Dell Data Protection | Dell Data Guardian für Mac

Administratorhandbuch v1.2

GUID-5B8DE7B7-879F-45A4-88E0-732155904029

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

GUID-559E7DE2-5F31-4AF0-8A01-987470FAB58C

Dell Data Guardian Administratorhandbuch für Mac

2017 - 04

Inhaltsverzeichnis

Einführung in Dell Data Guardian für Mac

In diesem Handbuch erhalten Sie die erforderlichen Informationen für die Verwaltung der Cloud-Clientsoftware für Mac.

GUID-DC905DCF-89A3-4B94-B120-B1ED63272AA5

Übersicht

Dell Data Guardian für Mac schützt Daten in Cloud-basierten File-Sharing-Systemen. Mac OS X-Computer mit Data Guardian können Dateien in Cloud-basierten File-Sharing-Systemen anzeigen, ändern und zur sicheren Speicherung verschlüsseln.

Mit Data Guardian für Mac bzw. Windows verschlüsselte Dateien können problemlos jeweils wechselseitig geöffnet werden.

Data Guardian für Mac besteht aus den folgenden Komponenten:

- Data Guardian:
  - **Cloud-Verschlüsselung**: schützt Daten in Cloud-basierten File-Sharing-Systemen als .xen-Dateien.
  - **Geschützte Office-Dokumente:** schützt Office-Dokumente (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) in der Cloud und zeigt die ursprünglichen Dateinamen und Erweiterungen an. Geschützte Dateien können nur mit einem Data Guardian-Client geöffnet werden. Wenn versucht wird, die Dateien in einem anderen Programm zu öffnen, wird ein Deckblatt mit dem Hinweis, dass das Dokument geschützt ist, und Informationen darüber angezeigt, wie autorisierte Benutzer Zugriff auf die verschlüsselten Dateien anfordern können.

    Sie können Richtlinien nur für die Cloud-Verschlüsselung oder für beide Richtliniengruppen festlegen. Weitere Informationen dazu finden Sie in der *Administrator-Hilfe*.

    Data Guardian für Mac ist auf die Freigabe von Dateien innerhalb von Cloud-Verschlüsselungsanbietern ausgelegt. Wenn jedoch „Geschützte Office-Dokumente"-Richtlinien für Macs aktiviert sind, gehen alle Datei Überwachungs- und Rückverfolgbarkeitsdaten verloren, wenn die Datei vom Endbenutzer auf dem lokalen Mac gespeichert wird. Wenn in Ihrer Organisation eine strikte Datei-Überwachung und -Rückverfolgbarkeit benötigt wird, legen Sie die *Data Guardian*-Richtlinie *Mac zulassen* auf „Nicht ausgewählt" fest, um zu verhindern, dass Data Guardian auf Macs aktiviert wird.
- Security Server: Eine Komponente des Dell Servers für die Verwaltung von Data Guardian für Mac. Der Security Server gewährleistet die Sicherheit von Daten in der Cloud, unabhängig davon, für wen sie freigegeben werden. Der Security Server schützt zudem vor der Weitergabe vertraulicher Daten durch interne Geräte.
- Remote Management Console: bietet eine zentrale Verwaltung von Sicherheitsrichtlinien, kann in vorhandene Unternehmensverzeichnisse integriert werden und erstellt Berichte.

  Diese nahtlos ineinander greifenden Komponenten sorgen für eine sichere Umgebung, ohne die Benutzerfreundlichkeit zu beeinträchtigen.

GUID-B47CD81A-486F-43A5-916B-86A247C276EA

Kontaktieren des Dell ProSupports

Telefonischen Support rund um die Uhr für Ihr Dell Data Protection-Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Data Protection-Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport – Internationale Telefonnummern.

Dell Data Guardian-Anforderungen für Mac

In diesem Kapitel werden die Hardware- und Softwareanforderungen für den Client erläutert. Stellen Sie sicher, dass die Implementierungsumgebung die Anforderungen erfüllt, bevor Sie mit der Implementierung fortfahren.

ANMERKUNG:
IPv6 wird nicht unterstützt.

GUID-213663B0-B65F-4945-B2F1-5BEF78085BDF

Server

Data Guardian für Mac setzt voraus, dass der Client mit einem Dell Enterprise Server oder Dell Enterprise Server - VE, v9.6 oder höher verbunden ist.

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

Mac-Client-Hardware

Nachfolgend ist die unterstützte Hardware für den Mac-Client aufgeführt.

Mac-Hardware

- Intel Core 2 Duo-, Core i3-, Core i5-, Core i7- oder Xeon-Prozessor
- 2 GB RAM
- 10 GB freier Speicherplatz

GUID-3F5F6005-9FEE-46AE-8400-336215F15DB2

Betriebssysteme

Nachfolgend sind die unterstützten Betriebssysteme aufgeführt.

