Dell Data Guardian

Windows, Mac, 모바일 및 웹 관리자 가이드 v2.0

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.

Windows, Mac, 모바일 및 웹 관리자 가이드

2018 - 08

개정 A01

목차

1

소개

모든 정책 정보와 그 설명은 AdminHelp에서 찾으시기 바랍니다.

시작하기 전에

1 클라이언트 배포에 앞서 Dell Server를 설치합니다. 아래 나열된 가이드에서 해당되는 가이드를 찾아 지침을 따른 후 이 가이드의 지침을 따르십시오.

- *Security Management Server 설치 및 마이그레이션 가이드)*
- *Security Management Server Virtual 퀵 스타트 가이드 및 설치 가이드)*
- 정책이 원하는 대로 설정되었는지 확인합니다. **?**에서 사용할 수 있는 AdminHelp를 통해 검색합니다. ?는 화면 맨 오른쪽에 있습니다. 관리자 도움말은 정책을 설정 및 수정하고 Dell Server에서의 옵션을 이해할 수 있도록 돕는 페이지 수준의 도움말입니다.

2 이 문서의 요구 사항 장을 읽고 숙지하십시오.

3 사용자에게 클라이언트를 배포하십시오.

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

요구 사항

Dell Server

Windows, Mac 및 모바일용 Data Guardian을 사용하려면 Security Management Server 또는 Security Management Server Virtual v9.6 이상이 필요합니다. Data Guardian 웹 클라이언트를 사용하려면 Security Management Server 또는 Security Management Server Virtual v9.8 이상이 필요합니다. 이 문서의 목적에 알맞게 특정 버전을 언급해야 할 경우(예: Security Management Server Virtual 사용 시 다른 절차 적용)를 제외하고 양쪽 서버가 모두 Dell Server로 지칭됩니다.

Windows용 Data Guardian

- 배포 시에는 IT 모범 사례를 따라야 합니다. 예를 들어, 초기 테스트에서 테스트 환경을 통제하고 사용자에 대해 시간별 배포를 수행해야 합니다.
- 설치/업그레이드/설치 제거를 수행하는 사용자 계정은 로컬 또는 도메인 관리자여야 하며, 관리자 권한은 Microsoft SMS 또는 Dell KACE 등의 배포 도구를 사용하여 임시로 할당할 수 있습니다. 관리자 이외의 사용자는 상승된 권한을 가진 경우에도 지원되지 않습니다.
- 설치/설치 제거를 시작하기 전에 중요한 데이터를 모두 백업하십시오.
- 설치가 진행되는 동안에는 외부(USB) 드라이브 삽입 또는 제거를 비롯하여 컴퓨터를 변경하지 마십시오.
- Data Guardian은 Microsoft Office 2016 및 Microsoft Office 365 Business 및 Business Premium의 특정 버전에서 지원됩니다. Office 365 Business Essentials에서는 지원되지 않습니다.
- 클라우드 암호화를 위하여 컴퓨터에 할당 가능한 디스크 드라이브 하나(문자 값)가 있어야 합니다.
- 대상 장치가 https://yoursecurityservername.domain.com:8443/cloudweb/register 및 https://yoursecurityservername.domain.com:8443/cloudweb에 연결되어 있는지 확인하십시오.
- Data Guardian을 배포하기 전에 대상 장치에 클라우드 스토리지 계정이 아직 설정되지 않은 상태가 가장 좋습니다.

  사용자가 기존 계정을 유지하기로 결정할 경우 Data Guardian을 설치하기 전에 *암호화되지 않은* 상태로 유지하려는 파일을 동기화 클라이언트 외부로 이동해야 합니다.
- 클라이언트가 설치된 후 사용자는 컴퓨터를 다시 시작할 준비를 해야 합니다.
- Data Guardian은 동기화 클라이언트의 동작을 방해하지 않습니다. 그러므로 관리자와 최종 사용자는 Data Guardian을 배포하기 전에 이러한 애플리케이션의 작동 방식을 잘 알아야 합니다. 자세한 내용은 Box 지원의 경우 https://support.box.com/home, Dropbox 지원의 경우 https://www.dropbox.com/help, OneDrive 지원의 경우 http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other를 참조하십시오.
- 보호된 Office 문서는 Data Guardian의 도우미 솔루션인 Mozy는 물론 기타 클라우드, 이메일 및 NFS 스토리지 제품에서도 지원됩니다.
- Office 2010을 실행하는 경우: Office 문서와 매크로가 활성화된 문서를 보호하기 위한 정책이 설정된 경우에 사용자는 Office 2010 서비스 팩 1 이상이 있어야 합니다(v14.0.6029 이상). Microsoft Office 2010 제품군에 서비스 팩이 적용되었는지 확인하려면 https://support.microsoft.com/en-us/kb/2121559를 참조하십시오. 이 업데이트를 하지 않으면 보호된 문서에 액세스할 수 없습니다. 스윕 기능이 켜져 있지 않으면 정책에 상관 없이 새 Office 문서는 보호되지 않습니다. 다음에 스윕을 하면 Office 문서가 보호된 파일로 변환되지만 지원되는 Office 버전이 없으면 사용자가 해당 파일에 액세스할 수 없습니다.
- Dell 암호화가 필요하지는 않지만 사용되는 경우 Encryption 클라이언트는 v8.12 이상이어야 합니다.
- Data Guardian은 Windows 시스템 복원 도구 또는 Windows Insider Preview를 지원하지 않습니다.
- Microsoft의 폴더 재지정은 Data Guardian에서 지원되지 않습니다.
- IPv6는 클라우드 암호화에서 지원되지 않습니다.
- 최신 문서 자료와 기술 권고사항에 대해서는 www.dell.com/support를 정기적으로 확인하시기 바랍니다.

사전 요구 사항

아직 설치되지 않은 경우 설치 프로그램에서 Microsoft Visual C++ 2015 재배포 가능 패키지(x86 및 x64)를 설치합니다.

노트:

Windows 7 및 Windows 8.1의 경우 Windows Updates를 사용하여 컴퓨터를 최신 상태로 유지해야 합니다. 자세한 내용은 https://support.microsoft.com/en-us/help/2919355 및 https://support.microsoft.com/en-us/help/2999226을 참조하십시오.

Data Guardian에는 Microsoft .Net 4.5.2 이상이 필요합니다. Dell에서 배송된 모든 컴퓨터에는 .Net 4.5.2가 미리 설치되어 있습니다. 하지만 Dell 하드웨어를 설치하지 않거나 이전 Dell 하드웨어에서 Data Guardian을 업그레이드하는 경우에는 Data Guardian을 설치하기 전에 어떤 버전의 .Net이 설치되어 있는지 확인한 후, 필요에 따라 버전을 업데이트해야만 설치 및 업그레이드에 따른 문제를 방지할 수 있습니다. 설치되어 있는 .Net의 버전을 확인하려면 설치하고자 하는 컴퓨터에서 다음 지침을 따르십시오. http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx Microsoft .Net Framework 4.5.2를 설치하려면 https://www.microsoft.com/en-us/download/details.aspx?id=42643로 이동하십시오.

하드웨어

최소 하드웨어 요구 사항은 운영 체제의 최소 사양을 충족시켜야 합니다. 다음 표에 Windows 클라이언트를 사용할 수 있도록 지원되는 하드웨어가 나와 있습니다.

Windows 하드웨어

- 200MB의 사용 가능한 디스크 공간(운영 체제에 따라 다름)
- 10/100/1000 또는 Wi-Fi 네트워크 인터페이스 카드
- 설치 및 등록된 TCP/IP

엔터프라이즈에서 클라우드에 저장하기 위해 데이터를 암호화할 경우 디스크 드라이브에 할당할 수 있는 영문자 1개가 컴퓨터에 있어야 합니다.

운영 체제

다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제(32비트 및 64비트)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro 버전 1607(Anniversary Update/Redstone 1) - 버전 1803(Spring Creators Update/Redstone 4)

노트:

클라이언트가 이러한 운영 체제 중 하나가 아니면 차단됩니다. 필요한 경우 레지스트리 키를 설정하면 관리자가 차단을 재정의할 수 있습니다.

Redstone 4 지원의 경우 운영 체제를 업그레이드하기 전에 에이전트를 업그레이드해야 합니다.

노트:

Data Guardian은 Redstone 3 이상 버전의 Microsoft WDEG(Windows Defender Exploit Guard) 또는 Redstone 2 이하 버전의 EMET(Enhanced Mitigation Experience Toolkit)와 호환되지 않습니다.

Windows 7은 Data Guardian 감사 이벤트에 대한 지리 위치 정책과 함께 지원되지 않습니다.

Data Guardian은 한 대의 컴퓨터에 여러 버전의 Office를 지원하지 않습니다.

클라우드 스토리지 제공업체

다음 표에는 Windows용 Data Guardian에서 지원되는 클라우드 스토리지 공급자가 자세히 설명되어 있습니다. 클라우드 스토리지 공급자 업데이트는 자주 릴리스됩니다. 새 버전을 프로덕션 환경에 도입하기 전에 Data Guardian에서 테스트할 것을 권장합니다.

클라우드 스토리지 제공업체

- Dropbox
- Dropbox for Business(Windows 전용)

  노트:
  사용자의 회사에서 사용하는 Dell Server 버전에 따라, 업무 계정과 연결된 개인 Dropbox 계정 내의 모든 파일과 폴더가 암호화될 수 있습니다.

- Box

  노트:
  Box Tools 및 Box Edit는 Data Guardian에서 지원되지 않습니다. Box Tools를 사용하면 블루 스크린 상태가 발생할 수 있습니다.

- Google Drive

  노트:
  Google 백업 및 동기화가 지원되지 않습니다.

- OneDrive
- OneDrive for Business
- 통합 OneDrive

  노트:
  통합 OneDrive는 OneDrive 및 OneDrive for Business 모두를 위한 통합 동기화 클라이언트입니다.

Microsoft Office

Data Guardian은 다음과 같은 버전의 Office를 지원합니다. 그러나 Office 중 하나의 버전만 설치되어 있어야 합니다.

