Dell Data Protection | Endpoint Security Suite Enterprise

기본 설치 안내서 v1.4

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.

Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise 및 Dell Data Guardian 문서 세트에 사용된 등록된 상표 및 상표, 즉 Dell™, Dell 로고, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® 및 KACE™는 Dell Inc. Cylance® 및 CylancePROTECT의 상표이고 Cylance 로고는 미국에서 Cylance, Inc.의 등록된 상표입니다. 상표입니다. McAfee® 및 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 Dell EMC의 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. 소스 코드는 7-zip.org에서 찾아볼 수 있습니다. 라이센싱에는 GNU LGPL 라이센스 + unRAR 제한이 적용됩니다(www.7-zip.org/license.txt).

Endpoint Security Suite Enterprise 기본 설치 안내서

2017 - 04

개정 A01

목차

1

소개

이 안내서에서는 ESS 마스터 설치 프로그램을 사용하여 응용 프로그램을 설치 및 구성하는 방법을 자세히 설명합니다. 또한 기본적인 설치 지원을 제공합니다. 하위 설치 프로그램의 설치, EE Server/VE Server 구성에 관한 정보가 필요하거나 혹은 ESS 마스터 설치 프로그램의 기본적인 지원 범위를 벗어나는 내용의 정보가 필요할 경우, *Advanced 설치 안내서*를 참조하십시오.

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 Advanced Threat Prevention의 테넌트 프로비저닝합니다. Advanced Threat Prevention의 정책 집행이 활성화되기 전에 테넌트가 DDP Server에서 프로비전되어야 합니다.

3 이 문서의 요구 사항 장을 읽고 숙지하십시오.

4 최종 사용자에게 클라이언트를 배포하십시오.

이 안내서 사용

다음 순서에 따라 이 안내서를 사용합니다.

- 클라이언트 필수 구성 요소에 대해서는 요구 사항을 참조하십시오.
- 다음 중 하나를 선택하십시오.
   - ESSE 마스터 설치 프로그램을 사용하여 대화형으로 설치

     또는
   - ESSE 마스터 설치 프로그램을 사용하여 명령줄을 통해 설치

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 번호를 확인하십시오.

2

요구 사항

모든 클라이언트

- 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.
- ESSE 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

- Microsoft .Net Framework 4.5.2 이상이 ESSE 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=42643으로 이동하십시오.
- ControlVault용 드라이버 및 펌웨어, 지문 판독기 및 스마트 카드는(아래 참조) ESSE 마스터 설치 프로그램 또는 하위 설치 프로그램 실행 파일에 포함되어 있지 않습니다. 드라이버 및 펌웨어는 최신 상태로 유지해야 하며 http://www.dell.com/support에서 컴퓨터 모델을 선택하여 다운로드하십시오. 인증 하드웨어에 따라 적절한 드라이버 및 펌웨어를 다운로드하십시오.

  - 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. ControlVault 드라이버 설치 지침은 Dell ControlVault 드라이버 및 펌웨어 업데이트에 제시되어 있습니다.

모든 클라이언트 - 하드웨어

- 다음 표에 지원되는 컴퓨터 하드웨어가 나와 있습니다.

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

모든 클라이언트 - 언어 지원

- Encryption Advanced Threat Prevention 및 BitLocker Manager 클라이언트는 MUI(다국어 사용자 인터페이스)와 호환되며 다음 언어를 지원합니다. Remote Management Console에서 Advanced Threat Prevention 데이터는 영어로만 표시됩니다.

  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.
- 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.
- 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/SLN298707을 참조하거나 Dell ProSupport에 연락하여 도움을 받으십시오.
- 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

- ESSE 마스터 설치 프로그램에서 Microsoft Visual C++ 2012 업데이트 4를 설치합니다(컴퓨터에 이미 설치되어 있지 않은 경우).

필수 구성 요소

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

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

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

EMS(External Media Shield) 운영 체제

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

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

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

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

- macOS Sierra 10.12.0

Advanced Threat Prevention 클라이언트

- 컴퓨터에서 Dell Client Security Framework(EMAgent) 클라이언트가 검색되지 않으면 Advanced Threat Prevention 클라이언트를 설치할 수 없습니다. 설치를 시도해도 실패합니다.
- 클라이언트를 관리하는 Dell Enterprise Server/VE가 연결된 모드(기본)로 실행되고 있을 때 Advanced Threat Prevention 설치를 완료하려면 컴퓨터가 네트워크에 연결되어 있어야 합니다. 하지만 관리하는 Dell 서버가 연결되지 않은 모드로 실행되고 있을 때는 Advanced Threat Prevention 설치에 네트워크 연결이 필요하지 ***않습니다***.
- Advanced Threat Prevention에 대한 테넌트를 프로비저닝하려면 Dell 서버가 인터넷에 연결되어 있어야 합니다.

  노트: Dell 서버가 연결되지 않은 모드로 실행되고 있을 때는 인터넷 연결이 필요하지 않습니다.
- 연결되지 않은 모드로 실행되는 Dell Enterprise Server/VE에서 관리하는 클라이언트 컴퓨터에는 선택 사양인 클라이언트 방화벽 및 웹 보호 기능을 설치해서는 ***안 됩니다***.
- 다른 공급업체의 안티바이러스, 안티멀웨어 및 안티스파이웨어 응용 프로그램이 Advanced Threat Prevention 클라이언트와 충돌할 수 있습니다. 가능한 경우 이러한 응용프로그램의 설치를 제거하십시오. 충돌하는 소프트웨어에 Windows Defender가 포함되지 않습니다. 방화벽 응용프로그램을 사용할 수 있습니다.

  다른 안티바이러스, 안티멀웨어 및 안티스파이웨어 응용 프로그램의 설치를 제거할 수 없는 경우에는 Dell 서버의 Advanced Threat Protection과 함께 다른 응용 프로그램에 대한 제외를 추가해야 할 수도 있습니다. Dell 서버에서 Advanced Threat Protection에 제외를 추가하는 방법에 관한 지침은 http://www.dell.com/support/article/us/en/04/SLN300970을(를) 참조하십시오. 다른 안티바이러스 응용 프로그램에 추가하기 위한 제외의 목록은 http://www.dell.com/support/article/us/en/19/SLN301134을(를) 참조하십시오.

Advanced Threat Prevention 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
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

고급 위협 방지 포트

- 고급 위협 방지 에이전트는 관리 콘솔 SaaS 플랫폼에서 관리되고 보고됩니다. 포트 443(https)은 통신하는 데 사용되며 에이전트가 콘솔과 통신하기 위해 방화벽에서 반드시 열려 있어야 합니다. 콘솔은 Amazon 웹 서비스에 의해 호스트되며 고정 IP가 없습니다. 어떠한 이유로든 포트 443이 차단되면 업데이트가 다운로드될 수 없기 때문에, 컴퓨터가 가장 최신 보호 기능을 사용할 수 없습니다. 클라이언트 컴퓨터가 다음과 같은 URL에 액세스할 수 있어야 합니다.

