# Dell Data Guardian

Administratorhandbuch Ver. 1.2

## 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.**



**Dell Data Guardian-Administratorhandbuch**

2017 - 04

Rev. A01

# Inhaltsverzeichnis

# 1

# Einleitung

Alle Richtlinieninformationen und deren Beschreibungen finden Sie in der AdminHelp.

## Vor der Installation

1 Installieren Sie den EE-Server/VE-Server, bevor Sie die Clients bereitstellen. Machen Sie das richtige Handbuch ausfindig (siehe unten), folgen Sie den Anweisungen, und kehren Sie anschließend zu diesem Handbuch zurück.

- *Installations- und Migrationshandbuch für DDP Enterprise Server*
- *Schnellanleitung und Installationshandbuch für DDP Enterprise Server – Virtual Edition*

Stellen Sie sicher, dass die Richtlinien wie gewünscht eingestellt sind. Durchsuchen Sie die AdminHilfe, die Sie über das **?** ganz rechts im Bildschirm aufrufen können. Die AdminHilfe ist eine seitenbezogene Hilfe, die eigens dafür entwickelt wurde, Sie bei der Einstellung und Änderung von Richtlinien zu unterstützten und mit den Optionen Ihres EE-Servers/VE-Servers vertraut zu machen.

2 Lesen Sie sich das Kapitel Anforderungen in diesem Dokument genau durch.

3 Stellen Sie Clients für die Endbenutzer bereit.

## Kontaktaufnahme mit dem Dell ProSupport

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.

Halten Sie bei Ihrem Anruf Ihren Service Code bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

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

2

# Anforderungen

## Server

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

## Data Guardian Client

- Bei der Implementierung sind die bewährten IT-Verfahren zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.
- Die Installation/Aktualisierung/Deinstallation kann nur von einem lokalen Benutzer oder einem Domänenadministrator durchgeführt werden, der über ein Implementierungstool wie Microsoft SMS oder KACE vorübergehend zugewiesen werden kann. Benutzer ohne Administratorstatus, aber mit höheren Rechten, werden nicht unterstützt.
- Sichern Sie vor der Installation/Deinstallation alle wichtigen Daten.
- Nehmen Sie während der Installation oder Deinstallation keine Änderungen am Computer vor, dazu gehört auch das Einsetzen oder Entfernen von externen (USB-)Laufwerken.
- Data Guardian bietet keine Unterstützung für Microsoft Office 365.
- Der Computer muss für Cloud-Verschlüsselung über ein zuweisbares Festplattenlaufwerk (Buchstabenwert) verfügen.
- Stellen Sie sicher, dass die Zielgeräte eine Verbindung zu https://sicherheitsservername.domäne.de:8443/cloudweb/register und https://sicherheitsservername.domäne.de:8443/cloudweb herstellen können.
- Vor der Implementierung von Data Guardian sollten auf den Zielgeräten möglichst keine Cloud-Speicher-Konten eingerichtet sein.

  Falls Endbenutzer ihre bereits vorhandenen Konten behalten möchten, ist darauf zu achten, dass sämtliche Dateien, die *unverschlüsselt* bleiben sollen, vor der Installation von Data Guardian aus dem Synchronisierungs-Client verschoben werden.
- Benutzer sollten beachten, dass ihre Computer nach Installation des Clients neu gestartet werden müssen.
- Data Guardian hat keinen Einfluss auf das Verhalten der Synchronisierungs-Clients. Aus diesem Grund sollten sich Administratoren und Endbenutzer mit der Funktionsweise dieser Anwendungen vertraut machen, bevor sie Data Guardian implementieren. Für weitere Informationen lesen Sie den Abschnitt Box-Support unter https://support.box.com/home, Dropbox-Support unter https://www.dropbox.com/help oder OneDrive-Support unter http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other
- Bei Ausführung von Office 2010: Wenn Richtlinien zum Schutz von Office-Dokumenten und Dokumente mit aktivierten Makros eingerichtet wurden, müssen die Benutzer über Office 2010 Service Pack 1 oder höher verfügen (Ver. 14.0.6029 oder höher). Unter https://support.microsoft.com/en-us/kb/2121559 erfahren Sie, wie Sie feststellen können, ob ein Service Pack auf eine Microsoft Office 2010 Suite angewendet wurde. Ohne diese Aktualisierung kann nicht auf geschützte Dokumente zugegriffen werden. Neue Office-Dokumente sind unabhängig von der Richtlinie ungeschützt, es sei denn die Suchfunktion ist aktiviert. Die nächste Suche konvertiert Office-Dokumente in geschützte Dateien, aber die Benutzer können ohne eine unterstützte Office-Version nicht darauf zugreifen.
- Obwohl Dell Encryption nicht erforderlich ist, sollte, sofern verwendet, der Verschlüsselungs-Client Ver. 8.12 oder höher sein.
- Data Guardian unterstützt das Windows Systemwiederherstellungstool nicht.
- Überprüfen Sie regelmäßig die Website www.dell.com/support, um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.

## Voraussetzungen für den Client

Falls noch nicht geschehen, installiert das Installationsprogramm Microsoft Visual C++ 2015 Redistributable Package (x86 und x64).

**ANMERKUNG:**

Für Windows 7 und Windows 8.1 sollten die Computer bezüglich der Windows-Updates auf dem neuesten Stand sein. Weitere Informationen finden Sie unter https://support.microsoft.com/en-us/help/2919355 und https://support.microsoft.com/en-us/help/2999226.

Microsoft .Net 4.5.2 (oder höher) ist für Data Guardian erforderlich. Auf allen von Dell werksseitig ausgelieferten Computern ist .Net 4.5.2 bereits vorinstalliert. Wenn Sie jedoch keine Dell-Hardware verwenden oder Data Guardian auf älterer Dell-Hardware aufrüsten, sollten Sie überprüfen, welche .Net-Version installiert ist und diese gegebenenfalls aktualisieren, bevor Sie Dell Data Guardian installieren, um Fehler bei der Installation/Aktualisierung zu vermeiden. Um die installierte Version von .Net zu überprüfen, folgen Sie auf dem Computer, auf dem die Installation vollzogen werden soll, den folgenden Anweisungen: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx.. Zur Installation von Microsoft .Net Framework 4.5.2 gehen Sie zu https://www.microsoft.com/en-us/download/details.aspx?id=42643.

# Windows-Client-Hardware

Die Mindestanforderungen für die Hardware müssen den Mindestspezifikationen des Betriebssystems entsprechen. In der folgenden Tabelle ist die unterstützte Hardware für den Windows-Client aufgeführt.

**Windows-Hardware**

- 200 MB freier Speicherplatz, je nach Betriebssystem
- Netzwerkschnittstellenkarte 10/100/1000 oder Wi-Fi
- TCP/IP installiert und aktiviert

Wenn Ihr Unternehmen Daten für die Speicherung in der Cloud verschlüsselt, muss auf Ihrem Computer ein Buchstabe für die Zuweisung zu einem Festplattenlaufwerk verfügbar sein.

