서는 공개 키 기반 보호기를 사용할 수 없습니다.
FVE_E_VOLUME_HANDLE_OPEN 0x80310059	BitLocker 드라이브 암호화가 이 드라이브에서 작업을 이미 수행하고 있습니다. 계속하기 전에 모든 작업을 완료하십시오.
FVE_E_NO_FEATURE_LICENSE 0x8031005A	이 버전의 Windows는 이 BitLocker 드라이브 암호화 기능을 지원하지 않습니다. 이 기능을 사용하려면 운영 체제를 업그레이드하십시오.
FVE_E_INVALID_STARTUP_OPTIONS 0x8031005B	BitLocker 시작 옵션에 대한 그룹 정책 설정이 충돌하여 적용할 수 없습니다. 자세한 내용은 시스템 관리자에게 문의하십시오.



상수/값	설명
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED 0x8031005C	복구 암호를 만들 수 없도록 그룹 정책이 설정되어 있습니다.
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	복구 암호를 만들도록 그룹 정책이 설정되어 있습니다.
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	복구 키를 만들 수 없도록 그룹 정책이 설정되어 있습니다.
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	복구 키를 만들도록 그룹 정책이 설정되어 있습니다.
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 0x80310060	시작 시 PIN을 사용할 수 없도록 그룹 정책이 설정되어 있습니다. 다른 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_STARTUP_PIN_REQUIRED 0x80310061	시작 시 PIN을 사용하도록 그룹 정책이 설정되어 있습니다. 이 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED 0x80310062	시작 키를 사용할 수 없도록 그룹 정책이 설정되어 있습니다. 다른 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_STARTUP_KEY_REQUIRED 0x80310063	시작 키를 사용하도록 그룹 정책이 설정되어 있습니다. 이 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED 0x80310064	시작 키 및 PIN을 사용할 수 없도록 그룹 정책이 설정되어 있습니다. 다른 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED 0x80310065	시작 키 및 PIN을 사용하도록 그룹 정책이 설정되어 있습니다. 이 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED 0x80310066	그룹 정책에서 시작 시 TPM만 사용을 허용하지 않습니다. 다른 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_STARTUP_TPM_REQUIRED 0x80310067	시작 시 TPM만 사용하도록 그룹 정책이 설정되어 있습니다. 이 BitLocker 시작 옵션을 선택하십시오.
FVE_E_POLICY_INVALID_PIN_LENGTH 0x80310068	제공된 PIN이 최소 또는 최대 길이 요구 사항에 맞지 않습니다.
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 0x80310069	드라이브의 현재 BitLocker 드라이브 암호화 버전에서는 키 보호기가 지원되지 않습니다. 드라이브를 업그레이드하여 키 보호기를 추가하십시오.
FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED 0x8031006A	암호를 만들 수 없도록 그룹 정책이 설정되어 있습니다.
FVE_E_POLICY_PASSPHRASE_REQUIRED	암호를 만들도록 그룹 정책이 설정되어 있습니다.



상수/값	설명
0x8031006B	
FVE_E_FIPS_PREVENTS_PASSPHRASE	FIPS를 따라야 하는 그룹 정책 설정 때문에 암호를 생성하거나 사용할 수 없습니다. 자세한 내용은 도메인 관리자에게 문의하십시오.
0x8031006C	
FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED	운영 체제 드라이브에 암호를 추가할 수 없습니다.
0x8031006D	
FVE_E_INVALID_BITLOCKER_OID	드라이브의 BitLocker OID(개체 식별자)가 잘못되거나 손상되었습니다. manage-BDE를 사용하여 이 드라이브의 OID를 다시 설정하십시오.
0x8031006E	
FVE_E_VOLUME_TOO_SMALL	드라이브가 너무 작아 BitLocker 드라이브 암호화를 사용할 수 없습니다.
0x8031006F	
FVE_E_DV_NOT_SUPPORTED_ON_FS	선택한 검색 드라이브 유형이 드라이브의 파일 시스템과 호환되지 않습니다. BitLocker To Go 검색 드라이브는 FAT로 포맷한 드라이브에서 만들어야 합니다.
0x80310070	
FVE_E_DV_NOT_ALLOWED_BY_GP	선택한 검색 드라이브 유형을 사용할 수 없도록 컴퓨터 그룹 정책이 설정되어 있습니다. BitLocker To Go와 함께 사용할 검색 드라이브를 만들 수 있도록 그룹 정책이 설정되어 있는지 확인하십시오.
0x80310071	
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED	스마트 카드 등의 사용자 인증서를 BitLocker 드라이브 암호화에 사용할 수 없도록 그룹 정책이 설정되어 있습니다.
0x80310072	
FVE_E_POLICY_USER_CERTIFICATE_REQUIRED	스마트 카드 같은 유효한 사용자 인증서를 BitLocker 드라이브 암호화에 사용하도록 그룹 정책이 설정되어 있습니다.
0x80310073	
FVE_E_POLICY_USER_CERT_MUST_BE_HW	BitLocker 드라이브 암호화에 스마트 카드 기반 키 보호기를 사용하도록 그룹 정책이 설정되어 있습니다.
0x80310074	
FVE_E_POLICY_USER_CONFIGURE_FDV_AUTO_UNLOCK_NOT_ALLOWED	BitLocker로 보호되는 고정 데이터 드라이브를 자동으로 잠금 해제할 수 없도록 그룹 정책이 설정되어 있습니다.
0x80310075	
FVE_E_POLICY_USER_CONFIGURE_RDV_AUTO_UNLOCK_NOT_ALLOWED	BitLocker로 보호되는 이동식 데이터 드라이브를 자동으로 잠금 해제할 수 없도록 그룹 정책이 설정되어 있습니다.
0x80310076	
FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED	이동식 데이터 드라이브에서 BitLocker 드라이브 암호화를 구성할 수 없도록 그룹 정책이 설정되어 있습니다.
0x80310077	
FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED	이동식 데이터 드라이브에서 BitLocker 드라이브 암호화를 켤 수 없도록 그룹 정책이 설정되어 있습니다. BitLocker를 켜야 하는 경우 시스템 관리자에게 문의하십시오.
0x80310078	
FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED	이동식 데이터 드라이브에서 BitLocker 드라이브 암호화를 끌 수 없도록 그룹 정책이 설정되어 있습니다. BitLocker를 꺼야 하는 경우 시스템 관리자에게 문의하십시오.
0x80310079	