Mac-Betriebssysteme

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.3 und 10.12.4

Android-Betriebssysteme

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

iOS-Betriebssysteme

- iOS 8.x
- iOS 9.x
- iOS 10.x–10.3

GUID-C4B25B4F-15E5-42AF-9493-D09F2473A534

Cloud-Speicheranbieter

Je nach Richtlinieneinstellungen kann Folgendes auf der Dell Data Guardian-Oberfläche angezeigt werden. Der Benutzer muss den Cloud-Synchronisierungs-Client nicht herunterladen oder installieren.

Cloud-Speicheranbieter

- Dropbox
- Box® ist eine eingetragene Marke von Box.
- Google Drive
- OneDrive
- OneDrive für Unternehmen

Data Guardian-Installationsaufgaben

GUID-168A1BC7-0DED-43F2-9A99-08FC43099963

Voraussetzungen

Stellen Sie Folgendes sicher, bevor Sie diese Aufgaben durchführen:

- Installieren Sie den Dell Server und die dazugehörigen Komponenten. Lesen Sie einen der folgenden Abschnitte:
  - *Enterprise Server-Installations- und Migrationshandbuch*
  - *Erste Schritte und Installationshandbuch für Enterprise Server – Virtual Edition*
- Weisen Sie in der Dell Remote Management Console eine geeignete Dell Administratorrolle zu.

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

Richtlinien

Per Standardeinstellung verschlüsselt Data Guardian Benutzerdateien und sendet Überprüfungsereignisse an den DDP EE-Server/VE-Server. Zum Zwecke dieses Dokuments werden beide Server als „Dell Server“ bezeichnet, sofern keine konkrete Version angegeben ist (wenn z. B. bei Verwendung des Dell Enterprise Server – VE ein anderes Verfahren notwendig ist).

Wenn Sie möchten, dass Ereignisse vom Typ „Audit“ Geolocation-Daten umfassen, müssen Sie die WLAN-Funktion aktivieren. Weitere Informationen zu Geolocation und Ereignisse vom Typ "Audit" finden Sie in der *Administrator-Hilfe*.

Zum Ändern des standardmäßigen Verhalten für die einzelnen unterstützten Cloud-Speicheranbieter legen Sie die *Cloud-Speicherschutzanbieter*-Richtlinie fest. Falls Ihr Unternehmen einen bestimmten Cloud-Speicheranbieter bevorzugt, setzen Sie diese Richtlinie für andere Anbieter auf **Blockieren**. Informationen zu Richtlinien finden Sie in der *Administrator-Hilfe*, auf die Sie über die Remote Management Console des Dell Servers zugreifen können.

ANMERKUNG:
Die Umgehungsoption dieser Richtlinie gilt für Windows. Wenn Sie die Umgehung für Mac auswählen, wird für den Endbenutzer „Zulassen“ angezeigt.

GUID-EE401419-8E85-45A9-9775-2C16EEE3FDB0

Aufgaben für Dell Enterprise Server

GUID-0E37A5B7-8FF3-4F1E-9A8E-AB49D649C05B

Security Server so einrichten, dass Downloads von Cloud-Clients zugelassen werden

DDP Enterprise Server

1 Wechseln Sie auf dem DDP Enterprise Server zu <Security Server-Installationsverzeichnis>\webapps\cloudweb\brand\dell\resources\.
2 Öffnen Sie die Datei **messages.properties** mit einem Texteditor.
3 Stellen Sie sicher, dass die Einträge wie folgt lauten:
Für die **lokale** Installation:

download.deviceWin.mode=local

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

Für die **Remote**-Installation:

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

```
download.deviceMac.remote.link=https://[Computername:IPAdresse]:[Port]/yourpath/filename.dmg
```

4 Speichern und schließen Sie die Dateien.
5 Wechseln Sie zu <Security Server-Installationsverzeichnis>, und erstellen Sie einen Ordner mit dem Namen „Download“ (Security Server\Download).
6 Erstellen Sie im Download-Ordner einen Ordner namens „CloudWeb“ (Security Server\Download\CloudWeb).
7 Fügen Sie die Dell Data Guardian-Installationsprogramme zu diesem Ordner hinzu.

Virtual Edition: Manuelles Installieren einer anderen Cloud-Client-Version

Es sind keine weiteren Maßnahmen erforderlich, um Benutzern das Herunterladen des neuesten Dell Data Guardian-Installationsprogramms zu erlauben. Das neueste Installationsprogramm ist bereits auf dem VE Security Server vorinstalliert.

Zum manuellen Installieren einer anderen Version des Data Guardian-Installationsprogramms auf dem VE Security Server aktualisieren Sie die Datei „message.properties“.