# Betriebssysteme

In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

**Windows-Betriebssysteme (32-Bit und 64-Bit)**

- Windows 7 SP0-SP1
- Windows 8,1
- Windows 10

**ANMERKUNG:**

Windows 7 wird mit der Geolocation-Richtlinie für Data Guardian-Audit-Ereignisse nicht unterstützt.

**Android-Betriebssysteme**

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

**iOS-Betriebssysteme**

- iOS 8.x
- iOS 9.x

- iOS 10.x–10.3

# Cloud Sync Clients

In der folgenden Tabelle sind Cloud-Synchronisierungs-Clients aufgeführt, die mit Data Guardian kompatibel sind. Für Synchronisierungs-Clients werden ziemlich häufig Aktualisierungen herausgegeben. Dell empfiehlt, neue Versionen von Synchronisierungs-Clients vor der Implementierung in die Produktionsumgebung zunächst mit Data Guardian zu testen.

**Cloud Sync Clients**

- Dropbox
- Dropbox für Unternehmen (nur Windows)

  **ANMERKUNG:**
  Je nach der von Ihrem Unternehmen verwendeten Dell Serverversion werden alle Dateien und Ordner in persönlichen Dropbox-Konten, die mit Geschäftskonten verknüpft sind, evtl. verschlüsselt.

- Box® ist eine eingetragene Marke von Box.

  **ANMERKUNG:**
  Die Felder „Tools“ und „Bearbeiten“ werden bei Data Guardian nicht unterstützt. Die Verwendung des Feldes „Tools“ kann zu einem BlueScreen-Zustand führen.

- Google Drive
- OneDrive
- OneDrive für Unternehmen
- Unified OneDrive

  **ANMERKUNG:**
  Unified OneDrive ist ein einheitlicher Synchronisierungs-Client für OneDrive und OneDrive für Unternehmen.

# Webbrowser

Sie können Data Guardian > Cloud-Verschlüsselung mit Internet Explorer, Mozilla Firefox oder Google Chrome verwenden.

**ANMERKUNG:**
Data Guardian > Cloud-Verschlüsselung bietet keine Unterstützung für den Microsoft Edge-Browser.

# Sprachunterstützung

Diese Clients sind MUI-konform (Multilingual User Interface) und unterstützen die folgenden Sprachen.

**Sprachunterstützung**

- EN: Englisch
- ES: Spanisch
- FR: Französisch
- JA: Japanisch
- KO: Koreanisch
- PT-BR: Portugiesisch, Brasilien

**Sprachunterstützung**

- IT: Italienisch
- DE: Deutsch
- PT-PT: Portugiesisch, Portugal

# 3

# Registrierungseinstellungen

- In diesem Abschnitt werden alle vom Dell ProSupport genehmigten Registrierungseinstellungen für lokale **Client**-Computer beschrieben, unabhängig vom Grund für Registrierungseinstellung. Falls eine Registrierungeinstellung für zwei Produkte gilt, wird sie in beiden Kategorien aufgeführt.
- Diese Registrierungsänderungen sollten nur von Administratoren ausgeführt werden und sind möglicherweise nicht für alle Szenarios geeignet oder funktionieren nicht in allen Szenarios.

## Data Guardian Client – Registry-Einstellungen

- Protokollebenen können zur Fehlerbehebung erhöht werden. So erstellen oder ändern Sie die folgenden Registrierungseinstellungen:

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

  „LogVerbosity“=dword:0x1f (31)

  Die Protokollebene ist standardmäßig auf 0xf (15) gesetzt.

  Mögliche Werte:

  Aus= 0x0 (0)

  Kritisch= 0x1 (1)

  Fehler= 0x3 (3)

  Warnung= 0x7 (7)

  Information= 0xf (15)

  Debuggen= 0x1f (31)

- Nach der Installation von Data Guardian werden interne Benutzer automatisch aktiviert. Falls erforderlich, können Sie eine Registry-Einstellung zur Übersteuerung der automatischen Aktivierung ändern.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  DWORD-Wert: DisableAutomaticActivation=1

  **ANMERKUNG:**
  Sie können auch die Aliase für Ihre Domäne auf dem Dell Server bestätigen. Siehe Fehlerbehebung bei Problemen mit der automatischen Aktivierung.

# Konfiguration von Servern für Data Guardian

Je nach den vom Administrator festgelegten Richtlinien werden Daten mit Data Guardian folgendermaßen geschützt:

- Cloud-basierte File-Sharing-Systeme - Windows-Computer oder mobile Geräte erfassen Daten, die für die Speicherung in der Cloud gedacht sind, verschlüsseln diese Daten und laden die verschlüsselten Daten anschließend in die Cloud.
- Lokal gespeicherte Office-Dokumente, die gemeinsam mit anderen Benutzern auf verschiedene Weise genutzt oder auf einem Wechselmedium gespeichert werden. Folgende Office-Dokumente können geschützt werden: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

Teilen Sie den Benutzern mit, ob Ihr Unternehmen Data Guardian nur mit Cloud-Speicherung, nur mit Office-Dokumenten oder mit beidem nutzt.

## Konfiguration von VE Server für Data Guardian

Um VE Server zur Unterstützung von Data Guardian zu konfigurieren, setzen Sie in der Remote Management Console eine oder beide Data Guardian Richtlinien auf „Ein“:

- *Geschützte Office-Dokumente* - nur Unternehmensebene
- *Cloud Verschlüsselung* - Unternehmens-, Endpunktgruppen- oder Endpunktebene

## Konfiguration von EE Server für Data Guardian

Um EE Server zur Unterstützung von Data Guardian zu konfigurieren, setzen Sie in der Remote Management Console eine oder beide Data Guardian Richtlinien auf „Ein“:

- *Geschützte Office-Dokumente* - nur Unternehmensebene
- *Cloud Verschlüsselung* - Unternehmens-, Endpunktgruppen- oder Endpunktebene

Richten Sie Security Server anschließend so ein, dass Downloads von Cloud-Clients zugelassen werden.

## Security Server so einrichten, dass Downloads von Data Guardian-Clients zugelassen werden

In diesem Abschnitt werden die Schritte erläutert, die erforderlich sind, damit Endbenutzer den Windows Data Guardian-Client von Ihrem Security Server herunterladen können.

1 Gehen Sie auf dem EE-Server zu **<Security Server-Installationsverzeichnis>\webapps\root\cloudweb\brand\dell\resources** und öffnen Sie die Datei „**messages.properties**“ mit einem Texteditor.