상수/값

설명

FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH

0x80310080

제공된 암호가 최소 암호 길이 요구 사항에 맞지 않습니다. 기본적으로 암호는 8자 이상이어야 합니다. 시스템 관리자에게 문의하여 해당 조직의 암호 길이 요구 사항을 확인하십시오.

FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE

0x80310081

암호가 시스템 관리자가 설정한 복잡성 요구 사항에 맞지 않습니다. 대/소문자, 숫자 및 기호를 추가해 보십시오.

FVE_E_RECOVERY_PARTITION

0x80310082

Windows 시스템 복구 옵션용으로 예약된 드라이브이기 때문에 드라이브를 암호화할 수 없습니다.

FVE_E_POLICY_CONFLICT_FDVRK_OFF_AUK_ON

0x80310083

그룹 정책 설정과 충돌하여 BitLocker 드라이브 암호화를 이 드라이브에 적용할 수 없습니다. 사용자 복구 옵션을 사용하지 않도록 설정한 경우에는 고정 데이터 드라이브를 자동으로 잠금 해제하도록 BitLocker를 구성할 수 없습니다. 키 유효성 검사 후에 BitLocker로 보호되는 고정 데이터 드라이브를 자동으로 잠금 해제하려면 시스템 관리자에게 문의하여 설정 충돌을 해결한 후 BitLocker를 사용하도록 설정하십시오.

FVE_E_POLICY_CONFLICT_RDVRK_OFF_AUK_ON

0x80310084

그룹 정책 설정과 충돌하여 BitLocker 드라이브 암호화를 이 드라이브에 적용할 수 없습니다. 사용자 복구 옵션을 사용하지 않도록 설정한 경우에는 이동식 데이터 드라이브를 자동으로 잠금 해제하도록 BitLocker를 구성할 수 없습니다. 키 유효성 검사 후에 BitLocker로 보호되는 이동식 데이터 드라이브를 자동으로 잠금 해제하려면 시스템 관리자에게 문의하여 설정 충돌을 해결한 후 BitLocker를 사용하도록 설정하십시오.

FVE_E_NON_BITLOCKER_OID

0x80310085

지정된 인증서의 EKU(확장된 키 사용) 특성으로 인해 BitLocker 드라이브 암호화에 사용할 수 없습니다. BitLocker에는 EKU 특성이 구성된 인증서가 필요하지 않지만 이 특성을 구성하는 경우 BitLocker에 대해 구성된 OID(개체 식별자)와 동일한 OID로 설정해야 합니다.

FVE_E_POLICY_PROHIBITS_SELFSIGNED

0x80310086

그룹 정책 설정과 충돌하여 BitLocker 드라이브 암호화를 현재 구성된 대로 이 드라이브에 적용할 수 없습니다. 드라이브 암호화를 위해 제공한 인증서가 자체 서명되어 있습니다. 자체 서명된 인증서를 사용할 수 없도록 현재 그룹 정책이 설정되어 있습니다. 인증 기관에서 새 인증서를 얻은 후 BitLocker를 사용하도록 설정하십시오.

FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRE D

0x80310087

그룹 정책 설정과 충돌하여 BitLocker 암호화를 이 드라이브에 적용할 수 없습니다. BitLocker로 보호되지 않는 드라이브에 대한 쓰기 액세스가 거부된 경우 USB 시작 키를 사용하도록 요구할 수 없습니다. 시스템 관리자를 통해 이러한 정책 충돌을 해결한 후 BitLocker를 사용하도록 설정하십시오.

FVE_E_CONV_RECOVERY_FAILED

0x80310088

운영 체제 드라이브의 복구 옵션에 대한 그룹 정책 설정과 충돌하여 BitLocker 드라이브 암호화를 이 드라이브에 적용할 수 없습니다. 복구 암호를 생성하는 것이 허용되지 않는 경우 Active Directory 도메인 서비스에 복구 정보를 저장하도록 요구할 수 없습니다. 시스템 관리자를 통해 이러한 정책 충돌을 해결한 후 BitLocker를 사용하도록 설정하십시오.

FVE_E_VIRTUALIZED_SPACE_TOO_BIG

0x80310089

요청한 가상화 크기가 너무 큼니다.

FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON

0x80310090

운영 체제 드라이브의 복구 옵션에 대한 그룹 정책 설정과 충돌하여 BitLocker 드라이브 암호화를 이 드라이브에 적용할 수 없습니다. 복구 암호를 생성하는 것이 허용되지 않는 경우 Active

	Directory 도메인 서비스에 복구 정보를 저장하도록 요구할 수 없습니다. 시스템 관리자를 통해 이러한 정책 충돌을 해결한 후 BitLocker를 사용하도록 설정하십시오.
FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON 0x80310091	고정 데이터 드라이브의 복구 옵션에 대한 그룹 정책 설정과 충돌하여 BitLocker 드라이브 암호화를 이 드라이브에 적용할 수 없습니다. 복구 암호를 생성하는 것이 허용되지 않는 경우 Active Directory 도메인 서비스에 복구 정보를 저장하도록 요구할 수 없습니다. 시스템 관리자를 통해 이러한 정책 충돌을 해결한 후 BitLocker를 사용하도록 설정하십시오.
FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON 0x80310092	이동식 데이터 드라이브의 복구 옵션에 대한 그룹 정책 설정과 충돌하여 BitLocker 드라이브 암호화를 이 드라이브에 적용할 수 없습니다. 복구 암호를 생성하는 것이 허용되지 않는 경우 Active Directory 도메인 서비스에 복구 정보를 저장하도록 요구할 수 없습니다. 시스템 관리자를 통해 이러한 정책 충돌을 해결한 후 BitLocker를 사용하도록 설정하십시오.
FVE_E_NON_BITLOCKER_KU 0x80310093	지정한 인증서의 KU(키 사용) 특성으로 인해 BitLocker 드라이브 암호화에 사용할 수 없습니다. BitLocker에는 KU 특성이 구성된 인증서가 필요하지 않지만 이 특성을 구성하는 경우 키 암호화 또는 키 계약으로 설정해야 합니다.
FVE_E_PRIVATEKEY_AUTH_FAILED 0x80310094	지정한 인증서에 연결된 개인 키를 인증할 수 없습니다. 개인 키 인증이 제공되지 않았거나 제공된 인증이 올바르지 않습니다.
FVE_E_REMOVAL_OF_DRA_FAILED 0x80310095	데이터 복구 에이전트 인증서를 제거하려면 인증서 스냅인을 사용해야 합니다.
FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME 0x80310096	이 드라이브는 Windows Vista 및 Windows Server 2008에 포함된 BitLocker 드라이브 암호화 버전을 사용하여 암호화되었는데 이 버전에서는 조직 식별자를 지원하지 않습니다. 이 드라이브에 조직 식별자를 지정하려면 "manage-bde -upgrade" 명령을 사용하여 드라이브 암호화를 최신 버전으로 업그레이드하십시오.
FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME 0x80310097	이 컴퓨터에서 드라이브의 잠금이 자동으로 해제되었기 때문에 드라이브의 잠금을 설정할 수 없습니다. 이 드라이브의 잠금을 설정하려면 자동 잠금 해제 보호기를 제거하십시오.
FVE_E_FIPS_HASH_KDF_NOT_ALLOWED 0x80310098	해당 스마트 카드는 ECC 스마트 카드에 대한 기본 BitLocker 키 파생 함수 SP800-56A를 지원하지 않습니다. FIPS 규격을 요구하는 그룹 정책 설정으로 인해 BitLocker에서 암호화를 위해 다른 키 파생 함수를 사용할 수 없습니다. FIPS 제한 환경에서는 FIPS 규격 스마트 카드를 사용해야 합니다.
FVE_E_ENH_PIN_INVALID 0x80310099	TPM 및 강화된 PIN에서 BitLocker 암호화 키를 가져올 수 없습니다. 숫자만 포함된 PIN를 사용해 보십시오.
FVE_E_INVALID_PIN_CHARS 0x8031009A	요청한 TPM PIN에 잘못된 문자가 있습니다.
FVE_E_INVALID_DATUM_TYPE 0x8031009B	드라이브에 저장된 관리 정보에 알 수 없는 유형이 있습니다. 이전 버전의 Windows를 사용하는 경우 최신 버전을 사용하여 드라이브에 액세스해 보십시오.
FVE_E_EFI_ONLY	해당 기능은 EFI 시스템에서만 지원됩니다.

