

# Dell Data Guardian

Benutzerhandbuch 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.

© 2017 Dell Inc. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

Eingetragene Marken und in der Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise und Dell Data Guardian Suite von Dokumenten verwendete Marken: Dell™ und das Logo von Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® und KACE™ und Marken von Dell Inc. Cylance®, CylancePROTECT und das Cylance Logo sind eingetragene Marken von Cylance, Inc. in den USA und anderen Ländern. McAfee® und das McAfee-Logo sind Marken oder eingetragene Marken von McAfee, Inc. in den USA und anderen Ländern. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, und Xeon® sind eingetragene Marken der Intel Corporation in den USA und anderen Ländern. Adobe®, Acrobat® und Flash® sind eingetragene Marken von Adobe Systems Incorporated. Authen Tec® und Eikon® sind eingetragene Marken von Authen Tec. AMD® ist eine eingetragene Marke von Advanced Micro Devices, Inc. Microsoft®, Windows® und 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®, und Visual C++® sind entweder Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern. VMware® ist eine eingetragene Marke oder eine Marke von VMware, Inc. in den USA oder anderen Ländern. Box® ist eine eingetragene Marke von Box. DropboxSM ist eine Dienstleistungsmarke von Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® und Google™ Play sind entweder Marken oder eingetragene Marken von Google Inc. in den Vereinigten Staaten oder anderen Ländern. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® und Siri® sind entweder Dienstleistungsmarken, Marken oder eingetragene Marken von Apple, Inc. in den Vereinigten Staaten oder anderen Ländern. GO ID®, RSA® und SecurID® sind eingetragene Marken von Dell EMC. EnCase™™ und Guidance Software® sind entweder Marken oder eingetragene Marken von Guidance Software. Entrust® ist eine eingetragene Marke von Entrust®, Inc. in den USA und anderen Ländern. InstallShield® ist eine eingetragene Marke von Flexera Software in den USA, China, der EU, Hong Kong, Japan, Taiwan und Großbritannien. Micron® und RealSSD® sind eingetragene Marken von Micron Technology, Inc. in den USA und anderen Ländern. Mozilla® Firefox® ist eine eingetragene Marke von Mozilla Foundation in den USA und/oder anderen Ländern. iOS® ist eine Marke oder eingetragene Marke von Cisco Systems, Inc. in den USA und bestimmten anderen Ländern und wird in Lizenz verwendet. Oracle® und Java® sind eingetragene Marken von Oracle und/oder seinen Tochtergesellschaften. Andere Namen können Marken ihrer jeweiligen Inhaber sein. SAMSUNG™™ ist eine Marke von SAMSUNG in den USA oder anderen Ländern. Seagate® ist eine eingetragene Marke von Seagate Technology LLC in den USA und/oder anderen Ländern. Travelstar® ist eine eingetragene Marke von HGST, Inc. in den USA und anderen Ländern. UNIX® ist eine eingetragene Marke von The Open Group. VALIDITY™™ ist eine Marke von Validity Sensors, Inc. in den USA und anderen Ländern. VeriSign® und andere zugehörige Marken sind Marken oder eingetragene Marken von VeriSign, Inc. oder seinen Tochtergesellschaften und verbundenen Unternehmen in den USA und anderen Ländern und werden von der Symantec Corporation in Lizenz verwendet. KVM on IP® ist eine eingetragene Marke von Video Products. Yahoo!® ist eine eingetragene Marke von Yahoo! Inc. Dieses Produkt verwendet Teile des Programms 7-Zip. Der Quellcode ist unter [7-zip.org](http://7-zip.org) verfügbar. Die Lizenzierung erfolgt gemäß der GNU LGPL-Lizenz und den unRAR-Beschränkungen ([7-zip.org/license.txt](http://7-zip.org/license.txt)).

### Dell Data Guardian – Benutzerhandbuch

2017 - 04

Rev. A01

<b>1 Einführung in Dell Data Guardian.....</b>	<b>5</b>
Übersicht.....	5
Zusätzlicher Support.....	5
<b>2 Dell Data Guardian – Anforderungen.....</b>	<b>6</b>
Server.....	6
Encryption-Client.....	6
Voraussetzungen für den Client.....	7
Windows-Client-Hardware.....	7
Betriebssysteme.....	7
Cloud Sync Clients.....	8
Webbrowser.....	8
<b>3 Benutzeraufgaben: Cloud-Verschlüsselung und geschützte Office-Dokumente.....</b>	<b>9</b>
Überblick über die Aufgaben.....	9
Data Guardian mit Cloud und geschützten Office-Dokumenten installieren.....	11
Zuvor vorhandene Ordner mit nicht verschlüsselten Dateien.....	11
Data Guardian auf Windows installieren.....	11
Data Guardian und Cloud-Verschlüsselung.....	12
Installieren eines Cloud Synchronisierungs-Clients.....	12
Arbeiten mit Ordnern und Dateien.....	14
Ordner und Dateien auf dem lokalen Computer und in der Cloud anzeigen.....	14
Ordner für einen internen Benutzer freigeben.....	16
Office-Dokumente mit dem geschützten Modus von Data Guardian verwenden.....	17
Ohne Internetverbindung arbeiten.....	22
Einschränkung der Zeichenzahl für Ordnerpfadnamen.....	22
Dropbox for Business.....	22
OneDrive for Business/Unified OneDrive.....	24
Dropbox.....	25
Box® ist eine eingetragene Marke von Box.....	27
Google Drive.....	28
OneDrive.....	29
Erklärung der Elemente des Taskleistenmenüs von Data Guardian.....	30
Ordner verwalten – Menü.....	32
Richtlinien auf Aktualisierungen überprüfen.....	32
Protokolldateien ausfindig machen.....	32
Data Guardian aufrüsten.....	32
Dell Feedback geben.....	32
Mögliche Probleme mit der Aktivierung: Cloud und geschützte Office-Dokumente.....	33
Data Guardian aktivieren.....	33
<b>4 Benutzeraufgaben: geschützte Office-Dokumente ohne Cloud-Verschlüsselung.....</b>	<b>34</b>
Überblick über die Aufgaben.....	34

Data Guardian für geschützte Office-Dokumente installieren.....	35
Data Guardian auf Windows installieren.....	35
Office-Dokumente mit dem geschützten Modus von Data Guardian verwenden.....	36
Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen.....	36
Arbeit mit Datei-Menüoptionen.....	37
Bestimmen, welche Dokumente mit abonniertem Modus geschützt werden.....	39
Zusätzliche Menüoptionen für geschützte Office-Dokumente.....	39
Ermitteln von Manipulationen an geschützten Office-Dokumenten.....	40
Externe Benutzer und geschützte Office-Dokumente.....	40
Erklärung der Elemente des Taskleistenmenüs von Data Guardian.....	41
Ordner verwalten – Menü.....	43
Protokolldateien ausfindig machen.....	43
Richtlinien auf Aktualisierungen überprüfen.....	43
Data Guardian aufrüsten.....	43
Dell Feedback geben.....	43
Mögliche Probleme mit der Aktivierung: geschützte Office-Dokumente.....	43
Data Guardian aktivieren.....	44
<b>5 Data Guardian Mobile mit iOS oder Android verwenden.....</b>	<b>45</b>
Voraussetzungen.....	45
Erste Schritte mit Data Guardian Mobile.....	45
Data Guardian auf einem iOS-Gerät.....	46
Fehlerbehebung bei iOS und Data Guardian.....	47
Data Guardian auf einem Android-Gerät.....	48
Sicherheitsüberlegungen für die Verwendung von Data Guardian mit Synchronisierungs-Clients.....	49
Protokolle.....	49
Dell Feedback geben.....	49
<b>6 Verwendung von Data Guardian als externer Benutzer.....</b>	<b>50</b>
Aufgaben interner Benutzer.....	50
.....	51
.....	51
Aufgaben externer Benutzer.....	52
Data Guardian aktivieren.....	53
Zugriff von einem internen Benutzer anfordern.....	53
Anzeigen eines geschützten Office-Dokuments.....	54
<b>7 Synchronisierungs-Client oder Data Guardian deinstallieren.....</b>	<b>55</b>
Einen Cloud-Synchronisierungs-Client deinstallieren.....	55
Data Guardian deinstallieren.....	55
<b>8 Häufig gestellte Fragen.....</b>	<b>57</b>
Verschiedene häufig gestellte Fragen.....	57
Häufig gestellte Fragen zu Office-Dokumenten und geschütztem Modus.....	58



# Einführung in Dell Data Guardian

Im *Dell Data Guardian-Benutzerhandbuch* finden Sie die nötigen Informationen zur Installation und Verwendung von Dell Data Guardian.

## Übersicht

Je nach den vom Administrator festgelegten Richtlinien werden Daten mit Dell 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.
- Office-Dokumente lokal gespeichert, für andere Benutzern freigegeben oder auf einem Wechselmedium gespeichert. Folgende Office-Dokumente können geschützt werden: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

### ANMERKUNG:

Ihr Administrator wird Ihnen mitteilen, ob Ihr Unternehmen Data Guardian nur mit Cloud-Speicherung, nur mit Office-Dokumenten oder mit beidem nutzt.

Sie können Data Guardian auf folgenden Plattformen einsetzen:

- Windows
- iOS
- Android
- Sowohl dieses Produkt als auch Data Guardian für Mac können vom jeweils anderen Produkt verschlüsselte Dateien öffnen.
  - Dieses Dokument bezieht sich nur auf Dell Data Guardian für Windows.
  - Benutzerinformationen zu Dell Data Guardian für Mac finden Sie in der Onlinehilfe der Software.

## Zusätzlicher Support

Sollten Sie noch Fragen haben, die in diesem Dokument nicht beantwortet werden, wenden Sie sich bitte an Ihren Administrator.



# Dell Data Guardian – Anforderungen

In diesem Kapitel werden die Hardware- und Softwareanforderungen für den Client erläutert.

## ANMERKUNG:

IPv6 wird nicht unterstützt.

## 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).

## Encryption-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.
- Obwohl der Encryption-Client nicht erforderlich ist, sollten nur Encryption-Clients ab Ver. 8.12 mit Data Guardian verwendet werden.
- Data Guardian bietet keine Unterstützung für Microsoft Office 365.
- Der Computer muss für die 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.
- Data Guardian unterstützt das Windows Systemwiederherstellungstool nicht.
- Überprüfen Sie regelmäßig die Website [www.dell.com/support](http://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](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.



# Benutzeraufgaben: Cloud-Verschlüsselung und geschützte Office-Dokumente

Der Administrator hat bereits Richtlinien für Data Guardian konfiguriert und informiert Sie, falls Ihr Unternehmen Data Guardian verwendet.

- Wie Sie Ihren Cloud-Synchronisierungs-Client verwalten
- Wie Sie Ihren Cloud-Synchronisierungs-Client sowie zusätzlichen Schutz von Office-Dokumenten verwalten: Wenn Ihr Unternehmen nur Office-Dokumente schützt, jedoch keinen Cloud-Synchronisierungs-Client verwaltet, befolgen Sie die Schritte in [Benutzeraufgaben: geschützte Office-Dokumente ohne Cloud-Verschlüsselung](#).


Wenn Ihr Unternehmen Data Guardian mit Cloud-Speicherung verwendet:

- Informieren Sie sich vor dem Einsatz von Data Guardian in der Online-Hilfe für Ihren Cloud-Speicheranbieter/Cloud-Synchronisierungs-Client darüber, wie Ihre Cloud-Speicheranwendung funktioniert. Dieses Dokument erläutert in erster Linie die Verwendung von Data Guardian.
- In der Regel bietet es sich an, einen Cloud-Synchronisierungs-Client zu installieren und zu verwenden. Ihr Unternehmen hat sich möglicherweise für einen bevorzugten Cloud-Synchronisierungs-Client entschieden und eine Richtlinie herausgegeben, die Sie berechtigt, nur diesen einen Client zu verwenden.

## Überblick über die Aufgaben

Diese Übersicht fasst die Schrittreihenfolge für die Installation und Verwendung von Data Guardian zusammen.

### Data Guardian und einen Cloud-Synchronisierungs-Client installieren

Aufgabe	Beschreibung	Weitere Informationen
Falls ein Cloud-Synchronisierungs-Client vor Data Guardian installiert wird	Bereits vorhandene Ordner und Dateien, die in die Cloud synchronisiert werden, werden nicht verschlüsselt.  <b>ANMERKUNG:</b> Bereits vorhandene Ordner und Dateien, die von der Cloud synchronisiert werden, werden verschlüsselt.	Siehe <a href="#">Zuvor vorhandene Ordner mit nicht verschlüsselten Dateien</a> .
Data Guardian installieren	Überprüfen Sie Folgendes:  Benutzer muss Data Guardian installieren  Der Administrator hat Data Guardian bereits installiert: Fahren Sie mit dem nächsten Schritt fort.	Benutzer installiert: Siehe <a href="#">Data Guardian auf Windows installieren</a> . Starten Sie das System neu, und fahren Sie mit dem nächsten Schritt fort.
Aktivierungsstatus überprüfen	Vergewissern Sie sich, dass das Data Guardian-Symbol in der Taskleiste mit einem grünen Häkchen  versehen ist.	Wenn das Symbol mit einem orangefarbenen Ausrufezeichen versehen ist, siehe <a href="#">Mögliche Probleme mit der Aktivierung: Cloud und geschützte Office-Dokumente</a> .



Aufgabe	Beschreibung	Weitere Informationen
Wenn Richtlinien Dokumente in der Cloud schützen, installieren Sie einen Cloud-Synchronisierungs-Client.	Unternehmens-Synchronisierungs-Client oder Basis-Synchronisierungs-Client	<a href="#">Cloud-Synchronisierungs-Client-Konten für Unternehmen</a>  oder  <a href="#">Standardmäßige Cloud-Synchronisierungs-Client-Konten</a>

**ANMERKUNG:**

Wenn Sie ein Office-Dokument öffnen und ein Deckblatt mit Installations- oder Aktivierungsinformationen angezeigt wird, hat Ihr Administrator möglicherweise Richtlinien zum Schutz von Office-Dokumenten festgelegt. Bestätigen Sie, dass Data Guardian installiert und aktiviert ist. Siehe [Mögliche Probleme mit der Aktivierung: Cloud und geschützte Office-Dokumente](#).

