Dell Encryption

관리자 유틸리티

참고, 주의 및 경고

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

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

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

© 2018 Dell Inc. 저작권 본사 소유. Dell, EMC 및 기타 상표는 Dell Inc. 또는 자회사의 상표입니다. 기타 상표는 각 소유자의 상표일 수 있습니다.

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).

관리자 유틸리티

2017 - 08

개정 A01

목차

1 소개 4
Dell ProSupport에 문의 4

2 Administrative Download Utility(CMGAd) 5
Forensic 모드 사용 5
관리 모드 사용 6

3 Administrative Launch Utility(CMGAlu) 7
Forensic 모드 사용 7
Forensic 모드 구문 7
관리 모드 사용 8
관리 모드 구문 8
백업 파일 모드 사용 8
백업 파일 구문 백업 8

4 Administrative Unlock Utility(CMGAu) 10
이전에 다운로드한 파일로 오프라인에서 작업하기 10
Forensic 모드에서 지금 다운로드 수행 10
관리 모드에서 지금 다운로드 수행 11

1

소개

이 문서에서는 암호화 키 회수 및 파일 액세스를 위한 유틸리티에 대해 설명합니다. 이러한 유틸리티는 다음과 같은 기능을 제공합니다.

키 다운로드 - CMGAd를 통해 관리자는 Dell Server에 연결되지 않은 컴퓨터에서 사용할 목적으로 키 자료 번들을 다운로드할 수 있습니다.

작업 실행 - CMGAlu 명령을 사용하면 관리자는 프로세스가 실행되고 있는 동안 컴퓨터에서 사용자 또는 일반 암호화된 파일의 잠금을 해제할 수 있습니다.

파일 잠금 해제 - CMGAu 명령을 사용하여 관리자는 슬레이브 드라이브, 사전 설치된 환경에서 부팅되는 컴퓨터 또는 활성화된 사용자가 로그인되지 않은 컴퓨터에서 사용자, 일반 또는 SDE 암호화된 파일에 액세스할 수 있습니다.

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 코드를 준비하십시오.

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

Administrative Download Utility(CMGAd)

이 유틸리티를 사용하면 Dell Server에 연결되지 않은 컴퓨터에 키 자료 번들을 다운로드하여 사용할 수 있습니다. 그러면 관리자 유틸리티가 이러한 오프라인 번들을 사용할 수 있습니다.

이 유틸리티는 애플리케이션에 전달되는 명령줄 매개변수에 따라 다음 방법 중 하나로 키 번들을 다운로드합니다.

- **Forensic 모드** - **-f** 가 명령줄에 전달되거나 사용된 명령줄 매개변수가 없는 경우에 사용됩니다.
- **관리 모드** - **-a**가 명령줄에 전달되는 경우에 사용됩니다.

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

Forensic 모드 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).

Forensic 모드 매개변수	설명
Device Server URL	정규화된 Security Server(Device Server) URL. https://securityserver.domain.com:8443/xapi/ 형식으로 입력합니다. Dell Server가 v7.7 이전 버전일 경우 https://deviceserver.domain.com:8081/xapi 형식으로 입력합니다(뒤에 슬래시 없이 다른 포트 번호 입력).
Dell Admin	Forensic 관리자 자격 증명을 사용하는 관리자의 이름(예: jdoe) (관리 콘솔에서 활성화됨)
암호	Forensic 관리자 암호
MCID	시스템 ID(예: machineID.domain.com)
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 매개변수에는 이 유틸리티에서 사용된 다양한 정보가 포함되어 있습니다.

다음을 클릭합니다.

3 *패스프레이즈*에서 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 모드 사용

보안 관리 서버 가상은 Key Server를 사용하지 않으므로 관리 모드로 보안 관리 서버 가상에서 키 번들을 가져올 수 없습니다. 클라이언트가 보안 관리 서버 가상에 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).

관리 모드 매개변수 설명

서버:	Key Server의 정규화된 호스트 이름(예: keyserver.domain.com).
포트 번호	기본 포트 번호는 8050
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	시스템 ID(예: machineID.domain.com)
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 매개변수에는 이 유틸리티에서 사용된 다양한 정보가 포함되어 있습니다.

다음을 클릭합니다.

3 *패스프레이즈*에서 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.

3

Administrative Launch Utility(CMGAlu)

이 유틸리티를 통해 관리자는 프로세스가 실행되고 있는 동안 컴퓨터에서 사용자 또는 일반 암호화된 파일의 잠금을 해제할 수 있습니다.