사용	응용 프로그램 프로토콜	전송 프로토콜	포트 번호	대상	방향
모든 통신	HTTPS	TCP	443	*.cylance.com에 모든 https 트래픽 허용	아웃바운드

BIOS 이미지 무결성 확인

Remote Management Console에서 *Enable BIOS Assurance* 정책이 선택되어 있으면 Cylance 테넌트가 최종 사용자 시스템에서 BIOS 해시의 유효성을 검사해 Dell 초기 버전에서 BIOS가 수정되지 않았음을 확인합니다. 수정된 경우 공격 벡터의 가능성이 있습니다. 위협이 감지되면 DDP Server에 알림이 전달되고 IT 관리자가 Remote Management Console에서 경고를 받습니다. 프로세스 개요는 BIOS 이미지 무결성 확인 프로세스를 참조하십시오.

노트: 사용자 지정 출하시 이미지는 BIOS가 수정되었기 때문에 이 기능과 함께 사용할 수 없습니다.

BIOS 이미지 무결성 확인이 지원되는 Dell 컴퓨터 모델

- Latitude 3470
- Latitude 3570
- Latitude 7275
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision 모바일 워크스테이션 3510
- Precision 모바일 워크스테이션 5510
- Precision 워크스테이션 3620
- Precision 워크스테이션 7510
- Precision 워크스테이션 7710
- Precision 워크스테이션 T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

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.

  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 로그온할 때까지 기다릴 수 없다는 것입니다. 이 문제를 해결하려면 BIOS에서 SATA 작동을 *RAID=On*에서 *AHCI* 로 변경합니다. 운영 체제에 AHCI 컨트롤러 드라이브가 사전 설치되어 있지 않은 경우 *RAID=On*에서 *AHCI* 로 전환할 때 파란색 화면이 표시됩니다.
- SED Management는 Server Encryption 또는 server OS의 Advanced Threat Prevention과 함께 사용할 경우에 지원되지 않습니다.

SED 클라이언트 필수 구성 요소

- ESSE 마스터 설치 프로그램에서 Microsoft Visual C++2010 SP1 **및** Microsoft Visual C++ 2012 업데이트 4를 설치합니다(컴퓨터에 이미 설치되어 있지 않은 경우).

전제조건

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

SED 클라이언트 하드웨어

국제 키보드

- 다음 표에는 UEFI 및 비 UEFI 컴퓨터에서 사전 부팅 인증이 지원되는 국제 키보드가 나열되어 있습니다.

국제 키보드 지원 - UEFI

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

국제 키보드 지원 - 비 UEFI

- AR - 아랍어(라틴 문자 사용)
- DE-CH - 독일어(스위스)
- DE-FR - 프랑스어(스위스)

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)

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

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

Advanced Authentication 클라이언트

- Advanced Authentication을 통해 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 등록한 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.com을 참조하십시오.

Advanced Authentication 클라이언트 하드웨어

- 다음 표에는 지원되는 인증 하드웨어가 자세히 설명되어 있습니다.

지문 및 스마트 카드 판독기

- 보안 모드의 Validity VFS495
- 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 노트북에 탑재된 비접촉식 카드 리더기를 이용한 비접촉식 카드

스마트 카드

- ActivIdentity 클라이언트를 사용하는 PKCS #11 스마트 카드

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

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

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 7에서 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

Android 운영 체제

- 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 사항을 검토하시기 바랍니다.
- PBA 파티션이 설정되었는지 확인하십시오. PBA 파티션이 설정되기 전에 BitLocker Manager를 설치한 경우 BitLocker를 사용할 수 없으며 BitLocker Manager가 작동하지 않습니다.
- 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.
- BitLocker Manager는 Server Encryption 또는 server OS의 Advanced Threat Prevention과 함께 사용할 경우에 지원되지 않습니다.

BitLocker Manager 클라이언트 필수 구성 요소

- ESSE 마스터 설치 프로그램에서 Microsoft Visual C++2010 SP1 **및** Microsoft Visual C++ 2012 업데이트 4를 설치합니다(컴퓨터에 이미 설치되어 있지 않은 경우).

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)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition(64비트)
- Windows Server 2016

ESSE 마스터 설치 프로그램을 사용하여 설치

- 명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.
- 기본이 아닌 포트를 사용하여 설치하려면 ESSE 마스터 설치 프로그램 대신 하위 설치 프로그램을 사용합니다.
- ESS 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 Authentication 및 Advanced Threat Prevention의 기능 사용 방법에 대해서는 *Endpoint Security Suite Enterprise 도움말*을 참조하십시오. <Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help에서 도움말에 액세스하십시오.
- 설치 후, 사용자가 시스템 트레이에서 Dell Data Protection 아이콘을 마우스 오른쪽 단추로 클릭하고 **정책 업데이트 확인**을 선택하여 정책을 업데이트해야 합니다.
- ESSE 마스터 설치 프로그램은 전체 제품군을 설치합니다. ESSE 마스터 설치 프로그램을 사용하여 설치하는 방법은 두 가지입니다. 다음 중 하나를 선택하십시오.
  - ESSE 마스터 설치 프로그램을 사용하여 대화형으로 설치

  또는

  - ESSE 마스터 설치 프로그램을 사용하여 명령줄을 통해 설치

ESSE 마스터 설치 프로그램을 사용하여 대화형으로 설치

- ESSE 마스터 설치 프로그램의 위치는 다음과 같습니다.
  - **Dell FTP 계정** - DDP-Endpoint-Security-Suite-1.x.x.xxx.zip에서 설치 번들을 찾습니다.
- 지침에 따라 ESS 마스터 설치 프로그램을 사용하여 Dell Endpoint Security Suite Enterprise을 대화형으로 설치합니다. 이 방법을 사용하면 제품군을 한 번에 한 대의 컴퓨터에 설치할 수 있습니다.

1. Dell 설치 미디어에서 **DDPSuite.exe**를 찾습니다. 로컬 컴퓨터로 복사합니다.
2. 설치 프로그램을 실행하려면 **DDPSuite.exe**를 두 번 클릭합니다. 몇 분 정도 걸릴 수 있습니다.
3. 시작 대화 상자에서 **다음**을 클릭하십시오.
4. 라이선스 계약서를 읽고 조건을 수락한 후 **다음**을 클릭합니다.
5. **Enterprise Server 이름** 필드에 대상 사용자를 관리할 EE Server/VE Server의 정규화된 호스트 이름(예: server.organization.com)을 입력합니다.

   Device Server URL 필드에 클라이언트가 통신할 Device Server(Security Server)의 URL을 입력합니다.

   형식은 https://server.organization.com:**8443**/xapi**/**(맨 끝의 슬래시 포함)입니다.

   다음을 클릭합니다.
6. **다음**을 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.
7. 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 Tools를 설치합니다.

*Advanced Authentication*은 고급 인증에 필요한 파일 및 서비스를 설치합니다.

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

*Threat Protection*은 바이러스, 스파이웨어, 원치 않는 프로그램이 있는지 검사하는 멀웨어 및 안티바이러스 보호 기능을 제공하는 Threat Protection 클라이언트, 네트워크나 인터넷을 통한 컴퓨터와 리소스 사이의 통신을 모니터링하는 클라이언트 방화벽, 웹 사이트의 안전 등급을 표시하거나 온라인 검색 중에 안전하지 않은 웹 사이트에 대한 액세스를 차단하는 웹 필터링을 설치합니다.

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

*Advanced Threat Protection*은 알려지거나 알려지지 않은 사이버 위협의 실행 또는 끝점 손상을 식별, 분류 및 방지하기 위해 알고리즘 과학 및 장치 학습을 사용하는 차세대 안티바이러스 보호 기능을 제공하는 Advanced Threat Prevention 클라이언트를 설치합니다.