상수/값	설명
0x8031009C	
FVE_E_MULTIPLE_NKP_CERTS	둘 이상의 네트워크 키 보호기 인증서가 시스템에서 발견되었습니다.
0x8031009D	
FVE_E_REMOVAL_OF_NKP_FAILED	네트워크 키 보호기 인증서를 제거하려면 인증서 스냅인을 사용해야 합니다.
0x8031009E	
FVE_E_INVALID_NKP_CERT	네트워크 키 보호기 인증서 저장소에서 잘못된 인증서가 발견되었습니다.
0x8031009F	
FVE_E_NO_EXISTING_PIN	이 드라이브가 PIN으로 보호되지 않습니다.
0x803100A0	
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH	올바른 현재 PIN을 입력하십시오.
0x803100A1	
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED	PIN 또는 암호를 변경하려면 관리자 계정으로 로그인해야 합니다. 관리자로서 PIN 또는 암호를 다시 설정하려면 링크를 클릭하십시오.
0x803100A2	
FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED	너무 많은 실패한 요청 이후 BitLocker가 PIN 및 암호 변경을 사용하지 못하도록 설정했습니다. 관리자로서 PIN 또는 암호를 다시 설정하려면 링크를 클릭하십시오.
0x803100A3	
FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII	시스템 관리자가 암호에 인쇄 가능한 ASCII 문자만 포함하도록 설정했습니다. 여기에는 약센트 없는 문자(A-Z, a-z), 숫자(0-9), 공백, 산술 기호, 일반 구두점, 구분 문자 및 기타 기호(# \$ & @ ^ _ ~)가 포함됩니다.
0x803100A4	
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE	BitLocker 드라이브 암호화는 씬 프로비저닝된 저장소에서 사용된 공간에 대한 암호화만 지원합니다.
0x803100A5	
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE	BitLocker 드라이브 암호화는 씬 프로비저닝된 저장소에서 사용 가능한 공간 지우기를 지원하지 않습니다.
0x803100A6	
FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE	필요한 인증 키 길이를 드라이브에서 지원하지 않습니다.
0x803100A7	
FVE_E_NO_EXISTING_PASSPHRASE	이 드라이브가 암호로 보호되지 않습니다.
0x803100A8	
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH	올바른 현재 암호를 입력하십시오.
0x803100A9	
FVE_E_PASSPHRASE_TOO_LONG	암호는 256자를 초과할 수 없습니다.
0x803100AA	



상수/값	설명
FVE_E_NO_PASSPHRASE_WITH_TPM 0x803100AB	드라이브에 TPM 보호기가 있으므로 암호 키 보호기를 추가할 수 없습니다.
FVE_E_NO_TPM_WITH_PASSPHRASE 0x803100AC	드라이브에 암호 보호기가 있으므로 TPM 키 보호기를 추가할 수 없습니다.
FVE_E_NOT_ALLOWED_ON_CSV_STACK 0x803100AD	이 명령은 지정한 CSV 볼륨의 코디네이터 노드에서만 수행할 수 있습니다.
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	이 명령은 클러스터에 포함된 볼륨에서 수행할 수 없습니다.
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 0x803100AF	그룹 정책 구성 때문에 BitLocker 소프트웨어 암호화를 사용하도록 BitLocker를 되돌리지 못했습니다.
FVE_E_EDRIVE_BAND_IN_USE 0x803100B0	드라이브의 하드웨어 암호화 기능이 이미 사용되고 있으므로 BitLocker에서 드라이브를 관리할 수 없습니다.
FVE_E_EDRIVE_DISALLOWED_BY_GP 0x803100B1	하드웨어 기반 암호화를 사용할 수 없도록 그룹 정책이 설정되어 있습니다.
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	지정한 드라이브가 하드웨어 기반 암호화를 지원하지 않습니다.
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	디스크 암호화 또는 암호 해독 도중에는 BitLocker를 업그레이드할 수 없습니다.
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	검색 볼륨은 하드웨어 암호화를 사용하는 볼륨에 대해 지원되지 않습니다.
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	사전 부팅 키보드가 검색되지 않았습니다. 사용자는 볼륨 잠금 해제를 위해 필요한 입력을 제공하지 못할 수 있습니다.
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	사전 부팅 키보드 또는 Windows 복구 환경이 검색되지 않았습니다. 사용자는 볼륨 잠금 해제를 위해 필요한 입력을 제공하지 못할 수 있습니다.
FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE 0x803100B7	시작 PIN을 만들도록 그룹 정책이 설정되어 있지만 이 장치에서는 사전 부팅 키보드를 사용할 수 없습니다. 사용자는 볼륨 잠금 해제를 위해 필요한 입력을 제공하지 못할 수 있습니다.
FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE 0x803100B8	복구 암호를 만들도록 그룹 정책이 설정되어 있지만 이 장치에서 사전 부팅 키보드 또는 Windows 복구 환경을 사용할 수 없습니다. 사용자는 볼륨 잠금 해제를 위해 필요한 입력을 제공하지 못할 수 있습니다.
FVE_E_WIPE_CANCEL_NOT_APPLICABLE	사용 가능한 공간 지우기가 현재 수행되지 않습니다.



