Dell Data Protection | Encryption

관리자 유틸리티

2014-05

목차

1

관리자 다운로드 유틸리티

이 유틸리티를 사용하면 엔터프라이즈 서버에 연결되어 있지 않은 컴퓨터에서 사용할 키 자료 번들을 다운로드할 수 있습니다. 그리고 이러한 번들을 관리자 유틸리티에서 오프라인으로 사용할 수 있습니다.

이 유틸리티는 응용 프로그램에 전달되는 명령줄 매개변수에 따라 다음 중 한 가지 방법을 사용하여 키 자료 번들을 다운로드합니다.

- **관리 모드** - 명령줄에 **-a**가 전달되었거나 사용하는 명령줄 매개 변수가 없는 경우 사용됩니다.
- **Forensic 모드** - 명령줄에 **-f**가 전달된 경우 사용됩니다.

로그 파일 위치는 다음과 같습니다.

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, 및 Windows 8.1 - C:\ProgramData\CmgAdmin.log

관리자 다운로드 유틸리티를 관리 모드로 사용

1. **cmgad.exe**를 더블 클릭하여 유틸리티를 시작합니다.

   또는

   관리자 다운로드 유틸리티가 있는 위치에서 명령 프롬프트를 열고 **cmgad.exe -a**(또는 cmgad.exe)를 입력합니다.

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

   서버: 키 서버의 정규화된 호스트 이름(예: keyserver.domain.com)

   포트 번호: 기본 포트는 8050입니다.

   서버 계정: 키 서버를 실행하는 도메인 사용자입니다. 형식은 도메인\사용자 이름입니다. 유틸리티를 실행하는 도메인 사용자에게 키 서버에서 다운로드를 수행할 권한이 있어야 합니다.

   MCID: 시스템 ID(예: machineID.domain.com)

   DCID: 16자리 Shield ID의 앞자리 수 8개

   다음 >을 클릭합니다.

3. **암호:** 필드에 다운로드 파일을 보호하기 위한 암호를 입력합니다. 암호는 8자 이상이어야 하고 영문자와 숫자를 최소 하나씩 포함해야 합니다.

   암호를 확인합니다.

   파일을 저장할 기본 이름과 위치를 승인하거나 **...**를 클릭하여 다른 위치를 선택합니다.

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

4. 완료되면 **마침**을 클릭합니다.

관리자 다운로드 유틸리티를 **Forensic** 모드로 사용

1. 관리자 다운로드 유틸리티가 있는 위치에서 명령 프롬프트를 열고 **cmgad.exe -f**를 입력합니다.
2. 다음 정보를 입력합니다(일부 필드는 미리 채워져 있을 수 있음).

   장치 서버 URL: 정규화된 장치 서버 URL

엔터프라이즈 서버가 v7.7 이전 버전인 경우 https://deviceserver.domain.com:8081/xapi 형식입니다.

엔터프라이즈 서버가 v7.7 및 이후 버전인 경우 https://deviceserver.domain.com:8443/xapi/ 형식입니다.

Dell 관리자: Forensic 관리자 자격 증명(엔터프라이즈 서버에 활성화됨)이 있는 관리자의 이름(예: jdoe)

암호: Forensic 관리자 암호

MCID: 시스템 ID(예: machineID.domain.com)

DCID: 16자리 Shield ID의 앞자리 수 8개

다음 >을 클릭합니다.

3 **암호:** 필드에 다운로드 파일을 보호하기 위한 암호를 입력합니다. 암호는 8자 이상이어야 하고 영문자와 숫자를 최소 하나씩 포함해야 합니다.

암호를 확인합니다.

파일을 저장할 기본 이름과 위치를 승인하거나 **...**를 클릭하여 다른 위치를 선택합니다.

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

4 완료되면 **마침**을 클릭합니다.

2

관리자 시작 유틸리티

이 명령줄 유틸리티를 사용하면 프로세스가 실행 중인 동안 관리자가 컴퓨터에서 사용자 또는 일반 암호화된 파일을 잠금 해제할 수 있습니다.

이 유틸리티는 관리 콘솔에서 작업을 시작하는 데 사용합니다. 이 유틸리티는 클라이언트 컴퓨터로 복사해야 하며, 사용자 또는 일반 암호화된 파일에 액세스해야 하는 작업은 관리 작업 명령줄을 유틸리티로 전달하여 이 유틸리티를 실행하도록 변경됩니다. 이 프로세스가 종료되면 유틸리티가 종료됩니다.