Microsoft Office

- Office 2010 SP2
- Office 2013 SP1
- Office 2016
- Office 365 ProPlus: 지연된 1705, 연 2회의 1708, 월간 1803

Mac용 Data Guardian

다음 목록에는 Mac 클라이언트를 사용할 수 있도록 지원되는 하드웨어가 나와 있습니다.

MAC 하드웨어

- Intel Core 2 Duo, Core i3, Core i5, Core i7 또는 Xeon 프로세서
- 2GB RAM
- 10GB의 사용 가능한 디스크 공간

운영 체제

다음 목록에 지원되는 운영 체제가 나와 있습니다.

Mac 운영 체제

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

클라우드 스토리지 제공업체

정책 설정에 따라 Mac 인터페이스용 Data Guardian에 다음이 표시될 수 있습니다. 사용자가 클라우드 동기화 클라이언트를 다운로드하거나 설치할 필요가 없습니다.

클라우드 스토리지 제공업체

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

모바일 애플리케이션용 Data Guardian

다음은 모바일용 Data Guardian에서 지원되는 운영 체제 목록입니다.

Android 운영 체제

- 4.4-4.4.4 KitKat
- 5.0-5.1.1 Lollipop

- 6.0-6.0.1 Marshmallow
- 7.0-7.1.2 Nougat
- 8.0-8.1 Oreo

iOS 운영 체제

- iOS 9.x
- iOS 10.x-10.3
- iOS 11-11.3

웹용 Data Guardian

Data Guardian 웹 클라이언트를 활성화하기 위해 관리자는 웹 클라이언트를 호스팅하고 Dell Server v9.8 이상과 통신하는 가상 컴퓨터를 설정합니다 .

다음 가상화된 환경을 사용하여 Data Guardian 웹 클라이언트를 배포할 수 있습니다.

가상 환경

- VMware ESXi 6.0
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-60/index.jsp를 참조하십시오.
- VMware ESXi 5.5
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-55/index.jsp를 참조하십시오.

웹 브라우저

Internet Explorer, Mozilla Firefox, Google Chrome 및 Microsoft Edge에서 Data Guardian을 사용할 수 있습니다.

Mac의 경우 Safari도 지원됩니다.

언어 지원

이 클라이언트는 MUI(다국어 사용자 인터페이스)와 호환되며 다음 언어를 지원합니다.

언어 지원

- EN - 영어
- ES - 스페인어
- FR - 프랑스어
- IT - 이탈리아어
- DE - 독일어
- JA - 일본어
- KO - 한국어
- PT-BR - 포르투갈어, 브라질
- PT-PT - 포르투갈어, 포르투갈(이베리아)

3

Windows에 Data Guardian 구성 및 설치

Data Guardian 클라이언트 레지스트리 설정

이 섹션에서는 레지스트리 설정 이유와 관계 없이 로컬 클라이언트 컴퓨터에 대해 Dell ProSupport에서 승인한 모든 레지스트리 설정에 대해 자세히 설명합니다. 레지스트리 설정에 두 제품이 겹치면 각 범주에 해당 설정이 나열됩니다.

이러한 레지스트리 변경 작업은 관리자만 수행할 수 있으며 일부 시나리오에서는 적절하지 않거나 작업하지 못할 수도 있습니다.

- 로깅 수준을 높이면 문제 해결에 도움이 될 수 있습니다. 다음 레지스트리 설정을 생성하거나 수정합니다.

  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  "LogVerbosity"=dword:0x1f (31)

  기본적으로 로그인 수준은 0xf (15)로 설정되어 있습니다.

  사용 가능한 값:

  해제=0x0 (0)

  위험=0x1 (1)

  오류=0x3 (3)

  경고=0x7 (7)

  정보=0xf (15)

  디버그=0x1f (31)

- Data Guardian 설치 후 내부 사용자가 자동으로 활성화됩니다. 필요한 경우 레지스트리 설정을 수정하여 자동 활성화를 재정의할 수 있습니다.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  DWORD Value: DisableAutomaticActivation=1

  노트:
  Dell Server에서 도메인의 별칭을 확인할 수도 있습니다. 자동 활성화 문제 해결을 참조하십시오.

Data Guardian용 서버 구성

관리자가 설정한 정책에 따라 Data Guardian은 다음과 같이 데이터를 보호합니다.

- 로컬에 저장되거나, 다양한 방식으로 다른 사용자와 공유되거나, 이동식 미디어에 저장되는 Office 문서. .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf 형식의 Office 문서를 보호할 수 있습니다.
- 클라우드 기반 파일 공유 시스템 - Windows 컴퓨터 또는 모바일 장치는 클라우드 저장소용 데이터를 수집하고 해당 데이터를 암호화한 다음, 암호화된 데이터를 클라우드에 업로드합니다.

엔터프라이즈가 Office 문서 전용, 클라우드 저장소 전용 또는 둘 다와 함께 Data Guardian을 사용하는지 여부를 사용자에게 알립니다.

Data Guardian용 Dell Security Management Server Virtual 구성

Data Guardian을 지원하도록 Security Management Server Virtual을 구성하려면 Management Console에서 Data Guardian 정책 하나 또는 둘 다를 **켜기**로 설정하십시오.

- *보호된 Office 문서* - 엔터프라이즈 수준만
- *클라우드 암호화* - 엔터프라이즈, 엔드포인트 그룹 또는 엔드포인트 수준

Data Guardian용 Dell Security Management Server 구성

Data Guardian을 지원하도록 Dell Security Management Server 구성하려면 Management Console에서 Data Guardian 정책 하나 또는 둘 다를 **설정**하십시오.

- *보호된 Office 문서* - 엔터프라이즈 수준만
- *클라우드 암호화* - 엔터프라이즈, 엔드포인트 그룹 또는 엔드포인트 수준

그런 다음 클라우드 클라이언트 다운로드를 허용하도록 Security Server를 구성합니다.

Data Guardian 다운로드를 허용하도록 Security Management Server 구성

이 섹션에는 사용자가 Security Management Server에서 Windows 클라이언트 Data Guardian을 다운로드할 수 있도록 허용하는 데 필요한 단계가 나와 있습니다.

1 Security Management Server에서 *<Security Server 설치 디렉토리>\webapps\root\cloudweb\brand\dell\resources*로 이동하고 텍스트 편집기를 사용해 *messages.properties* 파일을 엽니다.

2 항목이 다음과 같은지 확인하십시오.

```
download.deviceWin.mode=remote

download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe
```

3 항목을 다음으로 편집합니다.

```
download.deviceWin.remote.link.32=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_64bit_setup.exe
```

4 파일을 저장하고 닫습니다.

5 <Security Server 설치 디렉터리>로 이동한 다음 그 아래에 새 폴더를 만들고 이름을 Download로 지정합니다(Security Server\Download).

6 Download 폴더 안에 새 폴더를 만들고 이름을 cloudweb으로 지정합니다(Security Server\Download\cloudweb).

7 Data Guardian의 64비트 및 32비트 설치 파일을 cloudweb 폴더에 추가하고 이름을 각각 DataGuardian64.exe 및 DataGuardian32.exe로 바꿉니다.

이는 사용자가 정의하지만 versions.xml 파일의 파일명과 일치해야 합니다.

8 변경사항을 적용하려면 Security Server를 다시 시작하십시오.

Windows Data Guardian 클라이언트의 자동 다운로드를 위해 Security Management Server 구성(선택 사항)

자동 다운로드의 경우 versions.xml 파일과 이진 파일이 같은 위치에 있어야 합니다. 위치는 클라이언트가 액세스할 수 있어야 하므로 IIS가 될 수도 있고 사용자가 만든 **Security Server\Download\cloudweb** 폴더를 사용할 수도 있습니다. 클라우드 웹 폴더를 사용하는 경우에는 이 샘플 구성을 따르십시오.

1 **Security Server\Download\cloudweb** 폴더로 이동합니다. Data Guardian 클라이언트 다운로드를 허용하도록 보안 서버 구성의 6단계를 참조하십시오.
2 명명된 DataGuardianUpdate 아래에 폴더를 만듭니다.

> **노트:**
> 이 예에서는 DataGuardianUpdate를 사용했지만 사용자가 원하는 대로 다른 이름을 선택할 수 있습니다.

3 업데이트한 실행 파일을 DataGuardianUpdate 폴더에 저장합니다.
4 DataGuardianUpdate 폴더에 *versions.xml* 파일을 만듭니다.
5 텍스트 편집기를 사용해 *versions.xml*을 열고 파일 이름 경로가 환경에 맞는지 확인합니다.
예:

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

버전: 업데이트된 실행 파일의 파일 버전

setup.exe 파일 이름: 실행 파일의 설정 이름은 사용자가 정의하지만 messages.properties 파일의 설정 이름과 일치해야 합니다. Data Guardian 클라이언트 다운로드를 허용하도록 보안 서버 구성의 3단계를 참조하십시오.

6 파일을 저장하고 닫습니다.
7 이 폴더에 이진 파일을 추가합니다.
8 IIS를 사용하는 경우 IIS를 재시작합니다.
9 Dell 관리자 계정으로 Management Console에 로그인합니다.
10 왼쪽 창에서 **채우기** > **엔터프라이즈** 키 클릭하면 보안 정책 탭이 표시됩니다.
11 Data Guardian 기술 그룹에서 **클라우드 암호화** > **고급 설정 표시**를 클릭합니다.
12 *소프트웨어 업데이트 서버 URL* 정책으로 스크롤하고 **https://<YOUR HOST URL>/DataGuardianUpdate**를 입력합니다.

> **노트:**
> 위 예와 일치하는 예는 DataGuardianUpdate뿐입니다.

13 **저장**을 클릭하여 대기열에서 커밋할 정책 수정 사항을 저장합니다.
14 **관리** > **커밋**을 클릭합니다.
15 설명을 입력하고 **정책 커밋**을 클릭합니다.