상수/값	설명
0x803100B9	
FVE_E_SECUREBOOT_DISABLED	보안 부팅을 사용하도록 설정하지 않았으므로 BitLocker는 플랫폼 무결성을 위해 보안 부팅을 사용할 수 없습니다.
0x803100BA	
FVE_E_SECUREBOOT_CONFIGURATION_INVALID	보안 부팅 구성이 BitLocker에 대한 요구 사항을 충족하지 않으므로 BitLocker는 플랫폼 무결성을 위해 보안 부팅을 사용할 수 없습니다.
0x803100BB	
FVE_E_EDRIVE_DRY_RUN_FAILED	사용하는 컴퓨터가 BitLocker 하드웨어 기반 암호화를 지원하지 않습니다. 펌웨어 업데이트가 있는지 컴퓨터 제조업체에 문의하십시오.
0x803100BC	
FVE_E_SHADOW_COPY_PRESENT	드라이브에 볼륨 새도 복사본이 포함되어 있으므로 볼륨에 대해 BitLocker를 사용하도록 설정할 수 없습니다. 볼륨을 암호화하기 전에 모든 볼륨 새도 복사본을 제거하십시오.
0x803100BD	
FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS	고급 부팅 구성 데이터용 그룹 정책 설정에 잘못된 데이터가 포함되어 있으므로 BitLocker 드라이브 암호화를 이 드라이브에 적용할 수 없습니다. BitLocker를 사용하도록 설정하기 전에 시스템 관리자에게 잘못된 구성 문제를 해결하도록 요청하십시오.
0x803100BE	
FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE	이 PC의 펌웨어는 하드웨어 암호화를 지원하지 않습니다.
0x803100BF	
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED	너무 많은 실패한 요청 이후 BitLocker가 암호 변경을 사용하지 못하도록 설정했습니다. 관리자로서 암호를 다시 설정하려면 링크를 클릭하십시오.
0x803100C0	
FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISABLED	암호를 변경하려면 관리자 계정으로 로그인해야 합니다. 관리자로서 암호를 다시 설정하려면 링크를 클릭하십시오.
0x803100C1	
FVE_E_LIVEID_ACCOUNT_SUSPENDED	지정된 Microsoft 계정이 일시 중단되었으므로 BitLocker에서 복구 암호를 저장할 수 없습니다.
0x803100C2	
FVE_E_LIVEID_ACCOUNT_BLOCKED	지정된 Microsoft 계정이 차단되었으므로 BitLocker에서 복구 암호를 저장할 수 없습니다.
0x803100C3	
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES	이 PC는 장치 암호화를 지원하도록 프로비전되지 않았습니다. 모든 볼륨에서 BitLocker를 사용하도록 설정하여 장치 암호화 정책을 준수하십시오.
0x803100C4	
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED	암호화되지 않은 고정 데이터 볼륨이 있으므로 이 PC는 장치 암호화를 지원하지 않습니다.
0x803100C5	
FVE_E_DE_HARDWARE_NOT_COMPLIANT	이 PC는 장치 암호화를 지원하기 위한 하드웨어 요구 사항을 충족하지 않습니다.
0x803100C6	
FVE_E_DE_WINRE_NOT_CONFIGURED	WinRE가 적절히 구성되지 않았으므로 이 PC는 장치 암호화를 지원하지 않습니다.
0x803100C7	



