Dell Data Security

EnCase 통합 안내서

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 Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise 및 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).

EnCase 통합 안내서

2018 - 03

개정 A01

목차

1

소개

Dell Data Security는 Guidance Software, Inc.의 EnCase v6.15 디지털 포렌식 제품과 통합되어 Dell 암호화 파일에 대한 온라인 조사를 지원합니다. 이러한 통합을 통해 포렌식 조사관은 Dell 보안 데이터를 보거나 내보내거나 해당 데이터 내에서 검색할 수 있습니다. 적절한 포렌식 관리자 자격 증명을 사용하면 모든 Dell 보안 데이터는 추가적인 상호 작용 없이 해당 데이터를 암호화하는 데 사용된 키에 관계없이 암호 해독되어 조사관에게 표시됩니다. EnCase의 안전한 저장 기능은 케이스에 포렌식 관리자 자격 증명을 저장하므로 자격 증명을 다시 입력할 필요가 없습니다.

EnCase v6.15(32비트) 포렌식 통합에서 지원되는 사항은 다음과 같습니다.

- Windows v7.0.x 이상을 위한 Dell Data Security Encryption Enterprise
- Dell Security Management Server v7.0.1 이상

노트: Mac용 Dell Data Security Encryption Enterprise는 EnCase 포렌식 조사를 지원하지 않습니다.

Dell ProSupport에 문의

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

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

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

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

2

EnCase와 통합

EnCase API 활성화

노트: DMZ에 배포된 Dell Device Server에 이 API를 사용하지 마십시오. EnCase 통합에 대한 제한된 액세스로 내부 Dell Device Server를 사용하여 보안을 유지합니다.

v7.7 이전 버전의 Security Management Server

1 **<Dell install dir>\Enterprise Edition\Device Server\conf\context.properties**를 엽니다.
2 포렌식 통합 API를 활성화합니다.

service.forensic.enable=true

3 시작 메뉴에서 Dell Device Server를 중지했다가 다시 시작합니다.

포렌식 통합을 비활성화하려면 service.forensic.enable=false를 설정합니다.

v7.7 Security Management Server 이상

- 이 서비스는 Dell Server에서 기본적으로 활성화되어 있습니다.
- 포렌식 통합을 비활성화하려면 xapi.service.forensic.enable=false를 설정합니다.

시작 메뉴에서 Dell Device Server를 중지했다가 다시 시작합니다.

EnCase Integration Adapter 설치

1 EnCase를 실행 중인 컴퓨터에서 **CMGEnCaseIntegration.exe**를 더블 클릭합니다.
2 라이브러리 설치 프로그램 대화 상자가 표시되면 대상 EnCase 폴더가 올바른지 확인합니다.
3 **마침**을 클릭하여 CEGetBundle 및 Integration Adapter 파일을 \Program Files\EnCase6\Lib\Credant Technologies\CMG로 추출합니다.

EnCase와 함께 Dell Data Security 사용

암호화 키 가져오기

EnCase Enterprise 사용자 인터페이스를 사용하여 Dell Remote Management Console에서 암호화 키를 가져오고 이 컴퓨터 또는 증거 파일에 대한 모든 Dell 암호화 데이터를 암호 해독할 수 있습니다.

1 **온라인** 확인란을 선택합니다.
2 포렌식 관리자의 **사용자 이름**을 입력합니다.
3 포렌식 관리자의 **암호**를 입력합니다.
4 EnCase API가 활성화되어 있는 Dell Server의 URL을 입력합니다. 예:

   https://cred01.somedomain.com:8443/xapi/(Security Management Server가 v7.7 이상인 경우)

   https://cred01.somedomain.com:8081/xapi(Security Management Server가 v7.7 이전 버전인 경우)

   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet에서 Dell Server URI를 찾습니다.

   노트: Dell Server에서 키를 내보내려면 EnCase API가 활성화되어 있어야 합니다. 필요에 따라 EnCase 통합에만 독점적으로 사용되는 대체 Dell Device Server를 배포할 수 있습니다.

5 대상 컴퓨터 또는 증거 파일의 시스템 ID(MCID 및 고유 ID라고도 함)를 입력합니다.