Data Guardian이 설치된 컴퓨터에 이미지 재설치

컴퓨터에 이미지를 재설치해야 하고 Data Guardian이 설치된 경우, 사용자가 오프라인으로 작업했는지, 그리고 오프라인 상태에서 보호된 Office 문서를 만들었는지 확인하십시오. 그렇다면 해당 문서에 대한 오프라인 키가 생성되었으며 해당 키는 Dell Server에 에스크로되지 않았습니다

1 Dell Server에 에스크로되지 않은 Data Guardian 오프라인 생성 키를 복구하는 방법에 대한 자세한 내용은 *복구 가이드*를 참조하십시오.
2 컴퓨터의 이미지를 재설치하기 전에 오프라인 키 폴더를 확인하십시오.

첫 번째 에스크로 키가 생성되면 Data Guardian 폴더가 C:\Program Files\Dell에 추가됩니다. Data Guardian > OfflineKeys 폴더로 이동합니다. OfflineKeys 폴더가 없는 경우 사용자의 내 문서 폴더를 확인합니다.

관리 응용 프로그램용 Microsoft Exploit Guard 또는 EMET 비활성화

Windows 10에서는 다음 기능이 활성화되어 있거나 OS에 내장되어 있을 수 있습니다.

- Redstone 3 이상 - WDEG(Windows Defender Exploit Guard)
- Redstone 2 이하 - EMET(Enhanced Mitigation Experience Toolkit)

이러한 기능이 활성화되어 있거나 내장되어 있는 경우 Data Guardian용 관리 응용 프로그램이 비활성화되도록 구성해야 합니다.

- winword.exe
- powerpnt.exe
- excel.exe
- acrord32.exe

WDEG(Windows Defender Exploit Guard)

관리 응용 프로그램을 비활성화하려면 다음을 수행합니다.

1 **Windows Defender 보안 센터**로 이동합니다.
2 **앱 및 브라우저 컨트롤**을 클릭합니다.
3 화면 하단으로 스크롤하고 **악용 방지 설정**을 클릭합니다.
4 **프로그램 설정**을 선택합니다.
5 **+**를 클릭하여 위에 나열된 각각의 관리 응용 프로그램을 추가합니다.
6 각각의 관리 응용 프로그램 속성에서 *실행*로 설정되어 있는 옵션에 해당하는 *무효화* 확인란을 선택한 다음 옵션을 **해제**로 전환합니다.

> **노트:**
> 관리 응용 프로그램이 열린 상태에서 .exe를 재시작해야 한다는 대화 상자가 표시되면 다음 단계를 완료한 후 재시작합니다.

7 **적용**을 클릭합니다.
8 **예**를 클릭합니다.
변경한 옵션에 따라 관리 응용 프로그램이 프로그램 설정에 무효화 사항을 나열합니다.

EMET(Enhanced Mitigation Experience Toolkit)

관리 응용 프로그램을 비활성화하려면 다음을 수행합니다.

1 **응용 프로그램 구성**으로 이동합니다.
2 **ROP Caller Check** 및 **EAF(Export Address Table Address Filter)** 옵션에서 위에 나열된 관리 응용 프로그램에 해당하는 확인란의 선택을 취소합니다.

Cloud Storage Protection Provider 프로필 관리

Data Guardian은 사용자의 파일을 암호화하여 Dell Server에 감사 이벤트를 보냅니다. 지원되는 각 클라우드 스토리지 공급자에 대한 동작을 변경하려면 각 공급자를 다음 값 중 하나로 설정합니다.

값	설명
보호	공급자/연결을 허용하고, 파일을 암호화하고, 파일/폴더 작업에 관한 감사 이벤트를 보냅니다.
차단	공급자/연결에 대한 모든 액세스를 차단합니다.
허용	공급자/연결에서 암호화는 수행하지 않되 파일/폴더 감사를 수행하고 통과하도록 허용합니다.
무시	암호화나 감사 없이 공급자/연결 보호를 무시합니다. 이 값을 설정하면 클라우드 스토리지 공급자 폴더가 클라이언트 컴퓨터의 Data Guardian 가상 드라이브에 표시되지 않습니다.

자세한 내용은 Dell Server의 Remote Management Console에서 액세스할 수 있는 *관리자 도움말*을 참조하십시오.

전체 액세스 목록/블랙리스트에서 사용자 허용/거부

Data Guardian을 사용하기 위해 Dell Server에 등록할 수 있는 외부 사용자를 결정할 수 있습니다. 적절한 보안을 위해서는 이 목록을 설정하고 관리할 때 주의해야 합니다.

- 내부 사용자는 도메인 내에 있습니다.
- 외부 사용자는 비도메인 사용자로서, 내부 사용자가 업무용 문서를 공유하려는 다른 조직의 사용자이거나 비도메인 장치에서 자신의 컴퓨터에 액세스하려는 내부 사용자입니다.

조직 도메인에 속하지 않은 사용자가 Data Guardian을 사용할 수 있도록 등록을 허용하려면 다음을 수행하십시오.

1 Remote Management Console의 왼쪽 창에서 **관리 > 외부 사용자 관리**를 클릭합니다.
2 **추가**를 클릭합니다.
3 등록 액세스 유형 선택:

   블랙리스트 - 사용자 또는 도메인에 대한 등록을 차단합니다. 사용자가 보호된 Office 문서 또는 .xen 파일을 열 수 없습니다.

   전체 액세스 목록 - 사용자 또는 도메인에 대한 등록과 모든 파일 액세스를 허용합니다. 사용자나 도메인도 블랙리스트에 있는 경우 액세스가 허용되지 않습니다.
4 도메인/이메일 입력 필드에서 전체 도메인에 대한 액세스를 설정하려면 사용자의 도메인을 입력하고, 해당 사용자에 대한 액세스만 설정하려면 이메일 주소를 입력합니다.

   노트: 호스팅된 환경의 외부 모바일 사용자의 경우, 이메일이 소문자여야 합니다.
5 **추가**를 클릭합니다.

전체 액세스 목록/블랙리스트 사용에 대한 자세한 내용은 Management Console에서 액세스할 수 있는 *관리자 도움말*을 참조하십시오.

Data Guardian 설치

Data Guardian을 설치하는 두 가지 방법은 다음과 같습니다.

- Data Guardian을 대화형으로 설치
- 명령줄을 사용하여 Data Guardian 설치

Data Guardian 사용자가 다음 작업을 수행해야만 클라우드 동기화 클라이언트에서 파일 및 폴더가 보호됩니다. Data Guardian 클라이언트를 설치한 후 사용자가 클라우드 스토리지 공급자를 다운로드해야 합니다.

- 관리자는 사용할 클라우드 동기화 공급자를 지정해야 합니다.

  또는

- 조직에서 Dropbox for Business 또는 OneDrive for Business/Unified OneDrive 공급자 중 하나를 사용하는 경우에는 이를 다운로드하여 설치할 수 있는 링크를 제공합니다. Dropbox for Business 사용자는 Data Guardian을 통해 Dropbox for Business에 연결해야 합니다.

암호화되지 않은 파일이 담겨 있는 기존 폴더

Data Guardian을 배포하기 전에 대상 장치에 클라우드 저장소 공급자 계정이 아직 설정되지 않은 상태가 가장 좋습니다.

Data Guardian 설치 전에 로컬 컴퓨터와 동기화된 폴더를 사용하여 클라우드 저장소 공급자 계정이 설정된 경우:

- 클라우드로 동기화되는 기존의 파일 및 폴더는 일반 텍스트를 유지합니다.
- 이러한 기존 폴더에 추가하는 파일도 일반 텍스트를 유지합니다.
- 클라우드로부터 동기화되는 파일은 암호화됩니다.

  기존 파일을 암호화할 경우 DDG VDisk 가상 드라이브(Data Guardian이 설치될 때 생성됨)로 이동하고, 클라우드 동기화 클라이언트 내에 새 하위 폴더를 생성한 다음, 기존 파일을 해당 폴더로 이동합니다.

  또는

  콘텐츠가 큰 경우에는 관리자가 임시로 폴더 메뉴 관리를 요청할 수 있습니다.

폴더 메뉴 관리

임시로 일부 관리자가 둘 이상의 사용자가 공유하는 폴더에 대한 문제를 해결해야 할 수 있습니다. 관리자에게 폴더 관리 옵션에 대한 권한을 요청할 수 있습니다. 대개 이 옵션은 임시 옵션입니다.

Windows에서의 Data Guardian 대화형 설치

Data Guardian을 설치하려면 로컬 관리자여야 합니다. 사용자가 제품을 설치할 경우에는 사용자에게 설치 미디어의 위치를 알려주십시오.

시작하기 전에

서버 및 Data Guardian 제품에 따라 다음을 수행하십시오.

호스팅된 Dell 보안 센터	사내 환경(Dell Management Server용)	클라우드 암호화
향후 출시 예정	반드시 Dell Security Management Server의 이름을 알고 있어야 합니다.	컴퓨터에는 디스크 드라이브에 할당할 수 있는 영문자 하나가 있어야 합니다.

Data Guardian 설치

Data Guardian이 설치된 후에 컴퓨터를 다시 시작하기 위해 준비합니다.

1. Data Guardian 설치 프로그램을 다운로드하려면 관리자가 지정한 위치로 이동하십시오.
2. 운영 체제에 따라 32비트 또는 64비트 설치 프로그램(대개 **setup32.exe** 또는 **setup64.exe**)을 선택하고 로컬 컴퓨터에 복사합니다.
3. 파일을 더블 클릭하여 설치 관리자를 시작합니다.
4. 보안 경고가 표시되면 **실행**을 클릭합니다.
5. 언어를 선택하고 **확인**을 클릭합니다.
6. Microsoft Visual C++ 2015 재배포 가능 패키지 또는 Microsoft .NET Framework 4.5.2 Client Profile을 설치할 것인지 묻는 메시지가 표시되면 **확인**을 클릭합니다.

7 시작 화면에서 **다음**을 클릭합니다.

8 라이센스 계약서를 읽고 조건을 수락한 후 **다음**을 클릭합니다.