2 Stellen Sie sicher, dass die Einträge wie folgt lauten:

download.deviceWin.mode=remote

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

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

3 Bearbeiten Sie die Einträge wie folgt:

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

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

4 Speichern und schließen Sie die Datei.

5 Gehen Sie zu <Security Server-Installationsverzeichnis> und erstellen Sie dort einen neuen Ordner namens „Download“ (Security Server\Download).

6 Erstellen Sie im Ordner „Download“ einen neuen Ordner namens „Cloudweb“ (Security Server\Download\Cloudweb).

7 Speichern Sie die 64-Bit- und 32-Bit-Setup-Dateien für Data Guardian im Ordner „Cloudweb“ und benennen Sie sie beispielsweise in DataGuardian64.exe bzw. DataGuardian32.exe um.

Diese sind benutzerdefiniert, müssen jedoch mit den Dateinamen in der Datei „versions.xml“ übereinstimmen.

8 Starten Sie den Security Server neu, damit die Änderungen wirksam werden.

# EE-Server für automatische Downloads des Windows Data Guardian-Clients konfigurieren (optional)

Für automatische Downloads müssen die Datei „versions.xml“ und die Binärdateien sich am gleichen Speicherort befinden. Der Speicherort muss für den Client zugänglich sein, es könnte daher IIS sein, oder Sie könnten den **Security Server\Download\Cloudweb**-Ordner verwenden, den Sie erstellt haben. Hier ein Beispiel für die Konfiguration des Servers, wenn Sie den Cloudweb-Ordner verwenden.

1 Navigieren Sie zum Ordner **Security Server\Download\cloudweb**. (Siehe Schritt 6 in Security Server so einrichten, dass Downloads von Data Guardian-Clients zugelassen werden.)

2 Erstellen Sie einen Ordner mit dem Namen DataGuardianUpdate.

> **ANMERKUNG:**
> Sie können diesem Ordner auch einen anderen Namen als „DataGuardianUpdate“ geben.

3 Legen Sie die aktualisierten ausführbaren Dateien in den Ordner „DataGuardianUpdate“.

4 Erstellen Sie eine *versions.xml*-Datei im DataGuardianUpdate-Ordner.

5 Öffnen Sie mit einem Texteditor die Datei *versions.xml*, und überprüfen Sie, ob der Pfad zum Dateinamen für Ihre Umgebung stimmt.

Beispiel:

```
<?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>
```

Version: Dateiversion der aktualisierten ausführbaren Dateien

setup.exe-Dateiname: Der Setup-Name der ausführbaren Dateien wird vom Benutzer festgelegt, muss aber mit dem Setup-Namen in der Datei „messages.properties“ übereinstimmen. (Siehe Schritt 3 in Security Server so einrichten, dass Downloads von Data Guardian-Clients zugelassen werden.)

6 Speichern und schließen Sie die Datei.

7 Fügen Sie die Binärdateien zu diesem Ordner hinzu.

8 Wenn Sie IIS verwenden, starten Sie IIS neu.

9 Melden Sie sich als Dell Administrator bei der Remote Management Console an.

10 Klicken Sie im linken Fensterbereich auf **Bestückungen** > **Enterprise**, und die Registerkarte „Sicherheitsrichtlinien“ wird angezeigt.

11 Klicken Sie unter der Data Guardian-Technologiegruppe auf **Cloud-Verschlüsselung**.

12 Klicken Sie auf **Erweiterte Einstellungen anzeigen**.

13 Wechseln Sie zur Richtlinie *URL des Software-Update-Servers*, und geben Sie **https://<YOUR HOST URL > /DataGuardianUpdate** ein.

> **ANMERKUNG:**
> DataGuardianUpdate ist dabei der oben verwendete Beispielname.

14 Klicken Sie auf **Speichern**, um die Richtlinienänderungen in der Warteschlange zum Festlegen zu speichern.

15 Klicken Sie auf **Verwaltung** > **Bestätigen**.

16 Geben Sie eine Anmerkung ein und klicken Sie auf **Richtlinien festlegen**.

# Profile für Cloud-Speicherschutz-Anbieter verwalten

Data Guardian verschlüsselt Benutzerdateien und sendet Audit-Ereignisse an den EE-Server/VE-Server. Um das Verhalten für jeden unterstützten Cloud-Speicher-Anbieter zu ändern, stellen Sie jeden Anbieter auf einen dieser Werte ein:

| Wert | Beschreibung |
|---|---|
| Schützen | Anbieter bzw. Verbindung zulassen, Dateien verschlüsseln und Überprüfungsereignisse zur Datei/Ordneraktivität senden. |
| Blockieren | Den Zugriff auf den Anbieter bzw. die Verbindung sperren. |
| Zulassen | Anbieter bzw. Verbindung ohne Verschlüsselung zulassen, aber Datei/Ordneraktivität überprüfen. |
| Umgehen | Schutz des Anbieters bzw. der Verbindung ohne Verschlüsselung oder Überprüfung umgehen. Wenn dieser Wert festgelegt ist, wird der Ordner des Cloud-Speicheranbieters nicht im virtuellen Data Guardian-Laufwerk des Client-Computers angezeigt. |

Weitere Informationen finden Sie in der *Administrator-Hilfe*, auf die Sie über die Remote Management Console zugreifen können.

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

Sie können bestimmen, welche externe Benutzer sich beim EE-Server/VE zur Verwendung von Data Guardian anmelden können. Um eine entsprechende Sicherheit zu gewährleisten, stellen Sie sicher, dass Sie diese Listen sorgfältig einrichten und verwalten.

- Ein interner Benutzer befindet sich innerhalb der Domäne.
- Ein externer Benutzer ist ein Benutzer außerhalb der Domäne, entweder eine Person von einer anderen Organisation, an den ein interner Benutzer Freigabe sensible Geschäftsdokumente freigeben möchte, oder ein interner Benutzer, der von einem Gerät außerhalb der Domäne auf seinen Computer zugreifen möchte.

So lassen Sie einen Benutzer zu, der sich nicht auf der Domäne der Organisation befindet, um sich für die Verwendung von Data Guardian zu registrieren:

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.

# Erneutes Abbilden eines Computers mit Data Guardian

Wenn ein erneutes Abbild des Computers eines Remote-Benutzers erstellt werden muss und der Benutzer über Dell Data Guardian verfügt, fragen Sie, ob der Benutzer offline gearbeitet hat und währenddessen geschützte Office-Dokumente erstellt hat. Wenn dies der Fall ist, wurden für diese Dokumente Offline-Schlüssel generiert, und diese Schlüssel wurden nicht auf dem Dell Server hinterlegt.

1 Weitere Informationen zum Wiederherstellen von offline generierten Data Guardian-Schlüsseln, die nicht auf dem Dell Server hinterlegt wurden, finden Sie im *Wiederherstellungshandbuch*.

2 Überprüfen Sie, ob ein Ordner mit Offline-Schlüsseln vorhanden ist, bevor Sie ein erneutes Image des Computers des Benutzers erstellen.