**Data Guardian verwenden**

Aufgabe	Beschreibung	Weitere Informationen
Cloud-Synchronisierungs-Client in File Explorer anzeigen	Nach der Installation von Data Guardian plus einem Cloud-Synchronisierungs-Client wird ein DDG VDisk Virtual Drive im Datei-Explorer angezeigt.	Arbeiten mit Ordnern und Dateien  <a href="#">Zugriff auf Synchronisierungs-Client-Ordner und Dateien auf dem lokalen Computer</a>
Arbeiten mit dem Cloud-Synchronisierungs-Client auf dem DDG VDisk Virtual Drive	Auf dem DDG VDisk Virtual Drive können Sie Unterordner zum Cloud-Synchronisierungs-Client hinzufügen und anschließend Dateien in diese Unterordner ziehen oder dort erstellen.  Nach der Synchronisierung sind die Dateien sicher in der Cloud: Office-Dateien können geöffnet werden, es wird jedoch nur ein Deckblatt angezeigt; andere Dateien sind als .xen-Dateien verschlüsselt.  Auf dem lokalen virtuellen Laufwerk sind sie jedoch entschlüsselt und werden in Klartext angezeigt.  Weitere Informationen erhalten Sie, indem Sie auf den entsprechenden Link für Ihren Cloud-Synchronisierungs-Client klicken.	<b>Unternehmenskonto:</b>  <a href="#">Dropbox for Business</a>  <a href="#">OneDrive for Business/Unified OneDrive</a>  <b>Basiskonto:</b>  <a href="#">Dropbox</a>  <a href="#">Box® ist eine eingetragene Marke von Box.</a>  <a href="#">Google Drive</a>  <a href="#">OneDrive</a>
Taskleistenmenü anzeigen	Bietet hilfreiche Informationen zu Dateien, Ordnern und Fehlerbehebung.	<a href="#">Erklärung der Elemente des Taskleistenmenüs von Data Guardian</a>
Schützen von Office-Dokumenten, Dokumenten mit aktivierten Makros und .pdf-Dokumenten, wenn die Richtlinie aktiviert ist	Schützen Sie ein Office-Dokument (.docx, .pptx, .xlsx, .docm, .pptm, xlsx, .pdf), wenn Sie es erstellen. Es ist sicher, wenn Sie es für andere freigeben oder auf Wechselmedien speichern.	<a href="#">Office-Dokumente mit dem geschützten Modus von Data Guardian verwenden</a>  <ul style="list-style-type: none"> <li>• <a href="#">Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen</a></li> <li>• <a href="#">Arbeit mit Datei-Menüoptionen</a></li> </ul>
Einen Cloud-Ordner freigeben, um Dateien gemeinsam mit anderen zu verwenden	Ordner freigeben für:  Internen Benutzer (verfügt über eine E-Mail-Adresse innerhalb der Domäne)	Internen Benutzer – Lesen Sie die Online-Hilfe Ihres Cloud-Speicher-Anbieters.  Externer Benutzer: siehe <a href="#">Verwendung von Data Guardian als externer Benutzer</a> .



Externer Benutzer (verfügt über eine E-Mail-Adresse außerhalb der Domäne) –  
Wenden Sie sich an Ihren Administrator.

# Data Guardian mit Cloud und geschützten Office-Dokumenten installieren

## Zuvor vorhandene Ordner mit nicht verschlüsselten Dateien

Vor dem Einsatz von Dell Data Protection | Data Guardian (DDG VDisk) sollte auf den Zielgeräten möglichst noch kein Cloud-Speicheranbieter-Konto eingerichtet sein.

Wenn Sie bereits über ein Konto eines Cloud-Speicher-Anbieters mit Ordnern verfügen, die mit Ihrem lokalen Computer synchronisiert werden, und dann Data Guardian installieren:

- 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 bereits vorhandene Dateien verschlüsselt werden sollen, navigieren Sie zum DDG VDisk Virtual Drive, erstellen Sie einen neuen Unterordner innerhalb des Cloud-Synchronisierungs-Clients und verschieben Sie die bereits vorhandenen Dateien in diesen Ordner.

oder

Für große Datenmengen kann ein Manager oder Administrator vorübergehend das [Menü „Ordner verwalten“](#) anfordern.

## Data Guardian auf Windows 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 entweder das 32-Bit- oder 64-Bit-Installationsprogramm aus (in der Regel **setup32.exe** oder **Setup64.exe**) und kopieren es auf den 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++ 2010 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:\Program Files\Dell\Data Protection\Dell Data Guardian\** auszuführen.  
Unter **C:\** sollten Sie Data Guardian niemals im Ordner „Benutzer“ oder „Windows“ oder 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 Vergewissern Sie sich nach dem Neustart, dass das Data Guardian-Symbol in der Taskleiste mit einem grünen Häkchen  versehen ist.

## Data Guardian und Cloud-Verschlüsselung

Wenn Ihr Unternehmen Richtlinien zum Schutz von Daten in der Cloud festlegt und Sie bereits auf einem installierten Synchronisierungs-Client angemeldet sind, wird ein DDG VDisk Virtual Drive in Windows Explorer angezeigt.

### ANMERKUNG:

Data Guardian unterstützt keine Aufhebung der Bereitstellung des virtuellen Laufwerks.

Wenn Sie einen Synchronisierungs-Client installieren und sich dort anmelden möchten, lesen Sie den Abschnitt [Installieren eines Cloud-Synchronisierungs-Clients](#).

## Installieren eines Cloud Synchronisierungs-Clients

### Herunterladen und Installieren

In der Regel möchten Unternehmen, dass alle Benutzer den gleichen Cloud-Synchronisierungs-Client installieren. Falls dies auch bei Ihnen zutrifft, verwenden Sie den bevorzugten Cloud-Synchronisierungs-Client Ihres Unternehmens.

### ANMERKUNG:

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

### ANMERKUNG:

Derzeit unterstützt Data Guardian keine Synchronisierungs-Clients, die auf einem Bereitstellungspunkt installiert sind.

- 1 Installieren Sie den Cloud-Synchronisierungs-Client entweder in der Unternehmens- oder in der Basisversion:
  - **Cloud-Synchronisierungs-Client-Konten für Unternehmen**  
Falls Ihr Unternehmen eine Option für ein Unternehmenskonto anbietet, erhalten Sie von Ihrem Administrator einen Link zum Herunterladen und Installieren eines Unternehmenskontos. Folgende Optionen sind verfügbar:
    - **Dropbox für Unternehmen:** Wenn Sie Dropbox für Unternehmen installieren, müssen Sie [Dropbox für Unternehmen authentifizieren](#).
    - **OneDrive for Business/Unified OneDrive:** Eine ausführliche Anleitung finden Sie unter <https://support.microsoft.com/en-us/kb/2903984>.
  - **Standardmäßige Cloud-Synchronisierungs-Client-Konten**
    - **Dropbox:** siehe <https://www.dropbox.com/install>
    - **Box Sync:** siehe <https://www.box.com/box-for-devices>

- **Google Drive:** <https://www.google.com/drive/download/>
- **OneDrive/Unified OneDrive (Windows 7 und 8):** siehe <https://onedrive.live.com/about/en-us/download/>  
Ab Windows 8.1 ist OneDrive bereits vorinstalliert. Wenn Sie Windows Updates aktiviert haben, wird OneDrive durch Unified OneDrive ersetzt.

2 Nach der Installation und Anmeldung werden folgende Elemente angezeigt:

- Datei-Explorer-Feld wird ein DDG VDisk Virtual Drive hinzugefügt. Diesem virtuellen Laufwerk wird der Ordner „Cloud-Synchronisierungs-Client“ hinzugefügt.

Falls Sie mehrere Cloud-Synchronisierungs-Clients installieren, wird für jeden dieser Clients ein Ordner auf diesem Laufwerk angezeigt.

 **ANMERKUNG:**

Data Guardian unterstützt keine Aufhebung der Bereitstellung des virtuellen Laufwerks.

- Unter File Explorer > Favoriten wird ein Ordner für Ihren Cloud-Synchronisierungs-Client hinzugefügt.
- In der Taskleiste wird das Synchronisierungs-Client-Symbol angezeigt.
- Je nach Cloud-Speicher-Anbieter wird automatisch eine Synchronisierungs-Client-Verknüpfung auf dem Desktop erstellt.
- Nur im abonnierten Modus (aber nicht im erzwungenen geschützten Modus): Ein Ordner namens „Sichere Dokumente“ wird zum Stammverzeichnis des Ordners „Dokumente“ hinzugefügt. Siehe Ordner [Dokumente > Sichere Dokumente](#).

### Ändern des Buchstabens des virtuellen Laufwerks oder erstellen einer Verknüpfung

Nach der Installation von Data Guardian plus einem Cloud-Synchronisierungs-Client wird das Symbol für das DDG VDisk Virtual Drive im Datei-Explorer angezeigt. Es wird ein Laufwerksbuchstabe zugewiesen, wobei ein Buchstabe vom Ende des Alphabets verwendet wird.

So ändern Sie den Laufwerksbuchstaben:

- 1 Klicken Sie in der Taskleiste auf das Data Guardian-Symbol und wählen Sie **Laufwerk konfigurieren** aus.
- 2 Wählen Sie einen verfügbaren Buchstaben aus der Liste *Aktuell* aus.
- 3 Klicken Sie auf **Anwenden** oder **OK**.

Um das Symbol für das DDG VDisk Virtual Drive auf dem Desktop hinzuzufügen, klicken Sie mit der rechten Maustaste und wählen Sie **Verknüpfung erstellen** aus.

### Authentifizieren von Dropbox für Unternehmen

Falls Sie Dropbox für Unternehmen installieren, fordert Data Guardian Sie zur Authentifizierung auf.

Authentifizierung:

- 1 Nach der Installation von Data Guardian wird ein Authentifizierungsfenster geöffnet, oder Sie können das Data Guardian-Symbol anklicken und dann **Dropbox > Verbinden** auswählen.  
Das Authentifizierungsfenster benachrichtigt Sie, dass Data Guardian Zugriff auf Ihr Dropbox-Konto haben muss und gibt evtl. Anweisungen für Geschäfts- und persönliche Konten.

Für den Benutzer werden hier Kontextmenüoptionen angezeigt. Für das Unternehmen und Ihren Administrator ist dies besonders wichtig, da hier zusätzliche Sicherheitsmaßnahmen bereitgestellt werden.

- 2 Klicken Sie im Authentifizierungsfenster auf **Weiter**.
- 3 Falls ein Netzwerkbedrohungsschutz-Fenster geöffnet wird, klicken Sie auf **Ja**.
- 4 Geben Sie im Authentifizierungsfenster Ihre Domänen-E-Mail und Ihr Dropbox-Passwort ein.
- 5 Klicken Sie auf **Anmelden**.
- 6 Wenn Sie Ihre persönlichen und geschäftlichen Dropbox-Konten verknüpft haben, werden Sie jetzt zur Auswahl eines Kontos aufgefordert. Sie müssen Ihr Geschäftskonto auswählen.
- 7 Klicken Sie auf **Fertigstellen** oder warten Sie, bis das Fenster geschlossen wird.



# Arbeiten mit Ordnern und Dateien

Data Guardian arbeitet transparent mit Ihrem Cloud-Synchronisierungs-Client. Nachdem Ihr Administrator eine Richtlinie für die Aktivierung von Data Guardian festgelegt hat, werden die Dateien verschlüsselt und nach der Synchronisierung mit Ihrem lokalen Computer sicher in der Cloud abgelegt.

Befolgen Sie die Anweisungen in der Hilfe Ihres Cloud-Speicher-Anbieters, um folgende Aktionen auszuführen:

- Ordner erstellen
- Ordner und Dateien hochladen/herunterladen

## ANMERKUNG:

Zum Hochladen von Dateien müssen Sie diese in die Ordner auf das DDG VDisk Virtual Drive kopieren oder dorthin verschieben. Data Guardian unterstützt keine Verschiebung von Dateien per Drag and Drop von Ihrem lokalen Computer auf die Website oder Erstellung von Dateien direkt auf der Website des Cloud-Speicheranbieters.

- Ordner selektiv synchronisieren
- Geben Sie Ordner oder Dateien für interne Benutzer frei, die über Data Guardian verfügen. Siehe [Ordner für einen internen Benutzer freigeben](#).
- Ordner oder Dateien für externe Benutzer freigeben Siehe [Verwendung von Data Guardian als externer Benutzer](#).
- Freigabe für Ordner aufheben

## Ordner und Dateien auf dem lokalen Computer und in der Cloud anzeigen

### Zugriff auf Synchronisierungs-Client-Ordner und Dateien auf dem lokalen Computer

Für den Zugriff auf synchronisierte Ordner und Dateien klicken Sie auf das **DDG VDisk Virtual Drive** im Datei-Explorer. Ihr Cloud-Synchronisierungs-Client wird angezeigt.

Es gibt noch weitere Möglichkeiten, auf Ihren Cloud-Synchronisierungs-Client zuzugreifen.

- Wählen Sie in der Taskleiste das Synchronisierungs-Client-Symbol aus, und öffnen Sie den Synchronisierungs-Client-Ordner. Weitere Informationen finden Sie in der Hilfe Ihres Cloud-Speicher-Anbieters.

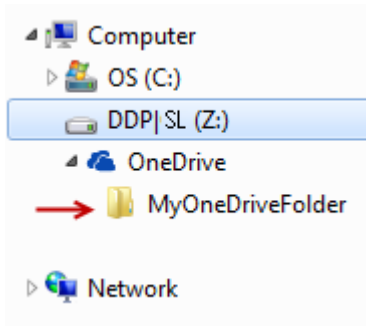


- Klicken Sie bei den Favoriten auf das Synchronisierungs-Client-Symbol.  
Wenn Sie in der Taskleiste oder bei den Favoriten auf das Synchronisierungs-Client-Symbol klicken, wird das DDG VDisk Virtual Drive hervorgehoben. Data Guardian leitet Sie zu diesem virtuellen Laufwerk weiter, auf dem Sie Ihre lokal entschlüsselten Ordner und Dateien in Klartext anzeigen können.

Sie können auch über eine Desktop-Verknüpfung auf Ordner und Dateien auf dem DDG VDisk Virtual Drive zugreifen. Siehe [Ändern des Buchstabens des virtuellen Laufwerks oder erstellen einer Verknüpfung](#).

### Ordner hinzufügen

Bei Data Guardian müssen Sie Unterordner zum Cloud-Synchronisierungsordner hinzufügen. Fügen Sie keine Dateien zum Stammverzeichnis des DDG VDisk Virtual Drive hinzu.



