

Dell Data Protection | Mac용 Dell Data Guardian

관리자 안내서 v1.2



참고, 주의 및 경고

① **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.

© 2017 Dell Inc. All rights reserved. Dell, EMC 및 기타 상표는 Dell Inc. 또는 자회사의 상표입니다. 기타 상표는 각 소유자의 상표일 수 있습니다.

Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise 및 Dell 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 www.7-zip.org에서 찾아볼 수 있습니다. 라이선스에는 GNU LGPL 라이선스 + unRAR 제한이 적용됩니다(www.7-zip.org/license.txt).

Mac용 Dell Data Guardian 관리자 안내서

2017 - 04

개정 A01

| | |
|--|-----------|
| 1 Mac용 Dell Data Guardian 소개 | 4 |
| 개요..... | 4 |
| Dell ProSupport에 문의..... | 4 |
| 2 Mac용 Dell Data Guardian 요구 사항 | 5 |
| 서버..... | 5 |
| Mac 클라이언트 하드웨어..... | 5 |
| 운영 체제..... | 5 |
| 클라우드 저장소 제공업체..... | 6 |
| 3 Data Guardian 설치 작업 | 7 |
| 필수 조건..... | 7 |
| 정책..... | 7 |
| Dell Enterprise Server 작업..... | 7 |
| 클라우드 클라이언트 다운로드를 허용하도록 보안 서버 설정..... | 7 |
| 전체 액세스 목록/거부 목록에서 사용자 허용/거부..... | 8 |
| Dropbox for Business 팀원 계정 원격 삭제..... | 10 |
| 클라이언트 작업..... | 11 |
| 필수 조건..... | 11 |
| 모범 사례..... | 11 |
| 클라이언트 설치..... | 11 |
| 4 Data Guardian 활성화 및 사용자 경험 | 13 |
| 최종 사용자 활성화..... | 13 |
| 사용자 인터페이스..... | 13 |
| 웹 사이트에서 체크아웃 옵션 방지..... | 14 |
| 응용 프로그램 기본 설정..... | 14 |
| Data Guardian 및 클라우드 동기화 클라이언트에 대한 보안 및 기타 고려사항..... | 16 |
| Google Drive..... | 16 |
| OneDrive for Business..... | 16 |
| 이 제품에 대한 피드백..... | 16 |
| 5 Data Guardian 설치 제거 작업 | 17 |
| 필수 조건..... | 17 |
| Data Guardian 제거..... | 17 |
| 6 용어집 | 18 |



Mac용 Dell Data Guardian 소개

본 설명서에서는 Mac용 클라우드 클라이언트 소프트웨어를 관리하는 데 필요한 정보를 제공합니다.

GUID-DC805DCF-88A3-4894-B120-B1ED63272AA5

개요

Mac용 Dell Data Guardian은 클라우드 기반 파일 공유 시스템의 데이터를 보호합니다. Data Guardian을 사용하는 Mac OS X 컴퓨터는 안전한 저장을 위해 클라우드 기반 파일 공유 시스템의 파일을 보고, 수정하고, 암호화할 수 있습니다.

Mac 및 Windows용 Data Guardian은 상호 간에 암호화된 파일을 열 수 있습니다.

Mac용 Data Guardian은 다음으로 구성되어 있습니다.

- Data Guardian:
 - **클라우드 암호화** - 클라우드 기반 파일 공유 시스템의 데이터를 .xen 파일로 보호합니다.
 - **보호된 Office 문서** - 클라우드의 Office 문서(.docx, .pptx, .xlsx, .docm, .pptm, .xslm)를 보호하고 원래 파일 이름과 확장자를 표시합니다. 보호되는 경우, Data Guardian 클라이언트에서만 이 파일을 열 수 있습니다. 다른 위치에서 파일을 열면 해당 문서가 보호되고 있음을 알리는 표지가 나타나고 권한이 있는 사용자가 암호화된 파일 액세스를 요청할 수 있는 방법을 설명합니다.

클라우드 암호화 전용 또는 두 정책 그룹에 대한 정책을 설정할 수 있습니다. 자세한 내용은 *관리자 도움말*을 참조하십시오.

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.