   Wenn die ersten hinterlegbaren Schlüssel erstellt werden, wird ein Data Guardian-Ordner zu **C: \Programme\Dell\Dell Data Protection** hinzugefügt. Navigieren Sie zum **Ordner Data Guardian > OfflineKeys**. Wenn kein „OfflineKeys“-Ordner vorhanden ist, überprüfen Sie den Ordner **Eigene Dokumente** des Benutzers.

5

# Data Guardian installieren

Es gibt zwei Möglichkeiten, Data Guardian zu installieren:

- Data Guardian interaktiv installieren
- Data Guardian mit der Befehlszeile installieren

Data Guardian-Benutzer müssen die folgenden Schritte ausführen, um die Dateien und Ordner in ihren Cloud Synchronisierungs-Clients zu schützen. Nach Abschluss der Installation des Data Guardian-Clients müssen Benutzer einen Cloud-Speicheranbieter herunterladen:

- Der Administrator sollte angeben, welcher Anbieter für Cloud-Synchronisation zu nutzen ist.

  oder

- Falls Ihr Unternehmen Dropbox für Unternehmen oder OneDrive für Unternehmen/einheitliches OneDrive verwendet, stellen Sie den Benutzern einen Link zum Herunterladen und Installieren bereit. Beachten Sie, dass Dropbox für Unternehmen-Benutzer die Verbindung zu Dropbox für Unternehmen über Data Guardian herstellen müssen.

## Zuvor vorhandene Ordner mit nicht verschlüsselten Dateien

Bei der Implementierung von Data Guardian sollten auf den Zielgeräten möglichst kein Cloud-Speicheranbieter-Konto eingerichtet sein.

Wenn ein Cloud-Speicheranbieterkonto für Ordner eingerichtet ist, die vor der Installation von Data Guardian auf den lokalen Computer synchronisiert werden:

- Bereits vorhandene Dateien und Ordner, die in die Cloud synchronisiert werden, werden weiterhin in Klartext angezeigt.
- Dateien, die Sie zu diesen bestehenden Ordnern hinzufügen, werden weiterhin in Klartext angezeigt.
- Dateien, die aus der Cloud synchronisiert werden, sind verschlüsselt.

  Wenn Sie bereits vorhandene Dateien verschlüsselt werden sollen, navigieren Sie zum DDG VDisk Virtual Drive (erstellt, wenn Data Guardian installiert wird), erstellen Sie einen neuen Unterordner innerhalb des Cloud-Synchronisierungs-Clients und verschieben Sie die bereits vorhandenen Dateien in diesen Ordner.

## Data Guardian installieren

Sie müssen ein lokaler Administrator auf dem Computer sein, um Data Guardian zu installieren.

Auf dem Computer muss ein Buchstabe verfügbar sein, der einem Festplattenlaufwerk zugewiesen werden kann.

Seien Sie darauf vorbereitet, dass Sie den Computer nach der Installation von Data Guardian neu starten müssen.

1. Um das Data Guardian-Installationsprogramm herunterzuladen, gehen Sie zu dem durch Ihren Administrator angegebenen Speicherort.
2. Je nach Betriebssystem wählen Sie das 32-Bit- oder 64-Bit-Installationsprogramm aus (in der Regel **setup32.exe** oder **setup64.exe**) und kopieren es auf Ihren lokalen Computer.
3. Starten Sie das Installationsprogramm per Doppelklick.
4. Falls Sie eine Sicherheitswarnung erhalten, klicken Sie auf **Ausführen**.
5. Wählen Sie eine Sprache aus und klicken Sie auf **OK**.

6 Klicken Sie auf **OK**, wenn Sie zur Installation von Microsoft Visual C++ 2015 Redistributable Package oder Microsoft .NET Framework 4.0 Client Profile aufgefordert werden.

7 Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.

8 Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen, und klicken Sie auf **Weiter**.

9 Klicken Sie auf dem Bildschirm des Zielordners auf **Weiter**, um die Installation am Standardort von **C:\Programme\Dell\Dell Data Protection\Dell Data Guardian** auszuführen.

Im Verzeichnis **C:** sollten Sie Data Guardian nicht im Ordner „Benutzer“ oder „Windows“ und nicht im Stammverzeichnis eines Laufwerks installieren. Anderenfalls wird ein Fehler ausgegeben.

10 Geben Sie im Feld *Servername:* den Servernamen ein, mit dem dieser Computer kommunizieren wird, wie z. B. server.domain.com. Sie müssen www oder http(s) nicht einschließen. Diese Informationen werden von Ihrem Administrator bereitgestellt.

Deaktivieren Sie das Kontrollkästchen *Enable SSL Trust Verification* (SSL-Trust-Prüfung aktivieren) nicht, es sei denn, Ihr Administrator fordert Sie dazu auf.

11 Klicken Sie auf **Weiter**.

12 Bestätigen Sie auf dem Bildschirm „Aktivierungsserverdaten bestätigen“, dass die Server-URL-Adresse korrekt ist. Das Installationsprogramm fügt www oder http(s) und den Port hinzu. Klicken Sie auf **Weiter**.

13 Wählen Sie im Fenster „Management Type“ (Verwaltungstyp) diese Option aus:

- Interne Nutzung: Ein Benutzer mit einer E-Mail-Adresse innerhalb der Domäne des Unternehmens.

14 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Der Installationsfortschritt wird in einem Statusfenster angezeigt.

15 Klicken Sie auf **Fertigstellen**, wenn der Bildschirm „Installation abgeschlossen“ angezeigt wird.

16 Klicken Sie auf **Ja**, um neu zu starten.

Die Installation von Data Guardian ist abgeschlossen.

17 Das Data Guardian-Taskleistensymbol zeigt nach der Aktivierung ein grünes Häkchen  an. Abhängig davon, wie Data Guardian innerhalb des Unternehmens bereitgestellt wird, erfolgt die Aktivierung möglicherweise nicht sofort.