   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield의 대상 컴퓨터 레지스트리에서 MCID를 찾습니다.

   Dell Remote Management Console의 왼쪽 창에서 **채우기 > 끝점**을 클릭합니다.

   - 해당 장치의 세부 정보 아이콘을 클릭합니다.
   - 상단 메뉴에서 **세부 정보 및 조치**를 클릭합니다.
   - *끝점 세부 정보* 영역에서 고유 ID를 찾습니다.

6 대상 컴퓨터 또는 증거 파일의 Shield ID(장치 ID, DCID, 복구 ID 또는 SCID라고도 함)를 입력합니다.

   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield의 대상 컴퓨터 레지스트리에서 DCID를 찾습니다.

   Dell Remote Management Console의 왼쪽 창에서 **채우기 > 끝점**을 클릭합니다.

   - 해당 장치의 **세부 정보** 아이콘을 클릭합니다.
   - 상단 메뉴에서 **세부 정보 및 조치**를 클릭합니다.
   - *Shield* 영역에서 복구 ID를 찾습니다.

   노트: MCID나 DCID 또는 두 ID를 모두 지정합니다. 가져온 케이스에는 지정된 시스템 ID나 Shield ID 또는 두 ID의 모든 키 자료가 포함되어 있습니다.

7 **확인**을 클릭합니다.

   암호 해독이 진행 중입니다.

   암호 해독이 완료되면 포렌식 검사를 위해 파일에 액세스할 수 있습니다. 암호 해독된 파일은 EnCase 모듈을 통해서만 볼 수 있으며 원래 소스 파일은 변경되지 않은 채 암호화된 상태로 유지됩니다.

4

Dell Data Security와 함께 EnCase 사용

CEGetBundle

CEGetBundle은 포렌식 관리자가 Dell Server에서 키 자료를 가져오는 데 사용할 수 있는 유틸리티입니다. 이 유틸리티는 Dell ProSupport를 통해 사용할 수 있습니다.

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

매개 변수
-L=CMG 5.3.x Server에서 키를 내보내기 위한 레거시 모드
URL=Device Server URL(<securityserver.organization.com>)
AdminName=관리자 사용자 이름
AdminPwd=관리자 암호
AdminDomain=관리자 도메인
MCID=대상 장치의 시스템 ID(고유 ID 또는 호스트 이름이라고도 함)
SCID=대상 Shield의 Shield Credant ID(DCID 또는 복구 ID라고도 함)
Username=키 자료 내보내기를 위한 대상 사용자(레거시 모드 전용)
OutputFile=내보낸 키 번들의 파일 이름
OutputPwd = 내보낸 키 번들의 암호
-R=백업 파일 모드 사용
BackupFile=백업 키가 포함된 실행 파일
BackupPwd=백업 파일에 사용되는 관리자 암호

노트: AdminDomain 매개 변수는 여러 도메인을 지원하도록 구성된 CMG Enterprise Edition 6.0 이상 서버에서 키를 내보내는 경우에만 제공되어야 합니다.

노트: 레거시 모드에서는 MCID, SCID 및 사용자 이름을 지정해야 합니다. 지정된 사용자에 대한 키 자료만 출력 파일에 추가됩니다. 사용자 또는 사용자 로밍 암호화가 활성화된 경우 암호 해독 대상 장치에서 각 사용자의 동일한 출력 파일 이름으로 이 도구를 실행해야 합니다. 각 사용자의 키 자료는 출력 파일에 추가됩니다.

명령줄의 예

- 다음 예에서는 MCID나 SCID 또는 둘 모두를 사용합니다. 지정된 시스템(MCID)이나 SCID 또는 둘 모두와 연관된 모든 키 자료는 덮어쓰기되는(있는 경우) 출력 파일에 저장됩니다.

```
CEGetBundle [-L] -XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dMCID] [-sSCID] [-uUsername] -oOutputFile -iOutputPwd
```

- 다음 예에서는 설치 프로그램으로 내보낸 백업 파일에서 키 자료를 추출합니다.

```
CEGetBundle -R -bBackupFile -ABackupPwd -oOutputFile -iOutputPwd
```