- Security Server - Mac용 Data Guardian을 관리하는 Dell 서버의 구성요소입니다. 보안 서버는 공유 대상과 상관없이 클라우드에서 데이터의 보안을 보장합니다 또한 보안 서버는 내부 장치가 중요한 데이터를 전달하지 못하도록 보호합니다.
- Remote Management Console - 중앙 집중식 보안 정책 관리를 제공하고, 기존 Enterprise 디렉터리와 통합하며, 보고서를 생성합니다.

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

GUID-B47CD81A-486F-43A5-816B-86A247C276EA

Dell ProSupport에 문의

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

또한, dell.com/support에서 Dell Data Protection 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 번호](#)를 확인하십시오.

Mac용 Dell Data Guardian 요구 사항

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

① 노트:
IPv6는 지원되지 않습니다.

GUID-213663B0-B65F-4945-B2F1-58EF78085BDF

서버

Mac용 Data Guardian에서는 클라이언트가 Dell Enterprise Server 또는 Dell Enterprise Server - VE, v9.6 이상에 연결되어야 합니다.

GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4

Mac 클라이언트 하드웨어

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

GUID-3F5F6005-9FEE-46AE-8400-338215F15DB2

운영 체제

다음 목록에 지원되는 운영 체제가 나와 있습니다.

Mac 운영 체제

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macos sierra 10.12.3 및 10.12.4



Android 운영 체제

- 4.4-4.4.4 KitKat
- 5.0-5.1.1 Lollipop
- 6.0 - 6.0.1 Marshmallow
- 7.0 Nougat

iOS 운영 체제

- iOS 8.x
- iOS 9.x
- iOS 10.x - 10.3

GUID-C4B25B4F-15E5-42AF-8493-D09F2473A534

클라우드 저장소 제공업체

정책 설정에 따라 Dell Data Guardian 인터페이스에 다음이 표시될 수 있습니다. 사용자가 클라우드 동기화 클라이언트를 다운로드하거나 설치할 필요가 없습니다.

클라우드 저장소 제공업체

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



Data Guardian 설치 작업

GUID-168A18C7-0DBD-43F2-9A99-08FC43099963

필수 조건

이러한 작업을 수행하기 전에 다음을 확인합니다.

- Dell 서버 및 해당 구성 요소를 설치합니다. 다음 섹션 중 하나 참조:
 - Enterprise Server 설치 및 마이그레이션 안내서
 - Enterprise Server 빠른 시작 안내서 및 설치 안내서
- Remote Management Console에서 적절한 Dell 관리자 역할을 할당합니다.

GUID-D9C4A912-436F-415D-9499-BAE4F1B53233

정책

기본적으로 Data Guardian은 사용자의 파일을 암호화하여 DDP EE Server/VE Server에 감사 이벤트를 보냅니다. 이 문서의 목적에 맞게 양쪽 서버가 특정 버전을 언급해야 할 경우(예: Dell Enterprise Server 사용 시 다른 절차 적용 - VE)를 제외하고 'Dell 서버'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 저장소 제공업체에 대한 기본 동작을 변경하려면 *클라우드 저장소 보호 제공업체* 정책을 설정합니다. 기업에서 특정 클라우드 저장소 제공업체를 선호하는 경우 다른 제공업체에 대해 이 정책을 **차단**으로 설정합니다. 정책에 대한 자세한 내용은 Dell 서버의 Remote Management Console에서 액세스할 수 있는 *관리자 도움말*을 참조하십시오.

① 노트:

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

GUID-EE401419-8E85-45A9-9775-2C18EEE3FD80

Dell Enterprise Server 작업

GUID-0E37A5B7-8FF3-4F1E-9A8E-AB49D849C05B

클라우드 클라이언트 다운로드를 허용하도록 보안 서버 설정

DDP Enterprise Server

- 1 DDP Enterprise 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 VE Security Server에 사전 설치되어 있습니다.

VE Security Server에 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.

GUID-40291F18-814A-40EC-9D60-A185154BA6FC

전체 액세스 목록/거부 목록에서 사용자 허용/거부

전체 액세스 목록과 거부 목록 항목에서 Data Guardian을 사용하도록 Dell 서버에 등록할 수 있는 사용자를 결정합니다.