# Data Guardian mit der Befehlszeile installieren

- Bei den Befehlszeilenschaltern und -parametern ist die Groß- und Kleinschreibung zu beachten.
- Stellen Sie sicher, dass Werte, die ein oder mehrere Sonderzeichen enthalten, z. B. eine Leerstelle in der Befehlszeile, zwischen in Escape-Zeichen gesetzte Anführungszeichen gesetzt werden.
- Die folgende Tabelle umfasst die für die Installation verfügbaren Schalter.

| Schalter | Erläuterung |
|---|---|
| /V | Gibt Variablen an die .msi-Datei innerhalb der setup.exe-Datei weiter. Der Inhalt muss immer von Anführungszeichen in Klartext umrahmt sein. |
| /S | Im Hintergrund |

| Option | Erläuterung |
|---|---|
| /QB | Fortschrittsdialogfeld mit der Schaltfläche **Abbrechen,** fordert zum Neustart auf |
| /QB! | Fortschrittsdialogfeld ohne die Schaltfläche **Abbrechen**, fordert zum Neustart auf |
| /QN | Keine Benutzeroberfläche |

- Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

| Parameter |
|---|
| SERVER= <Servername> (Vollqualifizierter Domänenname des Dell Server zur Aktivierung) |
| ENTERPRISE=1 (Interner Benutzer) |

| Parameter |
| --- |
| ENABLESSLTRUST=0 (SSL Trust-Validierung deaktivieren) |
| REBOOT=SUPPRESS (Null ermöglicht automatische Neustarts, SUPPRESS deaktiviert Neustart) |

**Beispiel für eine Befehlszeile**

- Im folgenden Beispiel wird Data Guardian im Hintergrundmodus für einen internen Benutzer installiert, ohne SSL Trust-Validierung, Protokolle werden gespeichert unter C:\Library\Logs\Install.log.

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

# Data Guardian mit Dropbox für Business verwenden

Data Guardian mit Dropbox für Unternehmen bietet neben den grundlegenden Funktionen die folgenden Zusatzfunktionen für Dropbox.

- Remote-Löschen eines Mitarbeiterkontos
- Sie können Richtlinien zur Kontrolle, wie Unternehmens- oder persönliche Dropbox-Ordner geschützt werden, festlegen. Wenn Ihr Unternehmen Unternehmens- und persönliche Konten erlaubt, sollten die Endbenutzer die Verschlüsselung dieser Kontentypen verstehen. Weitere Informationen finden Sie unter Richtlinie für Unternehmens- und persönliche Konten.

## Richtlinie für Unternehmens- und persönliche Konten

Ihr Unternehmen verfügt eventuell über Richtlinien ob Mitarbeiter Unternehmens- und persönliche Konten verwenden dürfen. Desweiteren erlaubt Ihr Unternehmen eventuell nur bestimmten Mitarbeitern, dass sie über ein Unternehmens- und persönliches Konto verfügen dürfen.

**ANMERKUNG:**
Sollte Ihr Unternehmen Unternehmens- und persönliche Konten erlauben und ein Endbenutzer entscheidet sich beide zu verwenden, sollte dieser Benutzer die Ordnerverwaltung für beide Kontotypen verstehen.

Die folgende Tabelle beschreibt die Verschlüsselung auf Basis der Richtlinieneinstellung *Dropbox verschlüsselt persönliche Ordner*.

| Verschlüsselung | Richtlinieneinstellung | Bereitstellungsüberlegungen |
|---|---|---|
| Verschlüsseln Sie alle Unternehmens- und persönlichen Dateien und Ordner. | Richtlinie > Dropbox verschlüsselt persönliche Ordner > auf **Ausgewählt**eingestellt (standardmäßig) | Bevor Data Guardian bereitgestellt wird, sollten die Benutzer bereits bestehende Unternehmensdateien, die sich in Cloud-Speicher-Synchronisierungsordnern befinden, an einem Speicherort außerhalb der Synchronisierungsordner sichern.<br><br>Benutzer mit persönlichen Dateien, die unverschlüsselt bleiben sollen, müssen die Dateien aus den geschäftlichen Synchronisierungsordnern entfernen oder Verlinkungen von persönlichen Konten von den Unternehmens-Synchronisierungs-Clients entfernen.<br><br>Nachdem Data Guardian bereitgestellt wurde, können die Cloud-Dateien und -Ordner nur auf Computern die Data Guardian ausführen, angezeigt werden. Lesen Sie für den Fall, dass ein persönlicher Ordner versehentlich verschlüsselt wurde, den Abschnitt „Ordner eines persönlichen Kontos entschlüsseln“ im Dell Data Guardian-Benutzerhandbuch. |
| Verschlüsseln Sie alle Unternehmenskonten-Dateien und Ordner. | Richtlinie > Dropbox verschlüsselt persönliche Ordner > auf **Nicht ausgewählt** eingestellt | Sie können die optionale Richtlinie „Meldung über das Verschlüsseln persönlicher Dropbox-Ordner“ verwenden, um eine |

| Verschlüsselung | Richtlinieneinstellung | Bereitstellungsüberlegungen |
|---|---|---|
| Erlauben Sie, dass persönliche Kontendateien und Ordner unverschlüsselt bleiben. | | benutzerdefinierte Meldung anzuzeigen, die die Benutzer daran erinnert, **keine** Unternehmensdateien in persönlichen Konten zu speichern, da diese Dateien nicht geschützt werden. Diese Meldung wird in den folgenden Fällen angezeigt.<br>• Jedes mal wenn sich der Benutzer anmeldet<br>• Wenn der Benutzer neue Dateien erstellt oder eine neue Datei oder einen neuen Ordner zu einem persönlichen Dropbox-Konto hinzufügt<br>Wenn Sie die Richtlinie „Dropbox verschlüsselt persönliche Ordner“ für einen Endpunkt oder eine Endpunktgruppe auf **Falsch** stellen, verbleiben alle persönliche Konten aller Benutzer dieser Endpunkte unverschlüsselt. |

# Unternehmens- und persönliche Ordner

Sollte Ihr Unternehmen über Dropbox für Unternehmen verfügen und den Endbenutzern Unternehmens- sowie persönliche Ordner erlauben, sollten Sie Berichte ausführen, die sicherstellen, dass alle Unternehmensdateien über die Dateiendungen XEN verfügen, für den Fall, dass ein Endbenutzer eine sensible unverschlüsselte Datei in einen Unternehmensordner kopiert. Siehe Data Guardian – Fehlerbehebung.

# Remote-Löschen eines 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**

- Bevor Sie das Remote-Löschen ausführen, sichern Sie alle Dateien oder Ordner des Mitarbeiterkontos, die das Unternehmen oder andere Dropbox-Benutzer des Unternehmens eventuell noch benötigen.
- Nur die Dropbox für Unternehmen-Administratoren können ein Dropbox für Unternehmenskonto über Fernzugriff löschen.
- Data Guardian muss aktiviert worden sein, und der Endbenutzer muss eine Verbindung zu Dropbox für Unternehmen hergestellt haben.

# Registrieren in der Remote Management Console

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

1. Wählen Sie in der Remote-Verwaltungskonsole **Dropbox-Verwaltung** im linken Fensterbereich aus.
2. Klicken Sie 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. Klicken Sie auf **Zulassen**, um den Zugriff auf Data Guardian zuzulassen. Eine Bestätigungsseite wird angezeigt, um anzuzeigen, dass eine Dropbox-Autorisierung zu dem VE-Server eingeräumt wurde.
5. Kehren Sie in der Remote-Verwaltungskonsole zurück zu **Dropbox-Verwaltung** und aktualisieren Sie die Seite. Der Name des Administrators wird angezeigt.

