Dell Endpoint Security Suite Enterprise for Mac

관리자 가이드 v2.9

2021 년 3 월
개정 A02

DELL EMC

참고, 주의 및 경고

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

주의: 주의사항은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

경고: 경고는 재산 손실, 신체적 상해 또는 사망 위험이 있음을 알려줍니다.

목차

1

소개

Mac용 Endpoint Security Suite Enterprise 관리자 안내서에서는 클라이언트 소프트웨어 배포와 설치에 필요한 정보를 제공합니다.

주제:

개요

Mac용 Endpoint Security Suite Enterprise는 운영 체제, 메모리 레이어, 암호화에 Advanced Threat Prevention를 제공하며, Dell Server에서 중앙 집중적으로 관리합니다. 중앙 집중식 관리, 통합 규정 준수 보고, 콘솔 위협 경고를 통해 기업에서 모든 끝점에 대한 규정 준수를 간편하게 적용하고 입증합니다. 보안 전문 지식으로 사전 정의된 정책 및 보고서 템플릿과 같은 기능을 구축하여 기업에서 IT 관리 비용을 절감하고 복잡성을 감소시키는 데 도움이 됩니다.

- Endpoint Security Suite Enterprise for Mac - 데이터의 클라이언트 암호화 및 Advanced Threat Prevention를 위한 소프트웨어 제품군
- 정책 프록시 - 정책 배포에 사용됨
- 보안 서버 - 클라이언트 암호화 소프트웨어 활성화에 사용됨
- Security Management Server 또는 Security Management Server Virtual - 중앙 집중식 보안 정책 관리 제공, 기존 Enterprise 디렉터리와 통합하고 보고서를 생성함 이 문서의 목적에 알맞게 양쪽 서버가 특정 버전을 언급해야 할 경우(예: Security Management Server Virtual 사용 시 다른 절차 적용)를 제외하고 Dell Server로 지칭됩니다.

  이러한 Dell 구성 요소는 원활하게 상호 작용하여 사용자 경험에 악영향을 주지 않고 안전한 모바일 환경을 제공합니다.

Mac용 Endpoint Security Suite Enterprise에는 두 개의 .dmg 파일이 있습니다. 한 개는 암호화 클라이언트용, 다른 한 개는 Advanced Threat Prevention용입니다. 두 개 모두 설치하거나 한 개만 설치할 수 있습니다.

FileVault 암호화

Dell Encryption은 Mac FileVault 전체 디스크 암호화를 관리할 수 있습니다. 암호화를 수행하고 다른 정책 설정이 작동하려면 *Dell 볼륨 암호화* 정책을 **켜짐**으로 설정해야 합니다. 추가 정책에 대한 자세한 내용은 *관리자 도움말*을 참조하십시오.

FileVault 암호화만 지원되며 Endpoint Security Suite Enterprise가 관리됩니다. 컴퓨터에서 *Dell 볼륨 암호화* 정책을 **실행**으로 설정하고 *Mac용 FileVault를 사용한 암호화*를 **해제**로 설정한 경우 암호화 클라이언트에 정책 충돌 메시지가 표시됩니다. 관리자는 두 정책을 모두 **실행**으로 설정해야 합니다.

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.

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

2

요구 사항

이 장에는 클라이언트 하드웨어와 소프트웨어 요구 사항이 나와 있습니다. 배포 작업을 계속하기 전에 배포 환경이 이런 요구 사항을 충족하는지 확인하십시오.

주제:

Encryption 클라이언트

Encryption 클라이언트 하드웨어

최소 하드웨어 요구 사항은 운영 체제의 최소 사양을 충족시켜야 합니다.

하드웨어
• 30MB의 사용 가능한 디스크 공간
• 10/100/1000 또는 Wi-Fi 네트워크 인터페이스 카드
• 시스템 디스크는 GPT(GUID Partition Table) 파티션 구성표로 분할되어야 하며 다음 중 하나로 포맷할 수 있습니다. ○ Mac OS X Extended Journaled(HFS+)는 FileVault를 적용하기 위해 코어 스토리지로 변환됩니다. ○ APFS(Apple File System)

Encryption 클라이언트 소프트웨어

다음 표에 지원되는 소프트웨어가 나와 있습니다.

운영 체제(64비트 커널)
• macOS High Sierra 10.13.6
• macOS Mojave 10.14.5 - 10.14.6
• macOS Catalina 10.15.5 - 10.15.6

노트: Dell Encryption은 macOS Big Sur을 지원하지 않습니다.

노트:

인증을 위해 네트워크 사용자 계정을 사용할 경우 FileVault 2 Management를 완전히 구성하기 위해 그 계정은 모바일 계정으로 설정되어 있어야 합니다.

암호화된 미디어

다음 표에는 Dell의 암호화된 외부 미디어에 액세스할 때 지원되는 운영 체제가 자세히 나와 있습니다.

노트:

Encryption External Media 지원:

- FAT32

- exFAT
- MBR(Master Boot Record) 또는 GPT(GUID Partition Table) 파티션 구성표로 이루어진 HFS Plus(MacOS Extended) 형식의 미디어. HFS Plus 활성화를 참조하십시오.

노트:

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

암호화된 미디어에 액세스할 수 있도록 지원되는 Windows 운영 체제(32비트 및 64비트)
• Microsoft Windows 7 SP1 - Enterprise - Professional - Ultimate
• Microsoft Windows 8.1 - Windows 8.1 Update 1 - Enterprise - Pro
• Microsoft Windows 10 - Education - Enterprise - Pro v1607(1주년 업데이트/Redstone 1)~v1909(2019년 11월 업데이트/19H2)
암호화된 미디어에 액세스할 수 있도록 지원되는 Mac 운영 체제(64비트 커널)
• macOS High Sierra 10.13.6 **노트:** macOS High Sierra 10.14.x에서 Encryption External Media를 사용하려면 Encryption Enterprise v8.16 이상이 필요합니다.
• macOS Mojave 10.14.5 - 10.14.6
• macOS Catalina 10.15.5 - 10.15.6

Advanced Threat Prevention

Advanced Threat Prevention 클라이언트를 설치하기 전에 설치 오류를 방지하기 위해 다른 벤더의 안티바이러스, 안티멀웨어 및 안티스파이웨어 응용프로그램을 설치 제거합니다.

Advanced Threat Prevention 하드웨어

최소 하드웨어 요구 사항은 운영 체제의 최소 사양을 충족시켜야 합니다.

하드웨어
• 500MB의 사용 가능한 디스크 공간(운영 체제에 따라 다름) • 2GB RAM • 10/100/1000 또는 Wi-Fi 네트워크 인터페이스 카드

Advanced Threat Prevention 소프트웨어

다음 표에 지원되는 소프트웨어가 나와 있습니다.

운영 체제(64비트 커널)
• Mac OS X Mavericks 10.9.5 • Mac OS X Yosemite 10.10.5 • macOS Sierra 10.12.6 **노트:** Mac OS X Mavericks 10.9.5, Mac OS X Yosemite 10.10.5 및 macOS Sierra 10.12는 Advanced Threat Prevention에서만 지원되며 Encryption 클라이언트에서는 지원되지 않습니다.
• macOS High Sierra 10.13.6 **노트:** Encryption 클라이언트에서 지원되는 특정 macOS High Sierra 버전은 Encryption 클라이언트 소프트웨어를 참조하십시오.
• macOS Mojave 10.14.5 - 10.14.6 **노트:** ATP 에이전트를 macOS Mojave에 설치할 수 있지만, 메모리 보호 기능과 스크립트 제어 기능이 자동으로 비활성화되며 현재 지원되지 않습니다.
• macOS Catalina 10.15.3 - 10.15.4

노트:

대소문자를 구분하는 파일 시스템은 지원하지 않습니다.

Advanced Threat Prevention 포트

- Advanced Threat Prevention 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

호환성

다음 표에는 Windows, Mac 및 Linux의 호환성이 자세히 나와 있습니다.

해당 없음 - 이 플랫폼에 기술이 적용되지 않습니다.

빈 필드 - 정책이 Endpoint Security Suite Enterprise에서 지원되지 않습니다.

기능	정책	Windows	macOS	Linux	
파일 작업					
	자동 격리(안전하지 않음)	x	x	x	
	자동 격리(비정상)	x	x	x	
	자동 업로드	x	x	x	

기능	정책	Windows	macOS	Linux	
	정책 안전 목록	x	x	x	
메모리 작업					
	메모리 보호	x	x	x	
악용					
	스택 피벗	x	x	x	
	스택 보호	x	x	x	
	덮어쓰기 코드	x	해당 없음		
	RAM 스크랩	x	해당 없음		
	악성 페이로드	x			
프로세스 주입					
	메모리 원격 할당	x	x	해당 없음	
	메모리 원격 매핑	x	x	해당 없음	
	메모리에 원격으로 쓰기	x	x	해당 없음	
	메모리에 PE를 원격으로 쓰기	x	해당 없음	해당 없음	
	원격 덮어쓰기 코드	x	해당 없음		
	메모리 원격 매핑 해제	x	해당 없음		
	원격 스레드 생성	x	x		
	원격 APC 예약됨	x	해당 없음	해당 없음	
	DYLD 주입		x	x	
에스컬레이션					
	LSASS 읽기	x	해당 없음	해당 없음	
	제로 할당	x	x		
보호 설정					
	실행 제어	x	x	x	
	장치의 서비스 종료 방지	x	x		
	안전하지 않은 실행 프로세스 및 하위 프로세스 삭제	x	x	x	
	백그라운드 위협 감지	x	x	x	
	새 파일 감시	x	x	x	
	스캔할 최대 아카이브 파일 크기	x	x	x	
	특정 폴더 제외	x	x	x	
	파일 샘플 복사	x			
응용 프로그램 제어					
	창 변경	x		x	
	폴더 제외	x			
에이전트 설정					

기능	정책	Windows	macOS	Linux	
	로그 파일 자동 업로드 활성화	x	x	x	
	바탕 화면 알림 활성화	x			
스크립트 제어					
	Active Script	x			
	Powershell	x			
	Office 매크로	x		해당 없음	
	Powershell 콘솔 사용 차단	x			
	이러한 폴더 및 하위 폴더에서 스크립트 승인	x			
	로깅 수준	x			
	자체 보호 수준	x			
	자동 업데이트	x			
	탐지 실행(에이전트 UI에서)	x			
	격리됨 삭제(에이전트 UI 및 콘솔 UI)	x			
	연결되지 않은 모드	x		x	
	상세 위협 데이터	x			
	인증서 안전 목록	x	x	해당 없음	
	맬웨어 샘플 복사	x	x	x	
	프록시 설정	x	x	x	
	수동 정책 확인(에이전트 UI)	x	x		

3

암호화 클라이언트 작업

주제:

Encryption 클라이언트 설치/업그레이드

이 섹션에서는 Encryption 클라이언트 for Mac 설치/업그레이드 및 활성화 프로세스를 안내합니다.

두 가지 방법으로 Encryption Client for Mac을 설치/업그레이드할 수 있습니다. 다음 중 **하나**를 선택하십시오.

- 대화형 설치/업그레이드 및 활성화 - 이것은 클라이언트 소프트웨어 패키지를 설치하거나 업그레이드하는 가장 쉬운 방법입니다. 하지만 이 방법에서는 어떤 사용자 지정도 허용되지 않습니다. Boot Camp 또는 아직 Dell에서 완전히 지원되지 않는 운영 체제 버전을 사용하려는 경우, 명령줄 설치/업그레이드 방법을 사용해야 합니다. Boot Camp 사용에 대한 자세한 내용은 Boot Camp 사용을 참조하십시오.
- 명령줄 설치/업그레이드 - 이것은 고급 설치/업그레이드 방법으로 명령줄 구문에 숙련된 관리자만 사용해야 합니다. .plist 수정을 통해 Boot Camp 또는 아직 Dell에서 완전히 지원되지 않는 운영 체제 버전을 사용하려는 경우, 이 방법을 사용하여 클라이언트 소프트웨어 패키지를 설치 또는 업그레이드해야 합니다. Boot Camp 사용에 대한 자세한 내용은 Boot Camp 사용을 참조하십시오.

  설치 프로그램 명령 옵션에 대한 자세한 내용은 http://developer.apple.com에서 Mac OS X 참조 라이브러리를 참조하십시오.http://developer.apple.com Dell에서는 Apple Remote Desktop과 같은 원격 배포 도구를 사용하여 클라이언트 설치 패키지를 배포할 것을 강력히 권장합니다.

  노트:

  Apple에서는 Endpoint Security Suite Enterprise for Mac 릴리스 간에 새로운 버전의 운영 체제를 자주 출시합니다. 가능한 많은 수의 고객을 지원하도록 이러한 경우를 위해 com.dell.ddp.plist 파일 수정이 허용되고 있습니다. Encryption Client for Mac과 호환이 가능하도록 Apple이 새 버전을 출시하는 즉시 이러한 버전에 대한 테스트가 시작됩니다.

사전 요구 사항

클라이언트 소프트웨어 배포 중에는 IT 모범 사례를 따르는 것이 좋습니다. 예를 들어, 초기 테스트에서 테스트 환경을 통제하고 사용자에 대해 시간별 배포를 수행해야 합니다.

시작하기 전에, 다음과 같은 사전 요구 사항이 충족되어 있는지 확인하십시오.

- Dell Server 및 해당 구성 요소가 이미 설치되어 있는지 확인합니다.

  Dell Server를 아직 설치하지 않은 경우, 아래의 해당 가이드에서 지침을 따릅니다.

  Security Management Server 설치 및 마이그레이션 가이드

  Security Management Server Virtual 퀵 스타트 가이드 및 설치 가이드
- 보안 서버 및 정책 프록시 URL이 있는지 확인합니다. 클라이언트 소프트웨어 설치와 활성화를 위해서는 두 가지 모두 필요합니다.
- 배포 시 기본이 아닌 구성을 사용하는 경우, 보안 서버의 포트 번호를 알아야 합니다. 클라이언트 소프트웨어 설치와 활성화를 위해 필요하기 때문입니다.

- 대상 컴퓨터에 보안 서버 및 정책 프록시가 네트워크로 연결되었는지 확인합니다.
- Active Directory 설치 시 도메인 사용자 계정이 Dell Server에서 사용하도록 구성되어야 합니다. 이 도메인 사용자 계정은 클라이언트 소프트웨어 활성화에 사용됩니다. 도메인 (네트워크) 인증을 위해 Mac 엔드포인트를 구성할 필요는 없습니다.

암호화 정책을 설정하기 전에 *Dell 볼륨 암호화* 정책이 *켜져 있어야* 합니다. *Mac용 FileVault를 사용한 암호화*와 *암호화 대상 볼륨* 정책을 이해해야 합니다.

암호화 정책에 대한 자세한 내용은 Mac 암호화 > Dell 볼륨 암호화를 참조하십시오.

대화형 설치 또는 업그레이드

클라이언트 소프트웨어를 설치하거나 업그레이드하고 활성화하려면 아래 단계를 따르십시오. 이런 단계를 수행하려면 관리자 계정이 있어야 합니다.

대화형 설치

노트:

시작하기 전에 사용자의 작업을 저장하고 애플리케이션을 닫습니다. 설치가 완료되는 즉시 컴퓨터를 재시동해야 합니다.

1. Dell 설치 미디어에서 Dell-Encryption-Enterprise-<version>.dmg 파일을 마운트합니다.
2. 패키지 설치 프로그램을 두 번 클릭합니다. 다음과 같은 메시지가 표시됩니다.
   이 패키지는 소프트웨어를 설치할 수 있는지 결정하기 위한 프로그램을 실행합니다.
3. **계속**을 클릭하여 진행합니다.
4. 시작 텍스트를 읽고 **계속**을 클릭합니다.
5. 라이선스 계약을 검토하고 **계속**을 클릭한 뒤 **동의**를 클릭하여 라이선스 계약의 조건을 수락합니다.
6. *도메인 주소* 필드에 대상 사용자에 대한 정규화된 도메인 이름을 입력합니다(예: *department.organization.com*).
7. *표시 이름(선택 사항)* 필드에서 *표시 이름*을 도메인의 NetBIOS(Windows 2000 이전) 이름으로 설정하십시오. 이 이름은 일반적으로 대문자입니다.

   설정된 경우, 이 필드가 *활성화* 대화 상자에 도메인 주소 대신 표시됩니다. 이 이름은 도메인 관리되는 Windows 컴퓨터의 *인증* 대화 상자에 표시되는 도메인 이름에 일관성을 제공합니다.

8. *보안 서버* 필드에 보안 서버 호스트 이름을 입력합니다.

   배포에 기본 구성 이외의 구성이 사용되는 경우 포트 필드와 *SSL 사용* 확인란을 업데이트합니다.

   연결이 설정되면 보안 서버 연결 표시등이 빨간색에서 녹색으로 바뀝니다.

9. *정책 프록시* 필드에서 정책 프록시 호스트 이름이 보안 서버 호스트와 일치하는 호스트로 자동으로 채워집니다. 정책 구성에 지정된 호스트가 없는 경우 이 호스트가 정책 프록시로 사용됩니다.

   연결이 설정되면 정책 프록시 연결 표시등이 빨간색에서 녹색으로 바뀝니다.

10. Dell 구성 대화 상자가 완료되고 보안 서버 및 정책 프록시로 연결이 설정되면 **계속**을 클릭하여 설치 유형을 표시합니다.
11. 특정 컴퓨터의 일부 설치는 *설치 유형* 대화 상자가 표시되기 전에 *대상 선택* 대화 상자가 표시됩니다. 그러면 표시되는 디스크 목록에서 현재 시스템 디스크를 선택합니다. 현재 시스템 디스크의 아이콘에는 디스크를 가리키는 녹색 화살표가 표시됩니다. **계속**을 클릭합니다.
12. 설치 유형이 표시되면 **설치**를 클릭하여 설치를 진행합니다.
13. 메시지가 표시되면 관리자 계정 자격 증명을 입력합니다. (MacOS X Installer 애플리케이션을 사용하려면 자격 증명이 필요합니다.)
14. **확인**을 클릭합니다.

    노트:

    설치가 완료된 직후, 컴퓨터를 재시작해야 합니다. 다른 애플리케이션에 파일이 열려 있어 재시작할 준비를 하지 못하는 경우 **취소**를 클릭한 뒤 작업을 저장하고 다른 애플리케이션을 닫으십시오.

15. **계속 설치**를 클릭합니다. 설치가 시작됩니다.
16. 설치가 완료되면 **재시작**을 클릭합니다.
17. Endpoint Security Suite Enterprise를 새로 설치하는 경우 *시스템 확장명이 차단됨* 대화 상자가 표시됩니다.

    kext 동의의 경우 이 대화 상자 중 하나 또는 둘 모두가 표시됩니다.

시스템 확장이 차단됨	시스템 확장이 차단됨
a. **확인**을 클릭합니다. b. **확인**을 클릭합니다. c. 이러한 확장명을 승인하려면 **시스템 기본 설정 > 보안 및 개인정보 보호**를 선택합니다. d. *개발자 Credant Technologies(Dell, Inc, formerly Credant Technologies)의 시스템 소프트웨어* 옆에 있는 **허용**을 클릭합니다. e. **확인**을 클릭합니다.	FDEEM 볼륨을 마운팅하기 위해 시스템 확장을 로드할 수 없는 경우 다음 단계를 수행하십시오. a. **시스템 환경설정 열기**를 클릭합니다. b. **확인**을 클릭합니다. c. **일반** 탭에서 *개발자 Credant Technologies(Dell, Inc, formerly Credant Technologies)의 시스템 소프트웨어* 옆에 있는 **허용**을 클릭합니다. d. **확인**을 클릭합니다.

이 허용 버튼은 설치 후 30분 이내에 사용할 수 있습니다. 이 단계를 건너뛰면 이 단계를 완료할 때까지 약 25분마다 대화 상자가 계속 표시됩니다.

18. 계속해서 MEncryption Client for Mac 활성화를 진행합니다.