## Dateien hinzufügen

Wenn Sie einem Ordner eine Datei hinzufügen, fügt Data Guardian dem Ordner im Internet automatisch eine Datei hinzu. Wenn Sie eine Datei gemeinsam mit einem externen Benutzer verwenden möchten, zieht Data Guardian die Datei „Zugriff auf sichere Dateien.html“ heran. Sie müssen diese Datei nicht öffnen oder herunterladen. Siehe [Verwendung von Data Guardian als externer Benutzer](#).

### **Ordner und Dateien des Synchronisierungs-Clients in der Cloud anzeigen**

Data Guardian verschlüsselt Ihre Daten in der Cloud, und Dateinamen haben eine .xen-Erweiterung. Das Symbol für die Datei kann je nach Cloud-Speicher-Anbieter unterschiedlich aussehen, es wird jedoch kein Inhalt angezeigt. Sie können die Dateien in der Cloud nicht öffnen. Sollte jemand unbefugt Zugriff auf Ihr Cloud-Speicher-Konto erlangen, kann diese Person Ihre Dateien ebenfalls nicht öffnen oder anzeigen. Dies sorgt für mehr Sicherheit in der Cloud. Sie können Dateien nur auf dem DDG VDisk Virtual Drive in Klartext anzeigen.

Gelegentlich kann beim Herunterladen einer .xen-Datei auf Ihren Desktop und ihrer Entschlüsselung eine Kopie der Datei mit einer .xen-Erweiterung verbleiben. Sie können die heruntergeladene Kopie der .xen-Datei löschen.

Falls Ihr Unternehmen zusätzliche Sicherheit für Ordner und Dateien in der Cloud verlangt, hat der Administrator die Möglichkeit, eine Richtlinie festzulegen, die das Ausblenden der Dateinamen in der Cloud und beim Herunterladen bewirkt. Sollte jemand unbefugt Zugriff auf Ihr Cloud-Speicher-Konto erlangen, kann diese Person weder Dateien öffnen, noch Dateinamen anzeigen.

### **Ordner und Dateien des Synchronisierungs-Clients auf einem lokalen Computer anzeigen, auf dem Data Guardian und ein virtuelles Laufwerk installiert sind**

Um die Benutzerfreundlichkeit von Data Guardian auf Ihrem lokalen Computer zu gewährleisten, werden Dateien beim Öffnen eines Ordners auf dem DDG VDisk Virtual Drive automatisch entschlüsselt und in Klartext angezeigt, selbst wenn diese als verschlüsselte Dateien in der Cloud geschützt sind.

### **Ordner und Dateien auf Geräten ohne Data Guardian schützen**

Wenn eine nicht befugte Person eine geschützte Datei aus der Cloud auf ein Gerät **ohne** Data Guardian lädt, kann die Person nicht auf Ihre Daten zugreifen. Basierend auf von Ihrem Administrator festgelegten Richtlinien:

- Office-Dokumente: das Dokument wird geöffnet, aber es wird nur ein Deckblatt mit einer unternehmensspezifischen Meldung angezeigt.
- Nicht Office-Dokumente: die Datei wird als .xen-Datei heruntergeladen. Die Person kann die Datei nicht öffnen.

#### **ANMERKUNG:**

Für interne Benutzer gilt: Wenn Sie eine Datei von einem Computer, auf dem Data Guardian installiert ist, auf ein Gerät herunterladen, auf dem es nicht installiert ist, können Sie die Datei nur anzeigen, wenn Sie Data Guardian als externer Benutzer installieren.



In bestimmten Situationen kann eine .xen-Datei auf einem Computer angezeigt werden, auf dem Data Guardian installiert ist. Dies kann der Fall sein, wenn die Internetverbindung getrennt wurde, bevor der Herunterladevorgang abgeschlossen war. Möglicherweise ist dann kein Schlüssel zum Öffnen der Dateien verfügbar. Ein Dialogfeld weist dann darauf hin, dass die Datei nicht entschlüsselt werden kann.

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 das DDG VDisk Virtual Drive wieder hoch.

### Auf dem DDG VDisk Virtual Drive nach Dateinamen und Inhalten suchen

Wenn Sie Dateinamen oder Inhalte auf dem DDG VDisk Virtual Drive suchen möchten, müssen Sie die Windows-Suchindizierung für das Laufwerk aktivieren.

#### ANMERKUNG:

Die Windows-Suchindizierung kann nur für Benutzer-Ordner aktiviert werden.

So aktivieren Sie die Windows-Suchindizierung für das DDG VDisk Virtual Drive:

- 1 Geben Sie in der Systemsteuerung **Suchindizierung** in das Suchfeld ein.
- 2 Wählen Sie **Indizierungsoptionen** aus.
- 3 Wählen Sie unter *Ausgewählte Orte ändern* das Kontrollkästchen für das DDG VDisk Virtual Drive aus.

#### ANMERKUNG:

Die übrigen Schritte können je nach Betriebssystem unterschiedlich sein.

- 4 Klicken Sie auf **OK**.
- 5 Klicken Sie in den Indizierungsoptionen auf **Schließen**.

Sie können das DDG VDisk Virtual Drive jetzt durchsuchen.

## Ordner für einen internen Benutzer freigeben

Ein interner Benutzer verfügt über eine E-Mail-Adresse innerhalb der Domäne des Unternehmens.

Um einen Ordner für einen internen Benutzer freizugeben, müssen Sie zur Website Ihres Cloud-Speicher-Anbieters wechseln und dort die Option **Freigeben**. Lesen Sie auch die Online-Hilfe Ihres Cloud-Speicher-Anbieters.

### Ordner mit Data Guardian und Box freigeben

Wählen Sie auf der Box-Website eine der folgenden Optionen.

Box-Website-Option	Optionen	Beschreibung
Freigeben	Verfügbar für Ordner und Dateien	Wenn das Fenster „Freigabe“ geöffnet wird, müssen Sie sicherstellen, dass „Downloads zulassen“ auf <b>Ja</b> eingestellt ist.
	Zugriff anzeigen	Nach dem Herunterladen von Dateien oder Ordnern müssen die Freigebenden den ZIP-Ordner extrahieren und anschließend Ordner und Dateien auf das DDG VDisk Virtual Drive verschieben.
Mitarbeiter einladen	Verfügbar für Ordner	Wenn das Einladungsfenster geöffnet wird, können Sie <b>Bearbeiter</b> oder <b>Betrachter</b> auswählen.
	Zugriff anzeigen oder bearbeiten	Die Freigebenden können den Ordner mit ihrem Computer synchronisieren, und es erfolgt eine Synchronisation mit dem DDG VDisk Virtual Drive.



# Office-Dokumente mit dem geschützten Modus von Data Guardian verwenden

Um die Unternehmenssicherheit zu erhöhen, kann Ihr Administrator eine Richtlinie zum Schutz von Dateien dieser Office-Anwendungen aktivieren:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Wenn eine nicht autorisierte Person auf eine geschützte Datei zugreift, bleibt die Datei verschlüsselt, zum Beispiel, wenn Sie:

- sie an eine E-Mail anhängen.
- Sie in einem Browser verschieben: In einigen Cloud-Synchronisierungs-Clients können Sie mit der rechten Maustaste auf einen Dateinamen klicken und **Verschieben** auswählen.
- sie im Netzwerk freigeben.
- sie bei einem Cloud-Speicheranbieter hochladen.
- sie auf Wechselmedien speichern.

Bei Office-Dokumenten wird möglicherweise ein Deckblatt mit Anweisungen für die Installation oder Aktivierung von Data Guardian angezeigt, zum Beispiel:

- Sie müssen Data Guardian installieren.
- Sie müssen Data Guardian aktivieren.
- Sie öffnen ein geschütztes Office-Dokument in der Cloud.
- Sie haben eine Office-Datei von Ihrem Computer, auf dem Data Guardian installiert ist, heruntergeladen auf ein persönliches Gerät, auf dem es nicht installiert ist.
- Ein unbefugter Benutzer greift auf eine Ihrer Office-Dateien zu: Das Deckblatt mit einer unternehmensspezifischen Meldung wird angezeigt, aber der Benutzer kann den Inhalt der Datei nicht anzeigen.

Wenn Ihr Unternehmen den geschützten Modus von Data Guardian verwendet, finden Sie weitere Informationen unter den folgenden Themen:

- [Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen](#)
- [Arbeit mit Datei-Menüoptionen](#)
- [Bestimmen, welche Dokumente mit abonniertem Modus geschützt werden](#)
- [Zusätzliche Menüoptionen für geschützte Office-Dokumente](#)
- [Externe Benutzer und geschützte Office-Dokumente](#)

## Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen

Um festzustellen, ob der Administrator Data Guardian-Richtlinien aktiviert hat, öffnen Sie ein Office-Dokument und wählen Sie **Datei** aus. Wenn *Geschütztes „Speichern unter“* im linken Fensterbereich angezeigt wird, werden Office-Dokumente zusätzlich geschützt.

Um das Maß an Sicherheit zu bestimmen, beachten Sie die Optionen, die aktiviert oder deaktiviert sind:

- **Abonnierter Modus:** Sie haben einige Optionen zur Auswahl, um festzulegen, welche Office-Dokumente geschützt werden sollen.
  - *Speichern unter* und *Geschütztes „Speichern unter“* sind aktiviert: Wenn Sie ein Office Dokument schützen möchten, wählen Sie **Geschütztes „Speichern unter“** aus.
  - *Drucken* und *Exportieren* können je nach Richtlinie aktiviert oder deaktiviert werden.
  - *Freigabe (Speichern und Senden Sie bei Office 2010)* ist aktiviert.



- Ordner **Dokumente > Sichere Dokumente**: Im abonnierten Modus (aber nicht im erzwungenen geschützten Modus) wird ein Ordner namens „Sichere Dokumente“ zum Stammverzeichnis des Ordners „Dokumente“ hinzugefügt. Office-Dokumente in diesem Ordner sind verschlüsselt. Wenn Sie ein geschütztes Office-Dokument aus diesem Ordner entfernen, bleibt es verschlüsselt. Wenn Sie den Ordner umbenennen, wird der Inhalt des umbenannten Ordners verschlüsselt. Wenn Sie den Ordner löschen, wird er neu erstellt.
- **Erzwungener geschützter Modus**: Ihr Unternehmen benötigt eine höhere Sicherheitsstufe.
  - *Speichern unter* ist deaktiviert und *Geschütztes „Speichern unter“* aktiviert: Sie müssen alle Office-Dokumente im geschützten Modus speichern.
  - *Drucken* und *Exportieren* können je nach Richtlinie aktiviert oder deaktiviert sein.
  - *Freigabe* (*Speichern und Senden Sie* bei Office 2010) ist deaktiviert.

**ANMERKUNG:**

Mit dem ForceProtect-Modus ermöglicht es die Richtlinie außerdem, dass zu bestimmten Zeiten auf Ihrem Computer nach ungeschützten Office-Dateien gesucht wird und diese in den geschützten Modus geändert werden. Sie müssen eingeloggt und mit dem Netzwerk verbunden sein, damit Data Guardian ungeschützte Office-Dateien suchen kann.

- Wenn Sie **Geschütztes „Speichern unter“** wählen, lautet die einzige Option im *Speichertyp*-Feld *Office geschützt*.
- **Datei > Info** unterscheidet sich, zum Beispiel:
  - Sowohl im abonnierten als auch im erzwungenen geschützten Modus: *Datumseinschränkung hinzufügen* zeigt an, ob der Administrator diese Richtlinie aktiviert hat. Siehe [Verbesserte Sicherheit durch Hinzufügen von Datumseinschränkungen](#).
  - Sowohl im abonnierten als auch im erzwungenen geschützten Modus: Eigenschaftsinformationen zu diesem Office-Dokument, wie z. B. Autor und Datum, werden für mehr Sicherheit ausgeblendet.
  - Schreibgeschützter Status: Weitere Informationen siehe unten.

**ANMERKUNG:**

Die Option *Dokument schützen* Option in Datei > Info bezieht sich auf Microsoft Office, nicht den geschützten Modus von Data Guardian.

Wenn Sie ein Office-Dokument öffnen und es den schreibgeschützten Modus angibt, überprüfen Sie Folgendes:

- Wenn *Geschütztes „Speichern unter“* nicht im linken Fensterbereich angezeigt wird, bezieht sich der schreibgeschützte Modus nicht auf Data Guardian-Richtlinien.
- Wenn der Administrator Richtlinien auf den erzwungenen geschützten Modus mit einer höheren Sicherheitsstufe festlegt, werden nicht geschützte Office-Dokumente im schreibgeschützten Modus geöffnet.

**ANMERKUNG:**

Für OneDrive: Wenn Sie ein geschütztes Office-Dokument über **Datei > Öffnen > OneDrive** öffnen und das Dokument schreibgeschützt ist, bestätigen Sie, dass Sie den OneDrive-Synchronisierungs-Client installiert und eingerichtet haben.

## Arbeit mit Datei-Menüoptionen

In dieser Tabelle sind Dateimenüoptionen für Office-Dokumente aufgeführt. Je nach der Sicherheitsstufe sind einige Optionen ausgegraut.

**ANMERKUNG:**

Derzeit werden integrierte Office-Dokumente im geschützten Office-Modus nicht unterstützt.