*Web Protection 및 Firewall*은 선택 사양 기능인, Web Protection 및 Firewall을 설치합니다. 클라이언트 방화벽은 해당 규칙 목록에서 들어오고 나가는 모든 트래픽을 검사합니다. 웹 차단은 웹 검색 및 다운로드를 모니터링하여 웹 사이트의 등급을 기반으로 위협이 감지될 때 정책에 따라 설정된 조치를 적용합니다.

> **노트: 동일한 컴퓨터에서 Threat Protection과 Advanced Threat Prevention을 함께 사용할 수 없습니다. 설치 프로그램이 자동으로 두 구성 요소 중 하나만 선택하도록 합니다. Threat Protection을 설치하려면 Endpoint Security Suite 고급 설치 안내서를 다운로드하여 지침을 따르십시오.**

선택이 완료되면 **다음**을 클릭합니다.

8 **설치**를 클릭하여 설치를 시작합니다. 설치는 몇 분 정도 걸릴 수 있습니다.

9 **예, 컴퓨터를 지금 다시 시작합니다**를 선택하고 **마침**을 클릭합니다.
설치가 완료됩니다.

ESSE 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 ESSE 마스터 설치 프로그램과 함께 사용할 수 있는 스위치에 대한 설명이 나와 있습니다.

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

매개 변수

- 다음 표에 ESSE 마스터 설치 프로그램과 함께 사용할 수 있는 매개 변수에 대한 설명이 나와 있습니다. ESSE 마스터 설치 프로그램에서 개별 구성 요소를 제외할 수 없지만 명령을 수신해 어떤 구성 요소를 설치해야 할지 지정할 수는 있습니다.

매개변수	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. ATP = 서버 OS에는 Advanced Threat Prevention ***만*** 있고, 워크스테이션 OS에는 Advanced Threat Prevention ***및*** Encryption이 있음 DE-ATP = 서버 OS의 Advanced Threat Prevention 및 Encryption. 서버 OS에 설치할 경우 ***에만*** 사용합니다. FEATURES 매개 변수가 지정되어 있지 않을 경우 서버 OS에서 기본 설치입니다. DE = Drive Encryption(Encryption 클라이언트)서버 OS에서는 설치 ***전용만*** 사용합니다. BLM = BitLocker Manager SED = 자체 암호화 드라이브 관리(EMAgent/Manager, PBA/GPE 드라이버)(워크스테이션 OS에 설치할 때에만 사용 가능함) ATP-WEBFIREWALL = 워크스테이션 OS의 Client Firewall 및 Web Protection DE-ATP-WEBFIREWALL = 서버 OS의 Client Firewall 및 Web Protection **노트: Enterprise Edition 또는 v1.4 이전 버전의 Endpoint Security Suite Enterprise에서 업그레이드하는 경우 Client Firewall 및 Web Protection을 설치하려면 ATP-WEBFIREWALL 또는 DE-ATP-WEBFIREWALL을 지정*해야 합니다*. 연결되지 않은 모드에서 실행되는 Dell Enterprise Server/VE에 의해 관리될 수 있도록 클라이언트 설치 시 ATP-WEBFIREWALL 또는 DE-ATP-WEBFIREWALL은 지정하지 마십시오.**
BLM_ONLY=1	명령줄에서 FEATURES=BLM을 사용하여 SED Management 플러그인을 제외할 때 사용해야 합니다.

명령줄의 예

- 명령줄 매개 변수는 대/소문자를 구분합니다.
- (워크스테이션 OS의 경우) 이 예에서는 ESSE 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).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- (워크스테이션 OS의 경우) 이 예에서는 표준 포트에서 ESSE 마스터 설치 프로그램을 사용하여 Advanced Threat Prevention 및 Encryption ***만*** 설치합니다(자동 설치, 기본 위치인 C:\Program Files\Dell\Dell Data Protection\에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (워크스테이션 OS의 경우) 이 예에서는 표준 포트에서 ESSE 마스터 설치 프로그램을 사용하여 Advanced Threat Prevention, Encryption 및 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).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-SED,
SUPPRESSREBOOT=1\""
```

- (워크스테이션 OS의 경우) 이 예에서는 표준 포트에서 ESSE 마스터 설치 프로그램을 사용하여 Advanced Threat Prevention, Encryption, Web Protection 및 Client Firewall을 설치합니다(자동 설치, 기본 위치인 C:\Program Files\Dell\Dell Data Protection\에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL\""
```

- (서버 OS의 경우) 이 예에서는 표준 포트에서 ESSE 마스터 설치 프로그램을 사용하여 Advanced Threat Prevention 및 Encryption ***만*** 설치합니다(자동 설치, 기본 위치인 C:\Program Files\Dell\Dell Data Protection\에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
```

- (서버 OS의 경우) 이 예에서는 표준 포트에서 ESSE 마스터 설치 프로그램을 사용하여 Advanced Threat Prevention, Encryption, Web Protection 및 Client Firewall을 설치합니다(자동 설치, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREWALL\""
```

- (서버 OS의 경우) 이 예에서는 표준 포트에서 ESSE 마스터 설치 프로그램을 사용하여 Advanced Threat Prevention***만*** 설치합니다(자동 설치, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (서버 OS의 경우) 이 예에서는 표준 포트에서 ESSE 마스터 설치 프로그램을 사용하여 Encryption***만*** 설치합니다(자동 설치, 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 설치, 지정된 EE Server/VE Server를 사용하도록 구성).

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE\""
```

4

ESSE 마스터 설치 프로그램을 사용하여 설치 제거

- 각 구성 요소를 별도로 설치 제거한 후에 ESSE 마스터 설치 프로그램을 설치 제거해야 합니다. **설치 제거 장애를 방지하려면 특정 순서대로** 클라이언트를 설치 제거해야 합니다.
- 하위 설치 프로그램을 가져오려면 ESSE 마스터 설치 프로그램에서 하위 설치 프로그램 추출의 지침을 따릅니다.
- 설치 작업과 설치 제거 작업에 동일한 버전의 ESSE 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 ESSE 마스터 설치 프로그램 설치 제거에 **대해서만** 설명합니다.
- 클라이언트를 다음 순서로 설치 제거합니다.

  a Encryption 클라이언트 설치 제거.

  b Advanced Threat Prevention 설치 제거

  c SED 및 Advanced Authentication 클라이언트 설치 제거. 이 작업을 수행하면 Dell Client Security Framework가 설치 제거되며 Advanced Threat Prevention이 설치 제거될 때까지 설치 제거할 수 없습니다.

  d BitLocker Manager 클라이언트 설치 제거
- ESSE 마스터 설치 프로그램 설치 제거를 계속 진행합니다.

ESSE 마스터 설치 프로그램 설치 제거

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

명령줄 설치 제거

- 다음 예에서는 ESSE 마스터 설치 프로그램을 자동으로 설치 제거합니다.

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

  완료되면 컴퓨터를 다시 부팅합니다.

하위 설치 프로그램을 사용하여 설치 제거

- 각 클라이언트를 개별적으로 설치 제거하려면 ESSE ESS 마스터 설치 프로그램에서 하위 설치 프로그램 추출에 나와 있는 대로 먼저 마스터 설치 프로그램에서 하위 실행 파일을 추출해야 합니다. 또는 .msi를 추출하는 관리자 설치를 실행해도 됩니다.
- 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 사용자에 대해 고유한 하위 설치 프로그램 설치 로그 파일을 C:\Users\<UserName>\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 /l C:\<any directory>\<any log file name>.log를 사용하여 로그 파일을 생성할 수 있습니다. 명령줄 설치 제거에서는 사용자 이름/암호가 로그 파일에 기록되므로 "/l*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 전달합니다. 콘텐츠는 항상 일반 텍스트 따옴표로 묶어야 합니다.
/s	자동 모드
/x	설치 제거 모드
/a	관리자 설치(모든 파일을 .msi 내에 복사)

노트:
/v를 사용하면 Microsoft 기본 옵션을 사용할 수 있습니다. 옵션 목록을 보려면 https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx 를 참조하십시오.

옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	**취소** 단추가 있는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb-	**취소** 단추가 있는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qb!	**취소** 단추가 없는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb!-	**취소** 단추가 없는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.

옵션	의미
/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 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

- **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 구성을 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.

명령줄 설치 제거

- ESSE 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 - Dell 서버에서 키 다운로드 0 - Encryption Removal Agent를 설치하지 않음
CMGSILENTMODE	자동 설치 제거 속성: 1 - 자동

매개변수	선택
	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 로그온된 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	Dell 서버의 포렌식 관리자 계정으로, 설치 제거나 키에 대한 포렌식 요청에 사용할 수 있습니다.
FORENSIC_ADMIN_PWD	Forensic 관리자 계정의 암호.
선택 사항 속성	
SVCLOGONUN	Encryption Removal Agent 서비스가 로그온된 사용자 이름(UPN 형식) 매개변수.
SVCLOGONPWD	로그온한 사용자의 암호.

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

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

MSI 명령:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
```