1 Wechseln Sie zu:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Öffnen Sie die Datei **messages.properties** mit einem Texteditor.
Für die **lokale** Installation:

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

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

Für die **Remote**-Installation:

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[Computername:IPAdresse]:[Port]/yourpath/filename.dmg
```

3 Speichern und schließen Sie die Dateien.
4 Kopieren Sie die Dateien in den Ordner /opt/dell/server/security-server/download/cloudweb.
5 Fügen Sie die Data Guardian-Installationsprogramme zu diesem Ordner hinzu.

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

Zulassen/Ablehnen von Benutzern auf der Full Access-Liste/Blacklist

Die Einträge in der Positiv- bzw. Negativliste legen fest, welche Benutzer sich beim Dell Server registrieren können, um Data Guardian zu verwenden.

Full Access-Liste

Die Positivliste ermöglicht es bestimmten Benutzern oder Benutzergruppen, sich beim Dell Server zu registrieren und Data Guardian zu nutzen.

Externe Benutzer müssen sich auf der Full Access-Liste befinden, um sich registrieren zu können. Die folgenden Beispiele veranschaulichen die Zulassung von Benutzern für die Registrierung:

Benutzertyp	Eingabe
Alle E-Mail-Adressen vom Typ firma.com	`organisation.com`
Einen bestimmten Benutzer	`jdoe@organisation.com`
Alle Gmail-Benutzer	`gmail.com`

Negativliste

Die Negativliste verhindert, dass sich bestimmte Benutzer oder Benutzergruppen beim Dell Server registrieren und Data Guardian verwenden. Benutzer, deren E-Mail-Adressen auf der Negativliste stehen, erhalten eine Nachricht, dass sie sich nicht für Data Guardian registrieren können.

ANMERKUNG:
Wenn ein Benutzer bereits registriert ist, verhindert diese Liste **nicht**, dass dieser Data Guardian verwendet.

Sie können mithilfe der Negativliste bestimmte Benutzer ausschließen, die Mitglied zugelassener Gruppen auf der Positivliste sind. Zusätzlich lassen sich ganze Domänen auf die Negativliste setzen, sodass sich kein Benutzer mit einer E-Mail-Adresse in dieser Domäne registrieren kann. Die folgenden Beispiele veranschaulichen die Unterbindung der Registrierung von Benutzern oder Gruppen beim Dell Server:

Benutzertyp	Eingabe
Alle E-Mail-Adressen vom Typ firma.com	`organisation.com`
Ein bestimmter Benutzer mit einer bestimmten E-Mail-Adresse	`jdoe@organisation.com`
Alle Gmail-Benutzer	`gmail.com`

Befolgen Sie die nachstehenden Anweisungen, um Änderungen an der Positivliste/Negativliste vorzunehmen:

1 Klicken Sie im linken Bereich der Remote-Verwaltungskonsole auf **Verwaltung > Verwaltung externer Benutzer**.

2 Klicken Sie auf **Hinzufügen**.

3 Wählen Sie den Typ des Registrierungszugriffs aus:

Blacklist – Blockiert die Registrierung für einen Benutzer oder eine Domäne. Der Benutzer kann ein geschütztes Office-Dokument oder eine .xen-Datei nicht öffnen.

Full Access-Liste – Gewährt Registrierung und Dateizugriff für einen Benutzer oder einer Domäne. Wenn ein Benutzer oder eine Domain auch auf der Blacklist ist, soll kein Zugriff gewährt werden.

4 Geben Sie im Feld „Enter Domain/Email“ (Domäne/E-Mail eingeben) entweder die Benutzerdomäne ein, um den Zugriff für die gesamte Domäne einzustellen, oder geben Sie die E-Mail-Adresse ein, um den Zugriff zur für diesen Benutzer einzustellen.

5 Klicken Sie auf **Hinzufügen**.

Weitere Informationen zur Verwendung der Full Access-Liste/Blacklist finden Sie in der *Administrator-Hilfe*, die über die Dell Server Remote Management Console zugänglich ist.

Einem externen Benutzer kann Zugriff von einem internen Benutzer anfordern, um den Schlüssel zu einer geschützten Datei zu erhalten. Wenn der interne Benutzer nicht verfügbar ist, können Sie die Remote Management Console zur Genehmigung oder Verweigerung des Zugriffs verwenden.

1 Wählen Sie **Verwaltung > Schlüsselanforderungsverwaltung**.
2 Weitere Informationen erhalten Sie durch Klicken auf **?.** (Hilfe).

GUID-038F598E-1FF3-4FC8-A419-2F628C92F934

Remote-Löschen eines Dropbox für Unternehmen-Mitarbeiterkontos

Sollte Ihr Unternehmen über Dropbox für Unternehmen verfügen, können Sie einen Mitarbeiter per Fernzugriff aus dem Dropbox für Unternehmen-Teamkonto löschen, z. B. wenn der Mitarbeiter das Unternehmen verlässt. Dateien und Ordner, die im Zusammenhang mit den Mitarbeiterkonto stehen, werden von allen Geräten, die von dem Konto genutzt werden, entfernt. Dies widerruft den Benutzerzugriff auf diese Dateien.