Dateimenü	Abonnierter Modus und geschützte Office-Dokumente	Erzwungener geschützter Modus für geschützte und ungeschützte Office-Dokumente
Öffnen Sie die Datei mit der	Dateien werden wie gewohnt geöffnet.	Nicht geschützte Dokumente werden im schreibgeschützten Modus geöffnet.
Speichern	<ul style="list-style-type: none"> <li>Optionen: Bereits geschütztes Dokument: Speicherung als geschützt. Ungeschützt: Speicherung als ungeschützt. Um es zu schützen, klicken Sie auf <b>Geschütztes „Speichern unter“</b>.</li> <li>Schreibgeschütztes Dokument: Ein Dialogfeld weist Sie darauf hin, dass Sie ein ungeschütztes Dokument nicht speichern können. Das Fenster „Speichern unter“ wird geöffnet und Sie müssen es mit einem anderen Dateinamen speichern.</li> <li>XEN-Datei: Sie können es im geschützten Modus öffnen und speichern, aber die .xen-Datei wird aus der Cloud entfernt. Das Office-Dokument verfügt über seine übliche Erweiterung, ist aber geschützt.</li> </ul>	<ul style="list-style-type: none"> <li>Das Dokument ist geschützt.</li> <li>Schreibgeschütztes Dokument: Sie können es bearbeiten, jedoch nicht das Original speichern. Wenn Sie auf „Speichern“ klicken, wird das Fenster „Als geschützt speichern“ geöffnet und Sie müssen es im geschützten Modus mit einem neuen Name speichern.</li> <li>Remote-Dokumente: Wenn Sie ein Dokument an einem Remote-Standort öffnen und es nicht geschützt ist, dann müssen Sie es auf Ihrem lokalen Laufwerk speichern, um es zu ändern und zu speichern. Sie können es nicht am Remote-Standort speichern.</li> </ul> <p><b>ANMERKUNG:</b> Durch Klicken auf „Speichern“ wird das Fenster „Speichern unter“ geöffnet, und die einzige Option im Feld „Speichertyp“ lautet „Office geschützt“ (Dokumente, Präsentation oder Excel-Arbeitsmappe).</p> <ul style="list-style-type: none"> <li>.xen Datei: Sie können es im geschützten Modus öffnen und speichern, aber die .xen-Datei wird aus der Cloud entfernt. Das Office-Dokument verfügt über seine übliche Erweiterung, ist aber geschützt.</li> </ul>
Speichern unter	Hat die Standardoptionen (aber nicht „Geschützter Modus“)	Deaktiviert
Geschütztes „Speichern unter“	Einzige Option im Feld „Speichertyp“ ist „Office geschützt“	Einzige Option im Feld „Speichertyp“ ist „Office geschützt“
Drucken	Möglicherweise aktiviert oder ausgegraut, basierend auf von Ihrem Administrator festgelegten Richtlinien. Wenn die Menüoption aktiviert ist, kann eine Richtlinie ein Wasserzeichen mit dem Benutzernamen, dem Domännennamen und der Computer-ID auf jeder Seite platzieren, wenn Sie drucken.	Je nach Richtlinie kann diese Option aktiviert oder grau unterlegt sein. Wenn die Menüoption aktiviert ist, kann eine Richtlinie ein Wasserzeichen mit dem Benutzernamen, dem Domännennamen und der Computer-ID auf jeder Seite platzieren, wenn Sie drucken.
Freigegeben	Aktiviert	Deaktiviert
Speichern und Senden (Office 2010)	Aktiviert	Deaktiviert Wenn „Drucken“ aktiviert ist, können Sie Drucken wählen, um das Dokument als PDF zu drucken.
Exportieren (Office 2013 und höher)	Möglicherweise aktiviert oder ausgegraut, basierend auf von Ihrem Administrator festgelegten Richtlinien.	Möglicherweise aktiviert oder ausgegraut, basierend auf von Ihrem Administrator festgelegten Richtlinien.
Geschützter Export  (Office 2013 und höher)	Wenn die Menüoption „Exportieren“ ausgegraut und „Geschützter Export“ aktiviert ist, wird das Dokument mit einem Wasserzeichen auf jeder Seite exportiert, das den Benutzernamen, den Domännennamen und die Computer-ID enthält.	Wenn die Menüoption „Exportieren“ ausgegraut und „Geschützter Export“ aktiviert ist, wird das Dokument mit einem Wasserzeichen auf jeder Seite exportiert, das den Benutzernamen, den Domännennamen und die Computer-ID enthält.
	<p><b>ANMERKUNG:</b> Wenn Sie ein Dokument im geschützten Modus für einen externen Benutzer exportieren, kann dieser es öffnen und anzeigen, jedoch nicht exportieren oder drucken.</p>	<p><b>ANMERKUNG:</b> Wenn Sie ein Dokument im geschützten Modus für einen externen Benutzer exportieren, kann dieser es öffnen und anzeigen, jedoch nicht exportieren oder drucken.</p>

## Online mit geschützten Office-Dokumenten arbeiten



Beim Erstellen von geschützten Office-Dokumenten gilt es als bewährtes Verfahren, online zu arbeiten, da für diese Dokumente Schlüssel generiert werden. Wenn ein erneutes Image Ihres Computers erforderlich war und Sie geschützte Office-Dokumente offline erstellt haben, teilen Sie dies unbedingt Ihrem Administrator mit.

### Online mit Dokumenten mit aktivierten Makros arbeiten

Bei einem geschützten Dokument mit aktivierten Makros ist das Makro vorhanden, aber blockiert. Allerdings kann Data Guardian ein Dokument mit aktivierten Makros derzeit erst prüfen, nachdem das neu geschützte Dokument (.docm, .pptm, .xlsm) geschlossen und wieder geöffnet wurde. Wenn Sie ein geschütztes Dokument mit einem Makro als ungeschützt speichern, müssen Sie das Dokument ebenfalls schließen und erneut öffnen, damit das Makro ausgeführt werden kann.

### Ein geschütztes Office-Dokument an eine Outlook-E-Mail anhängen

Wenn Sie ein geschütztes Office-Dokument an eine Outlook-E-Mail anhängen, wählen Sie **Einfügen** statt *Als Text einfügen* aus. *Als Text einfügen* fügt den Dokument-Inhalt direkt in den Text der E-Mail ein, und der Inhalt ist nicht mehr geschützt.

### Richtlinie für den abonnierten Modus

Wenn in Datei > Info, „Drucken“ ausgegraut ist, hat eine Data Guardian-Richtlinie das Drucken von geschützten Office-Dokumenten deaktiviert. Aktuell ist die Druckoption allerdings nicht ausgegraut, wenn Sie in Windows Explorer mit der rechten Maustaste auf ein geschütztes Office-Dokument klicken. Wenn Sie jedoch „Drucken“ wählen, geschieht Folgendes:

- Word: Ein Dialogfeld zeigt an, dass Word nicht mehr funktioniert.
- Excel: Ein Dialogfeld zeigt an, dass „Drucken“ durch eine Richtlinie deaktiviert ist.
- PowerPoint: Ein Dialogfeld zeigt an, dass „Drucken“ durch eine Richtlinie deaktiviert ist. Wenn Sie auf OK klicken, wird ein Deckblatt gedruckt, aus dem hervorgeht, dass das Dokument geschützt ist.

## Bestimmen, welche Dokumente mit abonniertem Modus geschützt werden

Im erzwungenen geschützten Modus werden alle Office-Dokumente geschützt. Wenn Sie im abonnierten Modus überprüfen möchten, ob ein Dokument geschützt ist oder nicht, öffnen Sie das Dokument, und in der Titelleiste wird es als geschützt aufgeführt.

## Zusätzliche Menüoptionen für geschützte Office-Dokumente

Die Art des Office-Dokuments, geschützt oder ungeschützt, kann sich folgendermaßen auswirken.

### **Rechtsklick > Schützen**

Sie können mit der rechten Maustaste auf ein Office-Dokument klicken und **Schützen** auswählen. Sie müssen Inhalte hinzufügen, damit die Menüoption angezeigt wird. Sie können kein leeres Dokument schützen.

### **Dateieigenschaften > Dell Data Guardian-Registerkarte**

Bei geschützten Office-Dokumenten können Sie mit der rechten Maustaste klicken und **Eigenschaften** auswählen, woraufhin eine **Dell Data Guardian**-Registerkarte mit Informationen, wie der Schlüssel-ID der Datei und Zugriffs- und Embargodaten angezeigt wird.

### **Einfügen**

Wenn Ihr Administrator eine Richtlinie zum Schutz von Office-Dokumente festlegt:

- Sie können Daten im ursprünglichen geschützten Dokument kopieren und einfügen.
- Sie können Daten nicht von einem geschützten Dokument kopieren und in ein ungeschütztes Dokument einfügen. Es wird nichts in der Zwischenablage angezeigt, und eine unternehmensspezifische Textnachricht besagt, dass Sie in das ungeschützte oder nicht verwaltete Dokument nichts einfügen können.

### ANMERKUNG:

Wenn Sie Text aus einem geschützten Dokument ausschneiden und die Meldung in einem ungeschützten Dokument erhalten, klicken Sie auf **Rückgängig machen** im geschützten Dokument, um den Text abzurufen.

#### **Drag-and-Drop im geschützten Modus**

Sie können Inhalte per Drag-and-Drop in ein geschütztes Word-Dokument verschieben. Derzeit ist die Drag-and-Drop-Funktion für geschützte PowerPoint- und Excel-Dateien deaktiviert.

#### **Drucken für Umschläge und Etiketten**

Wenn der Administrator eine Richtlinie zum Hinzufügen eines Wasserzeichens beim Drucken eines geschützten Office-Dokuments festgelegt hat, führen Sie die folgenden Schritte aus, um Umschläge oder Etiketten zu drucken:

- 1 In einem Word-Dokument wählen Sie die Registerkarte **Sendungen** aus.
- 2 Wählen Sie die Option **Umschläge** oder **Etiketten** aus.
- 3 Nachdem Sie Adresse oder Absender eingegeben haben, klicken Sie auf **Drucken**.

 **ANMERKUNG:** Wenn Sie eine andere Option zum Drucken verwenden und der Administrator eine Richtlinie zum Hinzufügen eines Wasserzeichens für gedruckte Office-Dokumente festgelegt hat, wird ein Wasserzeichen auf Ihrem Briefumschlag oder Etikett angezeigt.

## Ermitteln von Manipulationen an geschützten Office-Dokumenten

Data Guardian kann geschützte Office-Dokumente scannen, um einige Formen der Manipulation zu erkennen.

Wenn ein interner Benutzer ein geschütztes Office-Dokument manipuliert:

- Data Guardian kann einige Manipulationen reparieren oder wiederherstellen.
- Bei Manipulationen, die nicht repariert werden können, wird möglicherweise ein Dialogfeld angezeigt, das Sie darauf hinweist, dass die Datei manipuliert wurde und dass Sie sich an Ihren Administrator wenden sollten.

Wenn ein nicht autorisierter Benutzer ein geschütztes Office-Dokument öffnet, wird nur das Deckblatt angezeigt. Falls der nicht autorisierte Benutzer Änderungen am Deckblatt vornimmt, wird es von Data Guardian wiederhergestellt, wenn die Datei von einem autorisierten Benutzer erneut als geschützt gespeichert wird.

## Externe Benutzer und geschützte Office-Dokumente

### **Verbesserte Sicherheit durch Hinzufügen von Datumseinschränkungen**

Mit Data Guardian laden Sie ein geschütztes Office-Dokument in die Cloud und geben es frei:

- Alle internen Data Guardian-Benutzer können dieses anzeigen.
- Basierend auf der Richtlinie können externe Benutzer es anzeigen.

Wahlweise können Sie für mehr Sicherheit in Bezug auf externe Benutzer eine Datumseinschränkung hinzufügen, um den Zeitraum zu begrenzen, in dem ein externer Benutzer ein geschütztes Office-Dokument anzeigen kann.

- 1 Wählen Sie **Datei > Info > Datumseinschränkung**.
- 2 Wählen Sie aus der Dropdown-Liste ein Anfangs- und Enddatum und -uhrzeit für die Anzeige des Dokuments durch einen externen Benutzer aus.

### ANMERKUNG:

Startdatum und -uhrzeit können in der Zukunft liegen, falls Sie das Dokument senden möchten, aber verhindern wollen, dass der externe Benutzer es vor dem gewünschten Datum und der gewünschten Uhrzeit anzeigen kann.



3 Klicken Sie auf **OK**.

Das Dokument wird gespeichert, geschützt, geschlossen und wieder geöffnet.

**ANMERKUNG:**

Wenn Sie die Termine für ein ungeschütztes Office-Dokument ändern und dann auf „Abbrechen“ klicken, schützt Data Guardian die Datei nach wie vor.

**ANMERKUNG:**

Aktuell müssen Sie, wenn Sie Datumseinschränkungen zu einem ungeschützten Office-Dokument hinzufügen und es auf einem Netzlaufwerk speichern möchten, die Datei lokal speichern und dann in das Netzwerk kopieren.

Wenn ein externer Benutzer eine Datei nach dem Datums- und Zeitbereich öffnet, wird ein Dialogfeld angezeigt, das darauf hinweist, dass die Datei Zugriffsbeschränkungen unterliegt und der externe Benutzer sich an den Autor der Datei wenden kann. Das Dialogfeld zeigt keine Daten für den externen Benutzer an.

Wenn Sie ein Startdatum und eine Uhrzeit in der Zukunft festlegen und der externe Benutzer das Dokument vor diesem Zeitpunkt öffnet, weist ein Dialogfeld darauf hin, dass die Datei bis zu diesem Datum und dieser Uhrzeit aufgrund von Zugriffseinschränkungen nicht geöffnet werden kann.

## Ohne Internetverbindung arbeiten

Ohne Internetverbindung können Sie Cloud-Synchronisierungs-Dateien weiterhin mithilfe des Datei-Explorers auf Ihrem lokalen Laufwerk anzeigen. Das DDG VDisk Virtual Drive wird jedoch nicht angezeigt. Auch Änderungen werden nicht in der Cloud synchronisiert, solange keine Internetverbindung besteht.

## Einschränkung der Zeichenzahl für Ordnerpfadnamen

Windows-Pfadnamen dürfen höchstens 248 Zeichen enthalten.

In der Cloud gibt es diese Begrenzung nicht. Daher können Sie Ordner und Unterordner mit einem Pfadnamen erstellen, der über diese Beschränkung überschreitet. Lokal unter Windows werden jedoch keine Ordner erstellt, bei denen die Pfadnamen diese Beschränkung überschreiten. Stellen Sie daher sicher, dass Sie die Länge der Pfadnamen für Ordner und Unterordner auf 248 Zeichen beschränken.

## Dropbox für Business

Dropbox für Unternehmen hat spezifische Anforderungen. Siehe [Einen Cloud-Synchronisierungs-Client deinstallieren](#).

## Hilfe des Cloud-Speicher-Anbieters

Bevor Sie Data Guardian einsetzen, informieren Sie sich über den Cloud-Speicher-Anbieter. Support für Dropbox für Unternehmen erhalten Sie unter:

<https://www.dropbox.com/help>.

Obwohl Sie Dateien auf die Website Ihres Cloud-Speicher-Anbieters hochladen können, gilt es als bewährtes Verfahren, auf dem DDG VDisk Virtual Drive mit den Ordnern und Dateien zu arbeiten.

## Data Guardian und Dropbox für Unternehmen verbinden

Falls Ihr Unternehmen Dropbox für Unternehmen verwendet, müssen Sie Data Guardian zulassen, damit die Verbindung weiterhin besteht.