이 유틸리티는 관리 콘솔에서 작업을 실행하는 데 사용됩니다. 유틸리티는 대상 컴퓨터에 복사되어야 하며, 관리 작업에 대한 명령줄을 유틸리티에 전달함으로써, 사용자 또는 일반 암호화된 파일의 액세스가 필요한 모든 작업이 유틸리티를 실행하도록 변경됩니다. 한 번 프로세스가 종료되면 유틸리티도 종료됩니다.

이 유틸리티는 애플리케이션에 전달되는 명령줄 매개변수에 따라 다음 방법 중 하나로 파일 잠금을 해제합니다.

- **Forensic 모드** - **-f**가 명령줄에 전달되거나 명령줄에 전달된 매개변수가 없는 경우에 사용됩니다.
- **관리 모드** - **-k**가 명령줄에 전달되는 경우에 사용됩니다.
- **백업 파일 모드** - **-b**가 명령줄에 전달되는 경우에 사용됩니다.

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

Forensic 모드 사용

Forensic 모드 구문

```
CmgAlu -f -vX -aAdminName -AAdminPwd [-r] [-XURL [-dMCID] [-sSCID]] "command"
```

Forensic 모드 매개변수	설명
-f	Forensic 모드를 사용할 것임을 나타냅니다.
-vX	X는 로그 레벨을 나타냅니다. 로그 레벨은 0-5(0은 로그 없음/5는 디버그 수준)입니다.
AdminPwd	Forensic 관리자 암호
AdminName	Forensic 관리자 자격 증명을 사용하는 관리자의 사용자 이름
-r	레지스트리에서 Device Server URL 및 컴퓨터의 MCID(또는 SCID)를 로드하도록 유틸리티에 지시합니다. -r이 지정되어 있지 않으면 URL/Server 및 MCID(또는 SCID)가 제공되어야 합니다.
URL	전체 정규화된 Device Server URL Dell Server가 v7.7 이전 버전인 경우 https://deviceserver.domain.com:8081/xapi 형식입니다. Dell Server가 v7.7 이상 버전인 경우 https://deviceserver.domain.com:8443/xapi/ 형식입니다.
MCID	장치에 대한 Device ID를 잠금 해제합니다. MCID는 Device Unique ID 또는 호스트 이름으로도 알려져 있습니다.

Forensic 모드 매개변수	설명
SCID	장치에 대한 Shield ID를 잠금 해제합니다. SCID는 DCID 또는 Recovery ID로도 알려져 있습니다.
-?	명령줄 도움말.

관리 모드 사용

관리 모드 구문

```
CmgAlu -k -vX -aServerPrincipal -pPort [-r] [-XServer [-dMCID] [-sSCID]] "command"
```

관리 모드 매개변수	설명
-k	Kerberos(관리 모드)를 사용할 것임을 나타냅니다. 관리 모드에서 CmgAlu가 작동하려면 -k 플래그가 필요합니다.
-vX	X는 로그 레벨을 나타냅니다. 로그 레벨은 0-5(0은 로그 없음/5는 디버그 수준)입니다.
ServerPrincipal	Key Server가 실행 중인 AD 계정(도메인 계정).
포트	Key Server에 연결하기 위한 TCP 포트.
서버	Key Server 이름/IP 주소.
-r	레지스트리에서 Key Server 이름 및 컴퓨터의 MCID(또는 SCID)를 로드하도록 유틸리티에 지시합니다. –r이 지정되어 있지 않으면 Key Server 이름 및 MCID(또는 SCID)가 제공되어야 합니다.
MCID	장치에 대한 Device ID를 잠금 해제합니다. MCID는 Device Unique ID 또는 호스트 이름으로도 알려져 있습니다.
SCID	장치에 대한 Shield ID를 잠금 해제합니다. SCID는 DCID 또는 Recovery ID로도 알려져 있습니다.
-?	명령줄 도움말.

백업 파일 모드 사용

백업 파일 구문 백업

```
CmgAlu -vX -b"FilePath" -ABackupPwd "command"
```

백업 파일 모드 매개변수	설명
-vX	X는 로그 레벨을 나타냅니다. 로그 레벨은 0-5(0은 로그 없음/5는 디버그 수준)입니다.
-b"FilePath"	백업 파일의 파일 시스템 경로는 일반적으로 CMGA에서 다운로드한 출력 파일 또는 LSA 복구 파일입니다.

백업 파일 모드 매개변수	설명
-BackupPwd	백업 파일을 생성하는 데 사용되는 암호.
-?	명령줄 도움말.