완료되면 컴퓨터를 다시 부팅합니다.

- 다음 예에서는 포렌식 관리자 계정을 사용하여 암호화 클라이언트를 설치 제거하고 암호화 키를 다운로드합니다.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
```

MSI 명령:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn CMG_DECRYPT=1 CMGSILENTMODE=1
FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit
REBOOT=REALLYSUPPRESS
```

완료되면 컴퓨터를 다시 부팅합니다.

중요:
명령줄에 포렌식 관리자 암호를 사용하는 경우 다음 작업이 권장됩니다.

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.

노트:
일부 오래된 클라이언트의 경우 이스케이프 문자 \"를 매개변수 값 앞뒤에 놓아야 할 수 있습니다. 예:

```
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=\"domain\username\" DA_RUNASPWD=\"password\" /qn"
```

Advanced Threat Prevention 설치 제거

명령줄 설치 제거

- 다음 예에서는 Advanced Threat Prevention 클라이언트의 설치를 제거합니다. ***이 명령어는 관리자 명령 프롬프트에서 실행해야 합니다.***

  ```
  wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
  ```

  컴퓨터를 종료했다가 다시 시작한 후 Dell Client Security Framework 구성 요소를 설치 제거합니다.

- **중요: SED 및 Advanced Authentication 클라이언트를 모두 설치했거나 Preboot Authentication 인증을 활성화한 경우에는 SED 및 Advanced Authentication 클라이언트 설치 제거의 설치 제거 지침을 따르십시오.**

  다음 예는 Dell Client Security Framework 구성 요소만 설치 제거하고 SED와 Advanced Authentication 클라이언트는 제거하지 않습니다.

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

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 `True`에서 `False`로 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

- ESSE 마스터 설치 프로그램에서 추출된 후에 SED 클라이언트 설치 프로그램은 C:\extracted\Security Tools \EMAgent_XXbit_setup.exe에서 찾을 수 있습니다.
- ESSE 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

- ESSE 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.

6

고급 위협 방지의 테넌트 프로비저닝

조직에서 고급 위협 방지를 사용하는 경우 고급 위협 방지 강제 실행 정책이 활성화되기 전에 Dell 서버에서 테넌트를 프로비저닝해야 합니다.

필수 조건

- 시스템 관리자 역할의 관리자가 수행해야 합니다.
- Dell 서버에서 프로비저닝하려면 인터넷에 연결되어 있어야 합니다.
- Remote Management Console에서 고급 위협 방지 온라인 서비스 통합을 표시하려면 클라이언트에서 인터넷이 연결되어 있어야 합니다.
- 프로비저닝은 프로비저닝 중에 인증서에서 생성되는 토큰을 기반으로 합니다.
- Dell 서버에 고급 위협 방지 라이선스가 있어야 합니다.

테넌트 프로비전

1 원격 관리 콘솔에 로그인하고 **서비스 관리**로 이동합니다.

2 **Advanced Threat Protection 서비스 설정**을 클릭합니다. 이 시점에 오류가 발생하면 ATP 라이센스를 가져옵니다.

3 라이센스를 가져오면 안내된 설정이 시작됩니다. **다음**을 클릭하여 시작합니다.

4 EULA를 읽고 동의(확인란은 기본적으로 **꺼져** 있음)한 뒤 **Next(다음)**를 클릭합니다.

5 테넌트 프로비저닝을 위해 DDP Server에 자격 증명 확인을 제공합니다. **다음**을 클릭합니다. *Cylance 상표의 기존 테넌트를 프로비저닝하는 것은 지원되지 않습니다.*

6 인증서를 다운로드합니다. DDP Server에 대한 재해 시나리오가 있는 경우 복구하는 데 필요합니다. 이 인증서는 v9.2 "upgrader"를 통해 자동으로 백업되지 않습니다. 인증서를 다른 컴퓨터의 안전한 위치에 백업합니다. 인증서를 백업했다는 확인란을 선택하고 **Next(다음)**를 클릭합니다.

7 설정이 완료되었습니다. **확인**을 클릭합니다.

고급 위협 방지 에이전트 자동 업데이트 구성

Dell Server Remote Management Console에서 고급 위협 방지 에이전트 자동 업데이트를 받도록 등록할 수 있습니다. 에이전트 자동 업데이트를 받도록 등록하면 클라이언트가 Advanced Threat Prevention 서버에서 업데이트를 자동으로 다운로드하여 적용할 수 있습니다. 업데이트는 매월 릴리스됩니다.

노트: 에이전트 자동 업데이트는 Dell 서버 v9.4.1 이상에서 지원됩니다.

에이전트 자동 업데이트 받기

에이전트 자동 업데이트를 받도록 등록하려면 다음을 수행합니다.

1 Remote Management Console의 왼쪽 창에서 **관리** > **서비스 관리**를 클릭합니다.
2 **고급 위협** 탭의 에이전트 자동 업데이트에서 **켜짐** 단추를 클릭한 후 **환경설정 저장** 단추를 클릭합니다.
정보가 채워지고 자동 업데이트가 표시되기까지 시간이 소요될 수 있습니다.

에이전트 자동 업데이트 받기 중지

에이전트 자동 업데이트 받기를 중지하려면 다음을 수행합니다.

1 Remote Management Console의 왼쪽 창에서 **관리** > **서비스 관리**를 클릭합니다.
2 **고급 위협** 탭의 에이전트 자동 업데이트에서 **꺼짐** 단추를 클릭한 후 **환경설정 저장** 단추를 클릭합니다.