Voraussetzungen

ANMERKUNG:
Bevor Sie diesen Vorgang ausführen, müssen Sie alle Dateien oder Ordner des Mitarbeiterkontos, die das Unternehmen oder andere Dropbox-Benutzer des Unternehmens eventuell noch benötigen, sichern.

Nur die Dropbox für Unternehmen-Administratoren können ein Dropbox für Unternehmenskonto über Fernzugriff löschen.

Der Endbenutzer muss Dell Data Guardian aktiviert haben und mit Dropbox für Unternehmen verbunden sein.

Registrieren in der Remote Management Console

Es muss sich nur ein Dropbox für Unternehmen-Administrator registrieren.

1 Wählen Sie im linken Fensterbereich der Remote Management Console **Verwaltung** > **Dropbox-Verwaltung** aus.
2 Klicken Sie auf der Dropbox for Business-Seite auf **Registrieren**.
Der Browser öffnet die Seite Dropbox für Unternehmen.
3 Melden Sie sich, wenn Sie aufgefordert werden, bei der Dropbox mit Ihrem Dropbox für Unternehmen-Administrator-Konto an.
4 Um Zugriff auf auf Dell Data Guardian zu erhalten, klicken Sie auf **Zulassen**.
Eine Bestätigungsseite wird angezeigt, um anzuzeigen, dass eine Dropbox-Authorisierung zu dem DDP-Unternehmensserver - VE eingeräumt wurde.
5 Kehren Sie in der Remote Management Console zurück zu **Verwaltung** > **Dropbox-Verwaltung** und klicken Sie auf **Aktualisieren**.
Der Name des Administrators wird angezeigt.

ANMERKUNG:
In der Regel empfiehlt es sich, die Registrierung nicht aufzuheben. Um allerdings die Berechtigungen eines Dropbox für Unternehmen-Administrators zum Entfernen von Mitarbeitern aus dem Dropbox für Unternehmen-Team zu entziehen, klicken Sie auf **Registrierung aufheben**.

Remote-Löschen eines Mitarbeiterkontos

ANMERKUNG:
Die Remote-Löschen-Option steht nur für registrierte Dropbox für Unternehmen-Mitarbeiterkonten zur Verfügung. Wenn die Remote-Löschen-Option für das Benutzerkonto angezeigt wird, hat sich der Benutzer nicht für ein Dropbox für Unternehmen-Konto registriert.

1 Wählen Sie in der Remote-Verwaltungskonsole **Bestückungen** > **Benutzer** im linken Fensterbereich aus.

2 Nach dem angegebenen Benutzer suchen.

3 Greifen Sie auf die Seite **Benutzerdetails** zu.

4 Klicken Sie in der Befehlsspalte auf **Per remote löschen**.
Das Remote-Löschen wird ausgeführt.

> **ANMERKUNG:**
> Bevor Sie das Remote-Löschen ausführen, müssen Sie alle Dateien oder Ordner des Mitarbeiterkontos, die das Unternehmen oder andere Dropbox-Benutzer des Unternehmens eventuell noch benötigen, speichern.

5 Klicken Sie im Bestätigungsdialogfeld für den Vorgang „Per remote löschen“ auf **Ja**.
Die Benutzerdetailsseite führt das Datum auf an dem das Remote-Löscen ausgeführt wurde.

6 Aktualisieren Sie auf Ihrer Seite Dropbox für Unternehmen Administrator Console-Mitglieder die Liste der Mitarbeiter.
Der Benutzer wird aus der Liste entfernt. Sie können die Registerkarte **Entfernte Mitarbeiter** auswählen, um anzuzeigen, welche Benutzer entfernt wurden.

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

Client-Aufgaben

GUID-88098FA1-F419-45AD-A4BA-F5C30D04DDE3

Voraussetzungen

- Stellen Sie sicher, dass die Zielgeräte folgende Konnektivität herstellen können:
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- Stellen Sie sicher, dass der Benutzer, der die Installation durchführt, über ein lokales Administratorkonto für die Installation verfügt.
- Falls die Installation über die Befehlszeile erfolgt, sollten Sie sicherstellen, dass Sie über den vollständigen Domänennamen des Dell Security Servers verfügen, bei dem sich die Benutzer aktivieren.

GUID-5A15F45E-2F97-4EB4-90CD-66CD73275BAB

Bewährte Verfahren

Stellen Sie bei der Bereitstellung sicher, dass Sie nach bewährten IT-Verfahren vorgehen. Dies umfasst unter anderem Folgendes:

- Kontrollierte Testumgebungen für anfängliche Tests
- Stufenweise Bereitstellungen für Benutzer

GUID-CF4B86F3-DBAF-4834-B15B-8615EEA72B9D

Client-Installation

Benutzer, die zur Positivliste hinzugefügt wurden, können sich hier registrieren: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Sobald sich ein Benutzer registriert hat, erhält er eine E-Mail mit einem Link zu https://sicherheitsservername.domäne.de:8443/cloudweb, damit er sich dort anmelden und den entsprechenden Client herunterladen kann.