So stellen Sie die Verbindung her:

- 1 Klicken Sie in der Taskleiste auf das Data Guardian-Symbol und wählen Sie dann **Dropbox > verbinden**.
- 2 Lesen Sie im Dropbox-Authentifizierungsfenster die Informationen durch und klicken Sie dann auf **Weiter**.
- 3 Wenn Sie Ihre persönlichen und geschäftlichen Dropbox-Konten verknüpft haben, werden Sie jetzt zur Auswahl eines Kontos aufgefordert. Sie müssen Ihr Geschäftskonto auswählen.
- 4 Klicken Sie an der Eingabeaufforderung zum Zulassen von Data Guardian für den Zugriff auf Ihre Dropbox-Dateien und -Ordner auf **Zulassen**.
- 5 Klicken Sie auf **Fertigstellen**.

## Selektive Synchronisierung für Ordner einrichten

So können Sie Ordner selektiv synchronisieren:

- 1 Klicken Sie in der Taskleiste auf das Symbol **Dropbox für Unternehmen**.
- 2 Klicken Sie auf das Symbol **Einstellungen** und wählen Sie **Einstellungen** aus.
- 3 Klicken Sie auf die Registerkarte **Konto** und klicken Sie anschließend auf **Selektive Synchronisierung**.
- 4 Wählen Sie nur Ordner oder Unterordner aus, die Sie von Ihrem Computer synchronisieren möchten.
- 5 Klicken Sie auf **Aktualisieren**.
- 6 Klicken Sie im Dialog zur Bestätigung der Aktualisierung auf **OK**.
- 7 Klicken Sie im Fenster der Dropbox-Einstellungen auf **OK**.

Ein Popup zeigt in der Taskleiste an, dass Ordner synchronisiert werden.

Ihr Unternehmen bestimmt, ob Sie nur ein Geschäftskonto haben oder ob Sie Geschäfts- und persönliche Ordner verwenden dürfen. Wenn Sie über bereits vorhandene Ordner mit persönlichen Dateien oder Daten verfügen, die nicht verschlüsselt werden müssen, heben Sie die Auswahl dieser Ordner vor der Installation von Data Guardian auf. Andernfalls werden Ihre persönlichen Daten evtl. verschlüsselt.

## Taskleistensymbol für Dropbox für Unternehmen verwenden

Klicken Sie in der Taskleiste auf das Dropbox-Symbol.

- Für die Website: Wählen Sie das Globus-Symbol aus.

### ANMERKUNG:

Falls Sie Chrome oder Firefox zum Öffnen von Dropbox.com verwenden, stellen Sie sicher, dass Sie es schließen, wenn Sie mit der Arbeit an Dateien und Ordnern fertig sind. Auch wenn Sie eine weitere Registerkarte im Browser öffnen, wird der Inhalt verschlüsselt. Dazu gehören u. U. E-Mail, Anhänge oder Uploads, die mit dem Browser gemacht wurden.

- Für den Ordner: Wählen Sie das Dropbox-Ordner-Symbol aus. Daraufhin werden Sie zum DDG VDisk Virtual Drive weitergeleitet.

## Verwenden des Dropbox für Unternehmen-Kontextmenüs

Wenn Data Guardian in Windows Explorer installiert ist, hat Dropbox für Unternehmen ein zusätzliches Kontextmenü.



## **ANMERKUNG:**

Sie müssen Data Guardian mit Dropbox verbinden.

Zum Zugreifen auf das Kontextmenü in Windows Explorer, öffnen Sie einen Dropbox-Ordner und klicken Sie mit der rechten Maustaste auf eine Datei. Das Cloud-Symbol hat folgende Optionen:

- Sicheren Dropbox-Link freigeben
- Ansicht auf Dropbox.com
- Frühere Versionen ansehen

## Verwenden von Business und Personal Dropbox-Konten

Falls Ihr Unternehmen Dropbox für Unternehmen hat und es Ihnen außerdem gestattet, ein persönliches Dropbox-Konto mit Ihrem Geschäftskonto zu verknüpfen, stellen Sie sicher, dass Sie die von Ihrem Administrator für diese Konten eingestellten Richtlinien verstehen. Ein Unternehmen kann beispielsweise folgende Richtlinien festlegen:

- Sowohl geschäftliche als auch persönliche Dateien werden verschlüsselt.  
*oder*
- Nur geschäftliche Dateien und Ordner werden verschlüsselt. Persönliche Dateien bleiben unverschlüsselt.  
Ihr Unternehmen kann aus Sicherheitsgründen eine Überwachungsrichtlinie haben. Dateinamen im persönlichen Ordner werden protokolliert und an den Dell-Datenschutzserver gesandt.

Wenn Sie geschäftliche und persönliche Dropbox-Konten verwenden, speichern Sie geschäftliche Dateien nicht in Ihrem persönlichen Dropbox-Ordner.

### Entschlüsseln von Ordnern in einem persönlichen Konto

Wenn ein persönlicher Ordner unabsichtlich verschlüsselt wird, kann der Administrator temporären Zugriff gewähren, damit Sie die Verschlüsselung Ihrer Ordner verwalten können. Heben Sie die Markierung der Ordner auf, die entschlüsselt werden sollen. Sie können Ordner auch von der Synchronisierung entfernen, indem Sie die Verknüpfung des Kontos oder die Synchronisierung persönlicher Ordner aufheben, die nicht verschlüsselt sein sollen.

## OneDrive for Business/Unified OneDrive

### **ANMERKUNG:**

Data Guardian bietet keine Unterstützung für Microsoft Office 365.

### **ANMERKUNG:**

Die Datenfreigabe wird in OneDrive für Unternehmen nicht unterstützt.

## Hilfe des Cloud-Speicher-Anbieters

Bevor Sie Data Guardian einsetzen, informieren Sie sich über den Cloud-Speicher-Anbieter. Support für OneDrive für Unternehmen erhalten Sie unter:

<http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>.

Obwohl Sie Dateien auf die Website Ihres Cloud-Speicher-Anbieters hochladen können, gilt es als bewährtes Verfahren, auf dem DDG VDisk Virtual Drive mit den Ordnern und Dateien zu arbeiten.



## Selektive Synchronisierung für Ordner einrichten

So können Sie Ordner selektiv synchronisieren:

- 1 Klicken Sie in der Taskleiste mit der rechten Maustaste auf das **OneDrive for Business/Unified OneDrive**-Symbol und klicken Sie auf **Eine neue Bibliothek synchronisieren**.
- 2 Geben Sie die URL Ihrer Bibliothek ein.
- 3 Wählen Sie **Jetzt synchronisieren** aus.
- 4 Wählen Sie **Meine Dateien anzeigen** aus.

## Taskleistensymbol für OneDrive für Unternehmen verwenden

Gehen Sie in der Taskleiste folgendermaßen vor:

- Für die Website: Klicken Sie mit der rechten Maustaste und wählen Sie **Zu OneDrive.com wechseln** aus.
- Für den Ordner: Klicken Sie mit der rechten oder linken Maustaste und wählen Sie **Öffnen Sie Ihren Ordner für OneDrive for Business**. Dieser Schritt leitet Sie zum DDG VDisk Virtual Drive weiter.

## Sicherheitsüberlegungen für die Verwendung von Data Guardian mit OneDrive oder OneDrive for Business

Dell Data Guardian verschlüsselt Ordner und Dateien, um Daten zu sichern. Da Data Guardian mit Synchronisierungs-Clients arbeitet, sollten Sie folgende Überlegungen berücksichtigen.

- Wählen Sie beim Herunterladen nicht die Option „Abbrechen“. Anderenfalls wird ein Fehler ausgegeben. Wenn Sie eine Datei löschen möchten, warten Sie, bis der Herunterladevorgang abgeschlossen ist.
- Bei Verwendung von Windows 8.1 verfügt Microsoft OneDrive über Platzhalterdateien, die scheinbar im Synchronisierungs-Client vorhanden sind, jedoch tatsächlich nicht heruntergeladen wurden. Aus diesem Grund kann Dell Data Guardian sie nicht verschlüsseln. Wenn Sie eine Platzhalter-Datei öffnen, zeigt Data Guardian ein Dialogfeld an, das darüber informiert, dass die Datei nicht geschützt wird. Sie können mit der rechten Maustaste klicken und **Herunterladen**, und dann wandelt **Data Guardian** sie in eine .xen-Datei um.

## Dropbox

### Hilfe des Cloud-Speicher-Anbieters

Bevor Sie Data Guardian einsetzen, informieren Sie sich über den Cloud-Speicher-Anbieter. Dropbox-Support finden Sie unter <https://www.dropbox.com/help>.

Obwohl Sie Dateien in der Cloud erstellen oder auf die Website Ihres Cloud-Speicher-Anbieters hochladen können, gilt es als bewährtes Verfahren, auf dem DDG VDisk Virtual Drive mit den Ordnern und Dateien zu arbeiten.

#### ANMERKUNG:

Bei Dropbox und Data Guardian werden Office-Dateien, die Sie in der Cloud erstellen und von dort synchronisieren als .xen-Datei verschlüsselt. Daher werden sie auf der virtuellen Festplatte im schreibgeschützten Modus geöffnet. Sie können sie nicht bearbeiten.

Wenn Sie alle Ordner auf der virtuellen Festplatte löschen, werden die Dateien gelöscht, aber die Ordner können weiterhin vorhanden sein. Wenn dies der Fall ist, löschen Sie die Ordner in der Cloud.



## Selektive Synchronisierung für Ordner einrichten

So können Sie Ordner selektiv synchronisieren:

- 1 Klicken Sie in der Taskleiste auf das **Dropbox**-Symbol.
  - 2 Klicken Sie auf das Symbol **Einstellungen** und wählen Sie **Einstellungen** aus.
  - 3 Klicken Sie auf die Registerkarte **Konto** und klicken Sie anschließend auf **Selektive Synchronisierung**.
  - 4 Wählen Sie nur Ordner oder Unterordner aus, die Sie von Ihrem Computer synchronisieren möchten.
  - 5 Klicken Sie auf **Aktualisieren**.
  - 6 Klicken Sie im Dialog zur Bestätigung der Aktualisierung auf **OK**.
  - 7 Klicken Sie im Fenster der Dropbox-Einstellungen auf **OK**.
- Ein Popup zeigt in der Taskleiste an, dass Ordner synchronisiert werden.

## Taskleistensymbol für Dropbox verwenden

Klicken Sie in der Taskleiste auf das Dropbox-Symbol.

- Für die Website: Wählen Sie das Globus-Symbol aus.

### ANMERKUNG:

Falls Sie Chrome oder Firefox zum Öffnen von Dropbox.com verwenden, stellen Sie sicher, dass Sie es schließen, wenn Sie mit der Arbeit an Dateien und Ordnern fertig sind. Auch wenn Sie eine weitere Registerkarte im Browser öffnen, wird der Inhalt verschlüsselt. Dazu gehören u. U. E-Mail, Anhänge oder Uploads, die mit dem Browser gemacht wurden.

- Für den Ordner: Wählen Sie das Dropbox-Ordner-Symbol aus. Daraufhin werden Sie zum DDG VDisk Virtual Drive weitergeleitet.

## Sicherheitsüberlegungen für die Verwendung von Data Guardian mit Dropbox

Falls Sie eine virtuelle Maschine ausführen, ziehen Sie keine Dateien vom Server-Desktop in den Browser. Die Dateien werden in dem Fall nicht geschützt. Führen Sie einen der folgenden Schritte aus: Verwenden Sie im Browser die Option „Hochladen“ oder ziehen Sie die Datei auf dem Desktop auf das DDG VDisk Virtual Drive.

## Häufig gestellte Fragen zu Dropbox

### Frage

Mein Dropbox-Konto enthält Dateikonflikte. Wenn ich die Dateien aus der Cloud lösche, werden sie immer wieder erstellt.

### Antwort

Wenn ein Ordner bereits freigegeben war und dann mehrere Data Guardian-Konten gleichzeitig aktiviert werden, kann dies als gleichzeitige Erstellung dieser Dateien aufgefasst werden. Zum Schutz der Originaldatei erstellt Dropbox mehrere Dateien des gleichen Namens und Typs und legt sie in der Cloud ab. Data Guardian lässt daher die Erstellung der Dateien zu, ohne andere Vorgänge zu stören.

### Lösung

- 1 Alle Personen, für die diese Datei freigegeben sind, müssen die Synchronisierung des Ordners in der Dropbox-Anwendung deaktivieren. Siehe [Dropbox für Unternehmen](#).
- 2 Nachdem die Dateien und der Ordner auf allen lokalen Computern gelöscht worden sind, muss eine einzige Person auf die Cloud zugreifen und die duplizierten Dateien löschen.

Anschließend können alle Beteiligten den Ordner erneut auswählen und die Synchronisierung aktivieren.

## Box® ist eine eingetragene Marke von Box.

### Hilfe des Cloud-Speicher-Anbieters

Bevor Sie Data Guardian einsetzen, informieren Sie sich über den Cloud-Speicher-Anbieter. Box-Support finden Sie unter <https://support.box.com/home>.

Obwohl Sie Dateien auf die Website Ihres Cloud-Speicher-Anbieters hochladen können, gilt es als bewährtes Verfahren, auf dem DDG VDisk Virtual Drive mit den Ordnern und Dateien zu arbeiten.

#### **ANMERKUNG:**

Wenn Sie Internet Explorer verwenden, um Dateien beim Box-Cloud-Speicheranbieter hochzuladen oder eine Datei zu öffnen, kann es zu einer Verzögerung im Datei-Explorer-Fenster kommen.

#### **ANMERKUNG:**

Box Tools und Box Edit werden von Data Guardian nicht unterstützt. Die Verwendung von Box Tools kann zu einem BlueScreen-Zustand führen.

### Selektive Synchronisierung für Ordner einrichten

So können Sie Ordner selektiv synchronisieren:

- 1 Klicken Sie mit der rechten Maustaste in der Taskleiste auf das Box-Symbol und wählen Sie **Box-Website öffnen**.
- 2 Klicken Sie mit der rechten Maustaste auf der Cloud-Synchronisierungs-Website auf einen Ordner und wählen Sie **Ordner mit Computer synchronisieren**.
- 3 Klicken Sie im Fenster „Ordner synchronisieren“ auf **Ordner synchronisieren**.  
Das Taskleisten-Symbol gibt an, dass die Einstellungen angewandt werden. Dieser Vorgang kann mehrere Minuten dauern.
- 4 Wenn vollständig, navigieren Sie zu **Windows Explorer > Box Sync**. Die synchronisierten Ordner werden mit einem Häkchen angezeigt.