이동식 미디어가 있는 macOS 10.15 이상

기업에서 macOS 10.15 이상이 설치된 이동식 미디어를 사용하는 경우 사용자는 외부 미디어에 대해 전체 디스크 액세스를 활성화해야 합니다. 자세한 내용은 이동식 미디어에 대해 전체 디스크 액세스 활성화를 참조하십시오.

명령줄 설치/업그레이드

명령줄을 사용하여 클라이언트 소프트웨어를 설치하려면 다음과 같은 단계를 따릅니다.

명령줄 설치

1. Dell 설치 미디어에서 Dell-Encryption-Enterprise-<version>.dmg 파일을 마운트합니다.
2. **Install Dell Endpoint Security Suite Enterprise** 패키지와 **com.dell.ddp.plist** 파일을 로컬 드라이브에 복사합니다.
3. 필요하다면 Management Console에서 다음과 같은 정책을 수정합니다. 정책 설정은 .plist 파일 설정을 재정의합니다. Management Console에 정책이 없는 경우 .plist 설정을 사용합니다.
   - **인증 사용자 목록 없음** - 경우에 따라 지정된 사용자 또는 사용자 그룹이 Dell Server에 대하여 활성화를 할 필요가 없도록 이 정책을 편집하고 싶어할 수도 있습니다. 예를 들어 교육 시설의 경우, 교사들에게는 Dell Server에 자신의 컴퓨터를 활성화하라는 메시지가 표시되지만 랩 컴퓨터를 사용하는 학생들에게는 표시되지 않습니다. 랩 관리자는 클라이언트 도구를 실행하는 계정과 이 정책을 사용하여 학생 사용자가 활성화 메시지 없이 로그인할 수 있도록 설정합니다. 클라이언트 도구에 대한 자세한 내용은 클라이언트 도구를 참조하십시오. 기업에서 사용자 계정이 각각 어떤 Mac 컴퓨터에 연결되어 있는지 확인해야 할 경우, 모든 사용자를 Dell Server에 대해 활성화해야 기업에서 해당 속성을 편집하지 않습니다. 하지만 사용자가 Encryption External Media 미디어를 프로비저닝하려고 하는 경우에는 Dell Server에 대한 인증을 받아야 합니다.
4. .plist 파일을 열고 다음과 같이 모든 추가 자리 표시자 값을 편집합니다.

   노트:

   Apple에서는 Endpoint Security Suite Enterprise for Mac 릴리스 간에 새로운 버전의 운영 체제를 자주 출시합니다. 최대한 많은 고객을 지원하기 위해 Dell에서는 .plist 파일의 수정을 허용하여 이런 사례를 지원하고 있습니다. Apple에서 새 릴리스를 출시하면 Dell에서 이러한 버전을 테스트하여 Encryption Client for Mac과 호환되는지 확인합니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>NoAuthenticateUsers</key> [In this sample code, after one user activates the
computer against the Dell Server, other users can log in without being prompted to
activate.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, users from a specific domain name
can log in without being prompted to activate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
```

```
  <array>
  <string>;Kerberosv5;;*@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, specific users can log in without
being prompted to authenticate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string>
  <string>;Kerberosv5;;username2@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the default .plist
file, it must be added to the file. Add from <key> through </array> to allow a newer
version of operating system to be used. See Note above.]
  <array>
   <string>10.<x.x></string> [Operating system version]
  </array>
  <key>UseRecoveryKey</key>
  <false/> [This value is obsolete since current versions can use both personal and
institutional recovery keys for FileVault encryption.]
  <key>SecurityServers</key>
  <array>
   <dict>
      <key>Host</key>
      <string>securityserver.organization.com</string> [Replace this value with your
Security Server URL]
      <key>Port</key>
     <integer>8443</integer> [Beginning in v8.0, the default port number is 8443. However,
port number 8081 will still allow activations. In general, if your Dell Server is v8.0 or
later, use port 8443. If your Dell Server is pre-v8.0, use port 8081.]
      <key>UseSSL</key>
      <true/> [Dell recommends a true value]
   </dict>
  </array>
  <key>ReuseUniqueIdentifier</key>
  <false/> [When this value is set to true, the computer identifies itself to the Dell
Server by the same hostname it was activated with, regardless of changes to the computer
hostname.]
  <key>Domains</key>
  <array>
   <dict>
      <key>DisplayName</key>
      <string>COMPANY</string>
      <key>Domain</key>
      <string>department.organization.com</string> [Replace this value with the Domain URL
that users will activate against]
   </dict>
  </array>
  <key>PolicyProxies</key>
  <array>
   <dict>
      <key>Host</key>
      <string>policyproxy.organization.com</string> [Replace this value with your Policy
Proxy URL]
      <key>Port</key>
      <integer>8000</integer> [Leave as-is unless there is a conflict with an existing
port]
   </dict>
  </array>
  <key>Version</key>
  <integer>2</integer> [Do not modify]
  <key>MaxPasswordDelay</key>
  <integer>xxxx</integer> [Number of seconds to apply to the security policy, "Require
password XXXX after sleep or screen saver begins." The acceptable range is 0-32400.]
  <key>EMSTreatsUnsupportedFileSystemAs</key>
  <string>ignore</string> [For handling Mac OS Extended media. Possible values are ignore,
provisioningRejected, or unshieldable. ignore - the media is usable (default).
provisioningRejected - retains the value in the Dell Server policy, EMS Access to
unShielded Media. unshieldable - If the EMS Access to unShielded Media policy is set to
Block, the media is ejected. If the EMS Access to unShielded Media policy is not set to
Block, it is usable as provisioningRejected. The key and value are case sensitive.]
```

```
  <key>ClientActivationTimeout</key>
  <integer>120</integer> [Range: 5 to 300, inclusive. The default value is 30. The time in
seconds to give the Security Server time to respond to an activation attempt before giving
up. This plist value is valid for clients running v8.6.0.6627 or later.]
</dict>
</plist>
```

5. .plist 파일을 저장하고 닫습니다.
6. 각각의 대상 컴퓨터에 대해 패키지를 임시 폴더로 복사하고 com.dell.ddp.plist 파일을 **/Library/Preferences**에 복사합니다.
7. 다음과 같은 **설치 프로그램** 명령을 사용하여 패키지의 명령줄 설치를 수행합니다.
   sudo installer -pkg "Install Dell Endpoint Security Suite Enterprise.pkg" -target /
8. 다음 명령줄을 사용하여 컴퓨터를 다시 시작합니다.**sudo shutdown -r now**

   노트:

   macOS High Sierra(10.13)에서는 사용자가 새 타사 커널 확장을 승인하도록 SIP(System Integrity Protection)가 강화되었습니다. macOS High Sierra에서 커널 확장 허용에 대한 자세한 내용은 KB 문서 SLN307814를 참조하십시오.
9. 계속해서 Encryption Client for Mac 활성화를 진행합니다.

이동식 미디어가 있는 macOS 10.15 이상

기업에서 macOS 10.15 이상이 설치된 이동식 미디어를 사용하는 경우 사용자는 외부 미디어에 대해 전체 디스크 액세스를 활성화해야 합니다. 자세한 내용은 이동식 미디어에 대해 전체 디스크 액세스 활성화를 참조하십시오.

이동식 미디어에 대해 전체 디스크 액세스 활성화

기업에서 macOS 10.15 이상이 설치된 이동식 미디어를 사용하는 경우 사용자는 외부 미디어에 대해 전체 디스크 액세스를 활성화해야 합니다. 사용자에게 다음 메시지 중 하나가 표시됩니다.

- 클라이언트 소프트웨어를 설치한 후 외부 미디어에 대해 전체 디스크 액세스에 동의해야 한다는 메시지가 표시됩니다. **보안 및 개인 정보로 이동** 버튼을 클릭하고 아래 단계를 계속 진행합니다.
- 설치 후 메시지가 표시되지 않으면 이동식 미디어를 처음 마운트할 때 전체 디스크 액세스를 활성화하라는 메시지가 표시됩니다. Dell Encryption External Media 또는 EMS Explorer에서 이동식 볼륨의 파일에 액세스하려고 한다는 메시지가 표시됩니다. **확인**을 클릭하고 아래 단계를 계속 진행합니다.

자세한 내용은 KB 문서 SLN319972를 참조하십시오.

1. *시스템 환경 설정* > *보안 및 개인 정보*에서 **개인 정보** 탭을 클릭합니다.
2. 왼쪽 창에서 **전체 디스크 액세스**를 선택합니다.
   Dell Encryption External Media 앱이 표시되지 않습니다.
3. 하단에서 잠금 아이콘을 클릭하고 로컬 관리자 계정에 대한 자격 증명을 제공합니다.
   왼쪽 창의 > **파일 및 폴더**에서 사용자는 필요한 사용 권한을 제공하는 외부 미디어(EMS) 구성 요소를 확인할 수 있습니다.
4. 왼쪽 창에서 **전체 디스크 액세스**를 선택합니다.

   이제 *Dell Encryption External Media* 앱이 표시됩니다. 그러나 승인 요청이 보류 중인 경우에는 해당 앱의 확인란이 선택되지 않습니다.
5. 확인란을 선택하여 권한을 부여합니다.

   Dell Encryption External Media 앱이 표시되지 않을 경우 다음을 수행합니다.

   a. 오른쪽 창에서 더하기 아이콘(+)을 클릭합니다.
   b. **/Library/Dell/EMS**로 이동하여 **Dell Encryption External Media**를 선택합니다.
   c. **열기**를 클릭합니다.
   d. **전체 디스크 액세스**에서 *Dell Encryption External Media*의 확인란을 선택합니다.
6. **보안 및 개인 정보**를 닫습니다.

Encryption 클라이언트 활성화

활성화 프로세스는 Dell Server의 네트워크 사용자 계정을 Mac 컴퓨터와 연결하고 각 계정의 보안 정책을 검색하며 인벤토리 및 상태 업데이트를 전송합니다. 또한 복구 워크플로를 사용하고 포괄적인 준수 보고를 제공합니다. 각 사용자가 자신의 사용자 계정에 로그인할 때 클라이언트 소프트웨어는 컴퓨터에서 찾은 각 사용자 계정에 대한 활성화 프로세스를 수행합니다.

클라이언트 소프트웨어를 설치하고 Mac을 다시 시작한 후 사용자는 다음과 같이 로그인합니다.

1. Active Directory에 의해 관리되는 사용자 이름 및 암호를 입력합니다.

암호 대화 상자 시간이 초과하면 정책 탭에서 **새로 고침**을 누릅니다. 로컬 컴퓨터에서 정책 및 상태 보기 1단계를 참조하십시오.

2. 로그온할 도메인을 선택합니다.

   Dell Server에 멀티 도메인 지원이 구성되고 다른 도메인을 활성화에 사용해야 하는 경우 사용자 계정 이름(UPN)을 사용합니다. 이 이름은 *<username>@<domain>* 형태입니다.

3. 제공되는 옵션은 다음과 같습니다.
   - **활성화**를 클릭합니다.
     - 활성화에 성공하는 경우 활성화 성공을 나타내는 메시지가 표시됩니다. 이제 Encryption Client for Mac이 완벽하게 작동하고 Dell Server에서 관리됩니다.

       노트:

       Encryption External Media 필수 리소스와 관련하여 경고가 표시되면 **보안 및 개인 정보로 이동** 버튼을 클릭한 다음, 조직에서 요구하는 시스템 확장에 대해 **허용**을 클릭합니다. Encryption External Media가 올바르게 작동하려면 이 확장을 허용해야 합니다.
     - 활성화가 실패할 경우 클라이언트 소프트웨어에서는 올바른 도메인 자격 증명 입력 시도를 세 번까지 허용합니다. 세 번의 시도가 모두 실패할 경우 다음 사용자 로그인 시 도메인 자격 증명을 입력하기 위한 프롬프트가 다시 표시됩니다.
   - **나중에**를 클릭하여 대화 상자를 닫으면 다음 사용자 로그인 시 다시 표시됩니다.

     노트:

     원격 위치에서든 스크립트를 실행해서든 직접 작업하든 상관없이, 관리자가 Mac 컴퓨터의 드라이브를 복호화할 필요가 있을 때 클라이언트 소프트웨어에는 사용자가 관리자 권한으로 액세스할 수 있도록 허용하는 프롬프트가 표시되며 사용자는 자신의 암호를 입력해야 합니다.

     노트:

     FileVault 암호화를 위해 컴퓨터를 설정하고 파일이 암호화되어 있는 경우 이후에 시스템을 부팅할 수 있는 계정으로 로그인해야 합니다.
4. 다음 중 하나를 수행합니다.
   - 활성화 전에 암호화가 **설정되지 않은** 경우 암호화 프로세스를 계속 수행합니다.
   - 활성화 전에 암호화가 **설정된** 경우 암호화 정책 및 상태 보기를 계속 수행합니다.

암호화 정책 및 상태 보기

로컬 컴퓨터 또는 Management Console에서 암호화 정책 및 상태를 볼 수 있습니다.

로컬 컴퓨터에서 정책 및 상태 보기

로컬 컴퓨터에서 암호화 정책 및 암호화 상태를 보려면 아래 단계를 따르십시오.

1. *시스템 환경설정*을 실행하고 **Dell Encryption Enterprise**를 클릭합니다.
2. 이 컴퓨터에 설정된 현재 정책을 확인하려면 **정책**을 클릭합니다. 이 보기를 사용하여 이 컴퓨터에 대해 적용되는 특정 암호화 정책을 확인합니다.

   노트:

   정책 업데이트를 확인하려면 **새로 고침**을 클릭합니다.

   Management Console에 다음의 기술 그룹에서의 Mac 정책이 표시됩니다.

   - **Mac 암호화**
   - **이동식 미디어 암호화**

   설정하는 정책은 기업의 암호화 요구 사항에 따라 다릅니다.

   이 표는 정책 옵션을 나열합니다.

Mac 암호화 > Dell 볼륨 암호화

High Sierra 이상의 버전에서는 두 가지 정책을 모두 활성화해야 합니다. Sierra 및 이전 버전의 경우 이전 버전의 문서를 참조하십시오.	
Dell 볼륨 암호화	*켜짐* 또는 *꺼짐* 이것은 다른 모든 Dell 볼륨 암호화 정책의 마스터 정책입니다. 다른 모든 Dell 볼륨 암호화 정책을 적용하려면 이 정책을 *켜짐*으로 설정해야 합니다. *켜짐*으로 설정하면 암호화가 활성화되고, *암호화 대상 볼륨* **또는** *Mac용 FileVault 를 사용한 암호화* 정책을 기반으로 암호화되지 않은 볼륨에 대한 암호화가 시작됩니다. 기본 설정은 *켜짐*입니다. 꺼짐으로 설정하면 암호화가 비활성화되고 전체 또는 부분적으로 암호화된 볼륨에 대해 암호 해독 스윕이 시작됩니다.
Mac용 FileVault를 사용한 암호화	FileVault 암호화를 사용할 경우 먼저 Dell 볼륨 암호화를 *켜짐*으로 설정해야 합니다. Management Console에서 *Mac용 FileVault를 사용한 암호화* 정책이 선택되어 있는지 확인합니다. 활성화되면 퓨전 드라이브를 포함한 시스템 볼륨을 암호화하기 위해 *암호화 대상 볼륨* 정책 설정에 기반해 FileVault를 사용합니다.
Mac 암호화 > Mac Global 설정	
암호화 대상 볼륨	*시스템 볼륨만* 또는 *모든 고정 볼륨* *시스템 볼륨*만은 현재 실행 중인 시스템 볼륨만 보호합니다. **모든 고정 볼륨**은 모든 고정 디스크 및 현재 실행 중인 시스템 볼륨에서 모든 Mac OS 확장 볼륨을 보호합니다.

3. 모든 정책에 대한 설명은 Management Console에서 사용 가능한 *관리자 도움말*을 참조하십시오. *관리자 도움말*에서 특정 정책을 찾는 방법
   a. 검색 아이콘을 클릭합니다.
   b. *검색*에서 정책 이름을 따옴표와 함께 입력합니다.
   c. 표시된 주제 링크를 클릭합니다. 따옴표와 함께 입력한 정책 이름이 주제에서 강조됩니다.
4. **시스템 볼륨** 탭을 클릭하여 암호화 대상인 볼륨 상태를 확인할 수 있습니다.

시/도	설명
제외됨	볼륨이 암호화에서 제외됩니다. 이는 암호화가 비활성화되어 있을 때 암호화되지 않은 볼륨, 외부 볼륨, Mac OS X Extended(Journaled) 이외의 형식을 가진 볼륨, *암호화 대상 볼륨* 정책이 시스템 볼륨만으로 설정되었을 때 비 시스템 볼륨에 적용됩니다.
볼륨 암호화 준비 중...	클라이언트 소프트웨어가 현재 볼륨에 대한 암호화 프로세스를 시작 중이지만, 암호화 스윕을 시작하지는 않았습니다.
볼륨의 크기를 조정할 수 없음	볼륨의 크기를 적절히 조정할 수 없어 클라이언트 소프트웨어가 암호화를 시작할 수 없습니다. 이 메시지를 수신하면 Dell ProSupport에 문의한 뒤 로그 파일을 제공합니다.
암호화를 시작하기 전에 수리 필요	볼륨이 디스크 유틸리티 확인에 실패했습니다. 볼륨을 복구하려면 Apple Support 문서 HT1782(http://support.apple.com/kb/HT1782)의 지침을 따르십시오.
암호화 준비 완료. 재시작 보류 중...	재시작 후에 암호화가 시작됩니다.
암호화 정책 충돌	디스크가 잘못된 설정으로 암호화되어 있어 디스크를 정책 적용 대상으로 가져올 수 없습니다. Mac용 FileVault를 사용한 암호화를 참조하십시오.
Dell Server에 키를 에스크로하기 위해 대기 중...	암호화된 데이터를 모두 복구할 수 있도록 하기 위해 클라이언트는 모든 암호화 키가 Dell Server에 성공적으로 에스크로될 때까지 암호화 프로세스를 시작하지 않습니다. 클라이언트는 키가 에스크로될 때까지 이 상태에 있으면서 보안 서버 연결에 대해 폴링합니다.

시/도	설명
암호화	암호화 스윕이 진행 중입니다.
암호화됨	암호화 스윕이 완료되었습니다.
암호 해독	복호화 스윕이 진행 중입니다.
원래 상태로 복원 중...	클라이언트 소프트웨어가 *암호 해독* 프로세스 종료 시 파티션 구성표를 원래 상태로 복원 중입니다. 이는 "*볼륨 암호화 준비 중*" 상태와 동등한 복호화 스윕입니다.
복호화됨	복호화 스윕이 완료되었습니다.

색상	설명
녹색	암호화된 부분
빨간색	암호화되지 않은 부분
노란색	다시 암호화 중인 부분 예를 들어 암호화 알고리즘의 변경으로 인해 다시 암호화 중인 부분입니다. 데이터 보안은 계속 유지됩니다. 이는 단지 다른 유형의 암호화로 전환 중인 경우입니다.

시스템 볼륨 탭에는 컴퓨터에 연결되어 있고 GPT(GUID Partition Table) 형식의 디스크에 있는 모든 볼륨이 표시됩니다. 다음 표에는 내부 드라이브에 대한 볼륨 구성의 예가 나와 있습니다.

노트:

배지와 아이콘은 운영 체제에 따라 약간 다를 수 있습니다.

배지	볼륨 유형 및 상태
	현재 부팅된 Mac OS X 시스템 볼륨입니다. X 폴더 배지는 현재 부팅 파티션을 나타냅니다.
	암호화를 위해 구성된 볼륨. 보안 및 개인 정보 배지는 FileVault로 보호되는 파티션을 나타냅니다.
	암호화를 위해 구성된 비부팅 볼륨. 보안 및 개인 정보 배지는 FileVault로 보호되는 파티션을 나타냅니다.
	여러 개의 드라이브와 암호화 없음. **노트:** 배지가 없는 볼륨 아이콘은 디스크에 아무런 작업도 수행되지 않았음을 나타냅니다. 이것은 부팅 디스크가 아닙니다.

5. **이동식 미디어** 탭을 클릭하여 암호화 대상인 볼륨 상태를 확인할 수 있습니다. 다음 표에는 이동식 미디어에 대한 볼륨 구성의 예가 나와 있습니다.

   배지와 아이콘은 운영 체제에 따라 약간 다를 수 있습니다.

배지	상태
	흐릿한 볼륨 아이콘은 탑재되지 않은 장치를 표시합니다. 다음과 같은 이유 때문입니다. • 사용자가 장치를 프로비저닝하지 않기로 선택했을 수 있습니다. • 미디어가 차단되어 있을 수 있습니다. **노트:** 이 아이콘의 빨간색 원/슬래시 배지는 지원되지 않기 때문에 보호에서 제외되는 파티션을 표시합니다. 여기에는 FAT32 형식의 볼륨이 포함됩니다.
	포화 상태의 볼륨 아이콘은 탑재된 장치를 표시합니다. 쓰기 금지 배지를 통해 읽기 전용임을 표시합니다. 암호화가 활성화되었지만 미디어가 프로비저닝되지 않고 Shield로 보호할 수 없는 미디어에 대한 Encryption External Media 액세스가 읽기 전용으로 설정됩니다.
	Encryption External Media에 의해 암호화된 미디어는 Dell 배지로 표시됩니다.

Management Console에서 정책 및 상태 보기

Management Console에서 암호화 정책 및 암호화 상태를 보려면 아래 단계를 따르십시오.

1. Dell 관리자 계정으로 Management Console에 로그인합니다.
2. 왼쪽 창에서 **개체 > 엔드포인트**를 클릭합니다.
3. 워크스테이션의 경우, *호스트 이름* 필드에서 옵션을 클릭하거나 엔드포인트의 호스트 이름을 알고 있는 경우 *검색*에 입력합니다. 엔드포인트를 검색하기 위한 필터를 입력할 수도 있습니다.

   노트:

   와일드 카드 문자(*)를 사용할 수 있지만, 텍스트 처음이나 끝에는 필요하지 않습니다. 일반 이름, 범용 기본 이름 또는 sAMAccountName을 입력할 수 있습니다.
4. 적절한 엔드포인트를 클릭합니다.
5. **세부 정보 및 작업** 탭을 클릭합니다.

   엔드포인트 세부 정보 영역에는 Mac 컴퓨터에 대한 정보가 표시됩니다.

   Shield 세부 정보 영역에 클라이언트 소프트웨어에 대한 정보가 표시됩니다. 이 정보에는 해당 컴퓨터의 암호화 삭제 시작 및 종료 시간이 포함되어 있습니다.

   유효한 정책을 보려면 작업 영역에서 **유효한 정책 보기**를 클릭합니다.
6. **보안 정책** 탭을 클릭합니다. 이 탭에서 정책의 유형을 확장할 수 있으며 개별 정책을 변경할 수 있습니다.
   a. 작업을 마친 후 **저장**을 클릭합니다.
   b. 왼쪽 창에서 **관리** > **커밋**을 클릭합니다.

      노트:

      정책 변경 보류에 나타나는 수는 누적됩니다. 이는 다른 엔드포인트의 변경 사항이나 같은 계정을 사용하는 다른 관리자가 수행한 변경 사항을 포함할 수 있습니다.
   c. *명령* 상자에 변경 사항에 대한 설명을 입력하고 **정책 커밋**을 클릭합니다.
7. **사용자** 탭을 클릭합니다. 이 영역에는 이 Mac 컴퓨터에서 활성화된 사용자의 목록이 표시됩니다. 사용자 이름을 클릭하여 이 사용자가 활성화되어 있는 모든 컴퓨터에 대한 정보를 표시합니다.
8. **엔드포인트 그룹** 탭을 클릭합니다. 이 영역에는 이 Mac 컴퓨터가 속한 모든 엔드포인트 그룹이 표시됩니다.

시스템 볼륨

암호화 사용

다음은 지원되는 암호화입니다.

- 부팅 볼륨과 물리적 미디어를 공유하는 APFS(Apple File System) 볼륨
- GPT(GUID Partition Table) 파티션 구성표로 분할되어 있는 Mac OS X Extended(Journaled) 볼륨 및 시스템 디스크

활성화 전에 암호화가 설정되지 **않은** 경우 이 절차를 통해 클라이언트 컴퓨터에서 암호화를 설정할 수 있습니다. 이 프로세스를 사용하면 단일 컴퓨터에 대해서만 암호화를 사용할 수 있습니다. 원하는 경우 엔터프라이즈 레벨에서 모든 Mac 컴퓨터에 대한 암호화를 설정하도록 선택할 수 있습니다. *엔터프라이즈* 레벨에서 암호화를 활성화하는 방법에 대한 자세한 내용은 관리자 도움말을 참조하십시오.

1. Dell 관리자 계정으로 Management Console에 로그인합니다.
2. 왼쪽 패널에서 **채우기** > **엔드포인트**를 클릭합니다.
3. 워크스테이션의 경우, 호스트 이름 열에서 옵션을 클릭하거나 엔드포인트의 호스트 이름을 알고 있는 경우 *검색*에 입력합니다. 엔드포인트를 검색하기 위한 필터를 입력할 수도 있습니다.

   노트:

   와일드 카드 문자(*)를 사용할 수 있지만, 텍스트 처음이나 끝에는 필요하지 않습니다. 일반 이름, 범용 기본 이름 또는 sAMAccountName을 입력할 수 있습니다.

4. 적절한 엔드포인트를 클릭합니다.
5. *보안 정책* 페이지에서 **MAC 암호화** 기술 그룹을 클릭합니다.

   기본적으로 *Dell 볼륨 암호화* 마스터 정책이 *켜짐*으로 전환됩니다.

6. Mac에 퓨전 드라이브가 있는 경우, *Mac용 FileVault를 사용한 암호화 정책에 대한 확인란을 선택합니다.*

   노트:

   이 정책은 *Dell 볼륨 암호화* 정책 또한 *켜짐*으로 설정되어야 합니다. 그러나 FileVault 암호화가 사용되는 경우 그룹에 있는 다른 어떤 정책도 유효하지 않습니다. Mac 암호화 > Dell 볼륨 암호화를 참조하십시오.

7. FileVault가 선택되지 않은 경우(macOS Sierra 및 이하) 다른 정책을 원하는 대로 변경하십시오.

   모든 정책에 대한 설명은 Management Console에서 사용 가능한 *관리자 도움말*을 참조하십시오.

8. 작업을 마친 후 **저장**을 클릭합니다.
9. 왼쪽 창에서 **관리** > **커밋**을 클릭합니다.

   정책 변경 보류에 나타나는 수는 누적됩니다. 이는 다른 엔드포인트의 변경 사항이나 같은 계정을 사용하는 다른 관리자가 수행한 변경 사항을 포함할 수 있습니다.

10. 명령 상자에 변경 사항에 대한 설명을 입력하고 **정책 커밋**을 클릭합니다.
11. Dell Server가 정책을 보낸 후 로컬 컴퓨터에 대한 정책 설정을 보려면 Dell Encryption Enterprise 환경설정의 정책 패널에서 **새로 고침**을 클릭합니다.

암호화 프로세스

암호화 프로세스는 암호화가 활성화된 경우 부팅 볼륨의 상태에 따라 달라집니다.

노트:

사용자 데이터의 무결성을 유지하기 위해, 클라이언트 소프트웨어는 해당 볼륨에서 확인 프로세스가 성공할 때까지 볼륨 암호화를 시작하지 않습니다. 볼륨이 확인에 실패하면 클라이언트 소프트웨어에서 사용자에게 그 사실을 알리고 Dell Data Protection 환경설정에 실패를 보고합니다. 볼륨을 복구할 필요가 있는 경우 Apple Support 문서 HT1782(http://support.apple.com/kb/HT1782)를 참조하십시오. 클라이언트 소프트웨어는 다음에 컴퓨터를 다시 시작할 때 다시 확인을 시도합니다.

다음 중 하나를 선택합니다.

- 암호화되지 않은 볼륨의 FileVault 암호화
- 기존 FileVault 암호화 볼륨의 관리 인수

암호화되지 않은 볼륨의 FileVault 암호화

FileVault 암호화를 사용하면 PBA에 이름 없는 사용자가 추가로 표시됩니다. Dell Server가 장치에 정책을 적용하게 하므로 이 사용자를 삭제하지 마십시오. PBA 사용자가 제거되는 경우 사용자는 규정 정책의 해독 시작을 위한 조치를 취해야 할 수 있습니다.

1. 설치 및 활성화 후, FileVault 암호화가 활성화된 다음에 부팅하려는 계정에 로그인해야 합니다.
2. 드라이브의 유효성 검사와 볼륨 확인이 완료되기를 기다립니다.
3. 계정의 암호를 입력합니다.

   노트:

   이 대화 상자의 시간 제한을 허용하는 경우 암호 대화 상자가 다시 표시되도록 하려면 다시 부팅하거나 로그인해야 합니다.
4. **확인**을 클릭합니다.
5. 각 사용자에게 보안 토큰이 있는지 확인하십시오. https://www.dell.com/support/article/us/en/19/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en을 참조하십시오.

   사용자가 로그인한 계정이 모바일 네트워크 계정이 아닌 경우 대화 상자가 표시됩니다. 부팅 드라이브가 암호화된 후 FileVault 초기화 중에 로그인한 사용자만 이 드라이브를 부팅할 수 있습니다.

   이 계정은 로컬 또는 네트워크 모바일 계정이어야 합니다. 모바일 네트워크 계정이 아닌 계정을 모바일 네트워크로 변경하려면 **시스템 환경설정 > 사용자 및 그룹**으로 이동합니다. 다음 중 하나를 수행하십시오.

   - 계정을 모바일 계정으로 만듭니다.

     또는

   - 로컬 계정에 로그인하고 그 위치에서 FileVault를 초기화합니다.
6. **확인**을 클릭합니다.
7. 암호화 준비가 완료된 후 컴퓨터를 다시 시작합니다.

   노트:

   Management Console에 설정된 사용자 환경 정책에 따라 클라이언트 소프트웨어에서 사용자에게 컴퓨터를 다시 시작하라는 메시지를 표시할 수 있습니다.
8. 컴퓨터가 다시 시작된 후 클라이언트 소프트웨어용 네트워크에 컴퓨터를 연결하여 Dell Server에 복구 정보를 에스크로해야 합니다.

   클라이언트 소프트웨어는 사용자 로그인 전에 암호화 프로세스를 시작 및 완료하고 Management Console에 암호화 상태를 보고할 수 있습니다. 이를 통해 사용자 상호 작용이 없어도 모든 Mac 컴퓨터에서 규정 준수를 강제 실행할 수 있습니다.

FileVault 사용자를 추가하도록 정책을 수정

FileVault는 자동으로 암호화를 하여 디스크의 데이터를 보호합니다. 관리되는 FileVault 부팅 볼륨에서 여러 사용자가 디스크의 잠금을 해제할 수 있도록 Management Console의 정책을 수정하고 OpenDirectory 레코드 이름과 값의 사전을 사용하여 사용자가 자신을 FileVault 디스크에 추가할 수 있게 할 수 있습니다.

1. Management Console의 고급 *Mac 전역 설정* 정책에서 *FileVault 2 PBA 사용자 목록* 정책으로 스크롤합니다.
2. *FileVault 2 PBA 사용자 목록* 정책 필드에 지정하려는 사용자에 일치하는 규칙을 입력합니다. 예를 들어 어떤 키에 대한 `<string>*</string>`의 일치는 바인딩되는 OpenDirectory 서버에 있는 모든 사용자에 일치해야 합니다.

   태그는 대소문자를 구분하며 전체 값은 속성 목록의 사전 및 어레이 요소로 적절하게 구성되어야 합니다. 사전 키는 AND로 연결합니다. 어레이 값은 OR로 연결하기 때문에 어레이의 어떤 요소에 일치하면 전체 어레이에 일치하게 됩니다.

   노트:

   규칙을 잘못 구성하면 *Dell Encryption Enterprise> 기본 설정* 탭에 오류가 표시됩니다.

   아래의 <dict>에 두 키에 대한 예가 나와 있습니다.