전체 액세스 목록

전체 액세스 목록에서는 특정 사용자나 사용자 그룹이 Dell 서버에 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 |

거부 목록

거부 목록은 특정 사용자 또는 사용자 그룹이 Data Guardian을 사용하여 DDP Server에 등록하지 못하도록 합니다. 거부 목록에 이메일 주소가 입력된 사용자는 Data Guardian에 등록할 수 없다는 메시지를 받습니다.

① 노트:

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

거부 목록을 사용하여 전체 액세스 목록에 승인되어 있는 특정 사용자를 제외할 수 있습니다. 또한 와일드카드(*)를 사용하면 전체 도메인이 거부 목록에 등록되므로 해당 도메인에 이메일 주소가 있는 사용자가 등록하지 못합니다. 사용자 또는 그룹이 Dell 서버에 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/거부 목록을 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:

거부 목록 - 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 일 액세스를 허용합니다. 사용자나 도메인도 거부 목록에 있는 경우 액세스가 허용되지 않습니다.

- 4 도메인/이메일 입력 필드에서 사용자의 메인을 입력하면 전체 도메인에 대한 액세스가 설정되며 이메일 주소를 입력하면 해당 사용자에 대한 액세스만 설정됩니다.
- 5 **추가**를 클릭합니다.

전체 액세스 목록/거부 목록 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.



Dropbox for Business 팀원 계정 원격 삭제

회사에 Dropbox for Business가 있으면 회사 Dropbox for Business 팀 계정에서 원격으로 팀원을 제거할 수 있습니다(예: 사용자가 퇴사하는 경우). 팀원의 계정과 연결된 파일 및 폴더가 계정에서 사용되는 모든 장치에서 제거됩니다. 이렇게 하면 해당 파일에 대한 사용자의 액세스 권한이 취소됩니다.

필수 조건

① 노트:

이 절차를 수행하기 전에 팀원 계정에서 회사나 기타 Dropbox for Business 팀원에게 필요할 수 있는 파일 또는 폴더를 백업해야 합니다.

Dropbox for Business 관리자만 Dropbox for Business 계정을 원격 삭제할 수 있습니다.

최종 사용자는 Dell Data Guardian을 활성화하고 Dropbox for Business에 연결해야 합니다.

원격 관리 콘솔에서 등록

Dropbox for Business 관리자 한 명만 등록하면 됩니다.

- 1 Remote Management Console의 왼쪽 창에서 **관리 > Dropbox 관리**를 선택합니다.
- 2 Dropbox for Business 페이지에서 **등록**을 클릭합니다.
Dropbox for Business 사이트로 브라우저가 열립니다.
- 3 메시지가 나타나면 Dropbox for Business 관리자 계정을 사용하여 Dropbox에 로그인합니다.
- 4 Dell Data Guardian에 대한 액세스를 허용하려면 **허용**을 클릭합니다.
Dropbox 권한이 DDP Enterprise Server - VE에 부여되었음을 나타내기 위한 확인 페이지가 표시됩니다.
- 5 Remote Management Console에서 **관리 > Dropbox 관리**로 돌아가고 **새로 고침**을 클릭합니다.
관리자 이름이 표시됩니다.

① 노트:

일반적으로 가장 좋은 방법은 등록을 취소하지 않는 것입니다. 그러나 Dropbox for Business 팀에서 팀원을 제거하기 위한 Dropbox for Business 관리자의 권한을 무효화하려면 **등록 해제**를 클릭합니다.

팀원 계정 원격 삭제

① 노트:

원격 삭제 옵션은 등록된 Dropbox for Business 팀원 계정에서만 사용할 수 있습니다. 사용자 계정에 대해 원격 삭제 옵션이 표시되지 않으면 사용자가 Dropbox for Business 계정에 등록하지 않는 것입니다.

- 1 원격 관리 콘솔의 왼쪽 창에서 **채우기 > 사용자**를 선택합니다.
- 2 특정 사용자를 검색합니다.
- 3 **사용자 세부 정보** 페이지에 액세스합니다.
- 4 명령 열에서 **원격 삭제**를 클릭합니다.
원격 삭제가 수행됩니다.