상수/값	설명
FVE_E_DE_PROTECTION_SUSPENDED 0x803100C8	해당 볼륨에서 보호가 사용되지만 일시 중단되었습니다. 시스템에 적용되고 있는 업데이트 때문일 수 있습니다. 다시 부팅한 후 다시 시도해 보십시오.
FVE_E_DE_OS_VOLUME_NOT_PROTECTED 0x803100C9	이 PC는 장치 암호화를 지원하도록 프로비전되지 않았습니다.
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	너무 여러 번 잘못된 암호로 시도하여 장치 잠금이 트리거되었습니다.
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 0x803100CB	해당 볼륨에서 보호가 사용되지 않았습니다. 보호를 사용하도록 설정하려면 연결된 계정이 필요합니다. 이미 연결된 계정이 있는 데 이 오류가 표시되면 이벤트 로그에서 자세한 내용을 참조하십시오.
FVE_E_INVALID_PIN_CHARS_DETAILED 0x803100CC	PIN에는 숫자 0 ~ 9만 포함할 수 있습니다.
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	PC에서 카운터를 사용할 수 없으므로 BitLocker가 하드웨어 재생 보호를 사용할 수 없습니다.
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	카운터가 일치하지 않으므로 장치 잠금 상태 유효성 검사에 실패했습니다.
FVE_E_BUFFER_TOO_LARGE 0x803100CF	입력 버퍼가 너무 큼니다.



용어집

활성화 - 컴퓨터가 EE 서버/VE 서버에 등록되고 최소한 초기 정책 집합을 수신하면 활성화가 발생합니다.

Active Directory(AD) - Microsoft에서 Windows 도메인 네트워크용으로 만든 디렉터리 서비스입니다.

Advanced Authentication - Advanced Authentication 제품은 완벽하게 통합된 지문, 스마트 카드, 비접촉식 스마트 카드 판독기 옵션을 제공합니다. Advanced Authentication은 여러 가지 하드웨어 인증 방법을 관리하는 데 도움이 되며, 자체 암호화 드라이브 및 SSO를 통한 로그인을 지원하며, 사용자 자격 증명 및 암호를 관리합니다. 또한 Advanced Authentication을 사용하여 PC뿐만 아니라 모든 웹사이트, SaaS 또는 응용 프로그램에 액세스할 수 있습니다. 사용자가 자격 증명을 등록하면 Advanced Authentication은 해당 자격 증명을 사용하여 장치에 로그인하고 암호를 변경할 수 있도록 합니다.

Advanced Threat Protection - Advanced Threat Protection 제품은 알려지거나 알려지지 않은 사이버 위협의 실행 또는 끝점 손상을 식별, 분류 및 방지하기 위해 알고리즘 과학 및 장치 학습을 사용하는 차세대 안티바이러스 보호 기능을 제공합니다.

BitLocker Manager - Windows BitLocker는 데이터 및 운영 체제 파일 모두를 암호화하여 Windows 컴퓨터를 보호하도록 설계되었습니다. Dell은 BitLocker 배포의 보안을 강화하고 소유 비용을 간소화하여 절감할 수 있도록 중앙에서 관리되는 단일 콘솔을 제공합니다. 이 콘솔은 여러 가지 보안 문제를 해결하고 실제, 가상 또는 클라우드 기반의 BitLocker 이외의 플랫폼에서 암호화를 관리할 수 있는 통합된 접근 방식을 제공합니다. BitLocker Manager는 운영 체제, 고정 드라이브, BitLocker To Go에 대한 BitLocker 암호화를 지원합니다. BitLocker Manager를 통해 BitLocker를 기존의 암호화 요건에 원활하게 통합하고 보안 및 규정 준수를 간소화하는 동시에 최소한의 노력으로 BitLocker를 관리할 수 있습니다. BitLocker Manager는 키 복구, 정책 관리 및 시행, 자동화된 TPM 관리, FIPS 준수, 준수 보고를 위한 통합된 관리 방식을 제공합니다.

캐시된 자격 증명 - 캐시된 자격 증명은 사용자가 Active Directory에서 성공적으로 인증할 때 PBA 데이터베이스에 추가되는 자격 증명입니다. 이 사용자 정보는 사용자가 Active Directory에 연결할 수 없을 때에도(예: 랩톱을 집으로 가져갈 경우) 로그인할 수 있도록 유지됩니다.

Cloud Edition - Cloud Edition은 Dropbox, Dropbox for Business, Box, OneDrive 등과 같은 공용 클라우드 서비스에 저장된 데이터를 보호합니다. Cloud Edition은 파일이 클라우드 내부 및 외부로 이동될 때 데이터를 완벽하게 암호화합니다. Cloud Edition이 제공하는 기능은 다음과 같습니다. - 파일 활동, 동기화된 파일, 파일에 액세스한 사람, 위치, 시기, 준수 보고에 대한 감사 및 보고. - 파일 공유가 허용된 이메일 주소 목록 적용. - 클라우드 서비스, 폴더, 응용 프로그램 액세스에 대해 정책 적용. - 키 만료 및 폴링 기간 관리. - 관리자가 클라우드 서비스 공급자에 대해 알려진 모든 IP 주소를 모니터링하고 이를 응용 프로그램 프로세스에서 적용하여 암호화, 암호화 키, 데이터 복구, 정책, Forensic을 중앙에서 관리. Cloud Edition을 사용하면 iOS 및 Android를 실행하는 기기뿐만 아니라 개인 컴퓨터 또는 회사 컴퓨터에 데이터를 암호화할 수 있습니다.