```
<dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
     <string>;Kerberosv5;;user1@LKDC:*</string>
     <string>;Kerberosv5;;user2@LKDC:*</string>
     <string>;Kerberosv5;;user3@LKDC:*</string>
     <string>;Kerberosv5;;z*@LKDC:*</string>
```

```
    </array>
    <key>dsAttrTypeStandard:NFSHomeDirectory</key>
    <string>/Users/*</string>
</dict>
```

- 샘플 *AuthenticationAuthority* 키 항목에서는 *user1*, *user2* 및 *user3* 또는 *z*로 시작하는 모든 사용자 ID의 패턴을 지정합니다. 각 사용자에 대한 올바른 구문을 제공하는 대화 상자를 보려면 클라이언트에서 **제어-옵션-명령** 키를 누릅니다. 사용자에 대한 구문을 복사하고 Management Console에 붙여 넣습니다.

  노트:

  이 예에서 뒤에 나타나는 별표는 인증 기관 레코드의 후자의 일부를 나타냅니다. 별표는 OpenDirectory 레코드에서 콜론 뒤에 나오는 모든 정보와 일치하기 때문에 과소 지정을 피하기 위해 뒤에 나타나는 별표 대신에 전체 레코드를 포함시키는 것이 일반적입니다.

- NFSHomeDirectory 키를 사용하려면 첫 번째 키를 전달하는 모든 사용자가 */Users/*에 홈 디렉터리가 있어야 합니다.

  노트:

  사용자에 대한 홈 폴더가 없으면 만들어야 합니다.

3. 컴퓨터를 재부팅합니다.
4. 사용자에게 자신의 사용자 계정에 대한 FileVault 부팅을 활성화하도록 통보합니다. 사용자에게 로컬 또는 모바일 계정이 있어야 합니다. 네트워크 계정은 자동으로 모바일 계정으로 전환됩니다.

사용자가 자신의 FileVault 계정을 활성화하는 경우:

1. **시스템 환경설정**을 실행하고 **Dell Encryption Enterprise**를 클릭합니다.
2. **시스템 볼륨** 탭을 클릭하십시오.
3. 시스템 볼륨 드라이브 컨트롤 키를 클릭하고 **FileVault 부팅에 FileVault 사용자 추가**를 선택합니다.
4. *검색*에서 사용자의 이름을 입력하거나 아래로 스크롤합니다. 정책에서 정한 조건을 만족할 경우에만 사용자 계정이 표시됩니다.

   로컬 및 모바일 사용자의 경우 *사용자 활성화* 단추가 표시됩니다.

   네트워크 사용자의 경우 *사용자 변환 및 활성화* 단추가 표시됩니다.

   노트:

   FileVault를 부팅할 수 있는 사용자 계정 옆에 녹색 표시등이 표시됩니다.

5. **사용자 활성화** 또는 **사용자 변환 및 활성화**를 클릭합니다.
6. 선택한 계정에 대한 암호를 입력하고 **확인**을 클릭합니다. 진행률 표시기가 표시됩니다.
7. 성공 대화 상자에서 **완료**를 클릭합니다.

기존 FileVault 암호화 볼륨의 관리 인수

컴퓨터에 FileVault 암호화 볼륨이 이미 있고 Management Console에 FileVault 암호화가 사용되는 경우 Dell Encryption에서 볼륨 관리를 인수할 수 있습니다.

Dell 암호화에서 부팅 볼륨이 이미 암호화되어 있음을 감지하는 경우 Dell Encryption Enterprise 대화 상자가 표시됩니다. Dell 암호화에서 볼륨을 관리하도록 허용하려면 다음 단계를 따르십시오.

1. **개인 복구 키*또는* 부팅 가능한 계정 자격 증명**을 선택합니다.

   노트:

   macOS High Sierra 및 APFS(Apple File System)의 경우 **부팅 가능한 계정 자격 증명**을 선택해야 합니다.

   - **개인 복구 키 - 드라이브가 FileVault로 암호화될 때 수신한 개인 복구 키가 있는 경우**
     a. 키를 입력합니다.

        사용자에게 기존 키가 없는 경우 관리자에게 요청할 수 있습니다.

     b. **확인**을 클릭합니다.

     노트:

     관리 인수 프로세스가 완료된 후 새 개인 복구 키가 생성되고 에스크로됩니다. 이전 복구 키가 무효화되고 제거됩니다.

   - **부팅 가능한 계정 자격 증명 - 현재 볼륨에서 부팅 인가된 계정의 사용자 이름과 암호가 있는 경우**
     a. 사용자 이름 및 암호를 입력합니다.

     b. **확인**을 클릭합니다.

2. 이제 Dell에서 볼륨 암호화를 관리한다는 대화상자가 표시되면, **확인**을 클릭합니다.

   Dell 암호화에서 부팅 볼륨이 아닌 볼륨이 이미 암호화되어 있음을 감지하는 경우 암호를 입력하라는 메시지가 표시됩니다.

3. (FileVault 암호화된 부팅 볼륨이 아닌 볼륨만) Dell 암호화에서 이 볼륨의 관리를 가정하도록 허용하려면, 볼륨에 액세스하기 위한 암호를 입력합니다. 이 암호는 볼륨이 처음 FileVault로 암호화되었을 때 할당된 암호입니다.

   Dell이 볼륨의 암호화를 관리를 시작하면, 이전의 암호는 더 이상 유효하지 않습니다. 복구 도움이 필요한 경우 Dell 관리자가 볼륨의 복구 키를 검색할 수 있습니다.

   암호를 입력하지 않기로 선택하면, 볼륨의 컨텐츠는 접근 가능하고 FileVault로 암호화되지만 Dell이 암호화를 관리하지 않습니다.

노트:

Management Console에서 관리자는 현재 Dell Server가 엔드포인트를 관리하는 것을 볼 수 있습니다.

FileVault 복구 키 재활용

복구 번들에 보안 문제가 있거나 볼륨 또는 키가 손상된 경우 그 볼륨의 키 자료를 재활용할 수 있습니다.

Mac OS X의 부팅 및 비 부팅 드라이버에 대한 키를 재활용할 수 있습니다.

키 자료를 재활용하는 방법은 다음과 같습니다.

1. Management Console에서 복구 번들을 다운로드하여 컴퓨터 바탕 화면으로 복사합니다.
2. *시스템 환경설정*을 실행하고 **Dell Encryption Enterprise**를 클릭합니다.
3. **시스템 볼륨** 탭을 클릭하십시오.
4. 1단계의 복구 번들을 알맞은 파티션으로 끕니다.

   대화 상자에 FileVault 키 주기를 실행하라는 메시지가 표시됩니다.

5. **확인**을 클릭합니다.

   키 주기 실행에 성공했음을 확인하는 대화 상자가 표시됩니다.

6. **확인**을 클릭합니다.

   노트:

   이 드라이브에 대한 복구 번들의 키는 이제 더 이상 사용되지 않습니다. Management Console에서 새 복구 번들을 다운로드해야 합니다.

사용자 경험

보안을 최대화하기 위해 클라이언트 소프트웨어에서 Mac OS X 컴퓨터의 *자동 로그인* 기능을 비활성화합니다.

또한 *절전/화면 보호기 모드가 시작된 뒤에 클라이언트 소프트웨어에서 암호가 필요함* Mac OS X 기능을 강제 실행합니다 또한, 인증을 강제 실행하기 전에 절전/화면 보호기 모드에서 시간을 구성할 수 있습니다. 사용자는 클라이언트 소프트웨어를 사용하여 인증이 강제 실행되기 전에 최대 5분의 값을 설정할 수 있습니다.

사용자는 암호화 스윕이 진행됨에 따라 컴퓨터를 정상적으로 사용할 수 있습니다. 운영 체제가 계속 작동하는 동안 운영 체제를 포함하여 현재 부팅된 시스템 볼륨에 있는 모든 데이터가 암호화됩니다.

컴퓨터가 재시작되거나 시스템 절전 모드에 들어가는 경우 암호화 스윕이 일시 정지된 다음 재시작 또는 절전 모드 해제 후 자동으로 재개됩니다.

클라이언트 소프트웨어는 최대 절전 이미지 사용을 지원하지 않으며, 절전 중에 배터리가 완전히 방전되는 경우 컴퓨터를 재개하기 위해 Mac OS X *안전 절전* 기능에서 사용합니다.

사용자에게 미치는 영향을 줄이기 위해 클라이언트 소프트웨어는 시스템 절전 모드를 자동으로 업데이트하여 최대 절전을 비활성화하고 이 설정을 강제 실행합니다. 컴퓨터는 여전히 절전 모드로 들어갈 수 있지만, 현재 시스템 상태는 메모리에만 유지됩니다. 따라서 절전 중에 컴퓨터가 완전히 시스템 종료되는 경우 완전히 다시 시작되며, 이는 배터리가 방전되거나 배터리를 교체할 경우 발생할 수 있습니다.

허용 목록 규칙 복사

사용자는 숨겨진 메뉴 항목을 사용하여 이동식 미디어에 대한 허용 목록 규칙을 복사할 수 있습니다.

1. **시스템 환경설정**을 실행하고 **Dell Encryption Enterprise**를 클릭합니다.
2. **이동식 미디어** 탭을 선택합니다.
3. 마우스 오른쪽 버튼으로 드라이브 열을 클릭하는 동시에 명령 키를 누릅니다.

   숨겨진 메뉴 항목이 표시됩니다.
4. 현재 이동식 미디어에 대해 **허용 목록 규칙 복사**를 클릭합니다. 허용 목록 규칙이 클립보드에 복사되었습니다.
5. 클립보드에 액세스하고, 허용 목록 규칙을 복사해 관리자에게 보내십시오.

MAC 미디어 암호화 정책이 **켜짐**으로 전환되면 데이터가 암호화됩니다(Thunderbolt 드라이브 포함).

Thunderbolt 드라이브 또는 Encryption External Media에 암호화된 데이터 쓰기를 방지하기 위해 디바이스 또는 디바이스 그룹을 제외하려면 허용 목록 규칙을 사용하여 값을 수정할 수 있습니다.

허용 목록을 위한 특정 드라이브를 지정하기 위해 완벽한 규칙을 사용하십시오. 다음의 예시를 참고합니다.

bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101 II;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSERNUM=001CC0EC3447AA308699119F

노트:

샘플 값을 드라이브에 대한 정보로 바꾸어야 합니다.

노트:

HFS Plus를 활성화해야 합니다. HFS Plus 활성화를 참조하십시오.

Thunderbolt를 통해 연결 시 Mac 미디어 암호화 정책 강제 실행에서 SATA 디바이스를 제외하는 방법은 다음과 같습니다.

tbolt=1;bus=SATA

다음에 기반해 미디어를 Encryption External Media로부터 허용 목록에 추가하거나 제외할 수 있습니다.

- **미디어 크기**

  큰 미디어를 Encryption External Media 보호로부터 제외하기 위한 허용 목록 규칙:

  크기 <op> <size specifier>

  <op>는 =, <=, >=, <, > 등이 될 수 있음

  <size specifier>는 10진법 형식이며 {K, M, G, T} 중 선택 사항인 접미사를 포함해 1024가 아닌 1000에 정렬합니다. 예를 들어, 500000000 바이트 이상의 미디어 또는 드라이브를 Encryption External Media로부터 제외하려면 다음 중 하나를 사용합니다.

  크기 >= 500000000

  크기 >= 500000K

  크기 >= 500M
- **파일 시스템 유형**

  허용 목록 규칙:

  fstype=<fstype>

  <fstype>은 ExFAT, FAT 또는 HFS+일 수 있습니다.

두 가지를 모두 제외하려면, 다음의 1TB와 더 큰 HFS+ 미디어의 예시를 참고합니다.

size>=1T;fstype=HFS+

복구

때로는 암호화된 디스크에 있는 데이터에 액세스해야 할 수도 있습니다. Dell 관리자는 암호를 해독하지 않고 암호화된 디스크에 액세스할 수 있어 소중한 시간을 절약할 수 있습니다.

다양한 이유로 사용자의 암호화된 데이터에 액세스해야 할 수 있겠지만, 몇 가지 공통된 사용 사례는 다음과 같습니다.

- 직원이 회사를 그만두었는데 아무도 암호를 모르는 경우
- 사용자가 암호를 기억하지 못하는 경우

이 섹션에서는 FileVault 암호화가 복구될 끝점에 있을 때 FileVault 복구를 사용하는 프로세스를 안내합니다. FileVault는 macOS Sierra 10.12.6에서 실행 중인 암호화 클라이언트에서 사용할 수 있습니다. FileVault 복구는 퓨전 드라이브에도 사용됩니다.

볼륨 탑재

사전 요구 사항

- 복구 유틸리티를 실행하는 암호화되지 않은 외부 복구 볼륨 또는 컴퓨터
- 하드웨어에 따라 FireWire 또는 Thunderbolt 케이블
- 복구 대상 컴퓨터의 장치 ID/고유 ID - 대부분의 경우, 복구 대상 컴퓨터는 Management Console에서 소유자의 사용자 이름을 검색하고 그 사용자를 위해 암호화된 장치를 보면 찾을 수 있습니다. 고유 ID/디바이스 ID의 형식은 "John Doe's MacBook.Z4291LK58RH"입니다.
- Dell 설치 미디어

프로세스

1. Dell 관리자 계정으로 Management Console에 로그인합니다.
2. 왼쪽 창에서 **관리 > 엔드포인트 복구**를 클릭합니다.
3. *검색*에 엔드포인트의 정규화된 도메인 이름을 입력해 복구하고 검색 아이콘을 클릭합니다.
4. 장치의 **복구** 링크를 클릭합니다.
5. 엔드포인트가 고급 복구를 요구하는 경우 암호를 입력할 창이 나타납니다. 다운로드할 암호화 키 번들에 새로운 암호를 할당합니다.

   노트:

   복구 키에 액세스하려면 이 암호가 필요합니다.
6. 복구 작업을 수행하기 위해 복구 유틸리티를 실행할 외부 복구 볼륨 또는 컴퓨터에 복구 번들을 저장하려면 **다운로드**를 클릭한 뒤 **저장**을 클릭합니다.

   복구 파일 <machine_name.domain>.csv가 다운로드되었습니다.
7. 미리 만든 외부 복구 볼륨에서 대상 컴퓨터를 부팅합니다. 시스템 환경설정에서 시동 디스크 패널을 실행하고 복구 볼륨을 선택하거나 컴퓨터를 시작하는 동시에 **옵션** 키를 길게 누른 다음 부팅 전 Startup Manager에서 복구 볼륨을 선택하여 부팅 가능합니다.

   또는

   복구 대상 컴퓨터를 대상 디스크 모드로 부팅합니다. 시스템 환경설정에서 시동 디스크 패널을 실행하고 **대상 디스크 모드**를 클릭하거나 컴퓨터를 재시동하면서 **T** 키를 길게 눌러 부팅할 수 있습니다.

   노트:

   펌웨어 암호 보호를 설정하면 시동 시 T 키를 사용하여 대상 디스크 모드로 들어갈 수 없게 됩니다. 대상 디스크 모드에 대한 자세한 내용은 Apple의 http://support.apple.com/kb/HT1661을 참조하십시오.

   이제 하드웨어에 따라 FireWire 또는 Thunderbolt 케이블을 사용하여 복구 작업을 수행할 호스트 컴퓨터에 이 컴퓨터를 연결합니다.
8. Dell-Encryption-Enterprise-<version>.dmg를 마운트합니다.

   노트:

   복구 유틸리티는 복구 대상 컴퓨터에 설치된 클라이언트 소프트웨어와 동일하거나 좀 더 최신 버전이어야 합니다.
9. 복구가 필요한 볼륨 또는 드라이브를 선택하고 **계속**을 클릭합니다.

   드라이브를 선택하면 드라이브에 있는 모든 볼륨이 한 번에 복구됩니다.
10. 복구 번들(6단계에 저장)을 선택하고 **열기**를 클릭합니다.
11. **닫기**를 클릭합니다.

이제 찾기 창을 열어 일반적인 볼륨과 마찬가지로 암호화된 볼륨에 있는 데이터에 액세스할 수 있습니다. 볼륨 사이에서 파일이 전송될 때 모든 데이터는 투명하게 암호화 및 복호화됩니다.

FileVault 복구

관리되는 FileVault 암호화 볼륨의 복구는 Apple에서 결정하며 가능한 경우에는 이 절차가 자동으로 수행되지만, 몇 가지 추가적 단계가 필요합니다.

Dell Recovery 유틸리티는 볼륨 탑재, 또는 경우에 따라서는 볼륨 복호화를 보조하는 스크립트를 사용하여 Apple의 복구 도구 작업을 간소화합니다. FileVault 복구 기능은 Recovery HD와 페어링된 대상 파티션에 설치되어 있는 운영 체제에 의해 결정됩니다.

FileVault 암호화 볼륨은 Mac OS X 10.9.5 이상을 실행하는 모든 디스크 드라이브에 기록되는 Recovery HD 파티션에서만 복구 가능합니다. 이 요구 사항으로 인해 Dell Recovery 유틸리티에서 직접 복구 작업을 수행할 가능성이 사라집니다.

FileVault 복구 키가 개인 복구 키인지, 기관 복구 키인지에 따라 두 가지 복구 방법이 있습니다. 한 개의 유효한 복구 키는 항상 존재합니다. 개인 복구 키가 있는 경우 해당 키에 대한 가장 최근 항목을 사용하는 것이 좋습니다. 그 키가 작동하지 않으면 기관 복구 키 집합을 사용합니다.

- 개인 복구 키 - 기존 FileVault 암호화는 Dell Server에서 관리합니다. 복구 번들에 있는 가장 최신 항목에 RecoveryKey 항목이 포함된 경우 개인 복구 키 단계를 따르십시오. 다음은 RecoveryKey 예시입니다.

  ```
  RecoveryKey</key><string>C73W-CX2B-ANFY-HH3K-RLRE-LVAK</string>
  ```

- 복구 키체인(거의 사용되지 않음) - 이 복구 방법은 FileVault 기관 복구 키 사용에 기반합니다.

  복구 번들에 있는 가장 최신 항목에 KeychainKey 항목이 포함된 경우 복구 키체인 단계를 따르십시오. 다음은 KeychainKey 예시입니다.