① 노트:

원격 삭제를 선택하기 전에 원 계정에서 회사나 기타 Dropbox for Business 팀원에게 필요할 수 있는 파일 또는 폴더를 백업해야 합니다.

- 5 원격 삭제에 대한 확인에서 **예**를 클릭합니다.

사용자 세부 정보 페이지에 원격 삭제가 수행된 날짜가 나열됩니다.

- Dropbox for Business 관리자 콘솔 구성원 페이지에서 팀원 목록을 새로 고칩니다.
목록에서 사용자가 제거됩니다. **제거된 구성원** 탭을 선택하여 어떤 사용자가 제거되었는지 볼 수 있습니다.

GUID-B495F3E1-6516-4DFC-9107-4AA52FE296AB

클라이언트 작업

GUID-88098FA1-F419-45AD-A1BA-F5C30D04DDE3

필수 조건

- 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 Dell 보안 서버의 정규화된 도메인 이름을 사용하고 있는지 확인합니다.

GUID-5A15F45E-2F37-4EB4-90CD-66CD73275BAB

모범 사례

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

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

GUID-CF4B86F3-D8AF-4834-B15B-8813EEA7289D

클라이언트 설치

현재 허용 목록에 추가된 사용자는 <https://yoursecurityservername.domain.com:8443/cloudweb/register>에서 등록할 수 있습니다.

등록 후 사용자는 해당 클라이언트에 로그인하여 다운로드하도록 <https://yoursecurityservername.domain.com:8443/cloudweb>으로 안내하는 이메일을 받습니다.

일반적으로 최종 사용자는 등록 후 <https://yoursecurityservername.domain.com:8443/cloudweb>에서 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 사용자에게 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.

① 노트:

기업이 Cloud Edition에서 Data Guardian으로 업그레이드하는 경우, 사용자는 Data Guardian을 인증하고 클라우드 저장소 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 DDP-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 라이선스 계약 창에서 **계속**을 클릭합니다.
- 7 계속하려면 **동의**를 클릭합니다.
- 8 설치 유형 창에서 다음 중 하나를 수행합니다.
 - **설치**를 클릭한 다음 9단계로 이동합니다.
 - 대상 선택 창에서 아래에 있는 옵션을 선택하고, **계속**을 클릭한 다음, 9단계로 이동합니다.
 - 이 컴퓨터의 모든 사용자에게 설치
 - 나에 대해서만 설치
- 9 대화 상자에서 사용자 이름 및 암호를 입력하고 **소프트웨어 설치**를 클릭합니다.
- 10 요약 창에 **닫기**를 클릭합니다.
- 11 **최종 사용자 활성화**를 참조하십시오.

① 노트:

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

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 최종 사용자에게 Data Guardian을 활성화하도록 지시합니다. **최종 사용자 활성화**를 참조하십시오.

Data Guardian 활성화 및 사용자 경험

GUID-FCD7AF83-06D4-4D0C-8FA3-369265AB00E2

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 서버 창이 열리면 DDP 서버 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 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.

활성화되지 않거나 Dell Data Guardian 응용 프로그램 인증이 취소 또는 만료되면, 클라우드 저장소 제공업체 이름이 회색으로 표시됩니다.

- 5 왼쪽 창에서 클라우드 저장소 제공업체를 선택합니다.
자격 증명을 입력하라는 창이 열립니다.
- 6 인증에 대한 자세한 내용은 온라인 Dell Data Guardian 도움말을 참조하십시오.

GUID-9917238E-00E5-4F56-909D-C76F09426D53

사용자 인터페이스

Dell Data Guardian 인터페이스는 열 인터페이스 측면에서 OS X Finder **보기**와 유사합니다. 각 열은 선택한 클라우드 저장소 서비스에 있는 폴더를 나타냅니다.

① 노트:

제목 표시줄은 운영 체제에 따라 다를 수 있습니다.

파일을 암호화 및 해독하려면 클라우드 저장소 제공업체 웹 사이트가 아니라 Dell Data Guardian 인터페이스를 사용해야 합니다.

Dell Data Guardian 창에서 다음 작업을 수행할 수 있습니다.

- **파일 > 새 폴더** - 새 폴더 만들기.