Der Mac-Client braucht nicht vom Administrator installiert zu werden, denn die Benutzer können ihn normalerweise selbst (nach der Registrierung) über https://yoursecurityservername.domain.com:8443/cloudweb installieren.

Sie als Administrator können den Mac-Client jedoch auch selbst installieren, wenn dies von Ihrem Unternehmen gewünscht wird. Installieren Sie den Data Guardian-Client mit einer für Ihr Unternehmen verfügbaren Push-Technologie über die Benutzeroberfläche oder über die Befehlszeile. Endbenutzer müssen in diesem Fall jedoch trotzdem die Registrierung und Aktivierung selbst vornehmen.

Upgrade von früheren Versionen von Cloud Edition

Wenn ein Unternehmen verfügt über eine vorherige Version von Cloud Edition verfügt und ein Upgrade auf Data Guardian durchführt, wird die vorherige Version von Cloud Edition entfernt.

ANMERKUNG:
Wenn das Unternehmen ein Upgrade von Cloud Edition auf Data Guardian durchführt, müssen Benutzer Data Guardian authentifizieren und mit ihrem Cloud-Speicheranbieter neu verknüpfen. Weitere Informationen zur Authentifizierung finden Sie in der Dell Data Guardian-Onlinehilfe.

Installationsoptionen

Wählen Sie zum Installieren/Aktualisieren des Clients eine der folgenden Optionen aus:

- Interaktive Installation: Dies ist die einfachste Methode für die Installation von Data Guardian für Mac. Verwenden Sie diese Methode jedoch nur dann, wenn Sie die Clients nacheinander auf den Computern installieren möchten.

  oder

- Installation über die Befehlszeile: Für diese erweiterte Installationsmethode müssen Administratoren Erfahrung mit der-Befehlszeilensyntax haben. Diese Methode eignet sich für eine skriptgesteuerte Installation unter Verwendung von Batchdateien oder einer anderen verfügbaren Push-Technologie.

Interaktive Installation

1. Für den Data Guardian-Client suchen Sie das Installationsprogramm in **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Verwenden Sie die .**pkg-** Datei in DDPSL-Explorer-0.x.x.xxxx.dmg für Installationen oder Upgrades. Sie können dafür eine skriptgesteuerte Installation, Batchdateien oder eine andere in Ihrem Unternehmen verfügbare Push-Technologie nutzen.
3. Doppelklicken Sie auf das **Dell-Data-Guardian-x.x.x**-Paket.
4. Klicken Sie auf **Weiter**.
5. Klicken Sie im Fenster „Einführung“ auf **Fortfahren**.
6. Klicken Sie im Fenster „Softwarelizenzvereinbarung“ auf **Fortfahren**.
7. Klicken Sie auf **Zustimmen**, um fortzufahren.
8. Führen Sie im Fenster „Installationstyp“ einen der folgenden Schritte aus:
   - Klicken Sie auf **Installieren** und dann fahren Sie mit Schritt 9 fort.
   - Wählen Sie im Fenster für die Zielauswahl eine der nachfolgenden Optionen, klicken Sie auf **Installation fortsetzen** und fahren Sie dann mit Schritt 9 fort.
     - Installation für alle Benutzer dieses Computers durchführen
     - Installation nur für mich durchführen
9. Geben Sie Ihren Namen und Ihr Passwort in das Dialogfeld ein, und klicken Sie auf **Software installieren**.
10. Klicken Sie im Fenster „Zusammenfassung“ auf **Schließen**.
11. Siehe Endbenutzer-Aktivierung.

ANMERKUNG:
Wenn das Unternehmen ein Upgrade von Cloud Edition auf Data Guardian durchführt, müssen Benutzer Data Guardian authentifizieren und mit ihrem Cloud-Speicheranbieter neu verknüpfen. Weitere Informationen zur Authentifizierung finden Sie in der Dell Data Guardian-Onlinehilfe.

Installation über die Befehlszeile

1. Laden Sie die .dmg.
2. Führen Sie eine Installation über die Befehlszeile durch, indem Sie den folgenden Installationsbefehl ausgeben:

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

3 Leiten Sie die Endbenutzer bei der Aktivierung von Data Guardian an. Siehe Endbenutzer-Aktivierung.

Data Guardian-Aktivierung und -Benutzererfahrung

GUID-FCD7AF63-06D4-4D0C-8FA3-369265AB00E2

Endbenutzer-Aktivierung

Führen Sie nach dem erstmaligen Öffnen von Dell Data Guardian auf dem Mac die folgenden Schritte aus:

1 Wählen Sie im Finder **Anwendungen** aus, und doppelklicken Sie auf **Dell Data Guardian**.

2 Wenn das Dell Server-Fenster geöffnet wird, geben Sie die DDP-Serveradresse ein, und klicken Sie auf **Speichern**.

Das Fenster „Anmeldeinformationen“ wird angezeigt.

3 Geben Sie Ihre Domänen-E-Mail-Adresse und Ihr Domänenpasswort ein.

4 Klicken Sie auf **Anmelden**, um Dell Data Guardian zu aktivieren.