  ```
  KeychainKey</key><data>a3ljaAABAAAAA...
  ```

개인 복구 키

일반적으로, 부팅 볼륨은 암호화된 다른 어떤 볼륨에도 마운트할 수 있으므로 비부팅 볼륨을 복구하기 전에 부팅 볼륨을 복구하는 것이 모범 사례입니다. 부팅 볼륨을 복구하면 대체로 비부팅 볼륨과 관련된 문제가 수정됩니다.

사전 요구 사항

- 부팅 가능한 외장 드라이브
- 복구 대상 컴퓨터의 디바이스 ID/고유 ID. 대부분의 경우, 복구 대상 컴퓨터는 Management Console에서 소유자의 사용자 이름을 검색하고 그 사용자를 위해 암호화된 디바이스를 보면 찾을 수 있습니다. 장치 ID/고유 ID의 형식은 "John Doe's MacBook.Z4291LK58RH"입니다.
- Dell 설치 미디어

Management Console - 복구 번들 저장

1. Management Console을 엽니다.
2. 왼쪽 창에서 **개체 > 엔드포인트**를 클릭합니다.
3. 복구할 장치를 검색합니다.
4. 엔드포인트 세부 정보 페이지를 열기 위해 디바이스 이름을 클릭합니다.
5. **세부 정보 및 작업** 탭을 클릭합니다.
6. *Shield 세부 정보*에서 **장치 복구 키** 링크를 클릭합니다.
7. 복구 작업을 수행하기 위해 복구 유틸리티를 실행할 외부 복구 볼륨 또는 컴퓨터에 복구 번들을 저장하려면 **다운로드**를 클릭한 뒤 **저장**을 클릭합니다.
8. 복구 번들의 위치를 입력하고 **저장**을 클릭합니다.

프로세스 - .dmg를 마운트합니다.

1. 복구 번들을 복사하고 **Dell-Encryption-Enterprise-<version>.dmg** 파일을 부팅 가능한 USB 드라이브에 복사합니다.
2. 컴퓨터를 재시작하는 동시에 **옵션** 키를 길게 누른 다음 부팅 전 Startup Manager에서 외부 전체 OS 설치 볼륨을 선택하여 사전에 생성된 외부 전체 OS 설치 볼륨에서 대상 컴퓨터를 부팅합니다. 부팅 가능한 볼륨을 생성하려면 https://support.apple.com/en-us/HT202796을 참조하십시오.
3. **Dell-Encryption-Enterprise-<version>.dmg**를 마운트합니다.

프로세스 - Dell 복구 유틸리티를 시작하고 FileVault 볼륨을 복구합니다.

1. Dell 설치 미디어에 있는 유틸리티 폴더에서 Dell 복구 유틸리티를 시작합니다.

   Dell 복구 유틸리티 > 볼륨 선택 대화 상자가 표시됩니다.

   노트:

복구 유틸리티는 복구 대상 컴퓨터에 설치된 클라이언트 소프트웨어와 동일하거나 좀 더 최신 버전이어야 합니다.

2. *Dell 복구 유틸리티* > *볼륨 선택*에서 FileVault 볼륨을 선택합니다.
   - 운영 체제를 복구할 경우 동일한 운영 체제 이상의 컴퓨터로 부팅하는 것이 가장 좋습니다.
   - 비부팅 볼륨이 암호화되어 있는 경우 일반적으로 부팅 파티션을 먼저 복구합니다.
3. **계속**을 클릭합니다.
4. 복구 번들(앞에서 저장함)을 찾아 선택한 다음 **열기**를 클릭합니다.
5. *복구 레코드 선택* 대화 상자가 열리면 *에스크로 날짜* 열에서 개인 복구 키 유형에 대한 가장 최근 날짜를 선택하고 **계속**을 클릭합니다.

   노트:

   이전의 에스크로 날짜에서는 키가 더 이상 유효하지 않을 수 있습니다.

   *복구 작업 결과*가 표시됩니다.
   - 부팅 드라이브의 경우, 복구 도구에서는 표준 Apple FileVault 복구를 사용하여 부팅하도록 허용하는 개인 복구 키가 제공됩니다. 대상 파티션으로 부팅하고 Pre-Boot-Authentication에 대해 개인 복구 키를 입력합니다(OS에 따라 달라질 수 있음).
   - 비부팅 드라이브의 경우 개인 복구 키만 표시됩니다. 볼륨을 잠금 해제하고 마운트하기 위해 잠금 해제 버튼이 제공됩니다.
6. 다음 중 하나를 수행합니다.
   - 부팅 볼륨 복구(가장 일반적인 경우)
   - 비부팅 볼륨 복구(거의 사용되지 않음)

부팅 볼륨 복구(가장 일반적인 경우)

대부분의 복구 사례에서 이 옵션을 사용하여 부팅 볼륨을 복구합니다.

1. 키를 받아 적거나 **복구 키 인쇄**를 클릭합니다.
2. **닫기**를 클릭합니다.
3. 필요에 따라 부팅 전 Startup Manager를 사용하여 복구하려는 볼륨을 부팅합니다.

   컴퓨터에 여러 사용자에 대한 아이콘이 표시되거나 암호를 요구합니다.
4. 해당하는 경우 사용자를 선택한 다음 **?**를 클릭합니다. 클릭합니다.
5. 이때 표시되는 화살표를 클릭합니다.
6. 복구 키를 입력하고 **Enter** 키를 누릅니다.
7. 대화 상자에서 해당 사용자에 대한 새 암호를 입력합니다.

비부팅 볼륨 복구 옵션(거의 사용되지 않음) - 다음 중 하나를 수행합니다.

비부팅 볼륨 복구

부팅 볼륨이 손상되거나 지워졌고 보조 볼륨이 존재하는 경우, 이러한 비부팅 볼륨을 마운트할 수 있습니다.

1. **잠금 해제**를 클릭합니다. 볼륨을 마운트합니다.
2. **닫기**를 클릭합니다.

볼륨 해독 - 이 단추 클릭

1. **해독**을 클릭합니다. 대화 상자와 진행 표시줄이 해독 프로세스를 나타냅니다.
2. 완료되면 **닫기**를 클릭합니다.
3. 해독한 볼륨으로 부팅해 사용합니다.

볼륨 해독 - 터미널에서 명령을 실행

1. *볼륨 해독* 영역의 명령어를 복사합니다.
2. **닫기**를 클릭합니다.
3. 터미널에 명령을 실행하십시오.

복구 키체인

암호화되지 않은 복구 볼륨으로 부팅되는 동안 Dell 복구 유틸리티를 실행해야 합니다.

사전 요구 사항

- 복구 유틸리티를 실행하는 외부 복구 볼륨 또는 컴퓨터
- USB 드라이브

- Firewire 케이블
- Dell 설치 미디어

Management Console - 복구 번들 저장

1. Management Console을 엽니다.
2. 왼쪽 창에서 **개체 > 엔드포인트**를 클릭합니다.
3. 복구할 장치를 검색합니다.
4. 엔드포인트 세부 정보 페이지를 열기 위해 디바이스 이름을 클릭합니다.
5. **세부 정보 및 작업** 탭을 클릭합니다.
6. *Shield 세부 정보*에서 **장치 복구 키** 링크를 클릭합니다.
7. 복구 작업을 수행하기 위해 복구 유틸리티를 실행할 외부 복구 볼륨 또는 컴퓨터에 복구 번들을 저장하려면 **다운로드**를 클릭한 뒤 **저장**을 클릭합니다.
8. 복구 번들의 위치를 입력하고 **저장**을 클릭합니다.

프로세스

1. 외장형 드라이브를 복구해야 할 시스템에 연결합니다.

   외장 드라이브에는 Mac OS 부팅 볼륨이 있어야 합니다.
2. **옵션** 키를 길게 눌러 외장 드라이브로 부팅하고 부팅 선택 도구를 사용하여 이 볼륨에서 선택하고 부팅합니다.
3. Management Console에서 복구 번들을 복사합니다.
4. .dmg 설치 파일을 마운트합니다.
5. 유틸리티 폴더에서 Dell 복구 유틸리티를 실행합니다.

   Dell 복구 유틸리티 > 볼륨 선택 대화 상자가 표시됩니다.
6. 복구할 FileVault 볼륨을 선택하고 **계속**을 클릭합니다.

   복구 번들 선택 대화 상자가 표시됩니다.
7. 복구 번들을 선택하고 **열기**를 클릭합니다.

   두 개 이상의 복구 키가 해당 디스크에 존재하면 *복구 레코드 선택* 화면이 표시됩니다.
8. 에스크로 날짜 열에서 키 집합 복구 유형에 대한 가장 최근 날짜를 선택하고 **계속**을 클릭합니다.

   노트:

   이전의 에스크로 날짜에서는 키가 더 이상 유효하지 않을 수 있습니다.

   FileVault 복구 지침 대화 상자가 표시됩니다.
9. 지침을 읽고 **계속**을 클릭합니다.

   복구 작업 확인 대화 상자가 표시됩니다.
10. 복구할 FileVault 볼륨을 강조 표시하고 **계속**을 클릭합니다.

    복구 파일을 저장할 위치를 선택하라는 *복구 파일 위치 선택* 대화 상자가 표시됩니다.

    스크립트에는 데이터 파일에 대한 절대 경로가 포함되어 있으므로 이 위치는 복구에 사용할 위치여야 합니다. 이러한 파일을 Recovery HD로 **복사하지 마십시오**.

    USB 드라이브와 같은 이동식 드라이브의 루트에 이런 파일을 저장하는 것이 좋습니다.

    노트:

    복구 키를 저장하는 데 사용하는 USB 또는 다른 디스크에 모든 사용자가 읽기/쓰기 액세스 권한이 있고 디스크에 적당한 공간이 있는지 확인하십시오. 선택한 디스크에 대한 권한이 없거나 디스크의 공간이 부족한 경우 복구 키가 저장되지 않았음을 나타내는 오류가 표시됩니다.
11. 위치를 선택하고 **저장**을 클릭합니다.

    파일이 생성되었음을 알리는 *복구 작업 결과* 대화 상자가 표시됩니다.
12. **닫기**를 클릭합니다.
13. Recovery HD 볼륨이 부팅된 후 스크립트의 이름과 경로를 입력합니다.

    노트:

볼륨의 루트 가까이에 파일을 저장하면 입력해야 할 경로가 단축됩니다.

복구 작업 결과에 키가 표시됩니다.

복구 유틸리티는 선택한 위치로 파일을 출력한 다음, FileVault 볼륨을 탑재하거나 암호 해독하기 위해 Recovery HD 볼륨에서 실행할 필요가 있는 정확한 명령을 표시합니다.

14. 이런 파일이 생성된 후 마지막 *복구 작업 결과* 대화 상자에 표시되는 명령 문자열을 복사합니다.
15. 다음 중 한 가지 방법으로 Recovery HD를 다시 부팅합니다.
    - POST(Power-On/Self-Test) 벨소리가 나기 전에, 또한 컴퓨터 부팅 중에 **Command+R** 키를 동시에 길게 누릅니다.

      또는
    - 이전 버전의 Apple의 경우 **옵션** 키를 누르고 부팅 선택 도구를 사용하여 Recovery HD를 선택합니다.

      Mac OS X 유틸리티 대화 상자가 표시됩니다.
16. 도구 메뉴에서 **유틸리티 > 터미널**을 선택합니다.
17. 볼륨을 마운트하여 터미널에서 파일을 복사하거나 Disk Utility: In Terminal에서 디스크 이미지를 만들려면 전체 경로와 스크립트 이름 **fv2mount.sh**를 입력합니다. 예:

    /Volumes/recoveryFOB/fv2mount.sh
18. 컴퓨터를 재부팅합니다.

이동식 미디어

지원되는 형식

MBR(Master Boot Record) 또는 GPT(GUID Partition Table) 파티션 구성표로 FAT32, exFAT 또는 HFS Plus(Mac OS Extended) 형식의 미디어가 지원됩니다. HFS Plus를 활성화해야 합니다.

노트:

Mac에서는 현재 Encryption External Media에 대한 CD/DVD 기록을 지원하지 않습니다. 그러나 *EMS에서 Shield로 보호할 수 없는 미디어에 대한 액세스 차단* 정책이 선택되어 있더라도 CD/DVD 드라이브에 대한 액세스는 차단되지 않습니다.

HFS Plus 활성화

HFS Plus를 활성화하려면 .plist 파일에 다음을 추가합니다.

<key>EMSHFSPlusOptIn</key>

<true/>

노트:

프로덕션 환경에 처음 시도하기 전에 이 구성을 테스트하는 것이 좋습니다.

HFS Plus는 다음과 같은 항목을 지원하지 않습니다.

- 버전 관리 - 기존의 버전 관리 데이터가 디스크에서 제거됩니다.
- 하드 링크 - 이동식 미디어의 암호화 삭제 중에 파일이 암호화되지 않습니다. 대화 상자에 미디어를 꺼내라는 메시지가 표시됩니다.
- 미디어에는 타임 머신 백업이 포함됩니다.
  - 컴퓨터에서 타임 머신 백업 대상으로 인식되어 사용되는 미디어는 자동으로 허용 목록에 추가되므로 백업을 계속할 수 있습니다.
  - 타임 머신 백업이 설치된 다른 모든 이동식 미디어는 프로비저닝되지 않은 미디어와 보호되지 않는 미디어를 다루는 정책을 기반으로 합니다. *EMS에서 Shield로 보호할 수 없는 미디어에 액세스* 및 *EMS에서 Shield로 보호할 수 없는 미디어에 대한 액세스 차단* 정책을 참조하십시오.

    노트:

    아직 백업이 없는 새 드라이브의 경우, 사용자가 허용 목록 규칙을 복사하여 귀하에게 전송하면 허용 목록에 타임 머신 드라이브를 지정할 수 있습니다. 허용 목록 규칙 복사를 참조하십시오.

Encryption External Media 및 정책 업데이트

이동식 미디어가 프로비저닝되거나 복구된 시스템에서 탑재 시 정책이 이동식 미디어로 업데이트됩니다.

암호화 예외

확장된 특성은 이동식 미디어에서 암호화되지 않습니다.

이동식 미디어 탭의 오류

- Shield로 보호되지 않는 컴퓨터에서는 암호화된 파일을 복호화된 파일 버전으로 바꾸지 마십시오. 이럴 경우 나중에 복호화를 수행하지 못할 수 있습니다. 또한, 이는 이동식 미디어 탭에서 오류로 표시될 수 있습니다.
- 예를 들어 Encryption External Media의 제어 범위를 벗어나는 새 콘텐츠로 파일을 덮어쓴 다음 Encryption External Media에 탑재하는 것과 같이 EOF(end-of-file) 마커가 무효화되는 경우, 이동식 미디어 탭에 EOF 오류가 표시됩니다.
- 파일을 변환할 때 미디어에는 변환할 가장 큰 파일의 크기보다 많은 여유 공간이 있어야 합니다. 이동식 미디어 상태 영역에 노란색 경고 삼각형이 표시되면 이 삼각형을 클릭하십시오. 메시지에 *공간이 부족*하다고 표시되면 다음을 수행하십시오.
  1. 장치에서 확보해야 하는 공간의 양을 기록합니다. 보고서에 파일 목록과 크기가 표시됩니다.