8

ESSE 마스터 설치 프로그램에서 하위 설치 프로그램 추출

- ESSE 마스터 설치 프로그램은 마스터 설치 제거 프로그램이 아닙니다. 각 클라이언트를 별도로 설치 제거한 후에 ESSE 마스터 설치 프로그램을 설치 제거해야 합니다. 클라이언트를 설치 제거에 사용할 수 있도록 이 프로세스에 따라 ESSE 마스터 설치 프로그램에서 클라이언트를 추출하십시오.

1 Dell 설치 미디어에서 **DDPSuite.exe** 파일을 로컬 컴퓨터로 복사합니다.

2 **DDPSuite.exe** 파일과 동일한 위치에서 명령 프롬프트를 열고 다음을 입력합니다.

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

추출 경로는 63자를 초과할 수 없습니다.

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.
- 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 제거를 참조하십시오.

서비스 패널 - 도메인 계정 사용자 추가

1 EE Server에서 서비스 패널로 이동합니다(시작 > 실행...services.msc > OK(확인)).

2 Dell Key Server를 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)**를 선택합니다.

3 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.

4 Key Server 서비스를 다시 시작합니다(추가 작업을 위해 서비스 패널은 열어 둠).

5 <Key Server 설치 디렉터리> log.txt를 탐색하여 서비스가 올바르게 시작되었는지 확인합니다.

Key Server 구성 파일 - EE Server 통신에 대한 사용자 추가

1 <Key Server 설치 디렉터리>를 탐색합니다.

2 텍스트 편집기를 사용해 *Credant.KeyServer.exe.config*를 엽니다.

3 <add key="user" value="superadmin" />으로 이동한 다음 "superadmin" 값을 적절한 사용자 이름으로 변경합니다("superadmin"을 유지할 수도 있음).

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.

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.

Dell 관리자: jdoe 등과 같이 Forensic 관리자 자격 증명(Remote Management Console에 활성화됨)을 사용하는 관리자의 이름.

암호: Forensic 관리자 암호.

MCID: machineID.domain.com과 같은 시스템 ID.

DCID: 16자리 Shield ID의 처음 8개 숫자.

> **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.

다음을 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: machineID.domain.com과 같은 시스템 ID.

DCID: 16자리 Shield ID의 처음 8개 숫자.

> **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.

다음을 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.

문제 해결

모든 클라이언트 - 문제 해결

- ESSE m**스터 설치 프로그램 로그 파일**은 C:\ProgramData\Dell\Dell Data Protection\Installer에 있습니다.
- Windows는 로그인된 사용자에 대해 고유한 **하위 설치 프로그램 설치 로그 파일**을 C:\Users\<UserName>\AppData\Local\Temp.에 생성합니다.
- Windows는 로그인된 사용자에 대해 Visual C++ 등과 같은 클라이언트 필수 구성 요소의 로그 파일을 C:\Users\<UserName>\AppData\Local\Temp.의 %temp%에 생성합니다. **예:** C:\Users\<UserName>\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log
- 설치 대상 컴퓨터에 설치되는 Microsoft .Net 버전을 확인하려면 http://msdn.microsoft.com에 있는 지침을 따르십시오.

  전체 버전의 Microsoft .Net Framework 4.5를 설치하려면 https://www.microsoft.com/en-us/download/details.aspx?id=30653으로 이동하십시오.
- 설치 대상 컴퓨터에 Dell Access가 이전에 설치된 적이 있거나 현재 설치되어 있는 경우 *Dell Data Protection | Security Tools 호환성*을 참조하십시오. DDPlA는 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 증명이 도메인 관리자의 자격 증명이 아닙니다.

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" 대화 상자에 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 로그온합니다.
- 새 사용자가 시스템 트레이에서 Encryption 클라이언트 아이콘을 마우스 오른쪽 단추로 클릭하고 Dell Encryption 활성화를 선택합니다.

초기 활성화 프로세스는 다음과 같습니다.

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

> **노트:**
> 도메인 관리자 자격 증명에 대한 요구 사항은 지원되지 않는 다른 서버 환경으로 Server Encryption이 롤아웃되지 않도록 하기 위한 안전 조치입니다. 도메인 관리자 자격 증명에 대한 요구 사항을 비활성화하려면 시작하기 전에를 참조하십시오.

6 DDP Server는 엔터프라이즈 자격 증명 모음(Active Directory 또는 동급)에 자격 증명이 있는지 확인해 자격 증명이 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.

노트:
암호 및 DPAPI 인증은 이 계정에 사용되지 않으므로 가상 서버 사용자*만* 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.

- 정보 대화 상자를 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 로그온할 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.

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

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 않는 미디어 정책에 EMS 액세스를 *전체 액세스로* 설정하려는 경우, 저장소 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 저장소: 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 **고급**을 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 **검색**을 클릭합니다.

또는

1 **고급**을 클릭하여 보기 모드를 **간단히**로 전환하여 특정 폴더를 스캔합니다.
2 검색 설정으로 이동하고 **경로 검색** 필드에 폴더 경로를 입력합니다. 이 필드를 사용할 경우 드롭다운 상자에 선택한 사항이 무시됩니다.
3 WSScan 출력을 파일에 쓰지 않으려는 경우 **파일로 출력** 확인란의 선택을 취소합니다.
4 필요할 경우 *경로*에서 기본 경로와 파일 이름을 변경합니다.
5 기존 WSScan 출력 파일을 덮어쓰지 않으려는 경우 **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 문장 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 **검색**을 클릭합니다.

검색을 중지하려면 **검색 중지**를 클릭합니다. 표시된 메시지를 지우려면 **지우기**를 클릭합니다.

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.
KCID	키 컴퓨터 ID입니다. 위의 예에서와 같이, **"7vdlxrsb"**입니다. 매핑된 네트워크 드라이브를 스캔하는 경우 스캔 보고서가 KCID를 반환하지 않습니다.
UCID	사용자 ID입니다. 위의 예에서와 같이, **"_SDENCR_"**입니다. 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

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 제거될 때까지 암호 해독이 시작되지 않습니다.
- **초기 스윕** – 서비스가 초기 스윕을 실행하면서 암호화된 파일과 바이트 수를 계산합니다. 초기 스윕은 한 번만 실행됩니다.
- **암호 해독 스윕** – 서비스가 파일을 암호 해독하고 있으며 잠겨 있는 파일의 암호 해독을 요청할 수도 있습니다.
- **재부팅 시 암호 해독(부분적)** – 암호 해독 스윕이 완료되었으며 다음에 다시 시작하면 잠겨 있는 파일이 일부만 암호 해독됩니다.
- **재부팅 시 암호 해독** – 암호 해독 스윕이 완료되었으며 다음에 다시 시작하면 잠긴 파일이 모두 암호 해독됩니다.
- **모든 파일을 암호 해독할 수 없음** – 암호 해독 스윕이 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 스윕 중 오류가 발생했습니다.
  - LogVerbosity=2(또는 이상)가 설정되어 있으면 항상 로그 파일이 생성됩니다(로깅이 구성된 경우). 문제를 해결하려면 로그의 자세한 정도를 2로 설정하고 Encryption Removal Agent 서비스를 다시 시작해서 암호 해독 스윕을 한 번 더 강제 실행합니다.
- **완료** – 암호 해독 스윕이 완료되었습니다. 다음에 다시 시작할 때 서비스, 실행 파일, 드라이버 및 드라이버 실행 파일이 모두 삭제되도록 예약됩니다.