Nachdem die Dell Data Guardian-Anwendung geöffnet und erfolgreich aktiviert wurde, wird im linken Bereich der Name des Cloud-Speicheranbieters angezeigt.

Wenn in einer Unternehmensumgebung alle Benutzer denselben Cloud-Anbieter nutzen sollen, kann der Administrator eine Richtlinie festlegen, mit der nur der betreffende Anbieter aktiviert wird, während alle anderen Anbieter ausgeblendet werden.

Falls die Aktivierung nicht erfolgreich war oder wenn die Authentifizierung für die Dell Data Guardian-Anwendung widerrufen wurde oder abgelaufen ist, ist der Name des Cloud-Speicheranbieters ausgegraut.

5 Wählen Sie den Cloud-Speicheranbieter im linken Fensterbereich aus.

Es wird ein Fenster angezeigt, in dem Sie zur Eingabe Ihrer Anmeldeinformationen aufgefordert werden.

6 Weitere Informationen zur Authentifizierung finden Sie in der Dell Data Guardian-Onlinehilfe.

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

Benutzeroberfläche

Die Benutzeroberfläche von Dell Data Guardian ähnelt der *Spaltenansicht* in OS X Finder. Jede Spalte stellt einen Ordner des ausgewählten Cloud-Speicheranbieters dar.

ANMERKUNG:
Die Titelleiste kann je nach Betriebssystem unterschiedlich sein.

Sie sollten Dateien auf der Dell Data Guardian-Oberfläche verschlüsseln und entschlüsseln, und nicht auf der Website des Cloud-Speicheranbieters.

Folgende Aufgaben können Sie im Fenster von Dell Data Guardian durchführen:

- **Datei** > **Neuer Ordner** : zur Erstellung neuer Ordner.

ANMERKUNG:
Google Drive und OneDrive fügen automatisch einen Ordner vom Typ „Freigegeben“ hinzu. Die Datenfreigabe wird in OneDrive für Unternehmen jedoch nicht unterstützt.

- Kontextmenü – Wählen Sie einen oder mehrere Ordner im Hauptfenster aus. Drücken Sie die Strg-Taste und klicken Sie (oder klicken Sie mit der rechten Maustaste), und wählen Sie eine Menüoption aus:
  - **Download**
  - **Umbenennen**: Beim Umbenennen einer Datei in der Dell Data Guardian-Oberfläche synchronisiert Dell Data Guardian die Änderung auf der Cloud-Speicheranbieter-Website. Sie sollten eine .xen-Datei nicht auf der Website des Cloud-Speicheranbieters umbenennen. Dieser Vorgang würde nicht synchronisiert werden.
  - **Löschen**

    ANMERKUNG:
    In Google Drive mit Data Guardian gibt es keine Option zum Entfernen (entfernen in den Papierkorb). Es verfügt nur über die Option „Löschen“, um die Konformität mit anderen Data Guardian-Funktionen sicherzustellen.
- **Verknüpfung aufheben**: Um die Verknüpfung von Dell Data Guardian mit einem Cloud-Speicheranbieter aufzuheben, wählen Sie den Anbieter im linken Fensterbereich aus und öffnen Sie das Kontextmenü, indem Sie bei gedrückter Control-Taste mit der Maustaste klicken (oder einen Rechtsklick ausführen). Wählen Sie dann im Kontextmenü die Option „Verknüpfung aufheben“.

Zusätzliche Informationen zu Dateien und Ordnern:

- Um Dateien und Ordner zu den in Dell Data Guardian angezeigten Ordnern hinzuzufügen, ziehen Sie sie aus OS X Finder oder anderen Anwendungen, die das Drag-and-Drop-Verfahren unterstützen, in das Dell Data Guardian Fenster. Die Dateien werden basierend auf der derzeitigen Richtlinie verschlüsselt.
- Um Dateien in Anwendungen zu entschlüsseln und zu öffnen, doppelklicken Sie im Fenster von Dell Data Guardian auf die jeweilige Datei. Falls die Datei in einer externen Anwendung modifiziert wurde, wird die modifizierte Datei anschließend verschlüsselt und als neue Version zum Cloud-Speicheranbieter hochgeladen.
- Um eine unverschlüsselte lokale Kopie zu erstellen, ziehen Sie eine Datei oder einen Ordner aus dem Dell Data Guardian-Fenster in das Fenster von Finder.
- Die *Cloud-Verschlüsselung* von Data Guardian lässt die Bearbeitung von Dateien ohne Erweiterung nicht zu. Diese Dateien werden als schreibgeschützte Dateien behandelt. Um eine Datei ohne Erweiterung zu bearbeiten, laden Sie diese von der Website des Cloud-Speicheranbieters herunter, bearbeiten Sie sie, und laden Sie sie anschließend über die Dell Data Guardian-Oberfläche wieder hoch.
- Erweiterte Attribute werden nicht in die Cloud kopiert.

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

Vermeiden Sie die Verwendung der Option zum Auschecken auf der Website.

Data Guardian unterstützt nicht den Schutz oder die Verschlüsselung von Dateien, die mit der Option *Öffnen & Auschecken* auf der OneDrive for Business-Website oder einer beliebigen Cloud-Speicheranbieter-Website verwendeten werden. Wenn eine Datei geöffnet und ausgecheckt ist, verwenden Sie nicht den Befehl zum Öffnen auf der Dell Data Guardian-Oberfläche, da ansonsten das automatische Hochladen blockiert wird.