  2. 휴지통을 비웁니다. 공간을 확보하면 Encryption External Media가 추가 파일을 자동으로 암호화합니다.
  3. 파일이나 폴더를 삭제할 경우 휴지통을 다시 비워야 합니다.

감사 메시지

감사 메시지가 Dell Server로 전송됩니다.

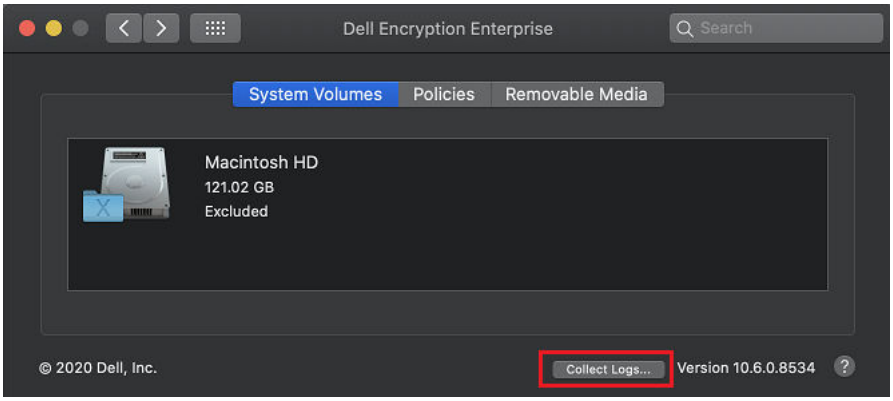
Endpoint Security Suite Enterprise for Mac에서 감사 메시지를 보려면 다음과 같이 하십시오.

1. Dell 관리자 계정으로 Management Console에 로그인합니다.
2. 왼쪽 창에서 **채우기 > 엔터프라이즈 또는 엔드포인트**를 클릭합니다.
3. **고급 위협 이벤트** 탭을 선택합니다.

자세한 내용은 *관리자 도움말*을 참조하십시오.

Endpoint Security Suite Enterprise에 대한 로그 파일 수집

시스템 환경 설정 > *Dell Encryption Enterprise* > *시스템 볼륨*에서 오른쪽 하단에 있는 *로그 수집* 버튼을 사용하면 관리자가 지원을 위해 로그를 미리 생성할 수 있습니다. 이 작업은 로그를 수집하는 동안 성능에 영향을 미칠 수 있습니다.



DellLogs.zip에는 Mac Encryption Enterprise 및 Advanced Threat Prevention에 대한 로그가 포함되어 있습니다. 로그를 수집하는 방법에 대한 자세한 내용은 http://www.dell.com/support/article/us/en/19/SLN303924을 참조하십시오.

Encryption 클라이언트 for Mac 제거

Dell Encryption Enterprise 제거 애플리케이션을 실행하여 클라이언트 소프트웨어를 제거할 수 있습니다. 클라이언트 소프트웨어를 설치 제거하려면 아래 단계를 따르십시오.

노트:

설치 제거 애플리케이션을 실행하기 전에 디스크가 완전히 복호화되어 있어야 합니다.

1. 디스크가 현재 암호화된 경우, Management Console에서 컴퓨터의 *Dell 볼륨 암호화* 정책을 **중지**하고 정책을 커밋합니다.

   시스템 환경설정에 액세스하여 클라이언트 소프트웨어가 디스크를 복호화할 수 있도록 컴퓨터를 제어할 것을 요구하는 대화 상자가 표시됩니다.

   a. **시스템 환경설정 열기**를 클릭합니다.

      거부를 선택하는 경우 제거 및 암호 해독 작업을 계속 진행할 수 없습니다.

   b. 관리자 암호를 입력합니다.
2. 디스크가 완전히 복호화된 후 (메시지가 표시되면) 컴퓨터를 다시 시작합니다.
3. 컴퓨터가 다시 시작되면 **Dell Encryption Enterprise 제거** 애플리케이션(Dell 설치 미디어의 Dell-Encryption-Enterprise-<version>.dmg에 있는 유틸리티 폴더에 있음)을 실행합니다.

   설치 제거 상태를 보여주는 메시지가 표시됩니다.

   이제 Encryption 클라이언트 for Mac이 제거되어 컴퓨터를 정상적으로 사용할 수 있습니다.

관리자로서 활성화

클라이언트 도구는 Mac 컴퓨터에서 클라이언트 소프트웨어를 활성화하고 클라이언트 소프트웨어를 검사하기 위한 새로운 방법을 관리자에게 제공합니다. 다음 두 가지 활성화 방법을 사용할 수 있습니다.

- 관리자 자격 증명을 사용하여 활성화
- 해당 컴퓨터에 아무런 영향을 미치지 않고 사용자를 에뮬레이트하는 임시 활성화.

두 가지 방법 모두 직접 셸을 통해 사용하거나 스크립트에서 사용할 수 있습니다.

노트:

같은 네트워크 계정으로 5대보다 많은 컴퓨터에서 클라이언트 소프트웨어를 활성화하지 마십시오. Dell Server로 인해 심각한 보안 취약성과 성능 저하가 발생할 수 있습니다.

사전 요구 사항

- Encryption client for Mac을 원격 컴퓨터에 설치해야 합니다.
- 원격 위치에서 활성화를 시도하기 전에 클라이언트 사용자 인터페이스를 통해 활성화하지 마십시오.

활성화

이 명령을 사용하여 관리자로서 클라이언트를 활성화합니다.

예:

client -a *username@domain.com password admin admin*

임시로 활성화

컴퓨터에 아무런 영향을 미치지 않고 클라이언트를 활성화하려면 이 명령을 사용합니다.

1. 셸을 열거나 스크립트를 사용하여 클라이언트 소프트웨어를 활성화합니다.

   client *-at username@domain.com password*

2. 클라이언트 도구를 사용하여 클라이언트 소프트웨어, 정책, 디스크 상태, 사용자 계정 등에 대한 정보를 검색합니다. 클라이언트 도구에 대한 자세한 내용은 클라이언트 도구를 참조하십시오.

노트:

활성화 후, 정책, 디스크 상태 및 사용자 정보를 포함한 클라이언트 소프트웨어에 대한 정보는 Dell Encryption Enterprise 환경 설정의 시스템 환경설정에서도 확인할 수 있습니다.

Encryption 클라이언트 참조

선택적 펌웨어 암호 보호 정보

노트:

최신 Mac 컴퓨터에서는 펌웨어 암호 보호 기능을 지원하지 않습니다. 펌웨어 암호 보호는 다음 모델에 지원됩니다.

- iMac10.*
- iMac11.*
- Macmini4.*
- MacBook7.*
- MacBookAir2.*
- MacBookPro7.*
- MacPro5.*
- XServe3.*

예를 들어 iMac10.1, iMac11.1 및 iMac11.2에서는 선택적 펌웨어 암호 보호(*로 표시됨)가 지원되지만 iMac12.1 이상에서는 지원되지 않습니다.

노트:

FirmwarePasswordMode 키 옵션이 선택 사항으로 설정되면 클라이언트에서 펌웨어 암호 보호 적용만 비활성화합니다. 기존의 펌웨어 암호 보호는 제거되지 **않습니다**. Mac OS X Firmware Password Utility를 사용하여 기존 펌웨어 암호를 제거할 수 있습니다.

암호화된 Mac 컴퓨터에 Boot Camp(Mac OS X Boot Camp 활성화 방법에서 지침 참조)를 사용하려는 경우 클라이언트에서 펌웨어 암호 보호를 **사용하지 않도록** 구성해야 합니다.

Mac 컴퓨터에서는 펌웨어 암호 보호를 사용하여 컴퓨터의 액세스 보안을 강화합니다. Mac 컴퓨터에서는 기본적으로 보호 기능이 *꺼짐* 상태입니다. 새로운 설치이든 또는 이전 클라이언트 버전에서 업그레이드를 하든지 간에 클라이언트 설치 중에 기존의 com.dell.ddp.plist 파일을 편집하여 *FirmwarePasswordMode* 키를 *필수* 또는 *선택 사항*으로 설정할 수 있습니다. *필수* 옵션은 펌웨어 암호 보호 기능을 적용하는 기본 설정이며, *선택 사항* 설정은 펌웨어 암호가 적용되지 않도록 합니다. 설치 또는 업그레이드 후에 클라이언트는 재시작 중에 수정된 설치 프로그램 com.dell.ddp.plist 파일을 평가합니다.

노트:

사용자가 컴퓨터의 보안 포스처를 변경하지 못하게 하기 위해, 클라이언트는 클라이언트 소프트웨어 설치 후 FirmwarePasswordMode 키에 대한 변경을 허용하지 않습니다.

디스크 복호화 프로세스를 시작한 다음에 암호화를 다시 활성화하여 설치 또는 업그레이드 후 이 키의 값을 변경할 수 있습니다.

Mac OS X 펌웨어 암호 보호가 **필수**인 경우, Encryption Client for Mac 설치/업그레이드에 설명된 일반적인 클라이언트 설치/업그레이드 절차를 따르십시오.

Boot Camp 사용

Mac OS X Boot Camp 지원

노트:

Boot Camp를 사용할 때 Dell Encryption Enterprise는 Windows 운영 체제를 암호화하지 않습니다. 또한 디바이스에 부팅 가능한 macOS 파티션이 두 개 이상 있는 경우 Encryption Enterprise는 기본 볼륨만 암호화합니다.

Boot Camp는 이중 부팅 구성의 Mac 컴퓨터에 Windows를 설치하는 데 보조적 역할을 하는 Mac OS X와 함께 포함된 유틸리티입니다. Boot Camp는 다음과 같은 Windows 체제에서 지원됩니다.

- Windows 7 및 7 Home Premium, Professional, Ultimate(64비트)
- Windows 8.1 및 8.1 Pro(64비트)

노트:

Windows 7에서는 Boot Camp 4 또는 5.1이 지원됩니다. Windows 8.1 이상에서는 Boot Camp 5.1만 지원됩니다.

Mac용 Endpoint Security Suite Enterprise가 설치된 컴퓨터의 Boot Camp에서 Windows용 Endpoint Security Suite Enterprise를 사용하려면 FileVault2가 설치된 암호화 클라이언트를 통해 시스템 볼륨을 암호화해야 합니다. 명령줄 설치/업그레이드에서 지침을 확인하십시오.

노트:

Windows 파티션이 Encryption External Media 후보인 경우 허용 목록에 등록해야 합니다. 그렇지 않으면 암호화됩니다. 허용 목록 규칙 복사를 참조하십시오.

노트:

Windows가 설치되어 있는지 확인한 후에 암호화를 활성화하는 클라이언트 정책을 배포해야 합니다. 클라이언트가 암호화 프로세스를 시작한 후에는 Boot Camp에서 요구되는 디스크 파티션 작업을 허용하지 않습니다.

Boot Camp에서 Windows용 Endpoint Security Suite Enterprise 복구

Boot Camp 볼륨을 실행 중인 Windows용 Endpoint Security Suite Enterprise를 복구하려면 외장 드라이브에도 Boot Camp 볼륨을 만들어야 합니다.

사전 요구 사항

- 부팅 가능한 외장 드라이브
- 복구 대상 컴퓨터의 디바이스 ID/고유 ID. 대부분의 경우, 복구 대상 컴퓨터는 Management Console에서 소유자의 사용자 이름을 검색하고 그 사용자를 위해 암호화된 디바이스를 보면 찾을 수 있습니다. 장치 ID/고유 ID의 형식은 "John Doe's MacBook.Z4291LK58RH"입니다.

프로세스

1. 외장 드라이브에서 Boot Camp 볼륨을 생성합니다.

   단계는 로컬 시스템에 Boot Camp 볼륨을 만드는 단계와 비슷합니다. http://www.apple.com/support/bootcamp/ 페이지를 참조하십시오.

2. Management Console에서 복구 번들을 다음 중 하나에 복사합니다.
   - 부팅 가능한 USB 드라이브

     또는

   - 외부 Boot Camp 볼륨의 FAT 파티션
3. 복구할 Boot Camp 볼륨과 함께 컴퓨터를 시스템 종료합니다.
4. 외장 드라이브를 컴퓨터에 연결합니다.

   이 드라이브에는 1단계에서 생성된 Boot Camp 볼륨이 포함되어 있습니다.

5. 외장 Boot Camp 드라이브에서 컴퓨터를 부팅하려면 컴퓨터 전원을 켜는 동안 다음 중 하나를 수행합니다.
   - POST(Power-On/Self-Test) 벨소리가 나기 전에, 또한 컴퓨터 부팅 중에 **Command+R** 키를 동시에 길게 누릅니다.

     또는

   - 이전 버전의 Apple의 경우 컴퓨터 전원을 켜는 동안 **옵션** 키를 누릅니다.

     Mac OS X 유틸리티 대화 상자가 표시됩니다.
6. 외장 드라이브에 있는 Boot Camp 볼륨(Windows)을 선택합니다.
7. USB 드라이브 또는 FAT 파티션에서(2단계에서 제공)를 복구 번들을 마우스 오른쪽 단추로 클릭하고 **관리자로 실행**을 선택합니다.
8. **예**를 클릭합니다.
9. Dell Encryption Enterprise 대화 상자에서 다음 중 한 옵션을 선택합니다.
   - *시스템 부팅 실패* - 사용자가 시스템으로 부팅할 수 없는 경우 첫 번째 옵션을 선택합니다.

또는

- *시스템에서 암호화된 데이터 액세스를 허용하지 않습니다.* - 사용자가 시스템에 로그인할 때 암호화된 일부 파일에 액세스할 수 없는 경우 두 번째 옵션을 선택합니다.두 번째 옵션을 선택합니다.

10. **다음**을 클릭합니다.

    백업 및 복구 정보 화면이 표시됩니다.

11. **다음**을 클릭합니다.
12. 복구할 Boot Camp 볼륨을 선택합니다.

    노트:

    이것은 외장 Boot Camp 볼륨이 **아닙니다.**

13. **다음**을 클릭합니다.
14. 이 파일과 연결된 암호를 입력합니다.
15. **다음**을 클릭합니다.
16. **복구**를 클릭합니다.
17. **마침**을 클릭합니다.
18. 다시 부팅하라는 메시지가 표시되면 **예**를 클릭합니다.
19. 시스템이 다시 부팅되고 Windows에 로그인할 수 있습니다.

펌웨어 암호 검색 방법

클라이언트 컴퓨터가 펌웨어 암호를 강제 적용하도록 구성되어 있더라도, 복구를 위해 꼭 필요하지 않을 수도 있습니다. 복구할 컴퓨터를 부팅할 수 있는 경우 시동 디스크 시스템 환경설정 창에서 부팅 대상을 설정합니다.

복구를 위해 펌웨어 암호가 필요한 경우(컴퓨터를 부팅할 수 없고 펌웨어 암호 보호가 적용되는 경우) 아래 단계를 따르십시오.

펌웨어 암호를 검색하려면 먼저 디스크의 암호화 키를 포함한 복구 번들을 검색해야 합니다.

1. Dell 관리자 계정으로 Management Console에 로그인합니다.
2. 왼쪽 창에서 **개체 > 엔드포인트**를 클릭합니다.
3. 복구할 장치를 검색합니다.
