# Encryption

## 시스템 요구 사항 v10.1

## 참고, 주의 및 경고

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

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

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



2018 - 11

개정 A01

# 목차

# 1

# 소개

이 문서는 Dell Encryption 요구 사항을 제시합니다.

모든 Dell Encryption 설명서를 확인하려면 www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals을 참조하십시오.

## Dell ProSupport에 문의

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

또한, dell.com/support에서 Dell 제품에 대한 온라인 지원도 가능합니다. 온라인 지원에는 드라이버, 매뉴얼, 기술 자문, FAQ 및 최근에 나타나는 문제도 포함됩니다.

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

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

2

# 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 사용자에 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 Security Management Server/Security Management Server Virtual와 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 - 사전 요구 사항

- Microsoft .Net Framework 4.5.2 이상이 마스터 설치 프로그램 및 하위 설치 프로그램 클라이언트에 필요합니다. 설치 프로그램은 Microsoft .Net Framework 구성 요소를 설치하지 *않습니다*.

  Dell에서 배송된 모든 컴퓨터에는 전체 버전의 Microsoft .Net Framework 4.5.2 이상이 미리 설치되어 있습니다. 하지만 Dell 하드웨어에 설치하지 않거나 이전 Dell 하드웨어에서 클라이언트를 업그레이드하는 경우에는, **클라이언트를 설치하기 전에** 어떤 버전의 Microsoft .Net이 설치되어 있는지 확인한 후 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 Microsoft .Net Framework 4.5.2를 설치하려면 https://www.microsoft.com/en-us/download/details.aspx?id=42643로 이동하십시오.
- 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/support에서 해당 컴퓨터 모델을 선택하여 다운로드할 수 있습니다. 인증 하드웨어에 따라 적절한 드라이버 및 펌웨어를 다운로드하십시오.
  - ControlVault
  - NEXT 생채 인식 지문 드라이버
  - 유효 지문 판독기 495 드라이버
  - O2Micro 스마트 카드 드라이버

## 모든 클라이언트 - 하드웨어

- 다음 표에 지원되는 컴퓨터 하드웨어가 나와 있습니다.

| 하드웨어 |
| --- |
| – Intel Pentium 또는 AMD 프로세서 |
| – 110MB의 사용 가능한 디스크 공간 |

| 하드웨어 |
| --- |
| – 512MB RAM |

**노트: 끝점에서 파일을 암호화하려면 추가적인 여유 디스크 공간이 필요합니다. 정책과 드라이브 크기에 따라 이 디스크 크기가 다릅니다.**

# 모든 클라이언트 - 현지화

- Encryption 및 BitLocker Manager 클라이언트는 MUI(다국어 사용자 인터페이스)와 호환되며 다음 언어로 현지화됩니다.

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

# Encryption 클라이언트

- 클라이언트 컴퓨터가 네트워크에 연결되어 있어야 활성화할 수 있습니다.
- 초기 암호화 시간을 줄이려면 Windows 디스크 정리 마법사를 실행하여 임시 파일 및 기타 불필요한 데이터를 모두 제거합니다.
- 암호화 스윕이 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.
- 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. 기업 이미지에 Encryption 클라이언트를 설치하는 방법에 대한 지침은 http://www.dell.com/support/article/us/en/19/SLN304039을 참조하십시오.
- 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 http://www.dell.com/support/article/us/en/19/SLN288353을 참조하거나 Dell ProSupport에 연락하여 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 사전 요구 사항

- 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.

**사전 요구 사항**

- Visual C++ 2012 업데이트 4 이상의 재배포 가능 패키지(x86 및 x64)
- Visual C++ 2015 업데이트 3 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 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 버전 1607(Anniversary Update/Redstone 1) - 버전 1803(April 2018 Update/Redstone 4)
- VMware Workstation 12.5 이상

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

# Encryption External Media 운영 체제

- 다음 표에는 Encryption External Media로 보호되는 미디어에 대한 액세스가 지원되는 운영 체제가 자세히 나와 있습니다.

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

**Encryption External Media로 보호받는 미디어(32 및 64비트)에 대한 액세스가 지원되는 Windows 운영 체제**

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer

**Encryption External Media로 보호받는 미디어(32 및 64비트)에 대한 액세스가 지원되는 Windows 운영 체제**

- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro 버전 1607(Anniversary Update/Redstone 1) - 버전 1803(April 2018 Update/Redstone 4)

**Encryption External Media로 보호되는 미디어에 대한 액세스가 지원되는 Mac 운영 체제(64비트 커널)**

- macOS Sierra 10.12.4 및 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

# Server Encryption 클라이언트

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

- Server Encryption은 Encryption Enterprise 및 Endpoint Security Suite Enterprise와만 호환됩니다.
- Server Encryption은 다음을 제공합니다.
  - 소프트웨어 암호화
  - 이동식 미디어 암호화
  - 포트 제어

  **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 외부 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 원격 데스크톱 연결이 설정된 경우가 아니라면 사용자가 컴퓨터를 사용할 수 없게 됩니다.

**Server Encryption은 다음에서 사용합니다.**

- 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 Encryption는 업계 최고의 바이러스 백신 공급자의 검증을 거쳤습니다. 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 SLN298707을 참조하거나 Dell ProSupport에 연락하여 도움을 받으십시오.

**지원 안 됨**

Server Encryption은 다음에서 사용하지 않습니다.

- Security Management Server/Security Management Server Virtual용 데이터베이스를 실행하는 Security Management Server/Security Management Server Virtual 또는 서버.
- Server Encryption은 Encryption Personal과 호환되지 않습니다.
- Server Encryption은 SED Management 또는 BitLocker Manager 클라이언트에서 지원되지 않습니다.
- DFS(Distributed File Systems)의 일부인 서버에 Server Encryption이 지원되지 않습니다.
- Server Encryption으로 들어가거나 나가는 마이그레이션은 지원되지 않습니다. Encryption External Media에서 Server Encryption으로 업그레이드하려면 Server Encryption을 설치하기 전에 이전 제품 또는 제품의 설치를 완전히 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 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.
- 인플레이스 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. 암호화된 데이터 복구에 대한 자세한 내용은 *Recovery Guide(복구 안내서)*를 참조하십시오.

# 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 SP1: Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro 버전 1607(Anniversary Update/Redstone 1) - 버전 1803(April 2018 Update/Redstone 4)

### 지원되는 서버 운영 체제

- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Datacenter Edition(Server Core은 지원되지 않음)
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition(Server Core는 지원되지 않음)
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition(Server Core은 지원되지 않음)

### UEFI 모드가 지원되는 운영 체제

- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro 버전 1607(Anniversary Update/Redstone 1) - 버전 1803(April 2018 Update/Redstone 4)

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

# Encryption External Media 운영 체제

다음 표에는 Encryption External Media로 보호되는 미디어에 대한 액세스가 지원되는 운영 체제가 자세히 나와 있습니다.

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

### Encryption External Media로 보호받는 미디어(32 및 64비트)에 대한 액세스가 지원되는 Windows 운영 체제

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Enterprise, Pro
- Windows 10: Education, Enterprise, Pro 버전 1607(Anniversary Update/Redstone 1) - 버전 1803(April 2018 Update/Redstone 4)

### 지원되는 서버 운영 체제

- Windows Server 2012 R2

### Encryption External Media로 보호되는 미디어에 대한 액세스가 지원되는 Mac 운영 체제(64비트 커널)

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14