9 대상 폴더 화면에서 **다음**을 클릭하여 C:\Program Files\Dell\Data Guardian\의 기본 위치에 설치를 합니다.

C:\의 Users 또는 Windows 폴더나 어떤 드라이브든 루트 폴더에 Data Guardian을 설치하면 안 됩니다. 이렇게 설치하면 오류가 발생합니다.

10 **사내 Dell Management Server** 키를 선택합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
향후 출시 예정	*Dell Management Server 이름:* 필드에서 컴퓨터가 통신하는 서버 이름(예: server.domain.com)을 입력합니다. www 또는 http(s)를 입력할 필요는 없습니다. 이 정보는 관리자가 제공합니다. 관리자가 지시하는 경우를 제외하고 *SSL 신뢰 확인 활성화* 확인란을 선택 해제하지 마십시오.

11 **다음**을 클릭합니다.

12 Dell Management Server 정보 확인 화면에서 서버 URL 주소가 올바른지 확인합니다. 설치 프로그램이 www 또는 http(s)와 포트를 추가합니다. **다음**을 클릭합니다.

13 관리 유형 창에서 이 옵션을 선택합니다.

- 내부 사용 - 회사 도메인 내부에 이메일 주소를 갖고 있는 사용자.

14 **설치**를 클릭하여 설치를 시작합니다.

상태 창에 설치 진행률이 표시됩니다.

15 설치 완료 화면이 표시되면 **마침**을 클릭합니다.

16 다시 시작하려면 **예**를 클릭합니다.

Data Guardian 설치가 완료되었습니다.

17 최종 사용자에게 활성화를 확인하라고 지시합니다. Data Guardian 시스템 트레이 아이콘에 녹색 체크 표시  가 표시됩니다. 엔터프라이즈 내에 Data Guardian이 배포된 방식에 따라 즉각 활성화되지 않을 수도 있습니다. 그렇지 않은 경우 최종 사용자가 수동으로 활성화해야 합니다. 호스팅된 환경에서 수동으로 활성화를 하려는 사용자는 컴퓨터 또는 Data Guardian 서비스를 재시작할 때마다 재활성화를 다시 시작해야 합니다. *Data Guardian User Guide(Data Guardian 사용자 가이드)*를 참조하십시오.

명령줄을 사용하여 Data Guardian 설치

- 명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.
- 명령줄에서 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표로 묶어야 합니다.
- 다음 표에 설치 시 사용할 수 있는 스위치 정보가 나와 있습니다.

스위치	의미
/V	변수를 setup.exe 내의 .msi로 전달합니다. 컨텐츠는 항상 일반 텍스트 따옴표로 묶어야 합니다.
/S	자동 모드

옵션	의미
/QB	**취소** 단추가 있는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/QB!	**취소** 단추가 없는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/QN	사용자 인터페이스 없음

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

매개 변수

SERVER=<ServerName>(활성화할 Dell Server의 FQDN)

ENTERPRISE=1(내부 사용자)

ENABLESSLTRUST=0(SSL 인증서 검증 비활성화)

REBOOT=SUPPRESS(Null은 자동 재부팅을 허용하고, SUPPRESS는 재부팅을 비활성화함)