고급 위협 방지 클라이언트 문제 해결

Windows PowerShell을 사용하여 제품 코드 찾기

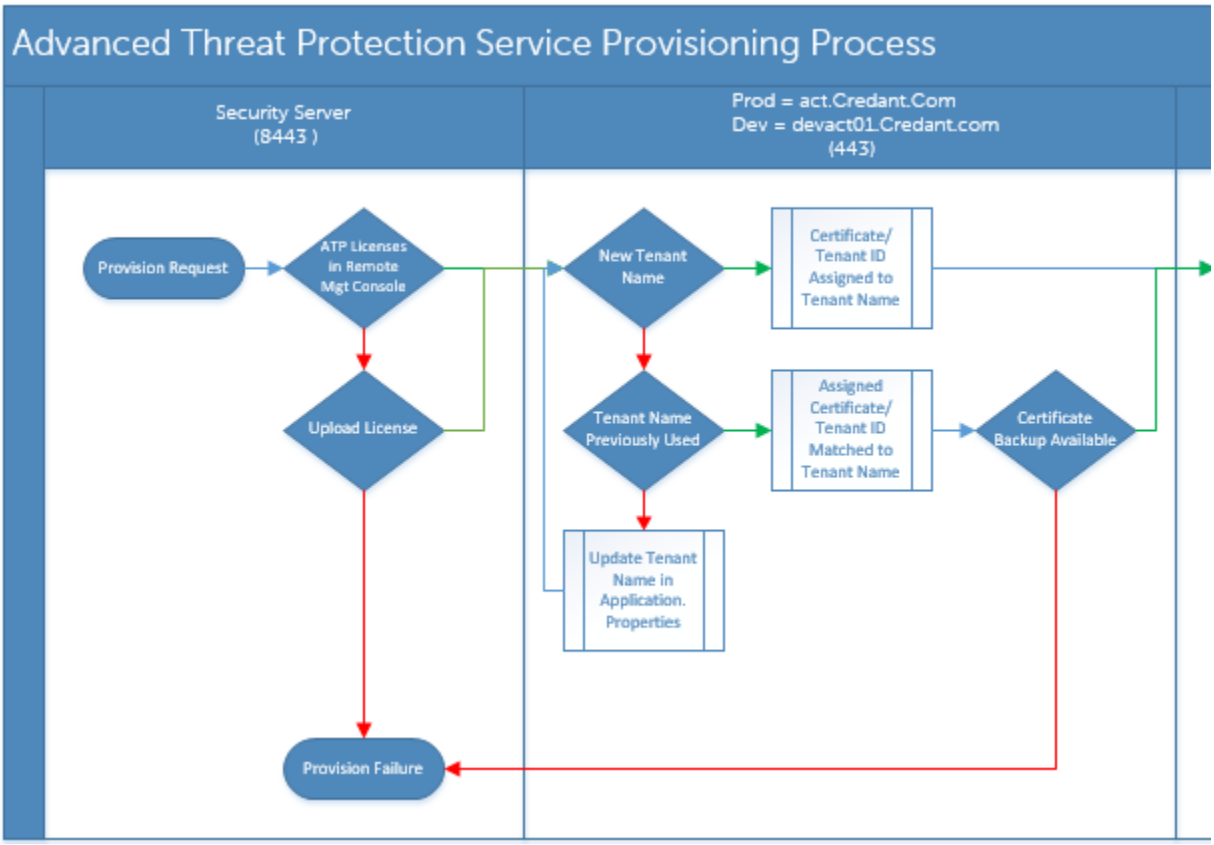
- 이 방법을 사용하면 제품 코드를 쉽게 식별할 수 있으며, 나중에 제품 코드가 변경되는 경우에도 찾을 수 있습니다.

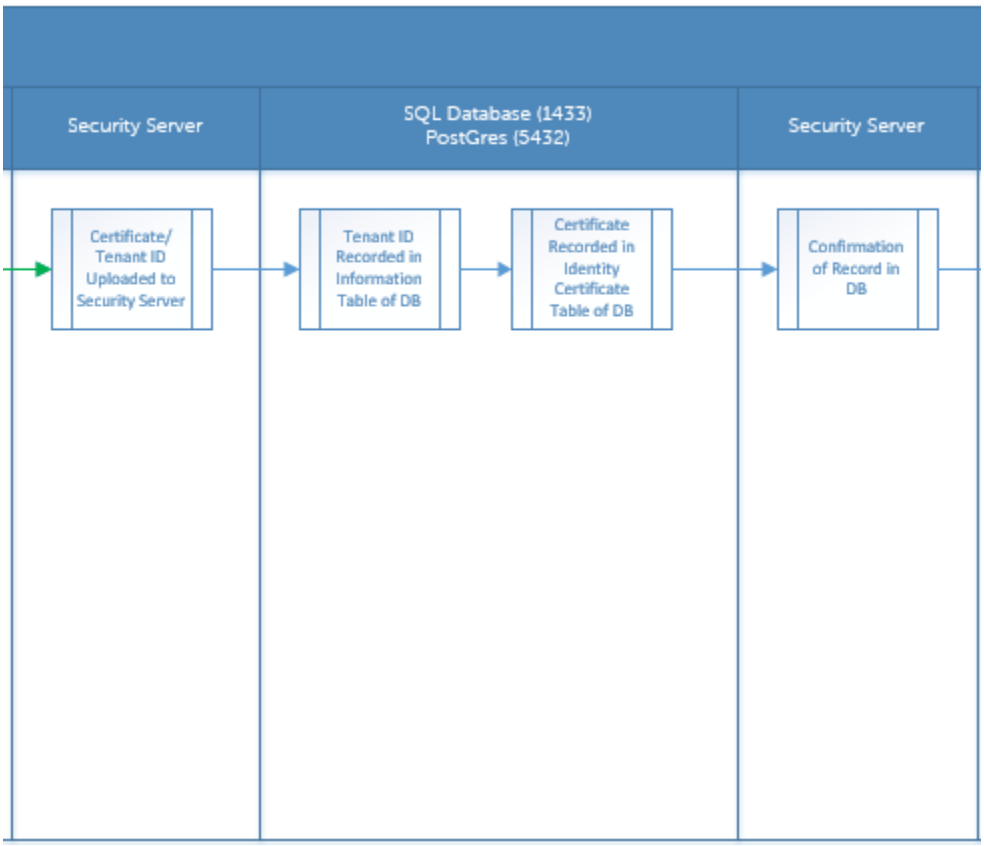
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