4

Administrative Unlock Utility(CMGAu)

이 유틸리티를 사용하여 슬레이브 드라이브, 사전 설치된 환경에서 부팅되는 컴퓨터 또는 활성화된 사용자가 로그인되지 않은 컴퓨터에서 사용자, 일반 또는 SDE 암호화된 파일에 액세스할 수 있습니다.

이 유틸리티는 다음과 같은 방법을 사용하여 키 자료 번들을 다운로드할 수 있습니다.

- **Forensic 모드** - **-f** 가 명령줄에 전달되거나 사용된 명령줄 매개변수가 없는 경우에 사용됩니다.
- **관리 모드** - **-a**가 명령줄에 전달되는 경우에 사용됩니다.

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

이전에 다운로드한 파일로 오프라인에서 작업하기

이전에 다운로드한 파일로 오프라인에서 작업하는 것을 선택한 경우, 실행 방법에 상관없이 CMGAu는 동일한 방식으로 작동합니다. 즉, .exe 파일을 더블 클릭하여 유틸리티를 실행하든, 명령줄에서 스위치를 사용하지 않고 실행하든, 아니면 명령줄에서 -f 스위치를 사용하여 실행하든 작업은 동일하다는 의미입니다.

1 CMGAu가 있는 명령 프롬프트를 열고 **cmgau.exe**를 입력합니다.
2 **예, 이전에 다운로드한 파일로 오프라인에서 작업**을 선택합니다. **다음 >**을 클릭합니다.
3 *다운로드된 파일*에서 저장된 키 자료의 위치를 찾습니다. 이 파일은 Administrative Download Utility를 사용할 때 저장되었습니다.
*패스프레이즈*에서 키 자료 파일을 보호하는 데 사용되었던 패스프레이즈를 입력합니다. 이 패스프레이즈는 Administrative Download Utility를 사용할 때 설정되었습니다.

다음 >을 클릭합니다.

키 자료가 성공적으로 잠금 해제되었다는 메시지가 표시됩니다. 이제 파일에 액세스할 수 있습니다.
4 **암호화된 파일 작업을 모두 완료하면 마침**을 클릭합니다. *마침을 클릭하면 암호화된 파일을 더 이상 사용할 수 없습니다.*

Forensic 모드에서 지금 다운로드 수행

1 CMGAu가 있는 명령 프롬프트를 열고 **cmgau.exe**를 입력합니다.
2 **아니요, 지금 서버에서 다운로드를 수행합니다**를 선택합니다. **다음 >**을 클릭합니다.
3 다음 정보를 입력합니다(일부 필드는 미리 채워져 있을 수 있음).

옵션	설명
Device Server URL:	전체 정규화된 Device Server URL. Dell Server가 v7.7 이전 버전인 경우 https://deviceserver.domain.com:8081/xapi 형식입니다. Dell Server가 v7.7 이상 버전인 경우 https://deviceserver.domain.com:8443/xapi/ 형식입니다.
Dell Admin:	Forensic 관리자 자격 증명을 사용하는 관리자의 이름(예: jdoe) (관리 콘솔에서 활성화됨)
암호:	Forensic 관리자 암호
MCID:	시스템 ID(예: machineID.domain.com)

옵션	설명
DCID:	16자리 Shield ID의 처음 8개 숫자.

다음 >을 클릭합니다.

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

4 **암호화된 파일 작업을 모두 완료하면 마침**을 클릭합니다. ***마침****을 클릭하면 암호화된 파일은 더 이상 사용할 수 없습니다.*

관리 모드에서 지금 다운로드 수행

1 CMGAu가 있는 명령 프롬프트를 열고 **cmgau.exe -a**를 입력합니다.

2 **아니요, 지금 서버에서 다운로드를 수행합니다**를 선택합니다. **다음 >**을 클릭합니다.

3 다음 정보를 입력합니다(일부 필드는 미리 채워져 있을 수 있음).

관리 모드 매개변수 설명

서버:	Key Server의 정규화된 호스트 이름(예: keyserver.domain.com)
포트 번호:	기본 포트 번호는 8050
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:	시스템 ID(예: machineID.domain.com)
DCID:	16자리 Shield ID의 처음 8개 숫자.

다음 >을 클릭합니다.

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

4 **암호화된 파일 작업을 모두 완료하면 마침**을 클릭합니다. ***마침****을 클릭하면 암호화된 파일은 더 이상 사용할 수 없습니다.*