### Taskleistensymbol für Box verwenden

Klicken Sie in der Taskleiste auf das Box-Symbol.

- Für die Website: Wählen Sie **Box-Website öffnen**.
- Für den Ordner: Wählen Sie den Ordner **Box Sync öffnen**. Dieser Schritt leitet Sie zum DDG VDisk Virtual Drive weiter.

### Häufig gestellte Fragen zum Box-Synchronisierungs-Client

#### **Frage**

Ich verwende den Box-Synchronisierungs-Client. Ich habe auf lokaler Ebene einen neuen Ordner erstellt und einige Dateien hinzugefügt. Der Synchronisierungs-Client scheint zwar zu funktionieren, aber in der Cloud wurde nichts erstellt.

#### **Antwort**



Der Box-Synchronisierungs-Client benötigt u. U. etwas Zeit für die Erfassung von Informationen über neue Ordner und Dateien. Das kann einige Minuten länger dauern als bei anderen Synchronisierungs-Clients. Warten Sie daher erst den Abschluss des Synchronisierungs-Clients ab, bevor Sie neue Ordner und Dateien erstellen.

### Frage

Ich verwende den Box-Synchronisierungs-Client. Da in meiner primären Partition kein Platz war, habe ich ihn auf ein anderes Laufwerk verschoben. Im Ordner für meine Box-Dateien wurden nun ein oder mehrere neue Ordner erstellt und mit **Neuer Ordner** benannt.

### Antwort

Wenn Dateien auf zwei Computern in eine gemeinsame freigegebene Datei synchronisiert werden und eine der beteiligten Personen den Ordner verschiebt, werden alle in der Freigabe erstellten neuen Ordner automatisch als leerer Ordner mit der Bezeichnung **Neuer Ordner** angezeigt.

### Lösung

Löschen Sie den neuen Ordner direkt in der Cloud. Er wird dann auf allen Systemen entfernt, für die der Ordner freigegeben ist.

## Sicherheitsüberlegungen für die Verwendung von Data Guardian mit Box

Wenn Sie eine Datei auf der Box Cloud-Website erstellen, wird sie synchronisiert. Sie wird jedoch als verschlüsselte Datei heruntergeladen.

Bei Internet Explorer kann es beim Hochladen oder Öffnen auf Box zu einer Verzögerung kommen.

## Google Drive

### Hilfe des Cloud-Speicher-Anbieters

Bevor Sie Data Guardian einsetzen, informieren Sie sich über den Cloud-Speicher-Anbieter. Support für Google Drive finden Sie unter <https://support.google.com/drive/?hl=en#topic=14940>.

Obwohl Sie Dateien auf die Website Ihres Cloud-Speicher-Anbieters hochladen können, gilt es als bewährtes Verfahren, auf dem DDG VDisk Virtual Drive mit den Ordnern und Dateien zu arbeiten.

## Selektive Synchronisierung für Ordner einrichten

So können Sie Ordner selektiv synchronisieren:

- 1 Klicken Sie in der Taskleiste auf das **Google Drive**-Symbol.
- 2 Wählen Sie das Symbol für Einstellungen aus.
- 3 Wählen Sie **Einstellungen** aus.
- 4 Zur selektiven Synchronisierung klicken Sie auf **Nur diese Ordner**.
- 5 Deaktivieren Sie das Kontrollkästchen derjenigen Ordner, die in der Cloud nicht geschützt werden müssen.
- 6 Klicken Sie auf **Anwenden**.
- 7 Um zu bestätigen, klicken Sie auf **Fortfahren**.

## Taskleistensymbol für Google Drive verwenden

Klicken Sie in der Taskleiste auf das Google Drive-Symbol.

- Für die Website: Wählen Sie **Google Drive im Web besuchen**.
- Für den Ordner: Wählen Sie den Ordner **Google Drive öffnen** aus. Dieser Schritt leitet Sie zum DDG VDisk Virtual Drive weiter.

## Sicherheitsüberlegungen für die Verwendung von Data Guardian und Google Drive

Data Guardian verschlüsselt Ordner und Dateien, um Daten zu schützen. Da Data Guardian mit Synchronisierungs-Clients arbeitet, sollten Sie folgende Überlegungen berücksichtigen.

- Die Unternehmenssicherheitsrichtlinie untersagt die Verwendung von Google Docs mit Data Guardian. Bei der Installation von Data Guardian informiert Sie ein Dialogfeld über diese Richtlinie. 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. Wenn Data Guardian unter Windows verwendet wird, werden Google Docs, die Sie erstellen, in Ihrem Google Docs-Synchronisierungs-Client-Ordner angezeigt.

Wenn Sie den Ordner öffnen, werden Sie jedoch darauf hingewiesen, dass Data Guardian das Dokument nicht verschlüsseln kann. Es kann auch sein, dass Ihr Administrator zur Sicherstellung der Datensicherheit Berichte ausführt, um Google Docs-Dateien zu identifizieren, die synchronisiert werden, um die Sicherheit von Daten zu verbessern.

- Google Drive-Optionen verfügen über **Entfernen** (verschiebt in den Papierkorb) und **Löschen**. Google Drive mit Data Guardian verfügt nur über „Löschen“, im Einklang mit anderen Data Guardian-Funktionen.

### ANMERKUNG:

Wenn Sie mehrere Dateien aus dem virtuellen Data Guardian-Laufwerk löschen und einige noch im Browser oder der Befehlszeile angezeigt werden, löschen Sie sie im Browser oder von der Befehlszeile aus.

- Wenn Sie Google Drive verwenden, erhalten Sie eventuell eine Warnung, dass Eigenschaften beim Kopieren von Dateien auf das DDG VDisk Virtual Drive verloren gehen. Dabei handelt es sich um Sicherheitsattribute.

## OneDrive

### ANMERKUNG:

Data Guardian bietet keine Unterstützung für Microsoft Office 365.

## Hilfe des Cloud-Speicher-Anbieters

Bevor Sie Data Guardian einsetzen, informieren Sie sich über den Cloud-Speicher-Anbieter. OneDrive-Support finden Sie unter <http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other>.

Obwohl Sie Dateien auf die Website Ihres Cloud-Speicher-Anbieters hochladen können, gilt es als bewährtes Verfahren, auf dem DDG VDisk Virtual Drive mit den Ordnern und Dateien zu arbeiten.



## Selektive Synchronisierung für Ordner einrichten

So können Sie Ordner selektiv synchronisieren:

- 1 Klicken Sie mit der rechten Maustaste in der Taskleiste auf das **OneDrive**-Symbol und klicken Sie auf **Einstellungen**.
- 2 Wählen Sie die Registerkarte **Ordner wählen** und klicken Sie dann auf **Ordner wählen**.
- 3 Wählen Sie dann **Zu synchronisierende Ordner wählen** aus.
- 4 Eine Liste von Ordnern wird angezeigt. Markieren Sie die Kästchen, um diese Ordner zu synchronisieren, oder heben Sie die Markierungen auf. Klicken Sie auf **OK**.
- 5 Klicken Sie auf **OK**.
- 6 Das Taskleisten-Symbol gibt an, dass die Einstellungen angewandt werden. Dieser Vorgang kann mehrere Minuten dauern.
- 7 Navigieren Sie anschließend zu **Windows Explorer > OneDrive**. Die synchronisierten Ordner werden mit einem Häkchen angezeigt.

## Taskleistensymbol für OneDrive verwenden

Gehen Sie in der Taskleiste folgendermaßen vor:

- Für die Website: Klicken Sie mit der rechten Maustaste und wählen Sie **Zu OneDrive.com wechseln** aus.
- Für den Ordner: Klicken Sie mit der rechten oder linken Maustaste und wählen Sie **Ihren OneDrive-Ordner öffnen** aus. Dieser Schritt leitet Sie zum DDG VDisk Virtual Drive weiter.

## Sicherheitsüberlegungen für die Verwendung von Data Guardian mit OneDrive oder OneDrive for Business

Siehe [Sicherheitsüberlegungen für die Verwendung von Data Guardian mit Synchronisierungs-Clients](#).

## Erklärung der Elemente des Taskleistenmenüs von Data Guardian

Details-Bildschirm

Der Data Guardian-Details-Bildschirm stellt hilfreiche Informationen bereit, wie z. B.:

- Für technischen Support können Sie Status- oder Versionsinformationen bereitstellen.
- Um einen nicht verschleierte Dateinamen zu sehen, der einer a.xen-Datei zugeordnet ist, wählen Sie **Dateien > Dateizustand**.
- Um nach einem Dateinamen zu suchen, wählen Sie Kopieren unten rechts und fügen den Inhalt in eine Wort-Datei ein.
- Um zu sehen, wer der Eigentümer eines Ordners ist, wählen Sie Ordner und rollen zur Spalte ORDNEREIGENTÜMER.

So greifen Sie auf den Details-Bildschirm zu:

Klicken Sie auf das Data Guardian-Taskleistensymbol und anschließend auf **Details...**

Oben links auf dem Bildschirm „Details“ werden folgende Informationen angezeigt:

**Servicestatus:** Status des Windows-Service von Data Guardian. Folgende Werte sind möglich: Beendet, Start ausstehend, Beenden ausstehend, Aktiv, Fortfahren ausstehend, Unterbrechen ausstehend, Unterbrochen

**Ausführungsstatus:** Der Aktivierungsstatus des Geräts. Folgende Werte sind möglich: Aktiv, Wird erneut aktiviert, Gesperrt, Wird gesperrt

**Benutzermodus:** Interner Benutzer: ein Benutzer innerhalb dieser Domänenadresse

**Externer Benutzer:** ein Benutzer außerhalb dieser Domänenadresse

**Registrierungs-E-Mail:** Für interne Benutzer ist dies die Domänen-E-Mail-Adresse. Für externe Benutzer ist dies die E-Mail, unter der sie registriert sind.

**Server URL:** DDP EE-Server/VE-Server, der mit diesem Client kommuniziert.

**Letzte Richtlinienänderung:** Datum und Zeitstempel des Zeitpunkts, an dem die Richtlinie zuletzt geändert und vom Client verwendet wurde.

**Richtlinienversion:** Die vom DDP EE-Server/VE-Server generierte Richtlinienversion.

Die Bereiche der **Dateien** und Ordner des Details-Bildschirms zeigen folgende Informationen an:

**Name:** Name der Datei

**Cloud:** Führt den verborgenen Dateinamen auf oder zeigt an, ob die Datei *Ungeschützt* ist.

**Dateizustand:** Dieser Wert gibt den Eigentümer des Ordners an. Der Wert wird von der Schlüssel-ID festgelegt.

**Verarbeitungszustand:** Gibt an, ob die Datei einen Schlüssel braucht oder *Abgeschlossen* ist.

**Unternehmen:** Führt den Standardserver auf. Wenn in dieser Spalte die Meldung *Fehler: Schlüssel nicht von Ihrem Server* angezeigt wird, gehört der Schlüssel nicht zum Server Ihres Unternehmens. Der Schlüssel für eine verschlüsselte Datei muss zum Server Ihres Unternehmens gehören.

**Schlüssel:** Die Schlüssel-ID, die diesem Ordner zugewiesen wurde. Neue Dateien nutzen diesen Schlüssel zur Verschlüsselung.

**Ordner:** Der vollständige Pfadname des Ordners.

**Letzte Änderung:** Das Datum, an dem die Datei geändert wurde.

**Beständigkeitszustand:** Dies gibt an, ob die Datei auf der Festplatte ist.

**XEN Datei-Lesevorgang:** *Wahr* oder *Falsch*.

**Browser erstellt:** *Wahr* oder *Falsch*.

Um Protokolldateien anzuzeigen, klicken Sie auf dem Bildschirm „Details“ unten links auf **Protokoll anzeigen**.

#### ANMERKUNG:

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

Der Bereich **Ordner** auf dem Bildschirm „Details“ enthält die folgenden Informationen:

**Name:** Name des Ordners

**Schlüssel:** Die Schlüssel-ID, die diesem Ordner zugewiesen wurde. Neue Dateien nutzen diesen Schlüssel zur Verschlüsselung.

**Sync-Client:** Der letzte Sync-Client, der diesen Ordner synchronisiert hat (siehe [Cloud-Synchronisierungs-Clients](#))

**Ordneureigentümer:** Dieser Wert gibt den Eigentümer des Ordners an. Der Wert wird von der Schlüssel-ID festgelegt.

**Überschreiben:** Die Optionen sind *Keine* und *Bereits vorhandene*. Zuvor vorhandene Dateien sind nicht geschützt. Falls Sie den Zugriff auf die Ordnerverwaltung und den Schutz einiger Dateien aufgehoben haben, gibt diese Spalte außerdem an, dass sie nicht geschützt sind.

**Verschleierungstyp:** Wenn Ihr Unternehmen Ihre Cloud-Speicherung verwaltet, ist dies eine Richtlinie, die für jeden Ordner festgelegt ist und angibt, welche Art von .xen-Dateien in der Cloud erstellt wird. Dies ist eine von Ihrem Administrator festgesetzte Richtlinie. Wenn Ihr Administrator *Nur Erweiterung* auswählt, wird der tatsächliche Dateiname mit der Erweiterung „.xen“ angezeigt. Falls Ihr Administrator *Guid*



auswählt, wird ein verschlüsselter Dateiname mit der Erweiterung „.xen“ angezeigt. Diese Richtlinieneinstellung gilt nur für neue Ordner. Die Standardeinstellung ist *Nur Erweiterung*.

## Ordner verwalten – Menü

Einige Manager oder Administratoren müssen möglicherweise vorübergehend Fehler in von mehr als einem Benutzer gemeinsam genutzten Ordnern beheben. Sie können bei Ihrem Administrator die Genehmigung für die Option „Ordner verwalten“ anfordern. Normalerweise ist dies eine temporäre Option.

## Richtlinien auf Aktualisierungen überprüfen

Falls Ihr Administrator eine Richtlinie ändert und Sie über eine Richtlinienaktualisierung unterrichtet, gehen Sie zur Windows-Taskleiste, klicken Sie auf das Symbol **Dell Data Protection | Data Guardian** und wählen Sie **Auf Richtlinienaktualisierungen überprüfen**.

Wenn Ihr Administrator eine Richtlinie zum Schutz von in Microsoft Word erstellten Dateien ändert, müssen Sie Word schließen, damit diese Aktualisierung angewendet werden kann.