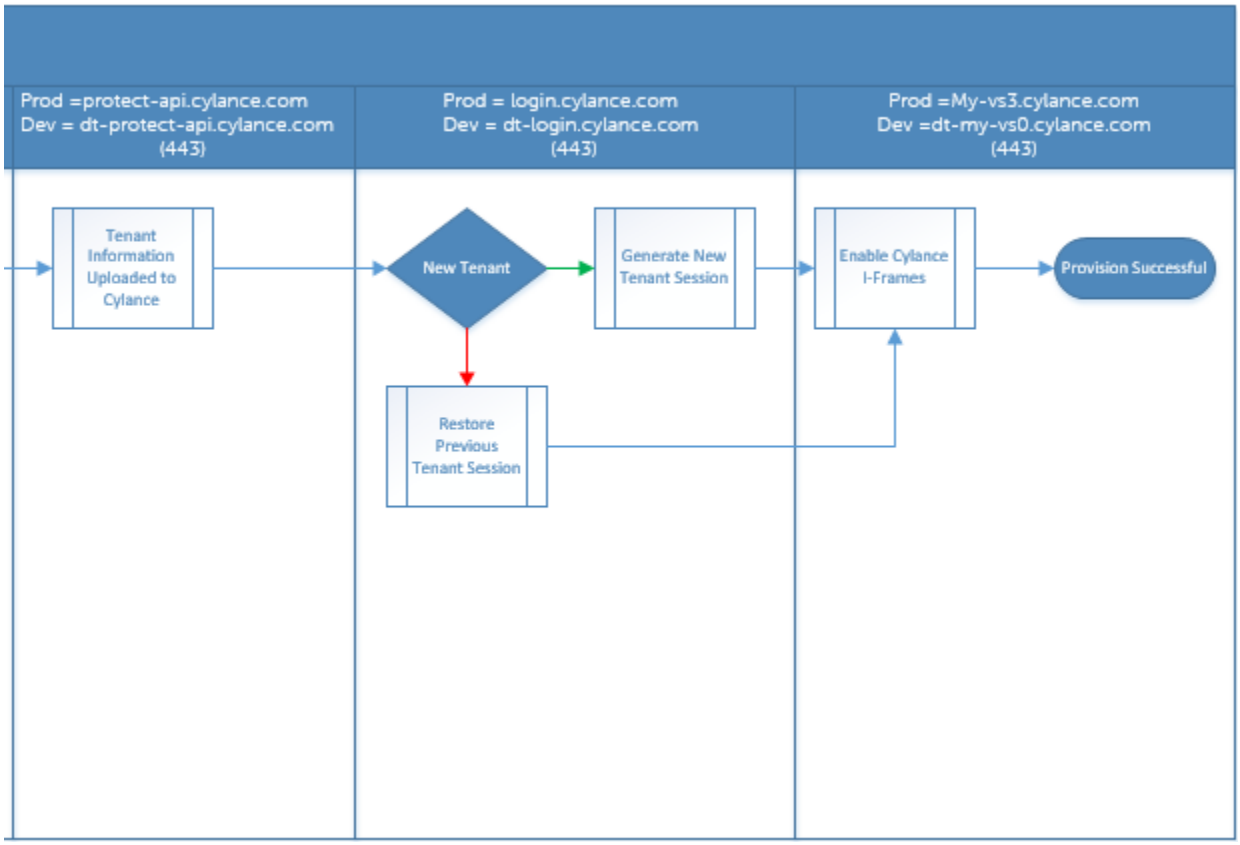
  전체 경로와 .msi 파일 이름(파일의 변환된 16진수 이름)과 함께 출력이 표시됩니다.

고급 위협 방지 프로비저닝 및 에이전트 통신

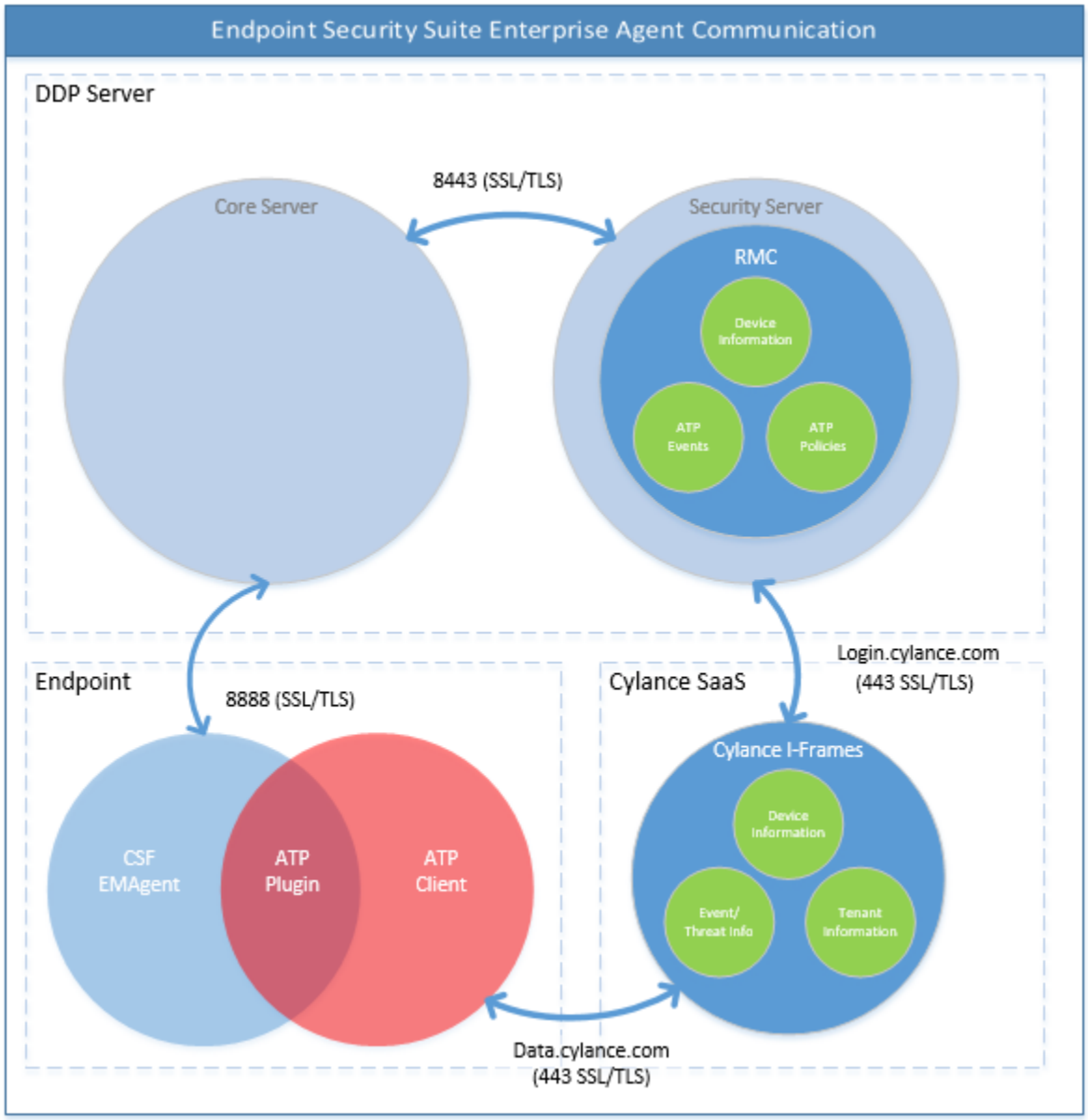
다음 다이어그램은 고급 위협 방지 서비스 프로비저닝 프로세스를 보여 줍니다.