① 노트:

Google Drive 및 OneDrive는 공유 폴더를 자동으로 추가합니다. 그러나, OneDrive for Business에서의 데이터 공유는 지원되지 않습니다.



- 컨텍스트 메뉴 - 기본 창에서 폴더나 파일을 하나 이상 선택합니다. 그런 다음, 컨트롤 키(또는 마우스 오른쪽 단추)를 클릭하고 다음 메뉴 옵션을 선택합니다.
 - **Dell Data Protection 파일 전송 사이트(CFT)에서 소프트웨어를 다운로드하십시오.**
 - **이름 변경** - Dell Data Guardian 인터페이스에서 파일 이름을 변경할 경우 Dell Data Guardian은 클라우드 저장소 제공업체 웹 사이트의 변경 사항을 동기화합니다. 클라우드 저장소 제공업체 웹 사이트에서 .xen 파일 이름은 변경하지 마십시오. 이 변경 사항은 동기화되지 않습니다.
 - **삭제**

① 노트:

Data Guardian이 포함된 Google Drive에는 제거(휴지통으로 제거) 옵션이 없습니다. 다른 Data Guardian 기능과 일관성을 유지하기 위해 삭제 옵션만 있습니다.

- **연결 해제** - 클라우드 저장소 제공업체에서 Dell Data Guardian 연결을 해제하려면 왼쪽 창에서 제공업체를 선택하고 컨트롤 키(또는 마우스 오른쪽 단추)를 클릭한 후 메뉴에서 연결 해제를 선택합니다.

파일 및 폴더에 대한 추가 정보:

- Dell Data Guardian 사용자 인터페이스에 표시된 폴더에 파일과 폴더를 추가하려면 OS X Finder 또는 기타 드래그 앤 드롭을 지원하는 응용 프로그램에서 파일과 폴더를 드래그합니다. 파일은 현재 정책을 기반으로 암호화됩니다.
- 응용 프로그램의 파일을 암호 해독하고 열려면 Dell Data Guardian 창에서 파일을 두 번 클릭합니다. 외부 응용 프로그램에서 이 파일을 수정하면 수정된 파일은 암호화되고 클라우드 저장소 제공업체에 새 버전으로 업로드됩니다.
- 암호화되지 않은 로컬 복사본을 만들려면 Dell Data Guardian 창에서 Finder로 파일이나 폴더를 드래그합니다.
- Data Guardian의 *클라우드 암호화*에서는 확장자 없는 파일의 수정을 허용하지 않습니다. 이러한 파일은 읽기 전용 파일로 처리됩니다. 확장자가 없는 파일을 편집하려면 클라우드 저장소 제공업체 웹 사이트에서 파일을 다운로드하고 편집한 다음 Dell Data Guardian 인터페이스를 통해 업로드합니다.
- 확장된 속성은 클라우드에 복사되지 않습니다.

GUID-12885ECF-2D63-4BD1-8719-260F247D161E

웹 사이트에서 체크아웃 옵션 방지

Data Guardian은 OneDrive for Business 웹 사이트 또는 클라우드 저장소 제공업체 웹 사이트에서 *열기 및 체크아웃* 옵션과 함께 사용되는 파일을 보호하거나 암호화하지 않습니다. 파일이 열려 있고 체크아웃된 경우 자동 업로드가 차단되므로 Dell Data Guardian 인터페이스에서 열기 명령을 사용하지 마십시오.

Data Guardian으로 파일을 보호할 경우 Dell Data Guardian 인터페이스를 사용하여 파일 작업을 하십시오.

클라우드 저장소 제공업체 웹 사이트에서 특별한 속성을 가진 파일에 대해 작업을 수행할 경우

- 1 Dell Data Guardian 인터페이스에서 컨트롤 키(또는 마우스 오른쪽 단추)로 파일을 클릭하고 **다운로드**를 선택합니다..
- 2 파일을 선택하고 편집합니다.
- 3 Dell Data Guardian 인터페이스를 통해 파일을 업로드합니다.

GUID-B18B3439-4C04-4F3A-AADA-DD5552F902D6

응용 프로그램 기본 설정

기본 설정을 실행하려면 다음을 수행하십시오.

- 1 Dell Data Guardian을 실행합니다.
- 2 Dell Data Guardian 메뉴 표시줄에서 **기본 설정**을 선택합니다.