## Protokolldateien ausfindig machen

Zu Fehlerbehebungszwecken kann es sein, dass Ihr Administrator Protokolldateien von Ihnen anfordert.

So können Sie Protokolldateien ausfindig machen:

- 1 Navigieren Sie zu
- 2 Wählen Sie **Xendow.Service.log** aus.

### ANMERKUNG:

Nachdem die Datei Xendow.Service.log eine Größe von 3 MB erreicht hat, wird sie als Xendow.Service1.log und dann als Xendow.Service2.log gespeichert.

## Data Guardian aufrüsten

Als bewährtes Verfahren gilt die Deinstallation der früheren Version mit anschließender Installation der aktuellen Version. Siehe [Data Guardian deinstallieren](#).

## Dell Feedback geben


Falls Ihr Administrator eine Feedback-Richtlinie aktiviert hat, können Sie Dell Feedback zu diesem Produkt geben. Das kurze Formular enthält zwei Fragen zu Ihrem Zufriedenheitsgrad mit einer Bewertungsskala (wobei 10 die höchste Kundenzufriedenheit bedeutet) und einem Kommentarfeld.

Um das Formular aufzurufen, klicken Sie auf das Data Guardian-Taskleistensymbol und wählen Sie **Feedback senden** aus.

Ist diese Funktion gemäß Richtlinie deaktiviert, wird die Option nicht angezeigt.



# Mögliche Probleme mit der Aktivierung: Cloud und geschützte Office-Dokumente

Wenn Sie Data Guardian installiert haben, aber das Data Guardian-Symbol in der Taskleiste nicht mit einem grünen Häkchen  versehen ist, beachten Sie Folgendes, je nachdem, ob Sie Cloud-Verschlüsselung, geschützte Office-Dokumente oder beides nutzen:

- Der Zugriff auf Cloud-Synchronisierungs-Websites ist gesperrt.
- Cloud-Synchronisierungsanwendungen können keine Verbindung zu ihren Webdiensten herstellen.
- Lokale synchronisierte Ordner werden während dieser Zeit nicht aktualisiert.
- Data Guardian kann vorhandene Office-Dokumente vor der Aktivierung in den geschützten Modus konvertieren. Wenn dies der Fall ist, wird ein Deckblatt mit Informationen zur Aktivierung angezeigt, wenn Sie ein Office-Dokument öffnen.

Führen Sie einen der folgenden Schritte aus:

- Starten Sie das System neu und melden Sie sich erneut mit einem UPN-Suffix, z. B. user\_name@domain.com, an.
- Fragen Sie Ihren Administrator, ob Sie das Kontrollkästchen **SSL-Prüfung aktivieren** nach der Installation von Data Guardian aktivieren sollten.
- Klären Sie mit Ihrem Systemadministrator, ob Sie Ihren Computer für die manuelle Aktivierung konfigurieren müssen. Siehe [Data Guardian aktivieren](#).

## Data Guardian aktivieren

Normalerweise wird Data Guardian nach Installation und Neustart automatisch aktiviert. Wenn der Systemadministrator Sie bittet, die Aktivierung manuell vorzunehmen, führen Sie die folgenden Schritte aus:

- 1 Melden Sie sich bei Windows an.  
In der Taskleiste wird ein Shield-Symbol mit einem orangefarbenen Ausrufezeichen angezeigt.
- 2 Klicken Sie in der Taskleiste auf das **Data Guardian**-Symbol und wählen Sie **Benutzeraktivierung** aus.
- 3 Geben Sie Ihre Domänen-E-Mail-Adresse und Ihr Domänenpasswort ein, und klicken Sie auf **Aktivieren**.  
Falls Sie ein interner Benutzer sind (also über eine E-Mail-Adresse innerhalb der Domäne verfügen), ignorieren Sie die Schaltfläche „Registrieren“. Nur externe Benutzer müssen sich registrieren.

Nach Abschluss der Aktivierung wird ein grünes Häkchen auf dem Data Guardian-Taskleistensymbol  angezeigt

- 4 Bestätigen Sie Ihren Benutzermodusstatus. Klicken Sie auf die Registerkarte -Taskleistensymbol und wählen Sie **Details** aus.
- 5 Bestätigen Sie oben den Benutzermodus:

**Intern:** Ein Benutzer mit einer E-Mail-Adresse innerhalb der Domäne des Unternehmens.

**Extern:** Ein Benutzer mit einer E-Mail-Adresse außerhalb der Domäne. Weitere Informationen finden Sie unter [Verwendung von Data Guardian als externer Benutzer](#).



# Benutzeraufgaben: geschützte Office-Dokumente ohne Cloud-Verschlüsselung

Der Administrator hat bereits Richtlinien für Data Guardian zum Schutz von Office-Dokumenten konfiguriert.


## ANMERKUNG:

Wenn Ihr Unternehmen zudem Ihren Cloud-Synchronisierungs-Client verwaltet, siehe [Benutzeraufgaben: geschützte Office-Dokumente ohne Cloud-Verschlüsselung](#).

## Überblick über die Aufgaben

Diese Übersicht fasst die Schrittreihenfolge für die Installation und Verwendung von Data Guardian zusammen.

### Data Guardian installieren

Aufgabe	Beschreibung	Weitere Informationen
Data Guardian installieren	Überprüfen Sie Folgendes:  Benutzer muss Data Guardian installieren  Administrator hat Data Guardian bereits installiert: Fahren Sie mit dem nächsten Schritt fort.	Benutzer installiert: Siehe <a href="#">Data Guardian auf Windows installieren</a> . Starten Sie das System neu, und fahren Sie mit dem nächsten Schritt fort.
Aktivierungsstatus überprüfen	Vergewissern Sie sich, dass das Data Guardian-Symbol in der Taskleiste mit einem grünen Häkchen  versehen ist.	Wenn das Symbol mit einem orangefarbenen Ausrufezeichen versehen ist, siehe <a href="#">Mögliche Probleme mit der Aktivierung: geschützte Office-Dokumente</a> .

### Data Guardian verwenden

Aufgabe	Beschreibung	Weitere Informationen
Taskleistenmenü anzeigen	Bietet hilfreiche Informationen zu Dateien, Ordnern und Fehlerbehebung.	<a href="#">Erklärung der Elemente des Taskleistenmenüs von Data Guardian</a>
Schützen von Office-Dokumenten und Dokumenten mit aktivierten Makros, wenn die Richtlinie aktiviert ist	Schützen Sie ein Office-Dokument (.docx, .pptx, .xlsx, .docm, .pptm, xlsx), wenn Sie es erstellen. Es ist sicher, wenn Sie es für andere freigeben oder auf Wechselmedien speichern.	<a href="#">Office-Dokumente mit dem geschützten Modus von Data Guardian verwenden</a>  <ul style="list-style-type: none"> <li>• Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen</li> <li>• <a href="#">Arbeit mit Datei-Menüoptionen</a></li> </ul>
Ordner freigeben, um Dateien gemeinsam mit anderen zu verwenden	Ordner freigeben für:  Internen Benutzer (verfügt über eine E-Mail-Adresse innerhalb der Domäne)	Internen Benutzer – Lesen Sie die Online-Hilfe Ihres Cloud-Speicher-Anbieters.  Externer Benutzer: siehe <a href="#">Verwendung von Data Guardian als externer Benutzer</a> .

Aufgabe	Beschreibung	Weitere Informationen
	Externer Benutzer (verfügt über eine E-Mail-Adresse außerhalb der Domäne) – Wenden Sie sich an Ihren Administrator.	

### ① ANMERKUNG:

Wenn Sie ein Office-Dokument öffnen und ein Deckblatt mit Installations- oder Aktivierungsinformationen angezeigt wird, hat Ihr Administrator möglicherweise Richtlinien zum Schutz von Office-Dokumenten festgelegt. Bestätigen Sie, dass Data Guardian installiert und aktiviert ist. Siehe [Mögliche Probleme mit der Aktivierung: geschützte Office-Dokumente](#).

# Data Guardian für geschützte Office-Dokumente installieren

## Data Guardian auf Windows 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.

- Um das Data Guardian-Installationsprogramm herunterzuladen, gehen Sie zu dem durch Ihren Administrator angegebenen Speicherort.
- Je nach Betriebssystem wählen Sie entweder das 32-Bit- oder 64-Bit-Installationsprogramm aus (in der Regel **setup32.exe** oder **Setup64.exe**) und kopieren es auf den lokalen Computer.
- Starten Sie das Installationsprogramm per Doppelklick.
- Falls Sie eine Sicherheitswarnung erhalten, klicken Sie auf **Ausführen**.
- Wählen Sie eine Sprache aus und klicken Sie auf **OK**.
- Klicken Sie auf **OK**, wenn Sie zur Installation von Microsoft Visual C++ 2010 Redistributable Package oder Microsoft .NET Framework 4.0 Client Profile aufgefordert werden.
- Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.
- Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen, und klicken Sie auf **Weiter**.
- Klicken Sie auf dem Bildschirm des Zielordners auf **Weiter**, um die Installation am Standardort von **C:\Program Files\Dell\Dell Data Protection\Dell Data Guardian\** auszuführen.  
Unter **C:\** sollten Sie Data Guardian niemals im Ordner „Benutzer“ oder „Windows“ oder im Stammverzeichnis eines Laufwerks installieren. Anderenfalls wird ein Fehler ausgegeben.
- 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.
- Klicken Sie auf **Weiter**.
- 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**.
- Wählen Sie im Fenster „Management Type“ (Verwaltungstyp) diese Option aus:
  - Interne Nutzung: Ein Benutzer mit einer E-Mail-Adresse innerhalb der Domäne des Unternehmens.
- Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.  
Der Installationsfortschritt wird in einem Statusfenster angezeigt.
- Klicken Sie auf **Fertigstellen**, wenn der Bildschirm „Installation abgeschlossen“ angezeigt wird.
- Klicken Sie auf **Ja**, um neu zu starten.  
Die Installation von Data Guardian ist abgeschlossen.



17 Vergewissern Sie sich nach dem Neustart, dass das Data Guardian-Symbol in der Taskleiste mit einem grünen Häkchen  versehen ist.

## Office-Dokumente mit dem geschützten Modus von Data Guardian verwenden

Um die Unternehmenssicherheit zu erhöhen, kann Ihr Administrator eine Richtlinie zum Schutz von Dateien dieser Office-Anwendungen aktivieren:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Wenn eine nicht autorisierte Person auf eine geschützte Datei zugreift, bleibt die Datei verschlüsselt, zum Beispiel, wenn Sie:

- sie an eine E-Mail anhängen.
- Sie in einem Browser verschieben: In einigen Cloud-Synchronisierungs-Clients können Sie mit der rechten Maustaste auf einen Dateinamen klicken und **Verschieben** auswählen.
- sie im Netzwerk freigeben.
- sie bei einem Cloud-Speicheranbieter hochladen.
- sie auf Wechselmedien speichern.

Bei Office-Dokumenten wird möglicherweise ein Deckblatt mit Anweisungen für die Installation oder Aktivierung von Data Guardian angezeigt, zum Beispiel:

- Sie müssen Data Guardian installieren.
- Sie müssen Data Guardian aktivieren.
- Sie öffnen ein geschütztes Office-Dokument in der Cloud.
- Sie haben eine Office-Datei von Ihrem Computer, auf dem Data Guardian installiert ist, heruntergeladen auf ein persönliches Gerät, auf dem es nicht installiert ist.
- Ein unbefugter Benutzer greift auf eine Ihrer Office-Dateien zu: Das Deckblatt mit einer unternehmensspezifischen Meldung wird angezeigt, aber der Benutzer kann den Inhalt der Datei nicht anzeigen.

Wenn Ihr Unternehmen den geschützten Modus von Data Guardian verwendet, finden Sie weitere Informationen unter den folgenden Themen:

- [Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen](#)
- [Arbeit mit Datei-Menüoptionen](#)
- [Bestimmen, welche Dokumente mit abonniertem Modus geschützt werden](#)
- [Zusätzliche Menüoptionen für geschützte Office-Dokumente](#)
- [Externe Benutzer und geschützte Office-Dokumente](#)

## Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen

Um festzustellen, ob der Administrator Data Guardian-Richtlinien aktiviert hat, öffnen Sie ein Office-Dokument und wählen Sie **Datei** aus. Wenn *Geschütztes „Speichern unter“* im linken Fensterbereich angezeigt wird, werden Office-Dokumente zusätzlich geschützt.

Um das Maß an Sicherheit zu bestimmen, beachten Sie die Optionen, die aktiviert oder deaktiviert sind:

- **Abonnierter Modus:** Sie haben einige Optionen zur Auswahl, um festzulegen, welche Office-Dokumente geschützt werden sollen.
  - *Speichern unter* und *Geschütztes „Speichern unter“* sind aktiviert: Wenn Sie ein Office Dokument schützen möchten, wählen Sie **Geschütztes „Speichern unter“** aus.

- *Drucken* und *Exportieren* können je nach Richtlinie aktiviert oder deaktiviert werden.
- *Freigabe* (*Speichern und Senden Sie* bei Office 2010) ist aktiviert.
- Ordner **Dokumente > Sichere Dokumente**: Im abonnierten Modus (aber nicht im erzwungenen geschützten Modus) wird ein Ordner namens „Sichere Dokumente“ zum Stammverzeichnis des Ordners „Dokumente“ hinzugefügt. Office-Dokumente in diesem Ordner sind verschlüsselt. Wenn Sie ein geschütztes Office-Dokument aus diesem Ordner entfernen, bleibt es verschlüsselt. Wenn Sie den Ordner umbenennen, wird der Inhalt des umbenannten Ordners verschlüsselt. Wenn Sie den Ordner löschen, wird er neu erstellt.
- **Erzwungener geschützter Modus**: Ihr Unternehmen benötigt eine höhere Sicherheitsstufe.
  - *Speichern unter* ist deaktiviert und *Geschütztes „Speichern unter“* aktiviert: Sie müssen alle Office-Dokumente im geschützten Modus speichern.
  - *Drucken* und *Exportieren* können je nach Richtlinie aktiviert oder deaktiviert sein.
  - *Freigabe* (*Speichern und Senden Sie* bei Office 2010) ist deaktiviert.