명령줄의 예

- 다음 예제에서는 내부 사용자용 Data Guardian을 자동으로 설치하며, SSL 인증서 검증은 포함되지 않고, 로그는 C:\Library\Logs\Install.log에 저장합니다.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library\Logs\install.log" ENABLESSLTRUST=0"
```

권한 부여 활성화를 위해 도메인 컨트롤러에서 GPO 설정

- 클라이언트에 Dell Digital Delivery 사용 권한이 부여되는 경우 다음 지침에 따라 도메인 컨트롤러에서 GPO를 설정하여 권한 부여를 사용하도록 설정합니다(Dell Server를 실행하는 서버와 다를 수 있음).
- 워크스테이션은 GPO가 적용된 OU의 구성원이어야 합니다.
- 아웃바운드 포트 443을 사용하여 Dell Server와 통신할 수 있는지 확인하십시오. 어떠한 이유로든 포트 443이 차단된 경우 권한 부여 기능이 작동하지 않습니다.

1. 클라이언트를 관리할 도메인 컨트롤러에서 **시작** > **관리 도구** > **그룹 정책 관리**를 클릭합니다.
2. 정책을 적용해야 하는 OU를 마우스 오른쪽 단추로 클릭하고 **이 도메인에서 GPO 만들기** 및 **여기에 연결...**을 선택합니다.
3. 새 GPO의 이름을 입력하고 원본 스타터 GPO에 대해 (없음)을 선택한 다음 **확인**을 클릭합니다.
4. 생성된 GPO를 마우스 오른쪽 단추로 클릭하고 **편집**을 선택합니다.
5. 그룹 정책 관리 편집기가 로드됩니다. **컴퓨터 구성** > **환경설정** > **Windows 설정** > **레지스트리** 에 액세스합니다.
6. 레지스트리를 마우스 오른쪽 단추로 클릭하고 **새로 만들기** > **레지스트리 항목** 을 선택합니다. 다음 작업을 완료합니다.

   작업: 생성

   하이브: HKEY_LOCAL_MACHINE

   키 경로: SOFTWARE\Dell\Dell Data Protection

   값 이름: Server

   값 유형: REG_SZ

   값 데이터: <Dell Server의 IP 주소>
7. **확인**을 클릭합니다.
8. 워크스테이션에서 로그아웃했다가 다시 로그인하거나 **gpupdate /force**를 실행하여 그룹 정책을 적용합니다.

Data Guardian 제거

- **최종 사용자**에게 로컬 관리자 계정이 있으면 Data Guardian을 직접 설치 제거할 수 있습니다. 자세한 내용은 *Data Guardian 사용 설명서*를 참조하십시오. 이 섹션에서는 Data Guardian 설치 제거를 위한 관리자 프로세스를 설명합니다.

중요: DDG VDisk 가상 드라이브의 비 Office 파일

Data Guardian을 설치 제거하기 전에 모든 중요한 파일을 DDG VDisk 가상 드라이브 외부로 이동하십시오. 최종 사용자의 컴퓨터에서 Data Guardian을 설치 제거하면 해당 클라우드에 있는 폴더와 파일이 암호화되어 읽을 수 없게 됩니다. 이 최종 사용자가 퇴사하고 해당 폴더 또는 파일을 공유하는 사용자가 없는 경우 데이터를 읽을 수 없지만 안전합니다(파일을 보고, Data Guardian을 다시 설치할 수 있음).

보호되는 Office 문서는 Data Guardian을 제거해도 암호화된 상태를 유지합니다. 암호를 해독하려면 *복구 안내서 > Data Guardian 복구*를 참조하십시오.

명령줄 설치 제거

- 마스터 설치 프로그램에서 추출된 후에 Data Guardian 클라이언트 설치 프로그램은 **C:\Dell\DataGuardian_XXbit_setup.exe**에서 찾을 수 있습니다.
- 다음 예에서는 Data Guardian 클라이언트를 자동으로 설치 제거합니다.

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

  메시지가 표시되면 컴퓨터를 재부팅합니다.

Dropbox for Business에서 Data Guardian 사용

Dropbox for Business를 사용하는 Data Guardian은 기본 Dropbox 외에 추가적인 기능을 제공합니다.

업무용 및 개인용 Dropbox 폴더가 보호되는 방법을 제어하는 정책을 설정할 수 있습니다. 회사에서 업무 및 개인 계정을 모두 허용할 경우 최종 사용자는 각 계정 유형의 암호화를 이해해야 합니다. 업무 및 개인 계정을 위한 정책을 참조하십시오.

업무 및 개인 계정을 위한 정책

회사에 팀원이 업무 및 개인 계정 중 어떤 것을 사용할 수 있는지에 대한 지침이 있을 수 있습니다. 또한 회사에서 특정 사용자가 업무 및 개인 계정을 소유하도록 허용할 수도 있습니다.

노트:

회사에서 업무 및 개인 계정을 모두 허용하고 최종 사용자가 둘 다 사용하도록 선택할 경우 사용자는 두 계정 유형의 폴더 관리를 이해하고 있어야 합니다.

다음 표에서는 *Dropbox 개인 폴더 암호화* 정책 설정을 기반으로 한 암호화에 대해 설명합니다.

암호화	정책 설정	배포 고려 사항
모든 업무 및 개인 파일과 폴더를 암호화합니다.	정책 > Dropbox 개인 폴더 암호화 > **선택됨**으로 설정(기본값)	Data Guardian이 배포되기 전에 사용자는 클라우드 스토리지 동기화 폴더에 있는 기존 업무 파일을 동기화 폴더 외부의 위치로 백업해야 합니다. 암호화되지 않은 상태로 유지해야 하는 개인 파일이 있는 사용자는 파일을 업무 동기화 폴더 외부로 이동하거나 업무 동기화 클라이언트에서 개인 계정의 연결을 해제해야 합니다. Data Guardian을 배포한 후에 Data Guardian을 실행하는 컴퓨터나 장치에서만 클라우드 파일과 폴더를 볼 수 있습니다. 개인 폴더가 우발적으로 암호화된 경우에는 Dell

암호화	정책 설정	배포 고려 사항
		Data Guardian 사용 설명서에서 "개인 계정의 폴더 암호 해독"을 참조하십시오.
모든 업무 계정 파일 및 폴더를 암호화합니다. 개인 계정 파일 및 폴더를 암호화하지 않은 상태로 유지하도록 허용합니다.	정책 > Dropbox 개인 폴더 암호화 > **선택되지 않음**으로 설정	선택 사항인 Dropbox 개인 폴더 메시지 암호화 정책을 사용하여 사용자에게 개인 계정에 업무 파일을 **저장하지 말라는** 사용자 지정된 메시지를 표시합니다. 이러한 파일은 보호되지 않기 때문입니다. 이 메시지는 다음과 같은 경우에 표시됩니다. • 사용자가 로그인할 때 • 사용자가 새 파일 또는 폴더를 생성하거나 개인 Dropbox 계정에 추가할 때 끝점 또는 끝점 그룹에 대해 Dropbox 개인 폴더 암호화 정책을 **거짓**으로 설정하면 해당 끝점에 있는 모든 사용자의 개인 계정이 암호화되지 않은 상태로 유지됩니다.

업무 및 개인 폴더

회사에 Dropbox for Business가 있고 최종 사용자가 업무 및 개인 폴더를 소유할 수 있도록 허용할 경우 최종 사용자가 보호되지 않은 중요한 파일을 업무 폴더에 복사할 경우에 대비해 보고서를 실행하여 모든 업무 파일에 .xen 파일 확장자가 있는지 확인해야 할 수도 있습니다. Data Guardian 문제 해결을 참조하십시오.

보고서 보기

Data Guardian 환경에 대한 정보는 Management Console에서 제공됩니다. 클라우드 동기화 클라이언트 폴더 및 보호된 Office 문서와 관련된 감사 이벤트의 경우 **보고 > 감사 이벤트**를 선택합니다.

장치 세부 정보, Shield 세부 정보 또는 감사 이벤트의 규정 준수 및 모니터링 목적에 관해서는 **보고 > 보고서 관리**를 참조하십시오.

자세한 내용은 Management Console에서 액세스할 수 있는 *관리자 도움말*을 참조하십시오.

Data Guardian 문제 해결

세부 정보 화면 사용

세부 정보 화면은 문제 해결이나 지원을 위해 사용할 수 있습니다. 예:

- 사용자가 암호화되지 않은 폴더를 생성할 경우 **세부 정보** > **파일** > **폴더 상태**을 선택하여 상태를 확인합니다.
- 최종 사용자가 지원을 요청할 경우, 고급 세부 정보 화면을 설정하고 **세부 정보** > **정책** 탭을 선택하라고 지시합니다. 이 탭에는 어떤 정책들이 시행되고 있는지 나열되어 있습니다.
- 문제 해결을 위한 로그를 봅니다.

고급 세부 정보 화면 사용

- **<Ctrl><Shift>**를 누른 상태에서 Data Guardian 시스템 트레이 아이콘을 클릭한 후 **세부 정보**를 선택합니다.
- 파일 및 폴더 외에도 다음이 표시됩니다.

보안: 키, 키 유형 및 상태를 나열합니다. 보호된 Office 파일이 Dell Server로 전송 될 때까지 이 창에 일시적으로 나열합니다. 시간은 폴링 간격에 따라 다릅니다.

감사: 모듈, 사용자 ID 및 이벤트 유형을 나열합니다. 정보가 이 감사 로그에서 대기 상태이다가 지정된 간격으로 Dell Server에 전송됩니다. 관리자는 감사의 Remote Management Console의 왼쪽 창에서 **감사 이벤트**를 볼 수 있습니다.

정책: 정책 이름과 값을 나열합니다.

로그 파일 보기

- 세부 정보 화면의 왼쪽 하단에서 **로그 보기**를 클릭합니다.

  로그 파일은 **C:\ProgramData\Dell\Data Guardian**에도 있습니다.

  보호된 Office 문서 로그 파일은 Custom.xml 폴더에 있습니다.

자동 활성화 문제 해결

일부 사용자에 대해 Data Guardian이 자동 활성화되지 않을 경우 Data Guardian 클라이언트 레지스트리 설정을 변경할 수 있습니다. 또한 Dell Server에서 별칭도 확인해야 합니다.

1 Management Console에서 **채우기 > 도메인**으로 이동하고 도메인 및 하위 도메인을 선택합니다.
2 도메인 세부 정보 페이지에서 **설정** 탭을 클릭합니다.
3 *별칭* 필드에서 모든 별칭이 올바른지 확인합니다.

임시 폴더 관리 권한 제공

관리자 또는 사용자에게 폴더를 관리할 수 있는 임시 권한을 부여할 수 있습니다. 예를 들어, Data Guardian을 설치하기 전에 사용자가 클라우드에 파일을 업로드한 경우 일부 사용자에게 임시 폴더 관리 권한을 제공하여 동기화 클라이언트 폴더 내에서 폴더 단위로 암호화를 관리할 수 있습니다.

폴더 관리 권한을 제공하려면 다음을 수행하십시오.

1 Management Console에 **채우기** > **엔드포인트**를 클릭합니다.
2 엔드포인트를 검색 또는 클릭한 다음, **보안 정책** 탭을 클릭합니다
3 **클라우드 암호화**를 선택한 다음, **고급 설정 표시**를 클릭합니다.
4 *폴더 관리 사용* 옆에 있는 확인란을 클릭하여 정책을 선택합니다.
5 **저장**을 클릭합니다.
6 왼쪽 창에서 **관리** > **커밋**을 클릭합니다.
7 설명을 입력하고 **정책 커밋**을 클릭합니다.

노트:
Dell은 폴더가 암호화되거나 문제 해결이 완료된 후 *폴더 관리 사용* 정책 확인란의 선택을 취소하여 해당 엔드포인트에 대한 정책을 비활성화할 것을 권장합니다.

엔드포인트에서 폴더를 관리하려면 다음을 수행하십시오.

1 동기화 클라이언트 폴더 내에 폴더를 만들고 파일을 추가하면 파일이 클라우드에서 암호화됩니다.
2 Data Guardian 시스템 트레이 아이콘을 클릭하고 **폴더 관리**를 선택합니다.

각 동기화 클라이언트에 대해, 클라우드 동기화 폴더의 계층 구조 보기가 표시됩니다. 기본적으로 모든 폴더가 선택되어 있습니다. 암호화하지 않을 폴더의 선택을 취소합니다. 폴더 관리에서 폴더를 선택 해제하면 암호 해독 스윕이 해당 폴더에 있는 기존 파일의 암호를 해독합니다. 해당 폴더의 새 파일은 로컬 드라이브 또는 클라우드에서 암호화되지 않습니다.

노트:
클라우드 또는 Data Guardian 가상 드라이브의 폴더 관리에서 선택 해제된 폴더로 암호화된 파일을 끌어 오면, 파일은 암호화된 상태로 유지되며 내용을 볼 수 없습니다. 폴더 관리 정책을 사용하지 않는 다른 Data Guardian 사용자와 폴더를 공유하면 해당 파일이 다른 사용자에게 암호화된 상태로 표시되므로 내용을 볼 수 없습니다.

3 기존 폴더를 암호화하려면 해당 폴더에 대한 암호화를 수동으로 설정합니다. 파일이 클라우드로 동기화되면 파일이 암호화됩니다.

자주 묻는 질문

폴더 관리 FAQ

질문

한 폴더 안의 파일들을 다른 사용자와 공유하였습니다. 시스템 트레이에서 **Data Guardian > 폴더 관리** 유틸리티를 사용하여 해당 폴더의 내용을 복호화하였습니다. 최근에, 제 파일들이 클라우드 내에서 다시 암호화되었습니다. 그 폴더가 폴더 관리 유틸리티에 더 이상 표시되지 않아서 그 파일들을 클라우드 내에서 더 이상 암호화를 해제할 수가 없습니다.

답변

암호화 키 ID는 특정 폴더에 파일을 추가하는 최초의 사용자에 기초하여 그 폴더와 연결됩니다. 사용자가 폴더를 하나 생성하고 거기에 아무 파일도 추가하지 않는다면, 파일의 키는 그 폴더와 연결되지 않습니다. 폴더에 암호화 키 ID가 설정된 사용자는 폴더 관리 유틸리티에서 폴더를 볼 수 있는 유일한 사용자입니다. 폴더에 암호화 키 ID가 설정된 사용자가 폴더 관리 유틸리티에서 그 폴더의 선택을 해제하고 다른 Data Guardian 사용자와 그 폴더를 공유할 경우, 두 번째 사용자의 Data Guardian이 내용을 다시 암호화할 것입니다.

해결 방법

1 새 폴더를 생성하십시오.

2 암호화해야 할 모든 파일을 새 폴더로 옮기십시오.

3 시스템 트레이에서, **Dell Data Guardian > 폴더 관리** 유틸리티를 다시 사용하여 그 파일들을 복호화합니다.

노트:
다른 Data Guardian 사용자와 공유하는 폴더의 내용을 복호화할 경우, 다른 사용자의 Data Guardian 클라이언트가 그 내용을 암호화하는 정책을 시행할 것입니다. 모범 사례는 폴더 관리 유틸리티를 사용하여 다른 Data Guardian 사용자와 공유하지 않는 파일만 복호화하는 것입니다.

질문

폴더 관리 유틸리티를 사용해 선택을 취소한 복호화된 폴더에 동기화하려고 합니다. 그런데 웹 브라우저를 통해 이것을 업로드하려고 시도하면 암호화된 파일밖에 업로드할 수가 없습니다.

답변

Data Guardian은 클라우드 내에서 폴더를 능동적으로 검색하도록 설계되어 있지 않습니다. 암호화가 해제된 폴더의 경우, Data Guardian이 동기화 클라이언트를 통해 동기화를 할 수 있습니다. 왜냐하면 Data Guardian이 그 환경을 제어하고 있기 때문입니다. 웹 브라우저를 통과하는 파일들은 암호화되어야 합니다.

해결 방법

파일을 동기화 폴더에 추가하십시오.

질문

최근에 컴퓨터에서 클라우드 기반 파일 공유 시스템을 설치 제거했는데 "폴더 관리" 유틸리티를 열어보니 동기화 클라이언트 중 하나가 여전히 옵션 있었습니다.

답변