**ANMERKUNG:**
In der Regel empfiehlt es sich, die Registrierung nicht aufzuheben. Um einem Administrator für „Dropbox für Unternehmen“ allerdings die Berechtigung zum Entfernen von Mitarbeitern aus „Dropbox für Unternehmen“ zu entziehen, klicken Sie auf **Registrierung aufheben**.

# Remote-Löschen eines Mitarbeiterkontos

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 Klicken Sie auf die Registerkarte **Details und Aktionen**.
4 Klicken Sie in der Befehlsspalte auf **Per remote löschen**.

**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, sichern.

5 Klicken Sie im Bestätigungsdialog „Remote-Löschen“ auf **Ja**. Die Benutzerdetailsseite führt das Datum auf an dem das Remote-Löscen ausgeführt wurde.
6 Aktualisieren Sie auf der 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 die entfernten Benutzer anzuzeigen.

# Berichte anzeigen

Informationen über Ihre Data Guardian-Umgebung sind in der Dell Server Remote Management Console verfügbar. Wählen Sie **Berichte > Audit-Ereignisse** für Audit-Ereignisse im Zusammenhang mit Cloud Synchronisierungs-Client-Ordnern und geschützten Office-Dokumente .

Weitere Informationen finden Sie in der *Administrator-Hilfe*, auf die Sie über die Remote Management Console zugreifen können.

# Data Guardian – Fehlerbehebung

## Verwenden Sie den Bildschirm „Details“

Sie können den **Details**-Bildschirm zur Fehlerbehebung oder für Support-Probleme verwenden. Beispiel:

- Wenn ein Benutzer einen Ordner erstellt, der jedoch nicht verschlüsselt wird, wählen Sie **Details** > **Dateien** > **Ordnerzustand** aus, um den Zustand zu überprüfen.
- Wenn Endbenutzer Support anfordern, können Sie sie anweisen, den Bildschirm „Erweiterte Details“ einzurichten und die Registerkarte **Details** > **Richtlinie** auszuwählen. Auf dieser Registerkarte werden die Richtlinien aufgelistet, die derzeit durchgesetzt werden.
- Sehen Sie sich die Protokolle zur Fehlerbehebung an.

## Verwenden Sie den Bildschirm „Erweiterte Details“

- Während Sie **<Strg><Umschalt>** gedrückt halten, klicken Sie auf das Data Guardian-Taskleistensymbol, und wählen Sie dann Details aus.
- Zusätzlich zu den Dateien und Ordnern wird das Folgende angezeigt:

  **Sicherheit**: Listet den Schlüssel, Schlüsseltyp und Zustand auf. In diesem Fensterbereich werden vorübergehend einige geschützte Office-Dateien aufgeführt, bis diese an den Server gesendet werden - Der Zeitraum hängt vom Abfrageintervall ab.

  **Überprüfung**: Listet die Module, die Benutzer-ID und den Ereignis-Typ auf. Die Informationen befinden sich in diesem Überwachungsprotokoll in einer Warteschlange und werden in festgelegten Intervallen an den EE Server/VE-Server gesendet. Der Administrator kann **Audit-Ereignisse** im linken Bereich der Remote Management Console zu Prüfzwecken anzeigen.

  **Richtlinie**: Listet alle Richtliniennamen und -werte auf.

## Protokolldateien anzeigen

- Klicken Sie im unteren, linken Bereich des Details-Bildschirms auf **Protokoll anzeigen** .

  Sie finden die Protokolldateien auch unter **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian**.

  Protokolldateien geschützter Office-Dokumente befinden sich im Custom.xml-Ordner.

## Fehlerbehebung bei Problemen mit der automatischen Aktivierung

Wenn Data Guardian nicht automatisch für mehrere Benutzer aktiviert wird, können Sie die Registrierungseinstellungen des Data Guardian-Clients ändern. Sie sollten auch die Aliase auf dem Dell Server überprüfen:

1. Navigieren Sie in der Remote Management Console zu **Bestückungen > Domänen** und wählen Sie eine Domäne und beliebige Subdomänen aus.
2. Klicken Sie auf der Seite „Domänendetails“ auf die Registerkarte **Einstellungen**.
3. Bestätigen Sie im Feld *Alias*, dass alle Aliase korrekt sind.

# Temporäre Ordnerverwaltungsrechte gewähren

Sie können einem Administrator oder Benutzer vorübergehende Rechte für die Verwaltung von Ordnern gewähren. Beispiel: Wenn Benutzer Dateien in die Cloud hochgeladen haben, bevor Data Guardian installiert wurde, können Sie bestimmten Benutzern temporäre Ordnerverwaltungsrechte zur Verwaltung der Verschlüsselung Ordner für Ordner innerhalb der Synchronisierungs-Client-Ordner gewähren.

So stellen Sie Ordnerverwaltungsrechte bereit:

1 Klicken Sie in der Remote-Verwaltungskonsole auf **Bestückungen** > **Endpunkte**.

2 Suchen Sie oder klicken Sie auf einen Endpunkt und anschließend auf die Registerkarte **Sicherheitsrichtlinien**.

3 Wählen Sie **Cloud-Verschlüsselung** aus, und klicken Sie dann auf **Erweiterte Einstellungen anzeigen**.

4 Klicken Sie auf das Kontrollkästchen neben dem *Ordnerverwaltung aktiviert,* um die Richtlinie auszuwählen.

5 Klicken Sie auf **Speichern**.

6 Klicken Sie im linken Fensterbereich auf **Verwaltung** > **Festlegen**.

7 Geben Sie eine Anmerkung ein und klicken Sie auf **Richtlinien festlegen**.

**ANMERKUNG:**
Dell empfiehlt, dass Sie nach der Verschlüsselung der Ordner oder Fehlerbehebung das Häkchen im Kontrollkästchen neben der Richtlinie *Ordnerverwaltung aktiviert* entfernen, um die Richtlinie für diesen Endpunkt zu deaktivieren.

So verwalten Sie Ordner am Endpunkt:

1 Erstellen Sie einen Ordner innerhalb des Synchronisierungs-Client-Ordners und fügen Sie Dateien hinzu, sodass die Dateien in der Cloud verschlüsselt werden.

2 Klicken Sie auf die Data Guardian-Taskleistensymbol und wählen Sie **Ordner verwalten** aus.

   Für jeden Synchronisierungs-Client wird eine Strukturansicht der Cloud-synchronisierten Ordner angezeigt. Alle Ordner sind standardmäßig ausgewählt. Deaktivieren Sie Ordner, die Sie nicht verschlüsseln möchten. Wenn Sie die Auswahl eines Ordners im Menü „Ordner verwalten“ aufheben, werden die in dem Ordner enthaltenen Dateien mit einer Entschlüsselungssuche entschlüsselt. Neue Dateien in diesem Ordner werden weder auf dem lokalen Laufwerk, noch in der Cloud verschlüsselt.