Verwenden Sie beim Schützen Ihrer Dateien mit Data Guardian die Dell Data Guardian-Schnittstelle zum Arbeiten mit Dateien.

Gehen Sie folgendermaßen vor, wenn Sie über die Website eines Cloud-Speicheranbieters an einer Datei mit besonderen Eigenschaften arbeiten möchten:

1. Drücken Sie auf der Dell Data Guardian-Oberfläche die Strg-Taste und klicken Sie auf eine Datei (oder klicken Sie mit der rechten Maustaste) und wählen Sie **Herunterladen**.
2. Wählen Sie die Datei aus, und bearbeiten Sie sie.
3. Laden Sie die Datei über die Dell Data Guardian-Schnittstelle hoch.

GUID-B18E3439-4C04-4F3A-AADA-DD5552F902D6

Anwendungsvoreinstellungen

So starten Sie die Voreinstellungen:

1 Starten Sie Dell Data Guardian.
2 Wählen Sie in der Dell Data Guardian Menüleiste **Einstellungen** aus.

ANMERKUNG:
Diese Informationen können Sie auch über das Hilfesymbol aufrufen.

Folgende Einstellungen können modifiziert werden:

- Ausblenden von Dateien, die mit „.“ beginnen: Standardmäßig ist das Kästchen aktiviert, und die Dateien werden ausgeblendet. Um ausgeblendete Dateien anzuzeigen, heben Sie die Markierung des Kästchens auf.

  ANMERKUNG:
  Im Allgemeinen sind Dateien mit einem vorangestellten Punkt als Trennzeichen im OS X Finder ausgeblendet.

- **Verknüpfung zu Cloud-Speicheranbieter aufheben**: Listet alle Cloud-Speicheranbieter auf, die von Data Guardian authentifiziert wurden. Um einen Cloud-Speicheranbieter aus Data Guardian zu entfernen, wählen Sie den Namen des Anbieters aus, und klicken Sie im Fenster „Voreinstellungen“ unten links auf das Minuszeichen (-).

Serverrichtlinien: Der DDP-Serveradministrator konfiguriert die folgenden Richtlinien, um anzugeben, wie Data Guardian Dateien und Ordner verwalten soll:

- **DDP Server** – Gibt die URL des Servers an.
- **Abfrageintervall** – Gibt das Intervall in Minuten an, in dem die Client-Software Richtlinienaktualisierungen abfragt.
- **Verschlüsseln**: Master-Verschlüsselungsrichtlinie, die die Verschlüsselung von Dateien und Ordnern auf der Cloud-Speicher-Website ermöglicht.
- **Nur Erweiterung** oder **Ausblenden**

  Nur Erweiterung (Standardeinstellung der Richtlinie) zeigt den Dateinamen auf der Website an.

  Falls ein Unternehmen zusätzlichen Schutz für Dateien verlangt, setzen Sie diese Richtlinie auf **Ausblenden**, um die Dateinamen auf der Cloud-Website auszublenden und nur den GUID-Namen anzuzeigen.

  ANMERKUNG:
  Wenn die Richtlinie zuerst auf „Nur Erweiterung“ gesetzt ist und Benutzer Dateien auf der Cloud-Website abgelegt haben, und die Richtlinie anschließend auf „Ausblenden“ gesetzt wird, werden die Namen der bereits auf der Website vorhandenen Dateien nicht ausgeblendet. Um die Namen der bereits vorhandenen Dateien auszublenden, muss der Benutzer diese herunterladen und anschließend über die Data Guardian-Oberfläche wieder hochladen. Wenn der Benutzer eine Datei bearbeitet, wird diese mit ausgeblendetem Dateinamen hochgeladen.

- **Geschützte Office-Dokumente:** schützt Office-Dokumente (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) in der Cloud, zeigt jedoch die Dateierweiterung und keine .xen-Erweiterung an.

  Wenn diese Richtlinie aktiviert ist, wird für Office-Dokumente (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) in der Cloud die Dateierweiterung und keine .xen-Erweiterung angezeigt. Die Datei kann jedoch nicht in der Cloud und auch nicht nach dem Download geöffnet werden. Wenn sie geöffnet wird, wird nur ein Deckblatt wird, das besagt, dass das Dokument geschützt ist. Wenn Sie Data Guardian installiert jedoch nicht authentifiziert haben, weist das Deckblatt darauf hin.
- **Audit-Ereignisse** – Wenn diese Option aktiviert ist, werden Ereignisse vom Typ "Audit" an den Dell Server gesendet.
- **Geografischer Standort** – Wenn diese Option aktiviert ist, werden Audit-Ereignisse an den Dell Server gesendet, die auch geografische Daten enthalten (Längen- und Breitengrad).

- **Rückrufsignal** – Wenn diese Option aktiviert ist, wird ein Rückrufsignal in alle geschützten Office-Dateien eingefügt.
- **Rückrufsignal URL** – Wenn diese Option aktiviert ist, wird die URL angegeben, die verwendet wird, wenn ein Rückrufsignal in geschützte Office-Dateien eingefügt wird.