Data Guardian은 타사 소프트웨어의 설치 또는 삭제 여부를 모니터링하지 않습니다. 이들 옵션이 여전히 목록에 존재하는 이유는 설계상, 이들 클라이언트가 삭제될 때 사용자의 기존 파일들을 삭제하지 않기 때문입니다. 이 파일들은 동기화 클라이언트가 더 이상 설치되어 있지 않더라도 Data Guardian에 의해 여전히 보호됩니다.

해결 방법

폴더 관리 유틸리티에서 제거된 동기화 클라이언트 옵션을 제거하려면 동기화 폴더에서 제외할 모든 폴더/파일을 이동한 다음 폴더를 삭제하십시오. 폴더를 삭제하고 나면 해당 폴더가 폴더 관리 유틸리티에 더 이상 나열되지 않습니다.

기타 자주 묻는 질문

질문

사용자가 보호된 Office 문서가 있는 Data Guardian을 갖고 있으므로 복사하거나 붙여 넣을 수 없습니다.

답변

Data Guardian의 경우 일부 기능은 systray를 통해 처리됩니다. 사용자가 systray를 수정했는지 여부를 확인합니다.

해결 방법

기본 systray 설정을 사용해야 합니다. 사용자는 기본 systray 설정을 유지해야 합니다.

질문

파일 이름 난독화 정책을 GUID에서 확장자만으로 변경했습니다. 그런데 이전에 동기화하던 폴더가 여전히 이러한 파일을 GUID 파일 이름의 다른 형식으로 암호화하고 있습니다. 그 이유는 무엇입니까?

답변

Security Management Server/Security Management Server Virtual에서 정책이 변경되어도 Data Guardian은 여전히 해당 폴더에 이전 정책을 유지합니다. 생성된 새 폴더에 새 정책이 적용되며 이 폴더는 **확장자만** 형식으로 암호화됩니다.

해결 방법

확장자만 형식을 이전 파일에 다시 적용하려면 이전 파일을 잘라내고 새 정책이 적용된 새 폴더에 붙여넣으십시오.

4

Mac에 Data Guardian 구성 및 설치

Mac용 Data Guardian은 클라우드 암호화 제공업체 내에서 파일을 공유하도록 설계되어 있습니다. 그러나 Mac에서 보호된 Office 문서 정책을 사용하는 경우 파일을 최종 사용자가 로컬 Mac에 저장하면 모든 파일 감사 및 추적 기능이 손실됩니다. 조직에서 엄격한 파일 감사 및 추적 기능이 필요한 경우 Mac에서 Data Guardian이 활성화되지 않도록 *Mac Data Guardian 활성화 허용* 정책을 **선택하지 않음**으로 설정하십시오.

서버 작업

사전 요구 사항

이러한 작업을 수행하기 전에 다음을 확인합니다.

- Dell Server 및 해당 구성 요소를 설치합니다. 다음 섹션 중 하나 참조:
  - *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)*
- Management Console에서 적절한 Dell 관리자 역할을 할당합니다.

정책

기본적으로 Data Guardian은 사용자의 파일을 암호화하여 Security Management Server Virtual에 감사 이벤트를 보냅니다. 이 문서의 목적에 알맞게 양쪽 서버가 특정 버전을 언급해야 할 경우(예: Security Management Server Virtual 사용 시 다른 절차 적용)를 제외하고 'Dell Server'로 지칭됩니다.

지리 위치 데이터를 감사 이벤트에 포함하려면 Wifi를 활성화해야 합니다. 지리 위치 및 감사 이벤트에 대한 자세한 내용은 *관리자 도움말*을 참조하십시오.

지원되는 각 클라우드 스토리지 제공업체에 대한 기본 동작을 변경하려면 *클라우드 스토리지 보호 제공업체* 정책을 설정합니다. 기업에서 특정 클라우드 스토리지 제공업체를 선호하는 경우 다른 제공업체에 대해 이 정책을 **차단**으로 설정합니다. 정책에 대한 자세한 내용은 Management Console에서 액세스할 수 있는 *관리자 도움말*을 참조하십시오.

노트:
이 정책의 무시 옵션은 Windows용입니다. Mac에 대해 무시를 선택할 경우 최종 사용자에게는 허용으로 표시됩니다.

클라우드 클라이언트 다운로드를 허용하도록 보안 서버 설정

이러한 작업을 수행하기 전에 다음을 확인합니다.

- Dell Server 및 해당 구성 요소를 설치합니다. 다음 섹션 중 하나 참조:
  - *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)*
- Management Console에서 적절한 Dell 관리자 역할을 할당합니다.

Security Management Server

1 Security Management Server에서 <Security Server 설치 디렉터리>\webapps\cloudweb\brand\dell\resources\로 이동합니다.
2 텍스트 편집기를 사용하여 **messages.properties** 파일을 엽니다.
3 항목이 다음과 같은지 확인하십시오.
로컬 설치의 경우:

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

원격 설치의 경우:

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

4 파일을 저장하고 닫습니다.
5 <Security Server 설치 디렉터리>로 이동한 다음 새 폴더를 만들고 이름을 Download로 지정합니다(Security Server\Download).
6 Download 폴더 내에서, CloudWeb 폴더(Security Server\Download\CloudWeb)를 만듭니다.
7 Dell Data Guardian 설치 프로그램을 해당 폴더에 추가합니다.

Virtual Edition: 다른 클라우드 클라이언트 버전을 수동으로 설치

사용자가 최신 Dell Data Guardian 설치 프로그램을 다운로드할 수 있도록 허용하는 데 작업이 필요하지 않습니다. 최신 설치 프로그램이 Security Management Server Virtual .보안 서버에 사전 설치되어 있습니다.

Security Management Server Virtual 보안 서버에 다른 Data Guardian 설치 프로그램 버전을 수동으로 설치하려면 message.properties 파일을 업데이트합니다.

1 다음으로 이동합니다.
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 텍스트 편집기를 사용하여 **messages.properties** 파일을 엽니다.
로컬 설치의 경우:

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

원격 설치의 경우:

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

3 파일을 저장하고 닫습니다.
4 파일을 /opt/dell/server/security-server/download/cloudweb에 복사합니다.
5 Data Guardian 설치 프로그램을 해당 폴더에 추가합니다.

전체 액세스 목록/블랙리스트에서 사용자 허용/거부

전체 액세스 목록과 블랙리스트 항목에서 Data Guardian을 사용하도록 Dell Server에 등록할 수 있는 사용자를 결정합니다.

전체 액세스 목록

전체 액세스 목록에서는 특정 사용자나 사용자 그룹이 Dell Server에 등록하고 Data Guardian을 사용할 수 있도록 허용합니다.

등록을 허용하려면 외부 사용자를 전체 액세스 목록에 배치해야 합니다. 사용자 등록을 허용하려면 다음 예제를 참조하십시오.

사용자 유형	Enter
모든 organization.com 이메일 주소	`organization.com`
특정 사용자	`jdoe@organization.com`
모든 Gmail 사용자	`gmail.com`

블랙리스트

블랙리스트는 특정 사용자 또는 사용자 그룹이 Data Guardian을 사용하여 Dell Server에 등록하지 못하도록 합니다. 블랙리스트에 이메일 주소가 입력된 사용자는 Data Guardian에 등록할 수 없다는 메시지를 받습니다.

노트:
사용자가 이미 등록된 경우 이 목록은 사용자가 Data Guardian을 사용하는 것을 금지하지 **않습니다.**

블랙리스트를 사용하여 전체 액세스 목록에 승인되어 있는 특정 사용자를 제외할 수 있습니다. 또한 와일드카드(*)를 사용하면 전체 도메인이 블랙리스트에 등록되므로 해당 도메인에 이메일 주소가 있는 사용자가 등록하지 못합니다. 사용자 또는 그룹이 Dell Server에 등록하지 못하도록 하려면 다음 예제를 참조하십시오.

사용자 유형	Enter
모든 organization.com 이메일 주소	`organization.com`
특정 사용자 및 해당 이메일 주소	`jdoe@organization.com`
모든 Gmail 사용자	`gmail.com`

전체 액세스 목록/블랙리스트를 수정하려면 다음 지침을 따르십시오.

1 Remote Management Console의 왼쪽 창에서 **관리 > 외부 사용자 관리**를 클릭합니다.
2 **추가**를 클릭합니다.
3 등록 액세스 유형 선택:

블랙리스트 - 사용자 또는 도메인에 대한 등록을 차단합니다. 사용자가 보호된 Office 문서 또는 .xen 파일을 열 수 없습니다.

전체 액세스 목록 - 사용자 또는 도메인에 대한 등록과 모든 파일 액세스를 허용합니다. 사용자나 도메인도 블랙리스트에 있는 경우 액세스가 허용되지 않습니다.

4 도메인/이메일 입력 필드에서 전체 도메인에 대한 액세스를 설정하려면 사용자의 도메인을 입력하고, 해당 사용자에 대한 액세스만 설정하려면 이메일 주소를 입력합니다.
5 **추가**를 클릭합니다.

전체 액세스 목록/블랙리스트 사용에 대한 자세한 내용은 Dell Server Remote Management Console에서 액세스할 수 있는 *관리자 도움말*을 참조하십시오.

외부 사용자는 내부 사용자로부터 보호된 파일의 키에 대한 액세스를 요청할 수 있습니다. 내부 사용자를 사용할 수 없는 경우 Remote Management Console을 사용하여 액세스를 승인 또는 거부할 수 있습니다.

1 **관리 > 키 요청 관리**를 선택합니다.
2 자세한 내용을 보려면 **?** (도움말)을 선택하십시오.

클라이언트 작업

필수 구성 요소

- 대상 장치가 다음에 연결되어 있는지 확인합니다.
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- 설치를 수행하는 사용자에게 설치를 위한 로컬 관리자 계정이 있는지 확인합니다.
- 명령줄을 사용하여 설치할 경우 사용자가 정품 인증할 보안 서버의 정규화된 도메인 이름을 사용하고 있는지 확인합니다.

모범 사례

배포 중에 IT 모범 사례를 따릅니다. 여기에는 다음이 포함되지만, 이에 제한되지 않습니다.

- 초기 검사를 위한 제어된 테스트 환경
- 사용자에게 시차를 둔 배포

클라이언트 설치

현재 허용 목록에 추가된 사용자는 https://yoursecurityservername.domain.com:8443/cloudweb/register에서 등록할 수 있습니다.

등록 후 사용자는 해당 클라이언트에 로그인하여 다운로드하도록 https://yoursecurityservername.domain.com:8443/cloudweb으로 안내하는 이메일을 받습니다.

일반적으로 최종 사용자는 등록 후 https://yoursecurityservername.domain.com:8443/cloudweb에서 직접 Mac 클라이언트를 설치합니다. 관리자의 Mac 클라이언트 설치는 선택 사항입니다.

그러나 조직에서 요구하면 Mac 클라이언트를 설치할 수 있습니다 Data Guardian 클라이언트는 각 조직에 지원되는 푸시 기술을 사용하여 명령줄로 설치하거나 사용자 인터페이스로 설치할 수 있습니다. 최종 사용자에 의한 등록 및 활성화는 모두 필요합니다.

Cloud Edition의 이전 버전에서 업그레이드

기업에 이전 버전의 Cloud Edition이 있고 Data Guardian으로 업그레이드한 경우 이전 버전의 Cloud Edition은 제거됩니다.

노트:
기업이 Cloud Edition에서 Data Guardian으로 업그레이드하는 경우, 사용자는 Data Guardian을 인증하고 클라우드 스토리지 제공업체와 다시 연결해야 합니다. 인증에 대한 자세한 내용은 온라인 Dell Data Guardian 도움말을 참조하십시오.

설치 옵션

클라이언트를 설치/업그레이드하려면, 다음 중 하나를 선택합니다.

- 대화형 설치 - Mac용 Data Guardian을 가장 쉽게 설치할 수 있는 방법입니다. 그러나 한 번에 한 컴퓨터에만 클라이언트를 설치하려는 경우에만 이 방법을 사용하십시오.

  또는
- 명령줄 설치 - 이 고급 설치 방법의 경우 관리자가 명령줄 구문을 숙지해야 합니다. 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 통한 스크립팅된 설치에 이 방법을 사용할 수 있습니다.

대화형 설치

1 Data Guardian 클라이언트의 경우 **Dell-Data-Guardian--0.x.x.xxxx.dmg**에서 설치 프로그램을 찾습니다.
2 DDPSL-Explorer-0.x.x.xxxx.dmg 내의 **.pkg** 파일을 사용하여 설치 또는 업그레이드합니다. 스크립팅된 설치, 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 사용할 수 있습니다.
3 **Dell-Data-Guardian-x.x.x** 패키지를 두 번 클릭합니다.
4 **계속**을 클릭합니다.
5 소개 창에서 **계속**을 클릭합니다.
6 소프트웨어 라이센스 계약 창에서 **계속**을 클릭합니다.
7 계속하려면 **동의**를 클릭합니다.
8 구성 유형 창에서 **사내 Dell Management Server** 키를 선택합니다.

노트:
호스팅된 Dell Security Center는 향후 버전에서 출시될 예정입니다.

9 설치 유형 창에서 다음 중 하나를 수행합니다.
- **설치**를 클릭한 다음 9단계로 이동합니다.
- **설치 위치 변경**을 클릭합니다.
  1 대상 선택 창에서 모든 사용자 또는 단일 사용자를 선택합니다.
  2 **계속**을 클릭합니다.
  3 **설치**를 클릭한 다음 9단계로 이동합니다.

10 대화 상자에서 사용자 이름 및 암호를 입력하고 **소프트웨어 설치**를 클릭합니다.
11 요약 창에 **닫기**를 클릭합니다.
12 최종 사용자 활성화를 참조하십시오.

노트:
기업이 Cloud Edition에서 Data Guardian으로 업그레이드하는 경우, 사용자는 Data Guardian을 인증하고 클라우드 스토리지 제공업체와 다시 연결해야 합니다. 인증에 대한 자세한 내용은 온라인 Dell Data Guardian 도움말을 참조하십시오.

13 Finder를 열려면 .dmg 창을 닫습니다.

명령줄 설치

1 . dmg를 마운트합니다.
2 다음과 같은 설치 프로그램 명령을 사용하여 패키지의 명령줄 설치를 수행합니다.