4. 엔드포인트 세부 정보 페이지를 열기 위해 장치 이름을 클릭합니다.
5. **세부 정보 및 작업** 탭을 클릭합니다.
6. *Shield 세부 정보*에서 **장치 복구 키** 링크를 클릭합니다.
7. 복구 작업을 수행하기 위해 복구 유틸리티를 실행할 외부 복구 볼륨 또는 컴퓨터에 복구 번들을 저장하려면 **다운로드**와 **저장**을 차례대로 클릭합니다.
8. 복구 번들을 열어 복구 대상 컴퓨터에 대한 펌웨어 암호를 검색합니다. 펌웨어 암호는 **FirmwarePassword** 키 뒤의 문자열 태그 내에 위치합니다.

   예:

   <key>FirmwarePassword</key>

   <string>Bo$vun8WDn</string>

클라이언트 도구

클라이언트 도구는 Mac 엔드포인트에서 실행되는 셸 명령입니다. 이 도구는 원격 위치에서 클라이언트를 활성화하거나 원격 관리 유틸리티를 통해 스크립트를 실행하는 데 사용됩니다. 관리자로서 클라이언트를 활성화하고 다음을 수행할 수 있습니다.

- 관리자로서 활성화
- 임시로 활성화
- Mac 클라이언트에서 정보 검색

클라이언트 도구를 수동으로 사용하려면 ssh 세션을 열고 명령줄에 필요한 명령을 입력합니다.

예:

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

client만 입력하면 사용 지침이 표시됩니다.

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/client

표 1. 클라이언트 도구 명령

명령	용도	구문	결과
활성화	사용자 인터페이스를 통하지 않고 Dell Server를 통해 Mac 클라이언트를 활성화합니다. 활성화하려면, 유효한 도메인 사용자 이름과 암호가 입력되어야 합니다. 클라이언트 도구를 통해 로그인된 사용자와 다른 로컬 사용자를 활성화할 수 있으며 해당 사용자와 도메인 자격 증명을 연결할 수 있습니다.	-a domainAccount domainPassword -a localAccount* domainAccount domainPassword **domainAccount**는 클라이언트 도구를 통해 활성화하는 데 사용되는 계정입니다. **localAccount**는 선택 사양이며 지정된 사용자가 없을 때 현재 사용자가 됩니다. 활성화 명령은 다음 형식을 사용합니다. client -a <user to activate*> <domainUser> <domainPassword> *인증 사용자 목록 없음* 정책을 사용하여 Dell Server에 활성화되지 않는 사용자 그룹을 생성하려면 선택적으로 클라이언트 도구를 사용하여 로그인한 계정이 아닌 다른 로컬 계정을 지정할 수 있습니다. 3단계의 인증 사용자 목록 없음 정책을 참조하십시오.	0 = 성공 2 = 활성화 실패함, 실패 이유 6 = 사용자를 찾을 수 없음
임시로 활성화	아무런 영향을 미치지 않고 Mac 클라이언트를 활성화합니다.	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
디스크	디스크 상태 요청	-d	디스크 ID, 암호화 상태 및 정책을 포함한 디스크 상태 표시 빈 중괄호가 반환되면 암호화된 디스크가 없다는 뜻입니다.
FileVault 변경 복구	FileVault 볼륨에 대한 주기 복구 키	-fc deviceId recoveryPassphrase -fc deviceId personalRecoveryKey -fc deviceId pathToKeychain keychainPassword -fc deviceId recoveryFile **노트:** deviceId는 논리 볼륨 UUID이거나 정확히 한 개의 LVUUID로 확인되어야 합니다. 종종 탑재 지점 또는 devnode가 효과가 있을 것입니다.	0 = 성공 7= LVUUID를 찾을 수 없음 10 = 자격 증명 실패 11 = 에스크로 실패
정책	Mac 클라이언트의 정책 요청	-p	정책 표시
서버	Mac 클라이언트를 대신하여 업데이트된 정책에 대해 Dell Server 폴링 **노트:** 폴링을 완료하는 데 몇 분 정도 걸릴 수 있습니다.	-s	0 = 성공 다른 값은 Dell Server 또는 Mac 클라이언트 소프트웨어가 사용 중이었거나 응답하지 않음을 나타내는 것입니다.

표 1. 클라이언트 도구 명령 (계속)

명령	용도	구문	결과
테스트	Mac 클라이언트의 활성화 상태 테스트	-t localAccount*	0 (domainAccount) = 성공 1 = 활성화되지 않음 6 = 사용자를 찾을 수 없음
사용자	사용자 정보 요청	-u localAccount*	사용자의 계정 정보에 다음 내용이 표시됩니다. 0 (account information) = 성공 6 = 사용자를 찾을 수 없음
버전	Mac 클라이언트의 버전 요청	-v	Mac 클라이언트의 버전이 표시됩니다(예: 8.x.x.xxxx).

* 다른 계정이 지정되지 않으면 클라이언트 도구를 사용하는 계정이 localAccount에 사용됩니다.

Plist 옵션

-plist 옵션을 선택하면 함께 결합되는 명령의 결과가 인쇄됩니다. 이 옵션은 해당 명령 다음에 나오며 결과가 plist로 인쇄되도록 하려면 인수 앞에 나타나야 합니다.

예

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -p -plist**

클라이언트에서 정책을 검색하여 인쇄합니다.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at -plist** *localAccount domainAccount domainPassword*

일시적으로 클라이언트를 활성화하고 결과를 인쇄합니다.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -s ; echo$?**

클라이언트를 대신하여 업데이트된 정책에 대해 Dell Server를 폴링하고 화면상에 표시합니다.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -d -plist**

클라이언트의 디스크 상태를 검색하고 인쇄합니다.

전역 반환 코드

오류 없음 0

매개변수 오류 4

인식되지 않는 명령 5

소켓 시간 초과 8

내부 오류 9

4

작업

주제:

Mac용 Advanced Threat Prevention 설치

이 섹션에서는 Advanced Threat Prevention 설치 프로세스를 안내합니다.

Advanced Threat Prevention를 설치하는 방법은 두 가지가 있습니다.

- 대화형 설치 - 이 방법이 설치하기에 가장 간단합니다. 하지만 이 방법에서는 어떤 사용자 지정도 허용되지 않습니다.
- 명령줄 설치 - 이것은 고급 설치/업그레이드 방법으로 명령줄 구문에 숙련된 관리자만 사용해야 합니다.

사전 요구 사항

클라이언트 소프트웨어 배포 중에는 IT 모범 사례를 따르는 것이 좋습니다. 예를 들어, 초기 테스트에서 테스트 환경을 통제하고 사용자에 대해 시간별 배포를 수행해야 합니다.

시작하기 전에, 다음과 같은 사전 요구 사항이 충족되어 있는지 확인하십시오.

- Dell Server 및 해당 구성 요소가 이미 설치되어 있는지 확인합니다.

  Dell Server를 아직 설치하지 않은 경우, 아래의 해당 가이드에서 지침을 따릅니다.

  Security Management Server Installation and Migration Guide(Security Management Server 설치 및 마이그레이션 가이드)

  Security Management Server Virtual Quick Start Guide and Installation Guide(Security Management Server Virtual 퀵 스타트 가이드 및 설치 가이드)

- Dell Server 호스트 이름과 포트가 있는지 확인합니다. 클라이언트 소프트웨어 설치를 위해서는 두 가지 모두 필요합니다.
- 대상 컴퓨터가 Dell Server와 네트워크로 연결되어 있어야 합니다.
- 클라이언트의 서버 인증서가 누락되었거나 자체 서명된 경우, 클라이언트 측면에 있는 SSL 인증서만 비활성화해야 합니다.

Advanced Threat Prevention를 위한 대화식 설치

이 섹션에서는 Mac용 고급 위협 방지 설치 프로세스를 안내합니다.

대화형 설치는 클라이언트 소프트웨어 패키지를 설치하거나 업그레이드하는 가장 쉬운 방법입니다. 하지만 이 방법에서는 어떤 사용자 지정도 허용되지 않습니다.

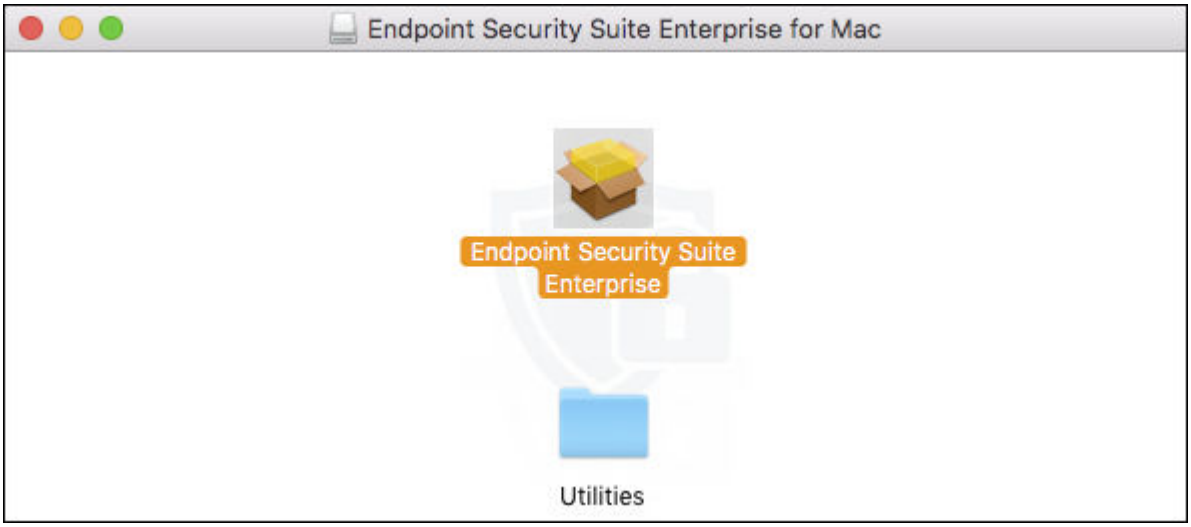
클라이언트 소프트웨어를 설치하려면 아래 단계를 따르십시오. 이런 단계를 수행하려면 관리자 계정이 있어야 합니다.

노트:

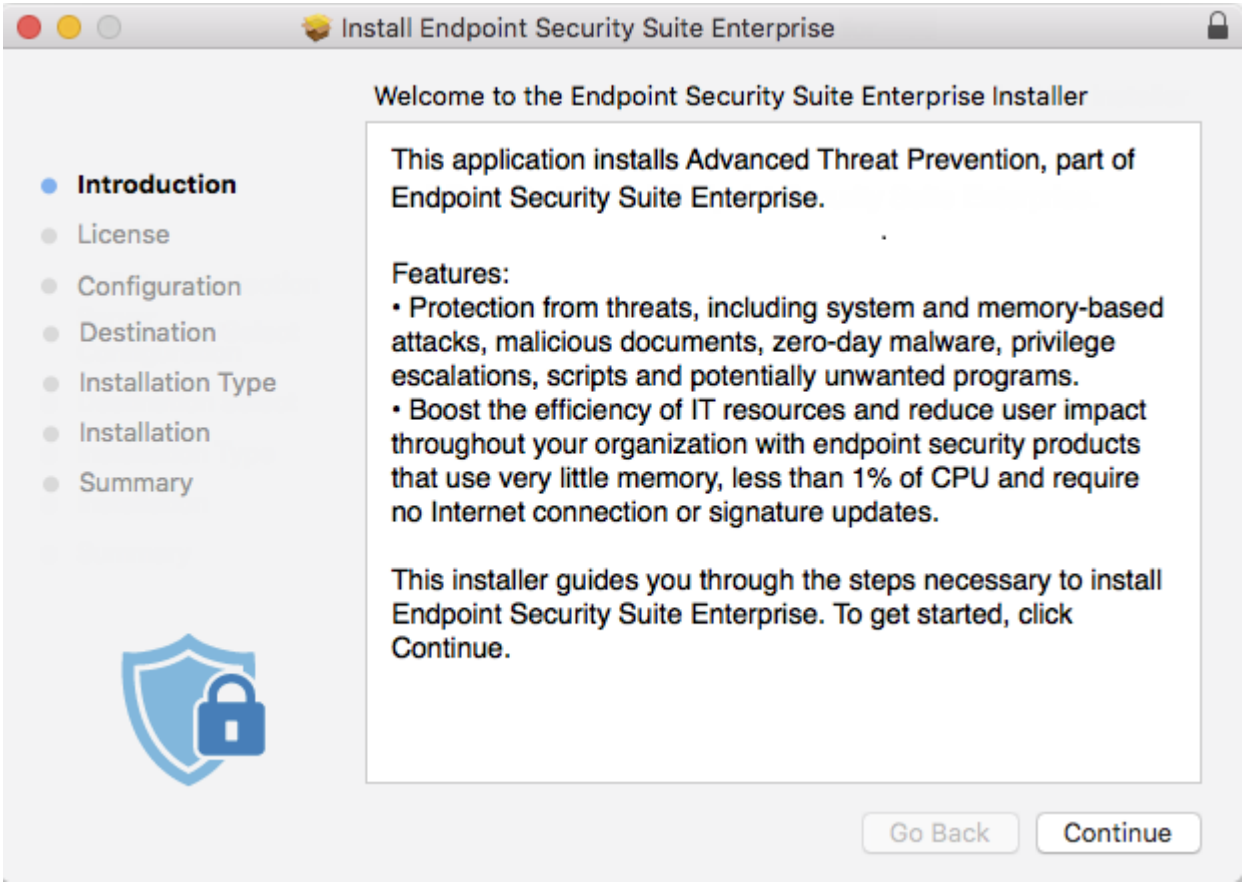
시작하기 전에, 사용자의 작업을 저장하고 다른 응용 프로그램을 닫으십시오.

1. Dell 설치 미디어에서 **Endpoint-Security-Suite-Enterprise-<version>.dmg** 파일을 마운트합니다.

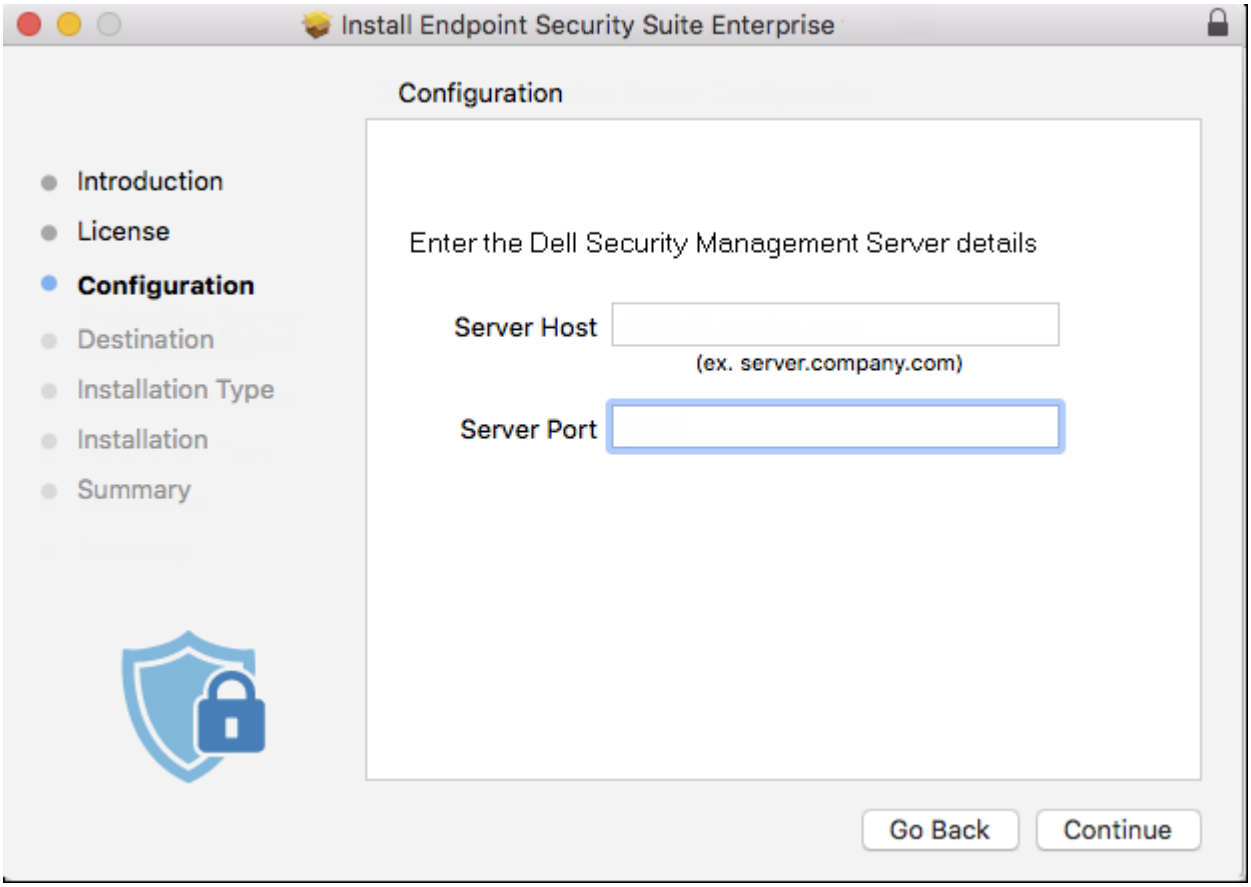
   Mac용 Endpoint Security Suite Enterprise 패키지가 열립니다.



2. **Endpoint Security Suite Enterprise** 패키지 설치 프로그램을 두 번 클릭합니다. 다음과 같은 메시지가 표시됩니다.
   이 패키지는 소프트웨어를 설치할 수 있는지 결정하기 위한 프로그램을 실행합니다.
3. **계속**을 클릭합니다.
4. 시작 텍스트를 읽고 **계속**을 클릭합니다.



5. 라이센스 계약을 검토하고 **계속**을 클릭한 뒤 **동의**를 클릭하여 라이센스 계약의 조건을 수락합니다.
6. *서버 호스트* 필드에 대상 사용자를 관리할 Dell Server의 정규화된 호스트 이름(예: server.organization.com)을 입력합니다.



7. *서버 포트* 필드에 **8888**을 입력하고 **계속**을 클릭합니다.
   연결이 설정되면 연결 표시등이 빨간색에서 녹색으로 바뀝니다.
   노트:
   포트는 Core 서버 서비스 포트이며 구성 가능합니다. 기본 포트 번호는 8888입니다.
8. 설치 화면에서 **설치**를 클릭합니다.
9. 메시지가 표시되면 (Mac OS X Installer 응용 프로그램에서 요구하는) 관리자 계정 자격 증명을 입력한 후 **소프트웨어 설치**를 클릭합니다.
10. 설치가 완료되면 **닫기**를 클릭합니다.
    Mac용 Advanced Threat Prevention 클라이언트가 설치되어 있습니다.
11. 패키지를 닫습니다.
12. 고급 위협 방지 설치 확인을 참조하십시오.

시스템이 Dell Server에 등록되어 있지 않은 경우 로그를 참조하여 Dell Server에 유효한 인증서가 있는지 확인하십시오. 고급 위협 방지를 위한 SSL 인증서 비활성화를 참조하십시오.

Advanced Threat Prevention 클라이언트의 대화형 제거

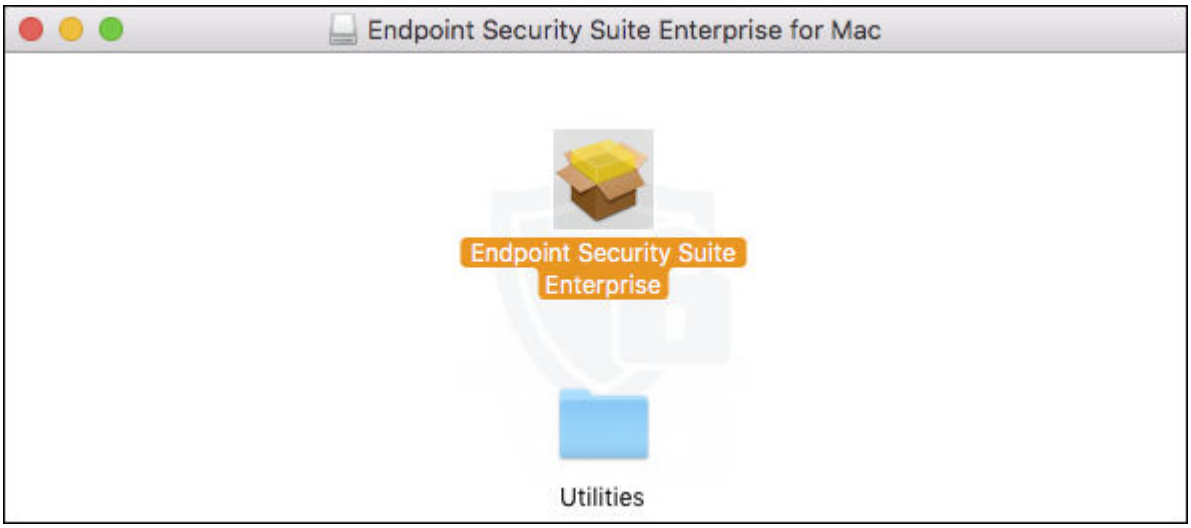
Endpoint Security Suite Enterprise제거 응용 프로그램을 실행하여 클라이언트 소프트웨어를 제거할 수 있습니다. 클라이언트 소프트웨어를 설치 제거하려면 아래 단계를 따르십시오.

1. Endpoint-Security-Suite-Enterprise-<version>.dmg 파일을 마운트합니다.
2. 유틸리티 폴더에서 **Endpoint Security Suite Enterprise 제거** 응용 프로그램을 실행합니다.
3. **제거를 클릭합니다**.
4. 메시지가 표시되면 (Mac OS X Installer 응용 프로그램에서 요구하는) 관리자 계정 자격 증명을 입력한 후 **확인**을 클릭합니다.
   설치 제거 상태를 보여주는 메시지가 표시됩니다.
5. 성공 확인 창에서 **확인**을 클릭합니다.
   이제 Mac용 Advanced Threat Prevention가 제거되어 컴퓨터를 정상적으로 사용할 수 있습니다.

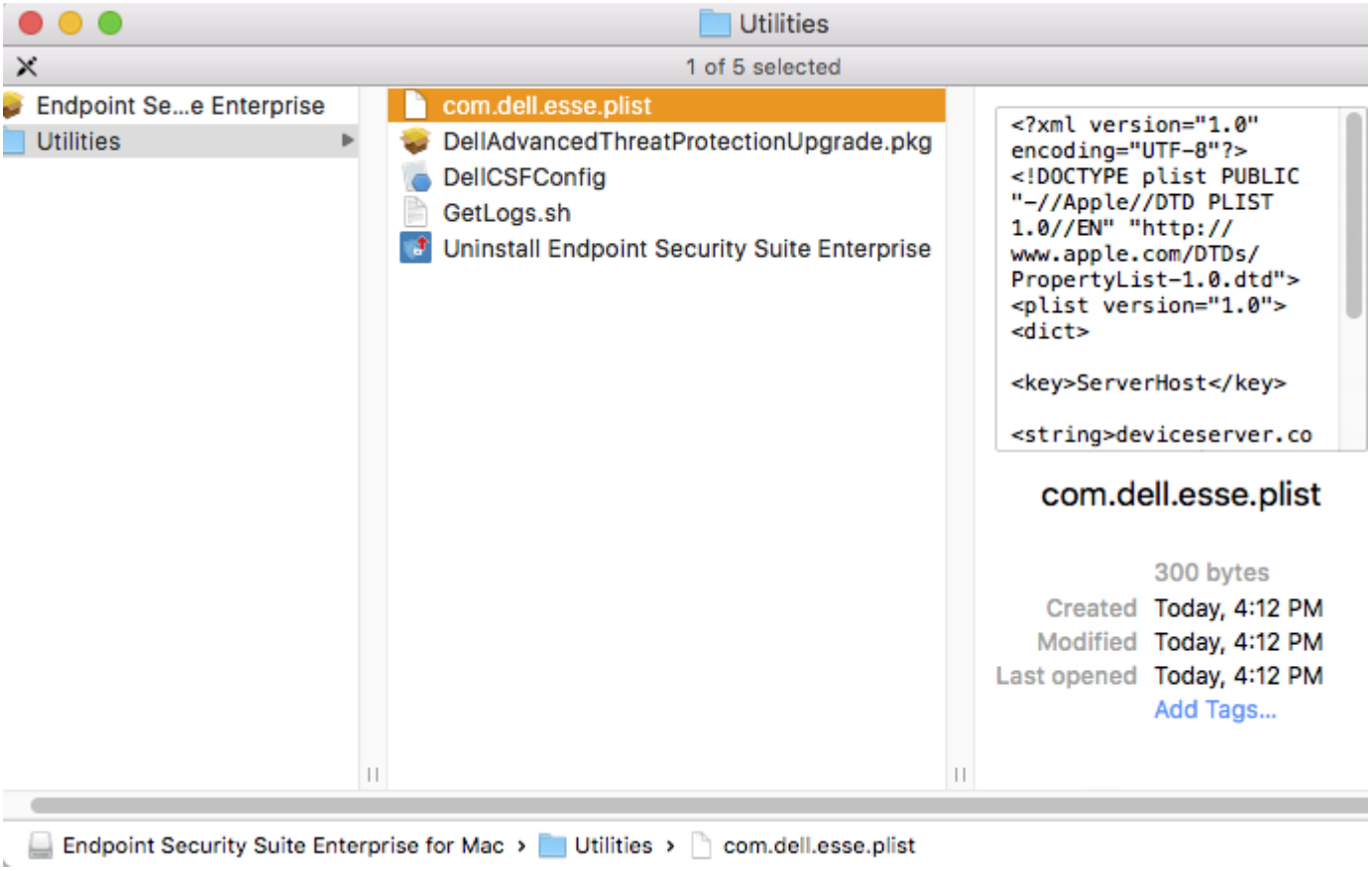
Advanced Threat Prevention를 위한 명령줄 설치

명령줄을 사용하여 Advanced Threat Prevention 클라이언트를 설치하려면 아래 단계를 따르십시오.

1. Dell 설치 미디어에서 Endpoint-Security-Suite-Enterprise-<version>.dmg 파일을 마운트합니다. Mac용 Endpoint Security Suite Enterprise 패키지가 열립니다.



2. 유틸리티 폴더에서 **com.dell.esse.plist** 파일을 로컬 드라이브에 복사합니다.



3. .plist 파일을 엽니다.
4. Dell Server의 정규화된 호스트 이름에서 자리 표시자 값을 편집하여 server.organization.com 및 포트 번호 **8888**과 같은 대상 사용자를 관리합니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
```

```
<plist version="1.0">
<dict>
  <key>ServerHost</key>
  <string>server.organization.com</string>
  <key>ServerPort</key>
  <string>8888</string>
  <array>
</dict>
</plist>
```