- **Cloud-Speicherschutzanbieter**: Ein Anbietername wird basierend auf den Richtlinieneinstellungen angezeigt. Mögliche Optionen sind **Box/ Dropbox/ Google Drive / OneDrive OneDrive for Business.**

  Aktivieren oder deaktivieren Sie die Verschlüsselung von Dateien, die zu diesem Cloud-Speicheranbieter hochgeladen werden. Einer der folgenden Werte wird angezeigt:

  - **Verschlüsseln**: Dateien, die in die Cloud gesendet werden, werden verschlüsselt.
  - **Zulassen**: Der Benutzer kann auf Dateien in der Cloud zugreifen, aber die an eine Cloud-Speicheranbieter-Website gesendeten Dateien werden nicht verschlüsselt.
  - **Blockiert**: Der Cloud-Speicheranbieter ist nicht verfügbar, weshalb der Name des Cloud-Speicheranbieters nicht im Hauptfenster angezeigt wird.

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

Sicherheits- und anderen Erwägungen für die Verwendung von Data Guardian mit Cloud-Synchronisierungs-Clients

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

Google Drive

Die *Cloud-Verschlüsselung* von Data Guardian verschlüsselt Ordner und Dateien in der Cloud, um Daten zu schützen. Beachten Sie folgende Aspekte.

- Eine Unternehmenssicherheitsrichtlinie mit dem Parameter „Schützen“ verbietet Verwendung von Google Docs mit Data Guardian. Wenn die Einstellung „Zulassen“ lautet, können Sie sie bearbeiten. Weitere Informationen erhalten Sie von Ihrem IT-Administrator.

  Google Drive enthält eine App mit dem Namen Google Docs, die es Benutzern ermöglicht, in Echtzeit gemeinsam an Dokumenten zu arbeiten. Die Zusammenarbeit findet jedoch auf einem Server von Google statt, und die Dateien werden nicht verschlüsselt. Google Docs, die Sie erstellen, werden im Google Docs-Ordner des jeweiligen Cloud-Speicheranbieters angezeigt.

  Wenn Sie den Ordner öffnen, werden Sie jedoch darauf hingewiesen, dass Data Guardian das Dokument nicht verschlüsseln kann.

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

OneDrive für Unternehmen

Die Datenfreigabe wird in OneDrive für Unternehmen nicht unterstützt.

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

Feedback zu diesem Produkt

Falls per Richtlinie aktiviert, können Benutzer Feedback zu Dell Data Guardian abgeben. Das Feedback-Formular ist verfügbar über die Menüleiste > **Feedback zu Dell Data geben**.

Data Guardian-Deinstallationsaufgaben

In diesem Abschnitt wird beschrieben, wie Administratoren Data Guardian deinstallieren. Wenn ein Endbenutzer über ein lokales Administratorkonto verfügt, kann er Data Guardian für Mac selbst deinstallieren.

GUID-0AEC84CA-AADA-44B7-A403-5D8C97FFAFD5

Voraussetzungen

Zur Deinstallation benötigen Sie ein lokales Administratorkonto.

GUID-C8A4F2ED-6FE8-4B26-A3FB-60795DD70304

Data Guardian deinstallieren

Wählen Sie eines der nachfolgenden Verfahren, um Data Guardian zu entfernen:

Finder

1 Halten Sie die Taste <Option> gedrückt, und wählen Sie **Gehe zu** aus der Menüleiste aus.
2 Öffnen Sie den Ordner **~/Library/Application Support/Dell**.
3 Entfernen Sie den Ordner **DataGuardian**.
4 Öffnen Sie über **Gehe zu** in der Menüleiste den Ordner „Applications“, und entfernen Sie die **Data Guardian**-Anwendung.

Terminal

Möglicherweise verfügen Sie an einem oder beiden der nachfolgenden Speicherorte über Data Guardian.

1 Verwenden Sie einen oder beide der nachfolgenden Befehle:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Entfernen Sie den Ordner **DataGuardian**.

Glossar

Aktivieren/Aktiviert – Eine Aktivierung erfolgt, wenn der Computer beim Dell Server registriert wurde und mindestens einen Satz mit Richtlinien erhalten hat.

Dell Server – Der Dell Server umfasst eine Reihe von Komponenten. Die Serverseite des Gesamtprodukts wird zusammenfassend als Dell Server bezeichnet.

Remote Management Console – Die Remote Management Console dient der unternehmensweiten Verwaltung der Installation. Die Dell Remote Management Console ist eine Komponente des Dell Servers.

Security Server: Eine Komponente des Dell Servers für die Verwaltung von Dell Data Guardian. Der Security Server gewährleistet die Sicherheit von Daten in der Cloud, unabhängig davon, für wen sie freigegeben werden. Der Security Server schützt zudem vor der Weitergabe vertraulicher Daten durch interne Geräte.

Externe Benutzer – Benutzer außerhalb der unternehmenseigenen Domänenadresse.