① 노트:

이 정보는 도움말 아이콘에서도 사용할 수 있습니다.



다음과 같은 설정을 수정할 수 있습니다.

- ""로 시작하는 파일 숨기기 - 기본적으로, 상자가 선택된 상태로 파일을 숨기고 있습니다. 숨겨진 파일을 보려면 확인란을 선택 해제합니다.

① 노트:

일반적으로, 점 분리자 접두어로 된 파일은 OS X Finder에 숨겨져 있습니다.

- **클라우드 저장소 제공업체 연결 해제** - Data Guardian에서 인증한 클라우드 저장소 제공업체가 나열됩니다. Data Guardian의 클라우드 저장소 제공업체를 제거하려면 해당 제공업체를 선택하고 기본 설정 창의 왼쪽 아래에 있는 빼기(-) 단추를 클릭합니다.

서버 정책 - DDP Server 관리자는 Data Guardian에서 파일과 폴더를 관리하는 방법을 제어하는 다음과 같은 정책을 설정합니다.

- **DDP Server** - 서버 URL이 나열됩니다.
- **폴링 간격** - 클라이언트 소프트웨어가 정책 업데이트를 폴링하는 간격을 분 단위로 보여줍니다.
- **암호화** - 클라우드 저장소 웹 사이트의 폴더 및 파일을 암호화할 수 있는 마스터 암호화 정책입니다.
- **확장자명만 또는 난독화**

확장자명만(기본 정책 설정)에서는 웹 사이트에 파일 이름을 표시합니다.

기업에서 파일을 추가로 보호해야 하는 경우 클라우드 웹 사이트의 파일 이름을 GUID 이름으로 숨기려면 이 정책을 **난독화**로 설정하십시오.

① 노트:

처음에는 정책이 확장자명만으로 설정되고 클라우드 웹 사이트에 사용자 파일이 있는 상태에서 정책이 난독화로 변경된 경우, 웹 사이트의 기존 파일 이름은 난독화되지 않습니다. 기존 파일 이름을 난독화하려면 사용자가 Data Guardian 인터페이스를 통해 파일을 다운로드한 다음 다시 업로드해야 합니다. 또는 사용자가 파일을 편집하면 난독화된 파일 이름으로 업로드됩니다.

- **보호된 Office 문서** - 클라우드의 Office 문서(.docx, .pptx, .xlsx, .docm, .pptm, .xlsm)를 보호하지만, .xen 확장자가 아니라 파일 확장자를 표시합니다.

이 정책이 활성화된 경우 클라우드의 Office 문서(.docx, .pptx, .xlsx, .docm, .pptm, .xlsm)에서 .xen 확장자가 아니라 파일 확장자를 표시합니다. 그러나 파일을 클라우드에서 열 수 없거나 다운로드한 경우에도 열 수 없습니다. 문서를 열면 문서가 보호되었다는 내용의 표지만 표시됩니다. Data Guardian을 설치했지만 인증하지 않은 경우 표지에 이런 내용이 표시됩니다.

- **감사 이벤트** - 활성화된 경우 Dell 서버로 감사 이벤트를 전송합니다.
- **지리적 위치** - 활성화된 경우 Dell 서버로 전송된 감사 이벤트에 지리적 위치 데이터(위도 및 경도)가 포함됩니다.
- **콜백 신호** - 활성화된 경우 각각의 보호된 Office 파일로 콜백 신호를 전송합니다.
- **콜백 신호 URL** - 활성화된 경우 콜백 신호가 Office 보호 파일에 삽입될 때 사용할 URL을 지정합니다.
- **클라우드 저장소 보호 제공업체** - 정책 설정에 따라 제공업체 이름이 표시됩니다. 옵션에는 **Box/ Dropbox/ Google Drive / OneDrive OneDrive for Business**가 있습니다.

클라우드 저장소 제공업체에 업로드된 파일의 암호화를 사용 또는 사용하지 않도록 설정합니다. 다음 중 하나가 표시됩니다.