일반 암호화 - 일반 키는 암호화된 파일이 생성된 장치에서 관리되는 모든 사용자가 이 파일에 액세스할 수 있도록 합니다.

비활성화 - Remote Management Console에서 SED Management가 FALSE(거짓)로 전환되면 비활성화가 발생합니다. 컴퓨터가 비활성화되면 PBA 데이터베이스가 삭제되고 캐시된 사용자 기록이 더 이상 존재하지 않게 됩니다.

Encryption 클라이언트 - Encryption 클라이언트는 끝점이 네트워크에 연결, 네트워크에서 분리, 분실 또는 도난 여부에 따라 보안 정책을 시행하는 장치 구성 요소입니다. 끝점에 신뢰할 수 있는 컴퓨팅 환경을 생성하는 Encryption 클라이언트는 장치 운영 체제에 추가적인 보안 계층을 형성하며 인증, 암호화, 권한 부여를 일관적으로 적용함으로써 중요한 정보를 최대한 보호할 수 있습니다.

암호화 키 - 대부분의 경우 Encryption 클라이언트는 사용자 키와 추가적인 2개의 암호화 키를 사용합니다. 예외: 모든 SDE 정책 및 보안 Windows 자격 증명 정책에서는 SDE 키를 사용합니다. Encrypt Windows 페이징 파일 암호화 정책 및 보안 Windows 최대 절전 모드 파일 정책은 자체 키인 GPK(General Purpose Key)를 사용합니다. 일반 키를 사용하면 파일이 생성된 장치에서 관리되는 모든 사용자가 파일에 액세스할 수 있습니다. 사용자 키를 사용하면 파일이 생성된 장치에서만 파일을 만든 사용자만 파일에 액세스할 수 있습니다. 사용자 로밍 키를 사용하면 Shield로 보호된 Windows(또는 Mac) 장치에서 파일을 만든 사용자만 파일에 액세스할 수 있습니다.

암호화 스왑 - 암호화 스왑은 포함된 파일의 암호화 상태를 올바르게 유지하기 위해 Shield로 보호된 끝점에서 암호화된 폴더를 스캔하는 프로세스입니다. 일반 파일 생성 및 이름 변경 작업으로는 암호화 스왑이 트리거되지 않습니다. 다음과 같이 암호화 스왑이 발생할 수 있는 시기와 그에 따른 스왑 횟수에 영향을 주는 요소를 파악하는 것이 중요합니다. - 암호화 스왑은 암호화를 활성화한 정책을 처음 수신할 때 발생합니다. 이것은 정책이 암호화를 사용하는 경우 활성화 직후 발생할 수 있습니다. - 로그인 시 워크스테이션 스캔 정책이 활성화되어 있으면 암호화가 지정된 폴더는 사용자가 로그인할 때마다 스왑됩니다. - 이후의 특정 정책 변경에 따라 스왑이 다시 발생할 수 있습니다. 암호화 폴더, 암호화 알고리즘, 암호화 키 용도(일반 및 사용자)의 정의에 관한 정책을 변경하는 경우 스왑이 트리거됩니다. 또한 암호화 사용 및 해제 전환 시 암호화 스왑이 트리거됩니다.

외부 사용자 - 조직의 도메인 주소 밖에 있는 사용자입니다. 내부 사용자는 이와 반대로 조직의 도메인 주소 안에 있는 사용자입니다.

컴퓨터 키 - 컴퓨터 키는 서버에 암호화가 설치되고 있을 때 서버의 파일 암호화 키 및 정책을 보호합니다. 컴퓨터 키는 DDP Server에 저장됩니다. 활성화가 진행되는 동안 새 서버는 DDP Server와 인증서를 교환하고 이 인증서를 이후의 인증에 사용합니다.

일회용 암호(OTP) - OTP는 단 한 번만 사용할 수 있는 암호로, 제한된 기간 동안에만 유효합니다. OTP를 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. OTP를 이용하려면 Security Console 및 Security Tools Mobile 앱을 사용하여 모바일 장치와 컴퓨터를 페어링해야 합니다. Security Tools Mobile 앱에서 생성된 모바일 장치의 암호는 Windows 로그인 화면에서 컴퓨터에 로그인하는 데 사용됩니다. 정책에 따라, 컴퓨터에 로그인할 때 OTP를 사용한 적이 없으면 암호가 만료되거나 분실한 경우 OTP 기능을 사용하여 컴퓨터에 대한 액세스 권한을 복구할 수 있습니다. OTP 기능은 그 밖에 인증이나 복구 목적으로 사용할 수도 있지만, 이 두 가지를 동시에 지원하지는 못합니다. OTP 보안은 생성된 암호가 1회용이며 유효 기간이 짧다는 점에서 다른 인증 방식의 보안 보다 강력하다고 할 수 있습니다.