   **ANMERKUNG:**
   Wenn Sie eine verschlüsselte Datei in einen Ordner verschieben, der entweder in der Cloud oder auf dem virtuellen DDP|SL-Laufwerk nicht ausgewählt ist, bleibt die Datei verschlüsselt, und Sie können den Inhalt nicht anzeigen. Denken Sie daran, dass bei der Freigabe des Ordners für einen anderen Data Guardian-Benutzer, der die Richtlinie „Ordner verwalten“ nicht aktiviert hat, die Dateien verschlüsselt bleiben und er/sie sie nicht anzeigen kann.

3 Um einen bereits vorhandenen Ordner zu verschlüsseln, aktivieren Sie die Verschlüsselung für diesen Ordner manuell. Die Dateien werden verschlüsselt, wenn die Dateien mit der Cloud synchronisiert werden.

# Häufig gestellte Fragen

**Häufig gestellte Fragen zur Ordnerverwaltung**

**Frage**

Ich habe einen Ordner mit Dateien, die ich für einen anderen Benutzer freigegeben habe. Ich habe in der Taskleiste das Dienstprogramm **Data Guardian > Ordner verwalten** verwendet, um den Inhalt dieses Ordners zu entschlüsseln. Vor kurzem wurden meine Dateien in der Cloud wieder verschlüsselt. Dieser Ordner wird nicht mehr im Dienstprogramm „Ordner verwalten“ angezeigt, und daher kann ich diese Dateien in der Cloud nicht mehr entschlüsseln.

**Antwort**

Eine Verschlüsselungsschlüssel-ID wurde basierend auf dem ersten Benutzer, der diesem Ordner eine Datei hinzugefügt hat, einem Ordner zugeordnet. Falls ein Benutzer einen Ordner erstellt und keine Dateien hinzufügt, ist sein/ihr Schlüssel diesem Ordner nicht zugeordnet. Der Benutzer, dessen Verschlüsselungsschlüssel-ID auf dem Ordner eingestellt wurde, ist der einzige, der den Ordner im Dienstprogramm „Ordner verwalten“ anzeigen kann. Falls der Benutzer, dessen Verschlüsselungsschlüssel-ID für den Ordner festgelegt ist, die Markierung des Ordners im Dienstprogramm „Ordner verwalten“ aufhebt und diesen Ordner für einen anderen Data Guardian-Benutzer freigibt, wird die Data Guardian-Instanz des zweiten Benutzers den Inhalt erneut verschlüsseln.

**Lösung**

1 Erstellen Sie einen neuen Ordner.

2 Verschieben Sie alle Dateien, die verschlüsselt werden sollen, in den neuen Ordner.

3 Verwenden Sie in der Taskleiste das Dienstprogramm **Dell Data Guardian** > **Ordner verwalten** nochmals, um diese Dateien zu entschlüsseln.

**ANMERKUNG:**

Falls Sie den Schutz des Inhalts eines Ordners aufheben, den Sie für andere Benutzer mit Data Guardian freigegeben haben, zwingt die Data Guardian-Instanz des anderen Benutzers die Richtlinie, sie zu verschlüsseln. Es hat sich bewährt, das Dienstprogramm „Ordner verwalten“ nur für die Entschlüsselung von Dateien zu verwenden, die nicht gemeinsam mit anderen Data Guardian-Benutzern verwendet werden.

**Frage**

Ich synchronisiere mit einem entschlüsselten Ordner, dessen Auswahl ich mit dem Dienstprogramm „Ordner verwalten“ aufgehoben habe. Wenn ich ihn jedoch über den Webbrowser hochladen möchte, geht das nur mit verschlüsselten Dateien.

**Antwort**

Data Guardian ist nicht für die aktive Suche nach Ordnern in der Cloud konzipiert. Bei unverschlüsselten Ordnern kann Data Guardian durch den Sync-Client synchronisieren, weil es diese Umgebung kontrolliert. Wenn Dateien über den Webbrowser übertragen werden, müssen sie verschlüsselt sein.

**Lösung**

Fügen Sie die Dateien zum Synchronisierungsordner hinzu.

**Frage**

Ich habe vor kurzem mein Cloud-basiertes Dateifreigabesystem von meinem Computer deinstalliert, aber als ich das Dienstprogramm „Ordner verwalten“ öffnete, war einer der Synchronisierungs-Clients noch als Option aufgeführt.

**Antwort**

Data Guardian überwacht keine Installation oder Deinstallation der Software von Drittanbietern. Diese Optionen werden weiterhin angezeigt, weil bei der Deinstallation dieser Clients nicht automatisch auch Ihre bestehenden Dateien entfernt werden. Diese Dateien sind daher auch weiterhin durch Data Guardian geschützt, obwohl der entsprechende Synchronisierungs-Client nicht mehr vorhanden ist.

**Lösung**

Um die Option für den deinstallierten Synchronisierungs-Client aus dem Dienstprogramm „Ordner verwalten“ zu entfernen, verschieben Sie Ordner/Dateien, die Sie behalten möchten aus dem Synchronisierungsordner und löschen Sie dann den Ordner. Nach dem Löschen des Ordners wird er nicht mehr im Dienstprogramm für die Ordnerverwaltung angezeigt.

**Verschiedene Häufig gestellte Fragen**

**Frage**

Ein Benutzer hat Data Guardian mit geschützten Office-Dokumenten geöffnet und kann nicht kopieren und einfügen.

**Antwort**

Bei Data Guardian erfolgen einige Funktionen über die Systemsteuerung. Überprüfen Sie, ob der Benutzer die Systemsteuerung geändert hat.

**Lösung**

Es müssen die Standardeinstellung der Systemsteuerung verwendet werden. Der Benutzer muss die Standardeinstellungen der Systemsteuerung beibehalten.

**Frage**

Ich habe die Richtlinie **Dateinamen verbergen** von GUID auf „Nur Erweiterung“ geändert. Die bislang synchronisierten Ordner verschlüsseln die Dateien jedoch immer noch im anderen Format mit GUID-Dateinamen. Warum?

**Antwort**

Wenn eine Richtlinie auf dem EE-Server/VE-Server geändert wird, behält Data Guardian die vorherige Richtlinie für den Ordner bei. Die Richtlinie wird auf alle neu erstellten Ordner angewendet, die daher im Format **Nur Erweiterung** verschlüsselt werden.

**Lösung**

Um das Format **Nur Erweiterung** auf die alten Dateien anzuwenden, verschieben Sie sie in einen neu erstellten Ordner, auf den die neue Richtlinie angewendet wurde.