Advanced Threat Protection Service Provisioning Process
Security Server
(8443)
Prod = act.Credant.Com
Dev = devact01.Credant.com
(443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB

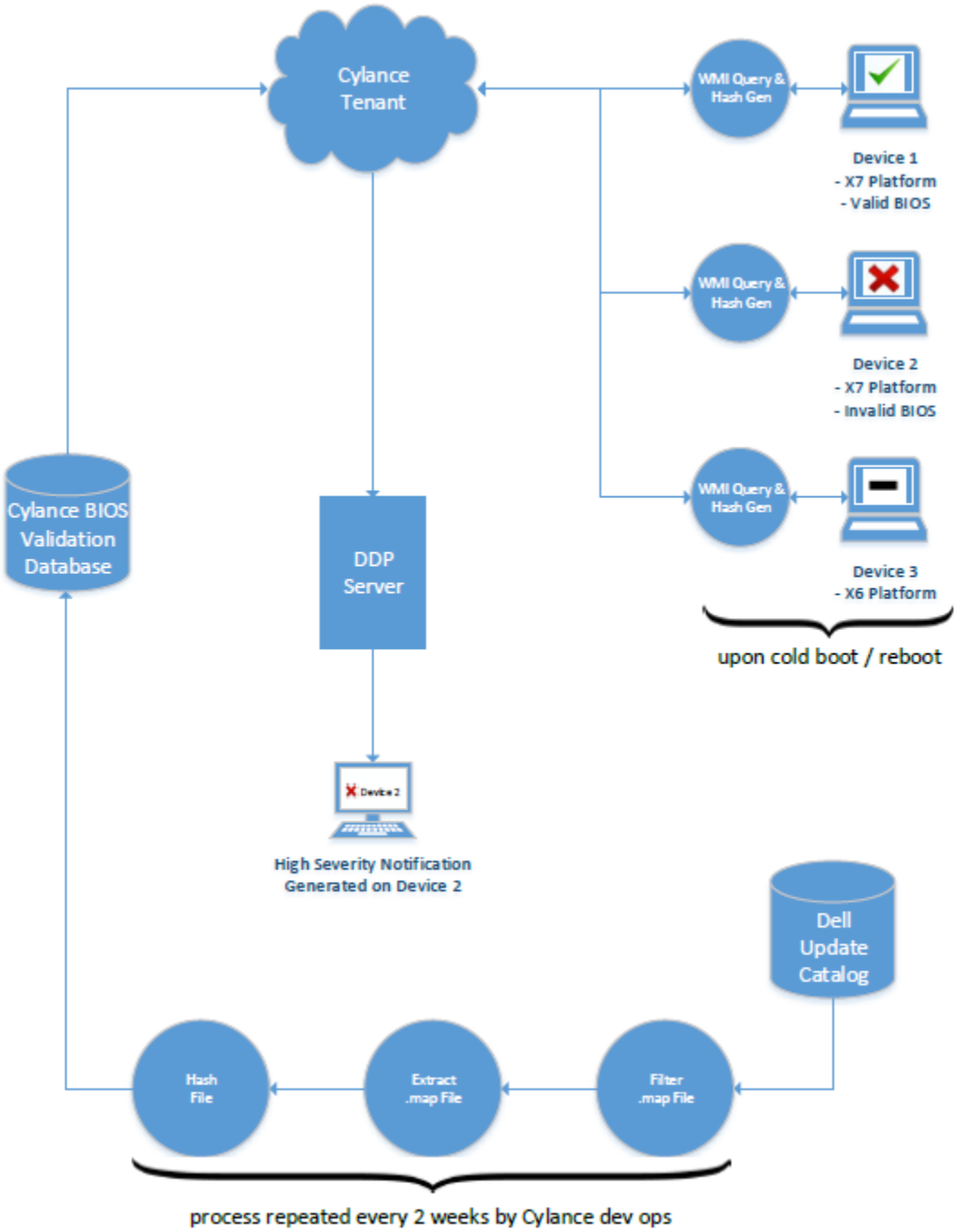


다음 그림은 고급 위협 방지 에이전트 통신 프로세스를 보여 줍니다.



BIOS 이미지 무결성 확인 프로세스

다음 다이어그램은 BIOS 이미지 무결성 확인 프로세스를 보여 줍니다. BIOS 이미지 무결성 확인이 지원되는 Dell 컴퓨터 모델 목록은 요구 사항 - BIOS 이미지 무결성 확인을 참조하십시오.



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 **드라이버 및 다운로드**를 선택합니다.
4 대상 컴퓨터의 **운영 체제**를 선택합니다.
5 **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.exe입니다.

계속을 클릭하여 시작합니다.

확인을 클릭하여 기본 위치인 C:\Dell\Drivers\<New Folder>에 드라이버 파일들을 압축 해제합니다.

예를 클릭하여 새 폴더 생성을 허용합니다.

성공적으로 압축 해제했다는 메시지가 표시되면 **확인**을 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 **다음**을 클릭합니다.

다음을 클릭하여 기본 위치인 C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.에 드라이버를 설치합니다.

완료 옵션을 선택하고 **다음**을 클릭합니다.

설치을 클릭하여 드라이버 설치를 시작합니다.

필요에 따라, 설치 프로그램 로그 파일을 표시하기 위해 확인란을 선택합니다. **마침**을 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 **계속**을 클릭하여 시작합니다.
4 **확인**을 클릭하여 기본 위치인 C:\Dell\Drivers\<New Folder>에 드라이버 파일들을 압축 해제합니다.
5 **예**를 클릭하여 새 폴더 생성을 허용합니다.
6 성공적으로 압축 해제했다는 메시지가 표시되면 **확인**을 클릭합니다.
7 압축 해제가 끝나면 파일들이 들어 있는 폴더가 표시될 것입니다. 그렇지 않다면, 파일들을 추출한 폴더로 이동하십시오. **펌웨어** 폴더를 선택합니다.
8 **ushupgrade.exe**를 더블 클릭하여 펌웨어 설치 프로그램을 시작합니다.
9 **시작**을 클릭하여 펌웨어 업그레이드를 시작합니다.

:

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

몇 가지 상태 메시지가 표시됩니다.

10 **재시작**을 클릭하여 펌웨어 업그레이드를 완료합니다.

Dell ControlVault 드라이버 및 펌웨어 업데이트가 완료됩니다.

12

용어집

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 웹 사이트, SaaS 또는 응용 프로그램에 액세스할 수 있습니다. 사용자가 자격 증명을 등록하면 Advanced Authentication은 해당 자격 증명을 사용하여 장치에 로그온하고 암호를 변경할 수 있도록 합니다.

Advanced Threat Prevention – Advanced Threat Prevention 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. 클라이언트 방화벽 기능(선택 사항)은 네트워크나 인터넷을 통한 컴퓨터와 리소스 사이의 통신을 모니터링하여 악의적일 수 있는 통신을 차단합니다. 웹 차단 기능(선택 사항)은 웹 사이트의 안전 등급과 보고에 기반하여 온라인 검색 중에 안전하지 않은 웹 사이트 및 이러한 웹 사이트로부터의 다운로드를 차단합니다.

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.

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

EMS(External Media Shield) - Dell 암호화 클라이언트 내의 이 서비스는 이동식 미디어 및 외부 저장 장치에 정책을 적용합니다.

EMS 액세스 코드 - Dell Enterprise Server/VE 내의 이 서비스는 사용자가 암호를 잊어 버렸고 더 이상 로그인할 수 없는 EMS(External Media Shield) 보호 장치의 복구를 허용합니다. 이 프로세스를 완료하면 사용자가 이동식 미디어 또는 외부 저장 장치에 설정된 암호를 재설정할 수 있습니다.

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.

끝점 - Dell Enterprise Server/VE에서 관리하는 컴퓨터 또는 모바일 하드웨어 장치입니다.

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

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 로그온 화면에서 컴퓨터에 로그온하는 데 사용됩니다. 정책에 따라, 컴퓨터에 로그온할 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 보안보다 강력하다고 할 수 있습니다.

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 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 Dell Enterprise Server/VE Remote Management Console에서 고유한 UCID 값이 할당됩니다.