노트:

포트는 Core 서버 서비스 포트이며 구성 가능합니다. 기본 포트 번호는 8888입니다.

5. 파일을 저장하고 닫습니다.
6. 각 대상 컴퓨터에서 **Mac용 Endpoint Security Suite Enterprise** 패키지 설치 프로그램을 임시 폴더에 복사하고 수정된 **com.dell.esse.plist** 파일을 **/Library/Preferences**에 복사합니다.
7. 메시지가 표시되면 사용자의 자격 증명을 입력합니다.
8. 터미널 창을 실행합니다.
9. 다음과 같은 **설치 프로그램** 명령을 사용하여 패키지의 명령줄 설치를 수행합니다.
   sudo installer -pkg /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Endpoint\ Security\ Suite\ Enterprise.pkg -target /

   노트:

   -pkg 경로는 .dmg 파일에서 발견된 .pkg 설치 프로그램에 대한 경로입니다.
10. **Enter** 키를 누릅니다.
11. ESSE 고급 위협 방지 설치 확인을 참조하십시오.

Mac용 Advanced Threat Prevention 명령줄 제거

명령줄을 사용하여 Advanced Threat Prevention 클라이언트를 제거하려면 아래 단계를 따르십시오.

1. 터미널 창을 실행합니다.
2. 다음과 같은 **제거** 명령을 사용하여 패키지의 명령줄 제거를 수행합니다.
   sudo /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/Uninstall\ Endpoint\ Security\ Suite\ Enterprise.app/Contents/MacOS/Uninstall\ Endpoint\ Security\ Suite\ Enterprise --noui

   노트: 명령의 끝에는 --noui 스위치가 포함되어 있습니다.
3. **Enter** 키를 누릅니다.
   이제 Mac용 Advanced Threat Prevention가 제거되어 컴퓨터를 정상적으로 사용할 수 있습니다.

Mac용 Advanced Threat Prevention 문제 해결

Advanced Threat Prevention를 위한 SSL 인증서 또는 정책 확인 비활성화

클라이언트의 서버 인증서가 누락되었거나 자체 서명된 경우, 클라이언트 측면에 있는 SSL 인증서만 비활성화해야 합니다.

사용자 환경에서 자체 서명된 인증서를 실행할 경우 PolicyCheck를 비활성화합니다.

사용자 환경에 자체 서명된 인증서가 있고, 인증서를 Mac의 키체인으로 가져오지 않은 경우 DisableCertTrust 및 DisablePolicyCheck를 모두 False로 설정합니다.

1. 클라이언트에서 터미널 창을 실행합니다.
2. DellCSFConfig.app에 대한 경로 입력:

   ```
   cd /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/DellCSFConfig.app/Contents/MacOS/
   ```
3. DellCSFConfig.app 실행:

   ```
   sudo DellCSFConfig.app/Contents/MacOS/DellCSFConfig
   ```

   기본 설정 시 다음이 표시됩니다.

```
Current Settings:
ServerHost = deviceserver.company.com
ServerPort = 8888
DisableCertTrust = False
DisablePolicyCheck = False
DumpXmlInventory = False
DumpPolicies = False
```

4. 옵션을 나열하려면 **-help**를 입력합니다.
5. 클라이언트에서 SSL 인증서를 비활성화하려면 `DisableCertTrust`를 **True**로 설정합니다.
6. 클라이언트에서 정책 서명 확인을 비활성화하려면 `DisablePolicyCheck`를 **True**로 설정합니다.

XML 인벤토리 및 정책 변경 사항을 로그 폴더에 추가

inventory.xml 또는 policies.xml 파일을 로그 폴더에 추가하려면 다음 단계를 따르십시오.

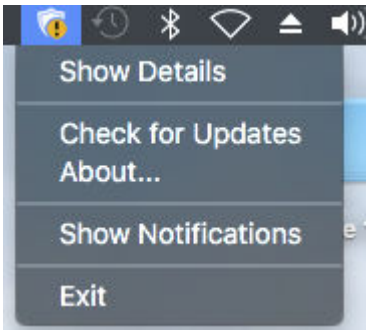
1. 위에 설명된 대로 DellCSFConfig.app을 실행합니다.
2. DumpXmlInventory를 **True**로 변경합니다.
3. DumpPolicies를 **True**로 변경합니다.

   정책이 변경되는 경우에만 정책 파일이 덤프됩니다.
4. inventory.xml를 및 policies.xml 로그 파일을 보려면 **/Library/Application\ Support/Dell/Dell\ Data\ Protection/**로 이동합니다.

Advanced Threat Prevention 설치 확인

선택적으로 설치를 확인할 수 있습니다.

1. 명령 표시줄의 고급 위협 방지 아이콘에 녹색 배지  가 있는지 확인합니다.
2. 아이콘에 느낌표가 있으면 마우스 오른쪽 단추로 클릭하고 **상세정보 표시**를 선택합니다. 등록되지 않은 것으로 나타날 수 있습니다.

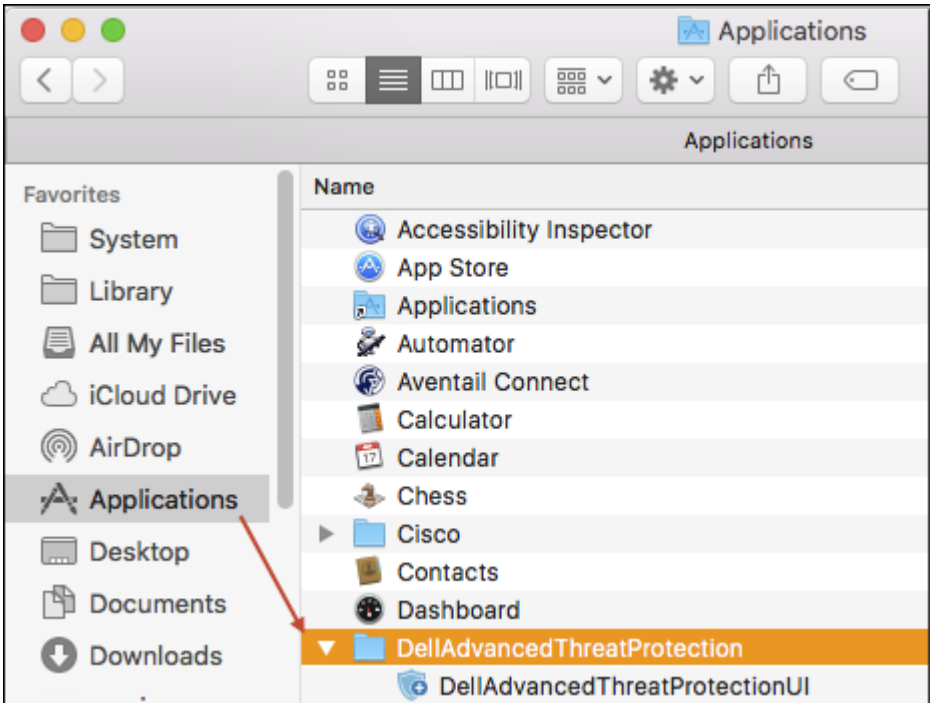


업데이트 확인 - Dell Server 정책 업데이트가 아니라 고급 위협 방지 엔진 업데이트인지 확인합니다.

정보 - 다음과 같은 내용이 포함되어 있습니다.

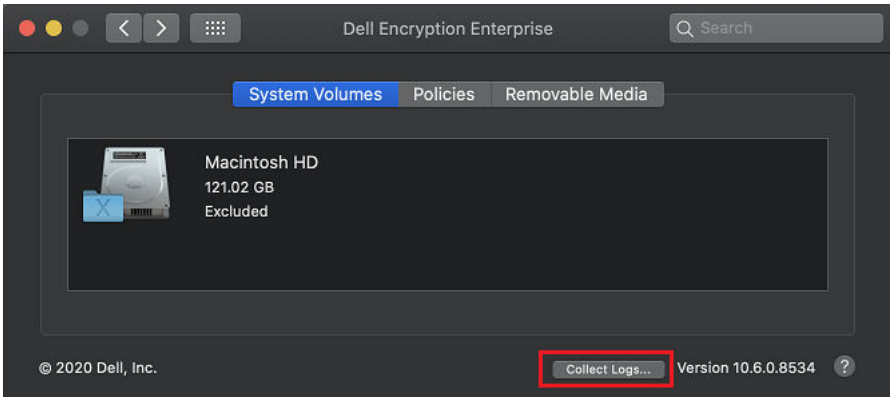
- 버전
- 정책 - [online]은 서버 기반 정책, [offline]은 Airgap 또는 오프라인 기반 정책을 나타냅니다.
- 일련 번호 - 지원 문의 시 사용합니다. 이 번호는 고유한 설치 식별자입니다.

3. 고급 위협 방지 폴더는 /Applications에 생성됩니다.



Endpoint Security Suite Enterprise에 대한 로그 파일 수집

시스템 환경 설정 > *Dell Encryption Enterprise* > *시스템 볼륨*에서 오른쪽 하단에 있는 *로그 수집* 버튼을 사용하면 관리자가 지원을 위해 로그를 미리 생성할 수 있습니다. 이 작업은 로그를 수집하는 동안 성능에 영향을 미칠 수 있습니다.



DellLogs.zip에는 Mac Encryption Enterprise 및 Advanced Threat Prevention에 대한 로그가 포함되어 있습니다. 로그를 수집하는 방법에 대한 자세한 내용은 http://www.dell.com/support/article/us/en/19/SLN303924을 참조하십시오.

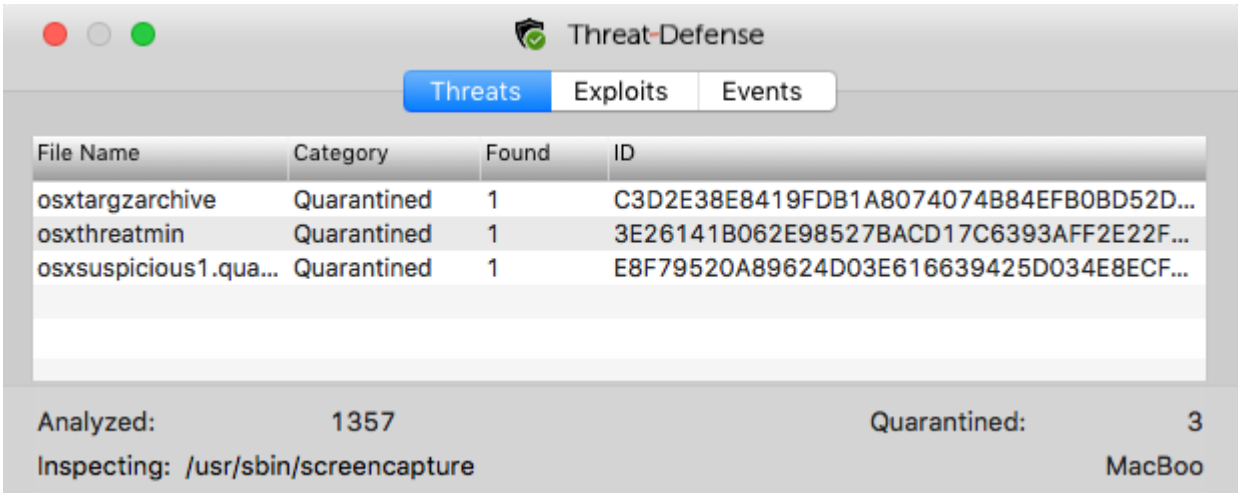
Advanced Threat Prevention 세부 정보 보기

끝점 컴퓨터에 고급 위협 방지 클라이언트가 설치되면 Dell Server에서 에이전트로 인식됩니다.

명령 표시줄에서 고급 위협 방지 아이콘 을 마우스 오른쪽 단추로 클릭한 뒤 **상세정보 표시**를 선택합니다. 고급 위협 방지 상세 정보 화면에는 다음과 같은 탭이 있습니다.

위협 탭

3개의 탭에는 장치에서 발견된 모든 위협 요소와 실시한 조치가 표시됩니다. 위협은 잠재적으로 안전하지 않은 파일 또는 프로그램으로 새로 감지된 이벤트로서 안내에 따른 수정이 필요한 이벤트 범주입니다.