# 8

# Glossar

Advanced Authentication – Das Produkt Advanced Authentication bietet Optionen für vollständig integrierte Fingerabdrücke, Smart Card und kontaktlose Smart Card-Leser. Advanced Authentication vereinfacht die Verwaltung all dieser Hardware-Authentifizierungsmethoden, unterstützt die Anmeldung bei selbstverschlüsselnden Laufwerken, SSO und verwaltet Benutzeranmeldeinformationen und Passwörter. Darüber hinaus kann Advanced Authentication nicht nur für den Zugriff auf PCs verwendet werden, sondern auch für den Zugriff auf beliebige Websites, SaaS oder Anwendungen. Nachdem der Benutzer seine Anmeldeinformationen eingetragen hat, ermöglicht Advanced Authentication deren Verwendung für die Anmeldung am Gerät und die Ersetzung des Passworts.

BitLocker Manager – Windows BitLocker schützt Windows-Computer durch die Verschlüsselung von Daten- und Betriebssystemdateien. Um die Sicherheit von BitLocker-Implementierungen zu erhöhen und Betriebskosten zu vereinfachen sowie zu verringern, bietet Dell eine einzige, zentrale Management Console. Diese Console nimmt sich zahlreicher Sicherheitsbedenken an und bietet einen integrierten Ansatz für die Verwaltung verschlüsselter Daten auf Plattformen, die nicht zu BitLocker gehören, seien sie physisch, virtuell oder cloudbasiert. BitLocker Manager unterstützt BitLocker-Verschlüsselung für Betriebssysteme, Festplattenlaufwerke und BitLocker To Go. Mit BitLocker Manager können Sie BitLocker nahtlos in Ihre bestehende Verschlüsselung integrieren und mit minimalem Verwaltungsaufwand sowohl die Sicherheit als auch die Compliance optimieren. BitLocker Manager bietet eine integrierte Verwaltung für die Wiederherstellung von Schlüsseln, Richtlinienverwaltung und -durchsetzung, automatisierte TPM-Verwaltung, FIPS-Compliance und Compliance Reporting.

Deaktivieren – Die Deaktivierung erfolgt, wenn SED Management in der Remote-Verwaltungskonsole auf OFF gesetzt wird. Nach der Deaktivierung des Computers wird die PBA -Datenbank gelöscht, und es gibt keine Aufzeichnung der im Cache gespeicherten Benutzer mehr.

EMS (External Media Shield) - externe Medienabschirmung - Dieses Service innerhalb des Dell Encryption Client wendet Richtlinien auf Wechseldatenträger und externe Speichergeräte an.

EMS-Zugriffscode - Dieses Service innerhalb des Dell Enterprise Server/VE ermöglicht die Wiederherstellung von EMS-geschützten Geräten, wenn der Benutzer sein Kennwort vergessen hat und sich nicht mehr anmelden kann. Nach Abschluss dieses Vorgangs kann der Benutzer das auf dem Wechseldatenträger oder einem externen Speichergerät festgelegte Kennwort zurücksetzen.

Encryption-Client – Der Encryption-Client ist die geräteinterne Komponente, die Sicherheitsrichtlinien durchsetzt, egal ob ein Endpunkt mit dem Netzwerk verbunden oder vom Netzwerk getrennt ist, verloren gegangen ist oder gestohlen wurde. Der Encryption-Client erzeugt eine vertrauenswürdige Computerumgebung für Endpunkte, indem er als Layer über dem Betriebssystem des Geräts fungiert und Authentifizierung, Verschlüsselung und Autorisierung lückenlos anwendet, um den Schutz vertraulicher Informationen zu maximieren.

Endpunkt – ein Computer oder eine mobile Hardwarekomponente, der/die von Dell Enterprise Server/VE verwaltet wird.

Verschlüsselungssuche – Bei einer Verschlüsselungssuche werden die zu verschlüsselnden Ordner auf einem mit einem Shield verwalteten Endpunkt durchsucht, um sicherzustellen, dass die enthaltenen Dateien den richtigen Verschlüsselungsstatus haben. Einfache Operationen zur Erstellung und Umbenennung von Dateien lösen keine Verschlüsselungssuche aus. Es ist wichtig zu verstehen, wann eine Verschlüsselungssuche stattfindet und wodurch die Dauer der Suche beeinflusst wird: Eine Verschlüsselungssuche erfolgt sofort nach Eingang einer Richtlinie mit aktivierter Verschlüsselung. Das kann unmittelbar nach der Aktivierung sein, wenn für Ihre Richtlinie die Verschlüsselung aktiviert ist. - Wenn die Richtlinie „Workstation bei Anmeldung durchsuchen“ aktiviert ist, werden die zur Verschlüsselung angegebenen Ordner bei jeder Benutzeranmeldung durchsucht. - Eine Suche kann unter bestimmten nachfolgenden Richtlinienänderungen erneut ausgelöst werden. Jeder Richtlinienänderung, die sich auf die Definition der Verschlüsselungsordner, der Verschlüsselungsalgorithmen oder der Verwendung der Verschlüsselungsschlüssel („Allgemein“ vs. „Benutzer“) bezieht, löst eine Suche aus. Auch beim Umschalten zwischen aktivierter und deaktivierter Verschlüsselung wird eine Verschlüsselungssuche ausgelöst.

Einmalpasswort (OTP) – Ein Einmalpasswort ist ein Passwort mit begrenzter Gültigkeit, das nur einmal verwendet werden kann. Für die OTP-Funktion muss ein TPM vorhanden, aktiviert und zugewiesen sein. Für die Aktivierung der OTP-Funktion muss ein Mobilgerät mit dem Computer über die Security Console und die Security Tools Mobile-App gekoppelt werden. Die Security Tools | Mobile-App generiert das

Passwort auf dem Mobilgerät, mit dem die Anmeldung auf dem Computer über den Windows-Anmeldebildschirm erfolgt. Je nach Richtlinie kann die OTP-Funktion verwendet werden, um den Zugriff auf den Computer wiederherzustellen, falls das Passwort abgelaufen ist oder vergessen wurde, vorausgesetzt, das OTP wurde nicht bereits für die Anmeldung am Computer verwendet. Die OTP-Funktion kann zur Authentifizierung oder zur Wiederherstellung verwendet werden, aber nicht für beides. OTP ist sicherer als einige andere Authentifizierungsmethoden, weil das generierte Passwort nur einmal verwendet werden kann und nach kurzer Zeit abläuft.

SED Management – SED Management ist eine Plattform für die sichere Verwaltung selbstverschlüsselnder Laufwerke. Selbstverschlüsselnde Laufwerke haben zwar eine eigene Verschlüsselungsfunktion, ihnen fehlt aber eine Plattform für die Verwaltung ihrer Verschlüsselung mit den verfügbaren Richtlinien. SED Management ist eine zentrale, skalierbare Verwaltungskomponente, mit der Sie Daten wirksamer schützen. SED Management beschleunigt und vereinfacht die Administration von Unternehmensdaten.