이 유틸리티는 응용 프로그램에 전달되는 명령줄 매개변수에 따라 다음 중 한 가지 방법을 사용하여 파일을 잠금 해제합니다.

- **관리 모드** - 스위치가 필요하지 않습니다.
- **Forensic 모드** - 명령줄에 **-f**가 전달된 경우 사용됩니다.
- **백업 파일의 모드** - 명령줄에 **-b** 가 전달된 경우 사용됩니다 .

로그 파일 위치는 다음과 같습니다.

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, 및 Windows 8.1 - C:\ProgramData\CmgAdmin.log

관리자 시작 유틸리티를 관리 모드로 사용

관리 모드 구문

CmgAlu -k -vX -aServerPrincipal -pPort [-r] [-XServer [-dMCID] [-sSCID]] “명령”

관리 모드 매개 변수	설명
-k	이 Kerberos (관리 모드) 를 사용할 수 있음을 나타냅니다 . 관리 모드에서 작업하기 위해 , CmgAlu 는 -K 플래그가 필요합니다 .
X	로그 수준입니다 . 범위는 0 ~ 5(0 은 로그가 없는 경우 /5 는 디버그 수준) 입니다 .
ServerPrincipal	키 서버가 실행 중인 AD 계정 (도메인 계정) 입니다 .
Port	키 서버에 연결할 TCP 포트입니다 .
Server	키 서버의 이름 /IP 주소입니다 .
-r	유틸리티에 레지스트리에서 컴퓨터의 키 서버 이름 및 MCID(또는 SCID) 를 로드하도록 지시합니다 . –r 이 지정되지 않은 경우에는 키 서버 이름 및 MCID(또는 SCID) 를 입력해야 합니다 .
MCID	잠금 해제할 장치의 장치 ID 입니다 . MCID 는 장치의 고유한 ID 또는 호스트 이름으로도 알려져 있습니다 .
SCID	잠금 해제할 장치의 Shield ID 입니다 . SCID 는 DCID 또는 복구 ID 라고도 합니다 .

관리 모드 매개 변수	설명
-?	명령줄 도움말입니다 .

관리자 시작 유틸리티를 **Forensic** 모드로 사용

Forensic 모드 구문

CmgAlu -f -vX -aAdminName -AAdminPwd [-r] [-XURL [-dMCID] [-sSCID]] “명령”

Forensic 모드 매개 변수	설명
-f	Forensic 모드가 사용됨을 나타냅니다 .
AdminName	Forensic 관리 자격 증명이 있는 관리자의 사용자 이름입니다 .
AdminPwd	Forensic 관리자 암호입니다 .
URL	정규화된 장치 서버의 URL 입니다 . 엔터프라이즈 서버가 v7.7 이전 버전인 경우 https://deviceserver.domain.com:8081/xapi 형식입니다 . 엔터프라이즈 서버가 v7.7 및 이후 버전인 경우 https://deviceserver.domain.com:8443/xapi/ 형식입니다 .
-r	유틸리티에 레지스트리에서 컴퓨터의 장치 서버 URL 및 MCID(또는 SCID) 를 로드하도록 지시합니다 . –r 이 지정되지 않은 경우에는 URL/ 서버 및 MCID(또는 SCID) 를 입력해야 합니다 .
X	로그 수준입니다 . 범위는 0 ~ 5(0 은 로그가 없는 경우 /5 는 디버그 수준) 입니다 .
MCID	잠금 해제할 장치의 장치 ID 입니다 . MCID 는 장치의 고유한 ID 또는 호스트 이름으로도 알려져 있습니다 .
SCID	잠금 해제할 장치의 Shield ID 입니다 . SCID 는 DCID 또는 복구 ID 라고도 합니다 .
-?	명령줄 도움말입니다 .

관리자 시작 유틸리티를 백업 파일의 모드로 사용

백업 파일의 모드 구문

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

백업 파일의 모드 매개 변수	설명
X	로그 수준입니다 . 범위는 0 ~ 5(0 은 로그가 없는 경우 /5 는 디버그 수준) 입니다 .
-b"FilePath"	백업 파일을 파일 시스템 경로 . 보통 , 이것은 LSA 복구 파일 또는 출력 파일이다 . 그것은 CmgAd 에서 다운로드됩니다 .
BackupPwd	암호는 백업 파일을 만드는 데 사용됩니다 .
-?	명령줄 도움말입니다 .