- **암호화** - 클라우드에 전송된 파일이 암호화됩니다.
- **허용** - 사용자는 클라우드에 있는 파일에 액세스할 수 있지만 클라우드 저장소 제공업체 웹 사이트에 전송된 파일은 암호화되지 않습니다.
- **차단됨** - 클라우드 저장소 제공업체를 사용할 수 없으며, 현재는 클라우드 저장소 제공업체 이름이 기본 창에 표시되지 않음을 뜻합니다.



GUID-74395D32-C5C3-46A5-A090-CE195AD50CC0

Data Guardian 및 클라우드 동기화 클라이언트에 대한 보안 및 기타 고려사항

GUID-ED3DC4CF-B650-4583-83F3-84FE0288BBC3

Google Drive

Data Guardian의 *클라우드 암호화*에서는 클라우드의 폴더 및 파일을 암호화하여 데이터를 보호합니다. 다음 고려 사항을 알고 있어야 합니다.

- 보호로 설정된 회사 보안 정책에서는 Data Guardian과 함께 Google Docs의 사용을 금지합니다. 허용으로 설정된 경우에는 해당 문서를 편집할 수 있습니다. 자세한 내용은 IT 관리자에게 문의하십시오.

Google Drive에는 사용자가 실시간으로 문서를 공동 작업할 수 있는 Google Docs 앱이 포함되어 있습니다. 하지만 공동 작업은 Google 서버에서 이루어지며 해당 파일이 암호화되지 않습니다. 사용자가 만든 Google Docs가 Google Docs 클라우드 저장소 제공 업체 폴더에 표시됩니다.

그러나 폴더를 열면 Data Guardian이 해당 문서를 암호화할 수 없음을 경고하는 대화 상자가 표시됩니다.

GUID-5454F808-40A1-4609-BED2-7D3D08391FC4

OneDrive for Business

OneDrive for Business에서는 데이터 공유가 지원되지 않습니다.

GUID-A6AA7EB4-E62B-44A2-BAC2-902473A21C42

이 제품에 대한 피드백

정책에서 활성화한 경우 사용자는 Dell Data Guardian에 대한 피드백을 제공할 수 있습니다. 메뉴 표시줄 > **Dell Data Protection 피드백** 제공에서 피드백 양식을 제공합니다.



Data Guardian 설치 제거 작업

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

GUID-0AECB4CA-AADA-44B7-A403-5D8C97FFAFD5

필수 조건

설치 제거를 수행하려면 로컬 관리자 계정이 있어야 합니다.

GUID-C8A4F2BD-6FE8-4B26-A3FB-60795DD70304

Data Guardian 제거

Data Guardian을 제거하려면 다음 중 하나를 수행합니다.

Finder

- 1 <option> 키를 누른 상태에서 메뉴 표시줄에서 **실행**을 선택합니다.
- 2 **~/Library/Application Support/Dell** 폴더를 엽니다.
- 3 **DataGuardian** 폴더를 제거합니다.
- 4 메뉴 표시줄의 **실행**에서 Applications 폴더를 열고 **Data Guardian** 응용 프로그램을 제거합니다.

Terminal

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

- 1 다음 명령 중 하나 또는 둘 다를 사용하십시오.
 - `rm -R ~/Applications/Data\ Guardian.app`
 - `rm -R ~/Library/Application Support/Dell/DataGuardian`
- 2 **DataGuardian** 폴더를 제거합니다.



용어집

활성화(됨) - 컴퓨터가 Dell 서버에 등록되고 최소한 초기 정책 집합을 수신하면 활성화가 발생합니다.

Dell 서버 - Dell 서버는 구성요소 모음으로 구성되어 있습니다. 제품의 서버 측 전체를 의미할 때를 총괄적으로 Dell 서버라고 합니다.

Remote Management Console - Remote Management Console은 전체 엔터프라이즈 배포를 위한 관리 콘솔로서, Dell Enterprise Server의 구성요소 중 하나입니다.

보안 서버 - Dell Data Guardian을 관리하는 Dell 서버의 구성요소입니다. 보안 서버는 공유 대상과 상관없이 클라우드에서 데이터의 보안을 보장합니다 또한 보안 서버는 내부 장치가 중요한 데이터를 전달하지 못하도록 보호합니다.

외부 사용자 - 조직의 도메인 주소 밖에 있는 사용자입니다.