```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```

3 사용자에게 Data Guardian을 활성화하도록 지시합니다. 최종 사용자 활성화를 참조하십시오.

최종 사용자 활성화

Mac에서 Dell Data Guardian을 처음으로 연 후에 다음 단계를 수행하십시오.

1 Finder에서 **응용 프로그램**을 선택하고 **Dell Data Guardian**을 두 번 클릭합니다.
2 Dell Server 창이 열리면 Dell Server 주소를 입력하고 **저장**을 클릭합니다.

자격 증명 창이 열립니다.

3 도메인 이메일 주소와 도메인 암호를 입력하고
4 **로그인**을 클릭하여 Dell Data Guardian을 활성화합니다.

Dell Data Guardian 응용 프로그램이 열리고 활성화되면 희미한 클라우드 저장소 제공업체 이름이 왼쪽 창에 활성화됩니다.

기업에서 모든 사용자가 동일한 클라우드 서비스를 사용하여 협업하기를 원한다면, 관리자는 해당 서비스만 활성화하고 다른 서비스가 표시되는 것을 차단하도록 정책을 설정할 수 있습니다.

Dell Data Guardian응용 프로그램 인증이 취소 또는 만료되면, 클라우드 저장소 제공업체 이름도 회색으로 표시됩니다.

5 왼쪽 창에서 클라우드 저장소 제공업체를 선택합니다.
자격 증명을 입력하라는 창이 열립니다. 인증되면 클라우드 저장소 제공업체 이름이 활성화됩니다.

6 인증에 대한 자세한 내용은 온라인 Dell Data Guardian 도움말을 참조하십시오.

Data Guardian 제거

이 섹션에서는 Data Guardian 설치 제거를 위한 관리자 프로세스를 설명합니다. 설치 제거를 수행하려면 로컬 관리자 계정이 있어야 합니다. 최종 사용자에게 로컬 관리자 계정이 있으면 Mac용 Data Guardian을 직접 설치 제거할 수 있습니다.

Data Guardian을 제거하려면 다음 중 하나를 수행합니다.

Finder

1 <option> 키를 누른 상태에서 메뉴 모음에서 **실행**을 선택합니다.
2 **~/Library/Application Support/Dell** 폴더를 엽니다.
3 마우스 오른쪽 단추로 **Dell DataGuardian** 폴더를 클릭하고 **휴지통으로 이동**을 선택합니다.
4 메뉴 모음의 **실행**에서 Applications 폴더를 열고 **Dell Data Guardian** 응용 프로그램을 휴지통으로 이동합니다.
5 **확인**을 클릭합니다.
6 메시지가 나타나면 관리자 암호를 입력합니다.

터미널

다음 위치 중 하나 또는 둘 다에 Data Guardian이 있을 수 있습니다.

1 다음 명령을 사용하십시오.
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 **Dell DataGuardian** 폴더를 제거합니다.

웹 클라이언트용 Data Guardian 구성 및 설치

이 웹 클라이언트에서 사용자가 Data Guardian 클라이언트를 설치하지 않고 보호되는 Office 문서 또는 .xen 파일을 볼 수 있습니다. 일반적으로 Security Management Server 또는 Security Management Server Virtual을 먼저 설치하는 것이 좋습니다.

OVA 파일 다운로드

초기에 설치할 때 Data-Guardian-웹은 가상 컴퓨터에서 실행되는 소프트웨어를 전달하는 OVA(Open Virtual Application) 파일로 제공됩니다.

OVA 파일을 다운로드하려면 다음을 수행하십시오.

1 Data Guardian 제품 지원 페이지로 이동합니다.
2 **드라이버 및 다운로드**를 클릭합니다.
3 "<OS 버전>의 사용 가능한 모든 업데이트 보기" 옆의 **OS 변경**을 클릭하고 **VMware ESXi 6.0** 또는 **VMware ESXi 5.5**를 선택합니다.
4 "보기 기준:" 아래에서 **모두 표시**를 선택합니다.
5 Dell Data Security에서 **다운로드**를 선택합니다.

웹용 Data Guardian 설치

Data-Guardian-Web용 설치 및 구성

시작하기 전에, 모든 시스템 및 가상 환경의 요구 사항이 충족되었는지 확인하십시오.

1 설치 미디어에서 Data Guardian 파일을 찾아 **Data-Guardian-Web-1.x.x.ova**를 두 번 클릭하여 VMware로 가져옵니다.
2 Data-Guardian-Web의 전원을 켭니다.
3 라이센스 계약에 사용되는 언어를 선택한 후 **EULA 표시**를 선택합니다.
4 계약서를 읽고 **EULA 동의**를 선택합니다.
5 사용 가능한 업데이트가 있는 경우 **채택**을 선택합니다.
6 기본 암호 변경 메시지가 표시되면 **예**를 선택합니다.
7 *ddguser 암호 설정* 화면에서, 현재(기본) 암호인 **ddguser**를 입력하고 고유한 암호를 입력한 후 다시 한번 입력한 다음 **확인**을 선택합니다.

   암호는 반드시 다음을 포함해야 합니다.

   - 8자 이상의 문자
   - 1자 이상의 대문자
   - 1개 이상의 숫자
   - 1자 이상의 특수 문자

8 *ddgconsole* 및 *ddgsupport* 계정에 대해 이전 단계를 반복합니다.

노트:
이름과 동일한 기본 암호를 유지하려면 **취소**를 클릭합니다. 암호를 수정하려면 현재 암호 필드에 **ddgconsole** 또는 **ddgsupport**를 입력합니다.

9 *호스트 이름 구성* 대화상자에서 백스페이스 키를 사용하여 기본 호스트 이름을 제거합니다. FQDN 호스트 이름을 입력하고 **확인**을 선택합니다.

10 여러 노드와 부하 분산 기능이 있는 경우 부하 분산 기능 호스트 이름을 입력합니다.

11 *네트워크 설정 구성* 대화상자에서 아래 옵션 중 하나를 선택한 다음 **확인**을 선택합니다.