PBA(Preboot Authentication) - PBA(Preboot Authentication)는 BIOS 또는 부팅 펌웨어를 확장하는 기능을 하며 운영 체제 외부에서 신뢰할 수 있는 인증 계층으로 안전한 변조 방지 환경을 보장합니다. PBA는 사용자에게 올바른 자격 증명이 있는지 확인할 때까지 하드 디스크에서 운영 체제 등의 데이터를 읽을 수 없도록 합니다.

SED Management - SED Management는 자체 암호화 드라이브를 안전하게 관리할 수 있는 플랫폼을 제공합니다. SED가 자체 암호화를 제공하기는 하지만 해당 암호화 및 사용 가능한 정책을 관리할 플랫폼은 없습니다. SED Management는 데이터를 더 효과적으로 보호하고 관리할 수 있게 해주는 확장 가능한 중앙 집중식 관리 구성요소입니다. SED Management를 통해 보다 빠르고 쉽게 회사 데이터를 관리할 수 있습니다.

Server 사용자 - 암호화 키 및 정책 업데이트 처리를 위해 Dell Data Protection | Server Encryption에서 생성하는 가상 사용자 계정입니다. 이 사용자 계정은 컴퓨터나 도메인의 기타 사용자 계정에 해당되지 않으며, 실제로 사용할 수 있는 사용자 이름 및 암호가 없습니다. 이 계정에는 Remote Management Console에서 고유한 UCID 값이 할당됩니다.

SDE(System Data Encryption) - SDE는 운영 체제와 프로그램 파일을 암호화하도록 설계되었습니다. 이러한 목적을 달성하기 위해 운영 체제가 부팅되는 동안 SDE가 해당 키를 열 수 있어야 합니다. 목적은 운영 체제에 대한 공격자의 오프라인 공격이나 변조를 방지하는 것입니다. SDE는 사용자 데이터에 사용하기 위한 용도가 아니며, 일반 및 사용자 키 암호화는 중요한 사용자 데이터에 사용하기 위한 용도입니다. 암호화 키 잠금을 해제하려면 사용자 암호가 필요하기 때문입니다. SDE 정책은 운영 체제가 부팅 프로세스를 시작하는 데 필요한 파일을 암호화하지 않습니다. SDE 정책은 부팅 전 인증을 요구하지 않으며 마스터 부트 레코드의 동작을 방해하지도 않습니다. 컴퓨터가 시작되면 사용자가 로그인하기 전에 암호화된 파일이 가용 상태가 되어 패치 관리, SMS, 백업 및 복구 도구를 사용할 수 있습니다. SDE 암호화를 비활성화하면 SDE 암호화 규칙 등과 같은 기타 SDE 정책과 관계 없이 관련 사용자에 대해 SDE로 암호화된 모든 파일 및 디렉터리의 자동 암호 해독이 트리거됩니다.

Threat Protection - Threat Protection 제품은 회사 컴퓨터를 보안 위협으로부터 보호하는 중앙 관리 정책을 기반으로 합니다. Threat Protection은 다음과 같은 기능으로 구성되어 있습니다. - 멀웨어 차단: 액세스할 때 또는 정책에 정의된 일정에 따라 항목을 자동 스캔하여 바이러스, 스파이웨어, 원치 않는 프로그램 및 기타 위협 요소 여부를 검사합니다. 클라이언트 방화벽 - 네트워크나 인터넷을 통한 컴퓨터와 리소스 사이의 통신을 모니터링하여 악의적일 수 있는 통신을 차단합니다. - 웹 차단: 웹 사이트의 안전 등급과 보고에 기반하여 온라인 검색 중에 안전하지 않은 웹 사이트 및 이러한 웹 사이트로부터의 다운로드를 차단합니다.

TPM(Trusted Platform Module) - TPM은 안전한 저장, 측정, 증명의 세 가지 주요 기능을 제공하는 보안 칩입니다. Encryption 클라이언트는 안전한 저장 기능 때문에 TPM을 사용합니다. TPM도 소프트웨어 자격 증명 모음에 대해 암호화된 컨테이너를 제공할 수 있습니다. TPM은 BitLocker Manager 및 OTP(일회용 암호) 기능을 사용하려는 경우에도 필요합니다.

사용자 암호화 - 사용자 키는 파일을 만든 장치에서 파일을 만든 사용자만 파일에 액세스할 수 있도록 합니다. Dell Data Protection | Server Encryption을 실행하면 사용자 암호화가 일반 암호화로 변환됩니다. 외장형 미디어 장치에 예외 하나가 발생합니다. 이 장치를 DDP|SE가 설치된 서버에 삽입하면 사용자 로밍 키를 통해 파일이 암호화됩니다.