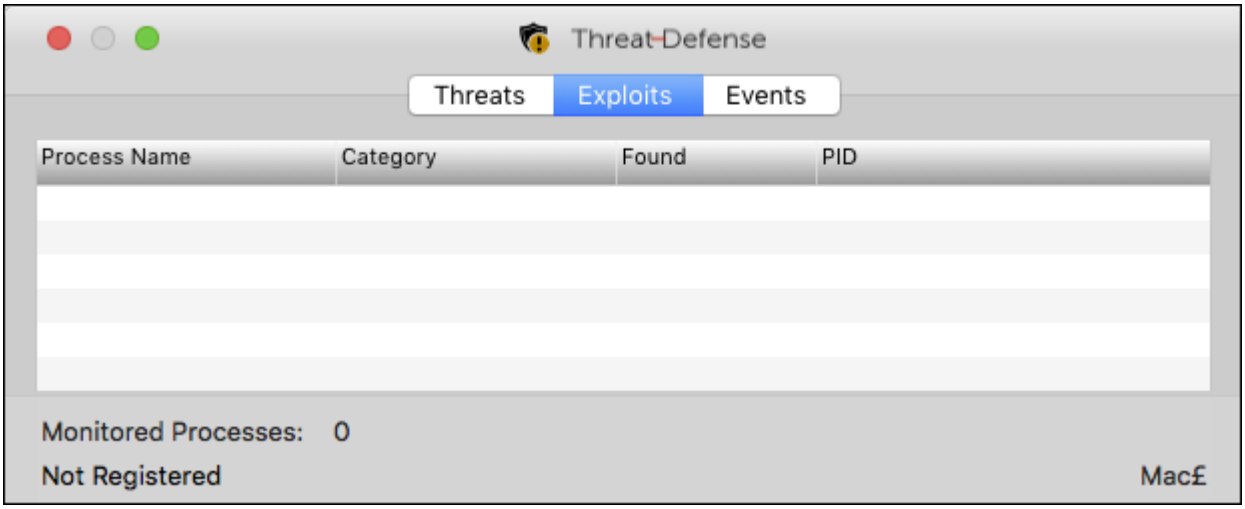
카테고리 열에는 다음과 같은 정보가 포함되어 있습니다.

- **안전하지 않음** - 맬웨어일 가능성이 높은 의심스러운 파일
- **비정상** - 맬웨어일 수 있는 의심스러운 파일
- **격리됨** - 장치에서 실행되지 않도록 원래 위치에서 이동되어 격리 폴더에 저장된 파일
- **면제됨** - 장치에서 실행이 허용된 파일.
- **삭제됨** - 조직 내에서 삭제된 파일. 제거된 파일은 면제된 파일, 안전 목록에 추가된 파일 및 장치의 차단된 폴더에서 삭제된 파일을 포함합니다.

Advanced Threat Prevention의 위협 분류에 대한 자세한 내용은 Management Console에서 사용 가능한 *관리자 도움말*을 참조하십시오.

익스플로잇 탭

익스플로잇 탭에는 위협으로 간주되는 악용 유형이 나열되어 있습니다.



Dell Server 정책은 시스템 악용이 감지된 경우 취해야 할 작업을 결정합니다.

- **무시** - 확인된 메모리 위반 사항에 대해 아무 조치를 취하지 않습니다.
- **경고** - 메모리 위반이 기록되고 Dell Server에 보고됩니다.
- **차단** - 응용 프로그램에서 메모리 위반 프로세스를 호출하려 하면 프로세스 호출을 차단합니다. 호출한 응용 프로그램은 계속해서 실행할 수 있습니다.

- **종료** - 응용 프로그램에서 메모리 위반 프로세스를 호출하려 하면 프로세스 호출을 차단합니다. 호출한 응용 프로그램이 종료됩니다.

다음과 같은 악용 유형이 감지되었습니다.

- 스택 피벗
- 스택 보호
- 스캐너 메모리 검색
- 악성 페이로드

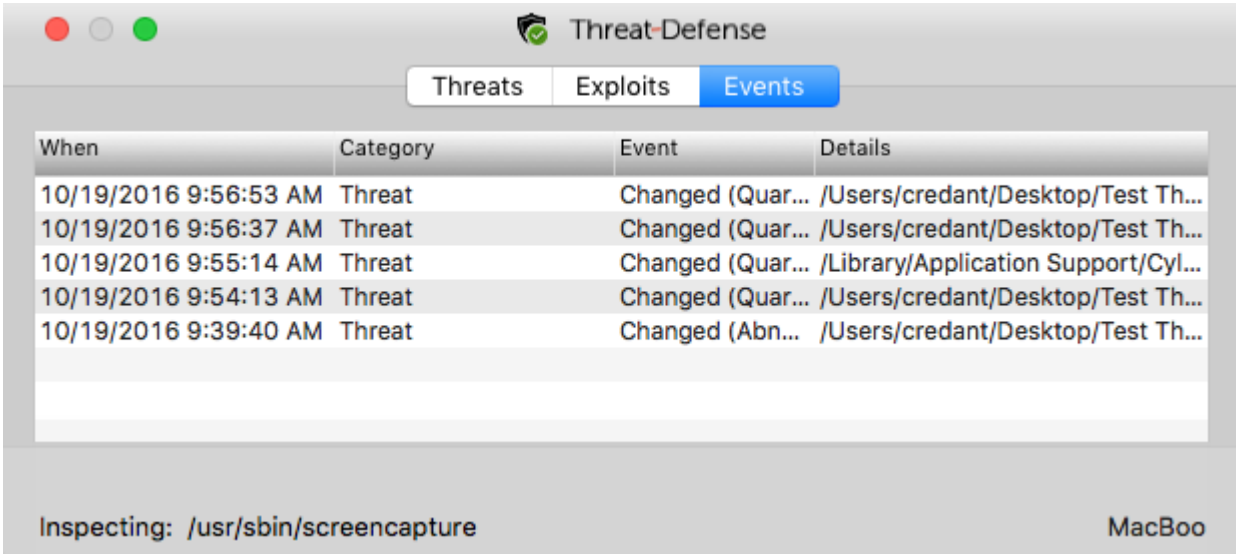
익스플로잇 정책에 대한 자세한 내용은 Management Console에서 사용 가능한 *관리자 도움말*을 참조하십시오.

이벤트 탭

노트:

이벤트가 반드시 위협을 의미하는 것은 아닙니다. 이벤트는 인식된 파일이나 프로그램이 격리되거나, 안전 목록에 추가되거나, 면제될 때 생성됩니다.

이벤트 탭에는 장치에서 발생한 모든 위협 이벤트가 표시되고 Advanced Threat Prevention에서 할당한 이벤트 유형별로 표시됩니다. 시스템이 다시 시작하면 데이터가 제거됩니다.



이벤트 유형 예시에는 다음이 포함됩니다.

위협 발견

위협 제거

위협 격리됨

위협 면제됨

위협 변경됨

테넌트 프로비저닝

Advanced Threat Prevention의 정책 집행이 활성화되기 전에 테넌트가 Dell Server에서 프로비전되어야 합니다.

사전 요구 사항

- 시스템 관리자 역할의 관리자가 수행해야 합니다.
- Dell Server에서 프로비저닝하려면 인터넷에 연결되어 있어야 합니다.
- Management Console에서 Advanced Threat Prevention 온라인 서비스 통합을 표시하려면 클라이언트에서 인터넷이 연결되어 있어야 합니다.
- 프로비저닝은 프로비저닝 중에 인증서에서 생성되는 토큰을 기반으로 합니다.
- Dell Server에 Advanced Threat Prevention 라이센스가 있어야 합니다.

테넌트 프로비저닝

1. Dell 관리자 계정으로 Management Console에 로그인합니다.
2. Management Console의 왼쪽 창에서 **관리 > 서비스 관리**를 클릭합니다.
3. **Advanced Threat Protection 서비스 설정**을 클릭합니다. 이때 오류가 발생하면 Advanced Threat Prevention 라이센스를 가져옵니다.
4. 라이센스를 가져오면 지침 제공되는 설정이 시작됩니다. **다음**을 클릭하여 시작합니다.
5. EULA를 읽고 동의한 후 **다음**을 클릭합니다.
6. 테넌트 프로비저닝을 위해 Dell Server에 유효한 자격 증명을 제공합니다. **다음**을 클릭합니다. *Cylance 상표의 기존 테넌트의 프로비저닝은 지원되지 않습니다.*
7. 인증서를 다운로드합니다. 이 인증서는 Dell Server에서 재해가 발생할 경우 복구에 필요합니다. 이 인증서는 자동으로 백업되지 않습니다. 인증서를 다른 컴퓨터의 안전한 위치에 백업합니다. 인증서를 백업한다는 옵션의 확인란을 선택하고 **다음**을 클릭합니다.
8. 설정이 완료됩니다. **확인**을 클릭합니다.

Advanced Threat Prevention 에이전트 자동 업데이트 구성

Management Console에서 Advanced Threat Prevention 에이전트 자동 업데이트를 받도록 등록할 수 있습니다. 에이전트 자동 업데이트를 받도록 등록하면 클라이언트가 Advanced Threat Prevention 서비스에서 업데이트를 자동으로 다운로드하여 적용할 수 있습니다. 업데이트는 매월 릴리스됩니다.

노트:

에이전트 자동 업데이트는 Dell Server v9.4.1 이상에서 지원됩니다.

에이전트 자동 업데이트 받기

에이전트 자동 업데이트를 받도록 등록하려면 다음을 수행합니다.

1. Management Console의 왼쪽 창에서 **관리** > **서비스 관리**를 클릭합니다.
2. *Advanced Threat* 탭의 *에이전트 자동 업데이트*에서 **켜짐** 단추를 클릭한 후 **환경설정 저장** 단추를 클릭합니다.

   정보가 채워지고 자동 업데이트가 표시되기까지 시간이 소요될 수 있습니다.

에이전트 자동 업데이트 받기 중지

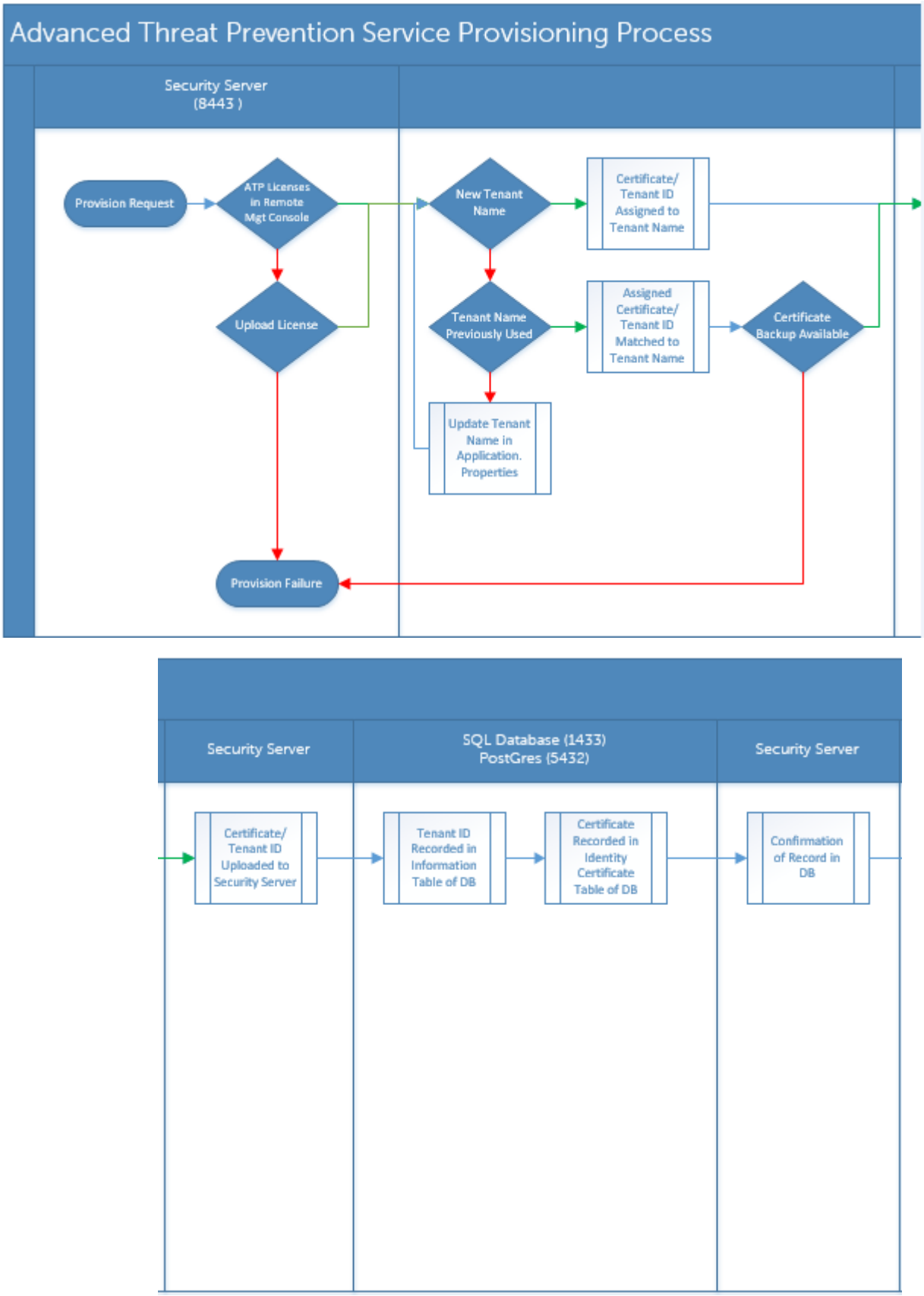
에이전트 자동 업데이트 받기를 중지하려면 다음을 수행합니다.

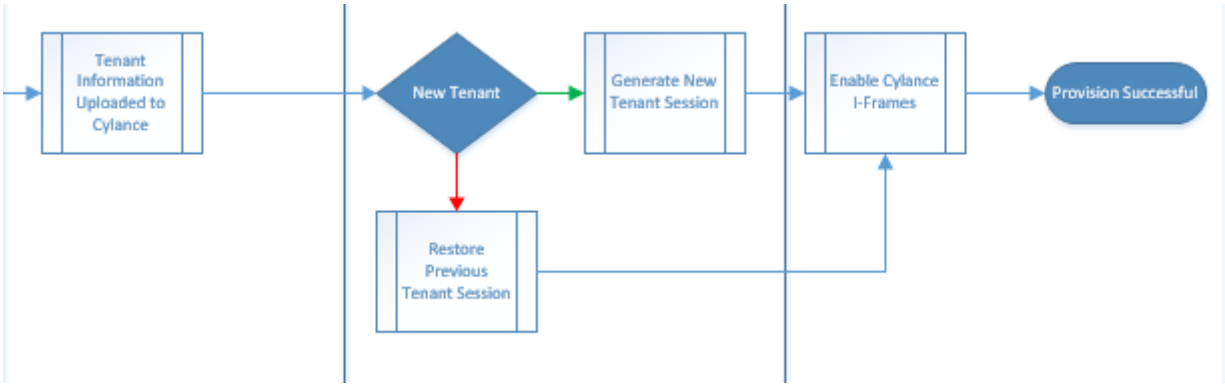
1. Management Console의 왼쪽 창에서 **관리** > **서비스 관리**를 클릭합니다.
2. *고급 위협* 탭의 *에이전트 자동 업데이트*에서 **꺼짐** 단추를 클릭한 후 **환경설정 저장** 단추를 클릭합니다.

Advanced Threat Prevention 문제 해결

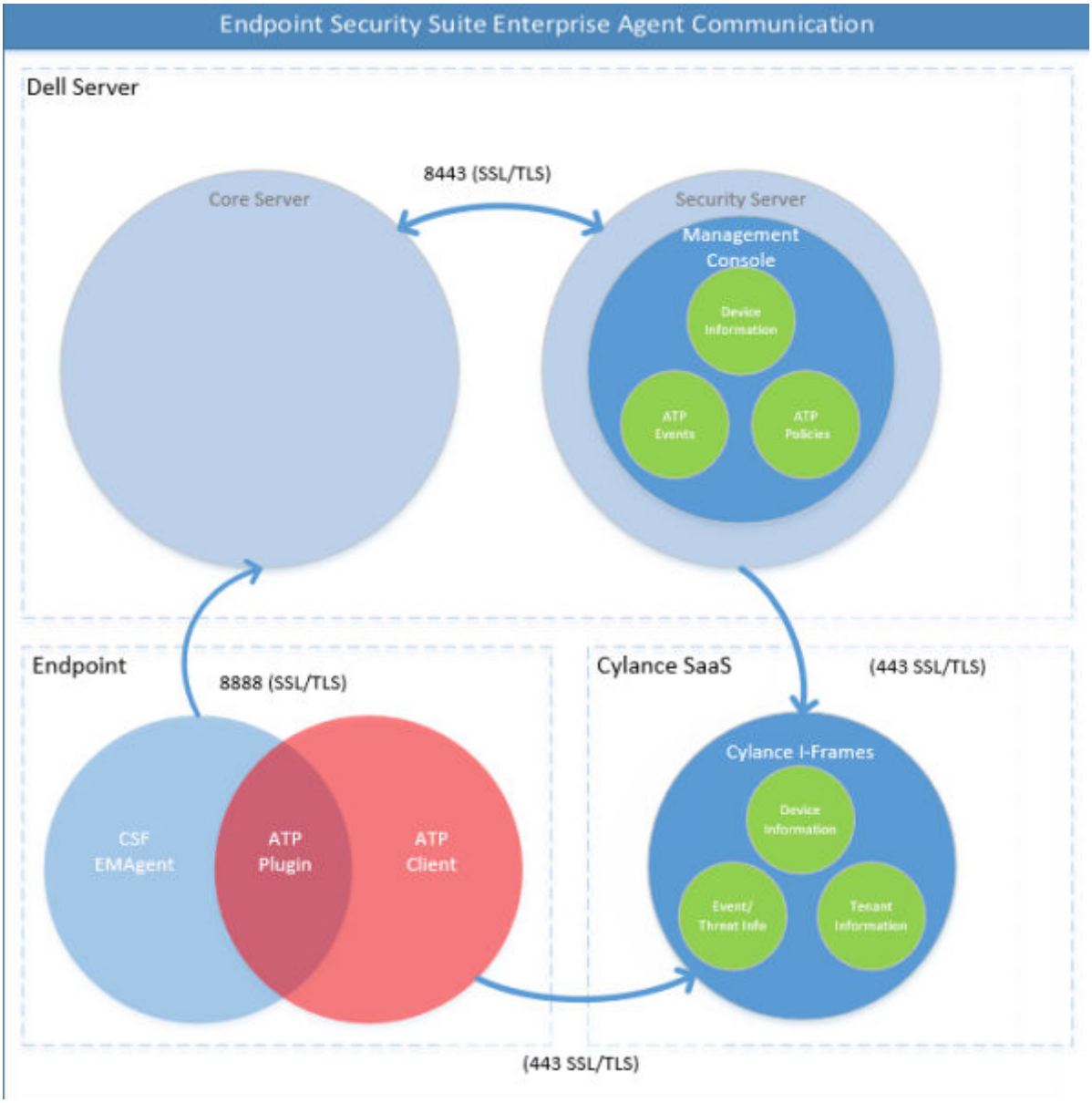
Advanced Threat Prevention 프로비저닝 및 에이전트 통신

다음 다이어그램은 Advanced Threat Prevention 서비스 프로비저닝 프로세스를 보여 줍니다.


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Tenant Name Previously Used
Certificate/ Tenant ID Assigned to Tenant Name
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 Advanced Threat Prevention 에이전트 통신 프로세스를 보여 줍니다.



5

용어집

보안 서버- Dell Encryption 활성화에 사용됩니다.

Policy Proxy- 클라이언트 소프트웨어에 대한 정책을 배포하는 데 사용됩니다.

Management Console - 전체 엔터프라이즈 배포를 위한 Dell 서버의 관리 콘솔입니다.

Shield - 가끔 설명서와 클라이언트 사용자 인터페이스에서 이 이름을 볼 수 있습니다. "Shield"는 Dell Encryption을 나타내는 데 사용되는 이름입니다.