3

관리자 잠금 해제 유틸리티

이 유틸리티를 사용하면 슬레이브로 연결된 드라이브, 사전 설치 환경에서 부팅된 컴퓨터 또는 활성화된 사용자가 로그인되어 있지 않은 컴퓨터의 사용자, 일반 또는 SDE 암호화된 파일에 액세스할 수 있습니다.

이 유틸리티는 다음 방법을 사용하여 키 자료 번들을 다운로드합니다.

- **관리 모드** - 스위치가 필요하지 않습니다. 이 모드가 기본 모드입니다.
- **Forensic 모드** - 명령줄에 **-f**가 전달된 경우 사용됩니다.

로그 파일 위치는 다음과 같습니다.

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, 및 Windows 8.1 - C:\ProgramData\CmgAdmin.log

관리자 잠금 해제 유틸리티를 사용하여 이전에 다운로드한 파일로 오프라인 작업

이전에 다운로드한 파일로 오프라인 작업을 할 경우, 시작 방법과 상관없이 CMGAu도 같은 방식으로 작동합니다. 즉, .exe를 더블 클릭하여 유틸리티를 시작하는 경우, 명령줄에서 아무 스위치 없이 시작하는 경우 또는 명령줄에서 -f 스위치를 사용하여 시작하는 경우 모두 동일하게 작동합니다.

1. **cmgau.exe**를 더블 클릭하여 유틸리티를 시작합니다.
2. **예, 이전에 다운로드한 파일로 오프라인 작업을 합니다**를 선택합니다. **다음 >**을 클릭합니다.
3. **다운로드한 파일:** 필드에서 저장된 키 자료가 있는 위치를 검색합니다. 이 파일은 관리자 다운로드 유틸리티를 사용할 때 저장된 파일입니다.

   암호: 필드에 키 자료 파일을 보호하는 데 사용한 암호를 입력합니다. 이 암호는 관리자 다운로드 유틸리티를 사용할 때 설정한 암호입니다.

   다음 >을 클릭합니다.

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

관리자 잠금 해제 유틸리티를 사용하여 관리 모드로 지금 서버에서 다운로드 수행

1. **cmgau.exe**를 더블 클릭하여 유틸리티를 시작합니다.

   또는

   관리자 잠금 해제 유틸리티가 있는 위치에서 명령 프롬프트를 열고 **cmgad.exe**를 입력합니다.
2. **아니요, 지금 서버에서 다운로드합니다**를 선택합니다. **다음 >**을 클릭합니다.

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

서버: 키 서버의 정규화된 호스트 이름(예: keyserver.domain.com)

포트 번호: 기본 포트는 8050입니다.

서버 계정: 키 서버를 실행하는 도메인 사용자입니다. 형식은 도메인\사용자 이름입니다. 유틸리티를 실행하는 도메인 사용자에게 키 서버에서 다운로드를 수행할 권한이 있어야 합니다.

MCID: 시스템 ID(예: machineID.domain.com)

DCID: 16자리 Shield ID의 앞자리 수 8개

다음 >을 클릭합니다.

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

4 암호화된 파일 작업을 마치면 **마침**을 클릭합니다. *마침을 클릭한 후에는 암호화된 파일을 더 이상 사용할 수 없습니다.*

관리자 잠금 해제 유틸리티를 사용하여 **Forensic** 모드로 지금 서버에서 다운로드 수행

1 관리자 잠금 해제 유틸리티가 있는 위치에서 명령 프롬프트를 열고 **cmgau.exe -f**를 입력합니다.

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

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

장치 서버 URL: 정규화된 장치 서버 URL입니다.

엔터프라이즈 서버가 v7.7 이전 버전인 경우 https://deviceserver.domain.com:8081/xapi 형식입니다.

엔터프라이즈 서버가 v7.7 및 이후 버전인 경우 https://deviceserver.domain.com:8443/xapi/ 형식입니다.

Dell 관리자: Forensic 관리자 자격 증명(엔터프라이즈 서버에 활성화됨)이 있는 관리자의 이름(예: jdoe)

암호: Forensic 관리자 암호

MCID: 시스템 ID(예: machineID.dell.com)

DCID: 16자리 Shield ID의 앞자리 수 8개

다음 >을 클릭합니다.

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

4 암호화된 파일 작업을 마치면 **마침**을 클릭합니다. *마침을 클릭한 후에는 암호화된 파일을 더 이상 사용할 수 없습니다.*


0 XXXXXA0 X