- (기본 설정) DHCP 사용
- (권장 설정) DHCP 사용 필드에서 스페이스바를 눌러 X를 제거하고 해당하는 경우 다음 주소를 수동으로 입력합니다. 고정 IP 네트워크 마스크 기본 게이트웨이 DNS 서버 1 DNS 서버 2 DNS 서버 3

노트:
고정 IP를 사용할 경우 DNS 서버에 호스트 항목도 만들어야 합니다.

12 SCP 화면이 표시되면 확인을 클릭하지 마십시오. 먼저, .cer 및 .key 파일을 응용프로그램에 추가하거나 CA의 .pfx 또는 .p7b 파일에서 추출해야 합니다. WinSCP 도구 사용을 참조하십시오.

노트:
이들을 추출하기 전에 scp 화면에서 OK를 클릭하면 Data-Guardian-Web을 다시 시작하고 *네트워크 설정 구성* 대화 상자로 이동해야 합니다.

WinSCP 도구 사용

Windows에서 ddgconsole 계정을 사용하여 SSL 인증서 파일 및 SSL 키 파일을 SCP합니다.

1 Windows에서 WinSCP 도구를 엽니다.
2 WinSCP 페이지에 호스트 이름을 입력합니다.
3 기본 ddgconsole 사용자 이름 및 기본 암호(또는 수정된 사용자 이름 및 암호)를 입력합니다.
4 **로그인**을 클릭합니다.
5 로컬 드라이브의 인증서와 키 및 .pfx 파일 또는 .p7b 파일을 **opt/dell/files** 디렉터리로 드래그합니다.
6 .pfx 파일 또는 .p7b 파일을 추가한 경우 메시지가 나타나면 암호를 입력합니다. 인증서와 키가 CA에서 추출되어 **apache2/ssl/folder**에 추가됩니다.
필요에 따라 .pfx 또는 .p7b 파일을 드래그하는 대신 수동으로 인증서를 추출할 수 있습니다. 다음은 샘플 코드입니다.

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
```

.pfx 파일에서 개인 키를 추출하는 샘플 코드:

```
openssl pkcs12 -in domain.pfx -nocerts -nodes -out domain.key
```

7 관리 콘솔의 SCP 화면으로 돌아갑니다.

관리 콘솔

관리 콘솔의 SCP 화면에서 다음을 수행합니다.

1 **확인**을 클릭합니다. 인증서가 나열된 *Apache2 역방향 프록시 인증서 설치* 화면이 열립니다.
2 인증서를 선택하고 **Enter** 키를 누릅니다.
3 다음 중 하나를 수행합니다.
- WinSCP 도구에서 키를 추가한 경우 다음 화면에서 해당 키를 선택하고 **Enter** 키를 누릅니다.
- WinSCP 도구에서 .pfx 파일 또는 .p7b 파일의 암호를 입력한 경우 메시지가 표시되면 암호를 입력하고 **확인**을 클릭합니다.

4 Dell Server 화면에서 서버 호스트 이름을 입력하고 **확인**을 클릭합니다. 프로비저닝할 때 사용할 URL을 나열하는 대화상자가 표시됩니다. URL의 형식은 **https://node.domain.com/edap-admin-ui/provision_node**입니다.

노트:
node.domain.com은 *호스트 이름 구성*에 입력한 이름입니다. URL은 이 노드를 가리킵니다.

5 브라우저를 열고 URL을 입력합니다.
6 Dell Data Guardian 노드 프로비저닝 페이지가 열리면 **노드 프로비저닝 시작**을 클릭합니다.

7 로그인 페이지에서 도메인 이름 및 암호를 입력하고 **로그인**을 클릭합니다. Dell Data Guardian 대화 상자에 프로비저닝이 성공했다는 메시지가 표시됩니다.

8 URL이 나열된 관리 콘솔 화면으로 돌아가 **확인**을 클릭합니다. 애플리케이션 서버가 다시 시작되고 Administration Console > 주 메뉴가 열립니다.

추가 작업:

- Data Guardian 웹 클라이언트에 액세스할 수 있도록 내부 사용자에 대한 URL을 제공합니다.
  - 단일 노드의 경우 URL은 **https://nodename/** 형식으로 되어 있습니다. 여기서 노드 이름은 *호스트 이름 구성* 화면에 입력한 호스트 이름을 반영합니다.
  - 여러 노드의 경우 URL은 **https://loadBalancerName/** 형식으로 되어 있습니다. 여기서 노드 이름은 *호스트 이름 구성*화면에 입력한 부하 분산 기능 호스트 이름을 반영합니다.
- 나중에 이 VM의 업데이트를 위해 서버에 액세스하거나 로그를 확인하려면 이 VM에 대해 SSH를 활성화해야 합니다. **기본 구성 > SSH 설정**을 선택하여 ddgsupport 사용자에 대해 SSH를 활성화합니다.
- Management Console에서 노드 기반 웹 포털 정책을 수정하는 경우 어플라이언스를 재부팅해야 합니다. 어플라이언스 재부팅을 참조하십시오. 재시작 후, ddguser 자격 증명을 사용하여 로그인해야 합니다.

Management Console 열기

Https://server.domain.com:8443/webui/에서 Management Console 열기

기본 자격 증명은 **superadmin/changeit**입니다.

Management Console 액세스를 위해 다음 웹 브라우저가 지원됩니다.

- Internet Explorer 11.x 이상
- Mozilla Firefox 41.x 이상
- Google Chrome 46.x 이상
- Safari

Data Guardian 기본 터미널 구성 작업

주 메뉴에서 기본 구성 작업에 액세스합니다.

호스트 이름 변경

이 작업은 언제든지 완료할 수 있습니다. 사용을 시작할 필요가 없습니다.

1 *기본 구성* 메뉴에서 **호스트 이름**을 선택합니다.

2 백스페이스 키를 사용하여 기존 Data-Guardian-Web 호스트 이름을 제거하고 새 호스트 이름으로 바꾼 다음 **확인**을 선택합니다.

네트워크 설정 변경

이 작업은 언제든지 완료할 수 있습니다. 사용을 시작할 필요가 없습니다.

1 *기본 구성* 메뉴에서 **네트워크**를 선택합니다.

2 *네트워크 설정 구성*화면에서 아래 옵션 중 하나를 선택한 다음 **확인**을 선택합니다.
   - (기본 설정) DHCP(IPv4) 사용
   - (권장 설정) DHCP 사용 필드에서 스페이스바를 눌러 X를 제거한 다음 해당하는 경우 다음 주소를 수동으로 입력합니다.

     고정 IP

     네트워크 마스크

기본 게이트웨이

DNS 서버 1

DNS 서버 2

DNS 서버 3

정적 구성을 위해 IPv6 또는 IPv4를 선택할 수 있습니다.

노트:
고정 IP를 사용할 경우 DNS 서버에 호스트 항목을 만들어야 합니다.

사용자 암호 변경

이 작업은 언제든지 완료할 수 있습니다. 사용을 시작할 필요가 없습니다.

다음 사용자의 암호를 변경할 수 있습니다.

- ddguser(터미널 관리자) - 이 사용자는 Data Guardian 터미널 및 해당 메뉴의 액세스 권한이 있습니다.
- ddgconsole(셸 액세스) - 이 사용자는 Data Guardian 셸 액세스 권한이 있습니다. Shell access is available for a network administrator to check and troubleshoot network connectivity.
- ddgsupport(Dell ProSupport 관리자) - 이 사용자는 Dell ProSupport 사용만을 위해 존재합니다. 보안 목적을 위해, 이 계정의 암호를 관리할 수 있습니다.

1 *기본 구성* 메뉴에서 **사용자 암호 변경**을 선택합니다.
2 *사용자 암호 변경* 화면에서, 변경할 사용자 암호를 선택하고 **Enter**를 선택합니다.
3 *암호 설정* 화면에서, 현재 암호를 입력하고 새 암호를 입력한 후 다시 한번 새 암호를 입력한 다음 **확인**을 선택합니다.
암호는 반드시 다음을 포함해야 합니다.

- 8자 이상의 문자
- 1자 이상의 대문자
- 1개 이상의 숫자
- 1자 이상의 특수 문자

노트: 다른 사용자 계정을 선택하려면 키보드의 "스페이스바" 키를 눌러 선택 목록을 표시합니다.

SSH 사용

이 작업은 언제든지 완료할 수 있습니다. 사용을 시작할 필요가 없습니다.

Support 관리자 로그인, 셸 액세스, 터미널 명령줄 인터페이스에 SSH를 사용할 수 있습니다.

1 *기본 구성* 메뉴에서 **SSH**를 선택합니다.
2 SSH를 사용할 사용자를 강조 표시하고 스페이스바를 눌러 **X**를 입력한 후 **확인**을 선택합니다.

서비스 시작 또는 중지

이 작업은 필요할 경우에만 수행합니다.

1 모든 서비스를 동시에 시작하거나 중지하려면 *기본 구성* 메뉴에서 **애플리케이션 시작** 또는 **애플리케이션 중지**를 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.

노트: 서버 상태 변경은 완료되기까지 최대 2분이 소요될 수 있습니다.

어플라이언스 재부팅

이 작업은 필요할 경우에만 수행합니다.

1 *기본 구성* 메뉴에서 **어플라이언스 재부팅**을 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.
3 재시작 후, Data Guardian에 로그인합니다.

어플라이언스 종료

이 작업은 필요할 경우에만 수행합니다.

1 *기본 구성* 메뉴에서, 아래로 스크롤하여 **어플라이언스 종료**를 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.
3 재시작 후, Data Guardian에 로그인합니다.

관리자 작업

Terminal 언어 설정 또는 변경

설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 주 메뉴에서 **언어 설정**을 선택합니다.
2 화살표 키를 사용하여 선호하는 언어를 선택합니다.

시스템 스냅숏 로그 생성

Dell ProSupport용 시스템 스냅숏 로그를 생성하려면, 주 메뉴에서 **지원 도구**를 선택합니다.

1 *지원 부서 도구* 메뉴에서 **시스템 스냅숏 로그 생성**을 선택합니다.
2 파일이 생성되었다는 메시지가 표시되면 **확인**을 선택합니다.