**ANMERKUNG:**

Mit dem ForceProtect-Modus ermöglicht es die Richtlinie außerdem, dass zu bestimmten Zeiten auf Ihrem Computer nach ungeschützten Office-Dateien gesucht wird und diese in den geschützten Modus geändert werden. Sie müssen eingeloggt und mit dem Netzwerk verbunden sein, damit Data Guardian ungeschützte Office-Dateien suchen kann.

- Wenn Sie **Geschütztes „Speichern unter“** wählen, lautet die einzige Option im *Speichertyp*-Feld *Office geschützt*.
- **Datei > Info** unterscheidet sich, zum Beispiel:
  - Sowohl im abonnierten als auch im erzwungenen geschützten Modus: *Datumseinschränkung hinzufügen* zeigt an, ob der Administrator diese Richtlinie aktiviert hat. Siehe [Verbesserte Sicherheit durch Hinzufügen von Datumseinschränkungen](#).
  - Sowohl im abonnierten als auch im erzwungenen geschützten Modus: Eigenschaftsinformationen zu diesem Office-Dokument, wie z. B. Autor und Datum, werden für mehr Sicherheit ausgeblendet.
  - Schreibgeschützter Status: Weitere Informationen siehe unten.

**ANMERKUNG:**

Die Option *Dokument schützen* Option in Datei > Info bezieht sich auf Microsoft Office, nicht den geschützten Modus von Data Guardian.

Wenn Sie ein Office-Dokument öffnen und es den schreibgeschützten Modus angibt, überprüfen Sie Folgendes:

- Wenn *Geschütztes „Speichern unter“* nicht im linken Fensterbereich angezeigt wird, bezieht sich der schreibgeschützte Modus nicht auf Data Guardian-Richtlinien.
- Wenn der Administrator Richtlinien auf den erzwungenen geschützten Modus mit einer höheren Sicherheitsstufe festlegt, werden nicht geschützte Office-Dokumente im schreibgeschützten Modus geöffnet.

**ANMERKUNG:**

Für OneDrive: Wenn Sie ein geschütztes Office-Dokument über **Datei > Öffnen > OneDrive** öffnen und das Dokument schreibgeschützt ist, bestätigen Sie, dass Sie den OneDrive-Synchronisierungs-Client installiert und eingerichtet haben.

## Arbeit mit Datei-Menüoptionen

In dieser Tabelle sind Dateimenüoptionen für Office-Dokumente aufgeführt. Je nach der Sicherheitsstufe sind einige Optionen ausgegraut.

**ANMERKUNG:**

Derzeit werden integrierte Office-Dokumente im geschützten Office-Modus nicht unterstützt.



Dateimenü	Abonnierter Modus und geschützte Office-Dokumente	Erzwungener geschützter Modus für geschützte und ungeschützte Office-Dokumente
Öffnen Sie die Datei mit der	Dateien werden wie gewohnt geöffnet.	Nicht geschützte Dokumente werden im schreibgeschützten Modus geöffnet.
Speichern	<ul style="list-style-type: none"> <li>Optionen: Bereits geschütztes Dokument: Speicherung als geschützt. Ungeschützt: Speicherung als ungeschützt. Um es zu schützen, klicken Sie auf <b>Geschütztes „Speichern unter“</b>.</li> <li>Schreibgeschütztes Dokument: Ein Dialogfeld weist Sie darauf hin, dass Sie ein ungeschütztes Dokument nicht speichern können. Das Fenster „Speichern unter“ wird geöffnet und Sie müssen es mit einem anderen Dateinamen speichern.</li> <li>XEN-Datei: Sie können es im geschützten Modus öffnen und speichern, aber die .xen-Datei wird aus der Cloud entfernt. Das Office-Dokument verfügt über seine übliche Erweiterung, ist aber geschützt.</li> </ul>	<ul style="list-style-type: none"> <li>Das Dokument ist geschützt.</li> <li>Schreibgeschütztes Dokument: Sie können es bearbeiten, jedoch nicht das Original speichern. Wenn Sie auf „Speichern“ klicken, wird das Fenster „Als geschützt speichern“ geöffnet und Sie müssen es im geschützten Modus mit einem neuen Name speichern.</li> <li>Remote-Dokumente: Wenn Sie ein Dokument an einem Remote-Standort öffnen und es nicht geschützt ist, dann müssen Sie es auf Ihrem lokalen Laufwerk speichern, um es zu ändern und zu speichern. Sie können es nicht am Remote-Standort speichern.</li> </ul> <p><b>ANMERKUNG:</b> Durch Klicken auf „Speichern“ wird das Fenster „Speichern unter“ geöffnet, und die einzige Option im Feld „Speichertyp“ lautet „Office geschützt“ (Dokumente, Präsentation oder Excel-Arbeitsmappe).</p> <ul style="list-style-type: none"> <li>.xen Datei: Sie können es im geschützten Modus öffnen und speichern, aber die .xen-Datei wird aus der Cloud entfernt. Das Office-Dokument verfügt über seine übliche Erweiterung, ist aber geschützt.</li> </ul>
Speichern unter	Hat die Standardoptionen (aber nicht „Geschützter Modus“)	Deaktiviert
Geschütztes „Speichern unter“	Einzige Option im Feld „Speichertyp“ ist „Office geschützt“	Einzige Option im Feld „Speichertyp“ ist „Office geschützt“
Drucken	Möglicherweise aktiviert oder ausgegraut, basierend auf von Ihrem Administrator festgelegten Richtlinien. Wenn die Menüoption aktiviert ist, kann eine Richtlinie ein Wasserzeichen mit dem Benutzernamen, dem Domännennamen und der Computer-ID auf jeder Seite platzieren, wenn Sie drucken.	Je nach Richtlinie kann diese Option aktiviert oder grau unterlegt sein. Wenn die Menüoption aktiviert ist, kann eine Richtlinie ein Wasserzeichen mit dem Benutzernamen, dem Domännennamen und der Computer-ID auf jeder Seite platzieren, wenn Sie drucken.
Freigeben	Aktiviert	Deaktiviert
Speichern und Senden (Office 2010)	Aktiviert	Deaktiviert Wenn „Drucken“ aktiviert ist, können Sie Drucken wählen, um das Dokument als PDF zu drucken.
Exportieren (Office 2013 und höher)	Möglicherweise aktiviert oder ausgegraut, basierend auf von Ihrem Administrator festgelegten Richtlinien.	Möglicherweise aktiviert oder ausgegraut, basierend auf von Ihrem Administrator festgelegten Richtlinien.
Geschützter Export  (Office 2013 und höher)	Wenn die Menüoption „Exportieren“ ausgegraut und „Geschützter Export“ aktiviert ist, wird das Dokument mit einem Wasserzeichen auf jeder Seite exportiert, das den Benutzernamen, den Domännennamen und die Computer-ID enthält.	Wenn die Menüoption „Exportieren“ ausgegraut und „Geschützter Export“ aktiviert ist, wird das Dokument mit einem Wasserzeichen auf jeder Seite exportiert, das den Benutzernamen, den Domännennamen und die Computer-ID enthält.
	<p><b>ANMERKUNG:</b> Wenn Sie ein Dokument im geschützten Modus für einen externen Benutzer exportieren, kann dieser es öffnen und anzeigen, jedoch nicht exportieren oder drucken.</p>	<p><b>ANMERKUNG:</b> Wenn Sie ein Dokument im geschützten Modus für einen externen Benutzer exportieren, kann dieser es öffnen und anzeigen, jedoch nicht exportieren oder drucken.</p>

## Online mit geschützten Office-Dokumenten arbeiten



Beim Erstellen von geschützten Office-Dokumenten gilt es als bewährtes Verfahren, online zu arbeiten, da für diese Dokumente Schlüssel generiert werden. Wenn ein erneutes Image Ihres Computers erforderlich war und Sie geschützte Office-Dokumente offline erstellt haben, teilen Sie dies unbedingt Ihrem Administrator mit.

### Online mit Dokumenten mit aktivierten Makros arbeiten

Bei einem geschützten Dokument mit aktivierten Makros ist das Makro vorhanden, aber blockiert. Allerdings kann Data Guardian ein Dokument mit aktivierten Makros derzeit erst prüfen, nachdem das neu geschützte Dokument (.docm, .pptm, .xlsm) geschlossen und wieder geöffnet wurde. Wenn Sie ein geschütztes Dokument mit einem Makro als ungeschützt speichern, müssen Sie das Dokument ebenfalls schließen und erneut öffnen, damit das Makro ausgeführt werden kann.

### Ein geschütztes Office-Dokument an eine Outlook-E-Mail anhängen

Wenn Sie ein geschütztes Office-Dokument an eine Outlook-E-Mail anhängen, wählen Sie **Einfügen** statt *Als Text einfügen* aus. *Als Text einfügen* fügt den Dokument-Inhalt direkt in den Text der E-Mail ein, und der Inhalt ist nicht mehr geschützt.

### Richtlinie für den abonnierten Modus

Wenn in Datei > Info, „Drucken“ ausgegraut ist, hat eine Data Guardian-Richtlinie das Drucken von geschützten Office-Dokumenten deaktiviert. Aktuell ist die Druckoption allerdings nicht ausgegraut, wenn Sie in Windows Explorer mit der rechten Maustaste auf ein geschütztes Office-Dokument klicken. Wenn Sie jedoch „Drucken“ wählen, geschieht Folgendes:

- Word: Ein Dialogfeld zeigt an, dass Word nicht mehr funktioniert.
- Excel: Ein Dialogfeld zeigt an, dass „Drucken“ durch eine Richtlinie deaktiviert ist.
- PowerPoint: Ein Dialogfeld zeigt an, dass „Drucken“ durch eine Richtlinie deaktiviert ist. Wenn Sie auf OK klicken, wird ein Deckblatt gedruckt, aus dem hervorgeht, dass das Dokument geschützt ist.

## Bestimmen, welche Dokumente mit abonniertem Modus geschützt werden

Im erzwungenen geschützten Modus werden alle Office-Dokumente geschützt. Wenn Sie im abonnierten Modus überprüfen möchten, ob ein Dokument geschützt ist oder nicht, öffnen Sie das Dokument, und in der Titelleiste wird es als geschützt aufgeführt.

## Zusätzliche Menüoptionen für geschützte Office-Dokumente

Die Art des Office-Dokuments, geschützt oder ungeschützt, kann sich folgendermaßen auswirken.

### **Rechtsklick > Schützen**

Sie können mit der rechten Maustaste auf ein Office-Dokument klicken und **Schützen** auswählen. Sie müssen Inhalte hinzufügen, damit die Menüoption angezeigt wird. Sie können kein leeres Dokument schützen.

### **Dateieigenschaften > Dell Data Guardian-Registerkarte**

Bei geschützten Office-Dokumenten können Sie mit der rechten Maustaste klicken und **Eigenschaften** auswählen, woraufhin eine **Dell Data Guardian-Registerkarte** mit Informationen, wie der Schlüssel-ID der Datei und Zugriffs- und Embargodaten angezeigt wird.

### **Einfügen**

Wenn Ihr Administrator eine Richtlinie zum Schutz von Office-Dokumente festlegt:

- Sie können Daten im ursprünglichen geschützten Dokument kopieren und einfügen.
- Sie können Daten nicht von einem geschützten Dokument kopieren und in ein ungeschütztes Dokument einfügen. Es wird nichts in der Zwischenablage angezeigt, und eine unternehmensspezifische Textnachricht besagt, dass Sie in das ungeschützte oder nicht verwaltete Dokument nichts einfügen können.



### ANMERKUNG:

Wenn Sie Text aus einem geschützten Dokument ausschneiden und die Meldung in einem ungeschützten Dokument erhalten, klicken Sie auf **Rückgängig machen** im geschützten Dokument, um den Text abzurufen.

#### **Drag-and-Drop im geschützten Modus**

Sie können Inhalte per Drag-and-Drop in ein geschütztes Word-Dokument verschieben. Derzeit ist die Drag-and-Drop-Funktion für geschützte PowerPoint- und Excel-Dateien deaktiviert.

#### **Drucken für Umschläge und Etiketten**

Wenn der Administrator eine Richtlinie zum Hinzufügen eines Wasserzeichens beim Drucken eines geschützten Office-Dokuments festgelegt hat, führen Sie die folgenden Schritte aus, um Umschläge oder Etiketten zu drucken:

- 1 In einem Word-Dokument wählen Sie die Registerkarte **Sendungen** aus.
- 2 Wählen Sie die Option **Umschläge** oder **Etiketten** aus.
- 3 Nachdem Sie Adresse oder Absender eingegeben haben, klicken Sie auf **Drucken**.

 **ANMERKUNG:** Wenn Sie eine andere Option zum Drucken verwenden und der Administrator eine Richtlinie zum Hinzufügen eines Wasserzeichens für gedruckte Office-Dokumente festgelegt hat, wird ein Wasserzeichen auf Ihrem Briefumschlag oder Etikett angezeigt.

## Ermitteln von Manipulationen an geschützten Office-Dokumenten

Data Guardian kann geschützte Office-Dokumente scannen, um einige Formen der Manipulation zu erkennen.

Wenn ein interner Benutzer ein geschütztes Office-Dokument manipuliert:

- Data Guardian kann einige Manipulationen reparieren oder wiederherstellen.
- Bei Manipulationen, die nicht repariert werden können, wird möglicherweise ein Dialogfeld angezeigt, das Sie darauf hinweist, dass die Datei manipuliert wurde und dass Sie sich an Ihren Administrator wenden sollten.

Wenn ein nicht autorisierter Benutzer ein geschütztes Office-Dokument öffnet, wird nur das Deckblatt angezeigt. Falls der nicht autorisierte Benutzer Änderungen am Deckblatt vornimmt, wird es von Data Guardian wiederhergestellt, wenn die Datei von einem autorisierten Benutzer erneut als geschützt gespeichert wird.

## Externe Benutzer und geschützte Office-Dokumente

### **Verbesserte Sicherheit durch Hinzufügen von Datumseinschränkungen**

Mit Data Guardian laden Sie ein geschütztes Office-Dokument in die Cloud und geben es frei:

- Alle internen Data Guardian-Benutzer können dieses anzeigen.
- Basierend auf der Richtlinie können externe Benutzer es anzeigen.

Wahlweise können Sie für mehr Sicherheit in Bezug auf externe Benutzer eine Datumseinschränkung hinzufügen, um den Zeitraum zu begrenzen, in dem ein externer Benutzer ein geschütztes Office-Dokument anzeigen kann.

- 1 Wählen Sie **Datei > Info > Datumseinschränkung**.
- 2 Wählen Sie aus der Dropdown-Liste ein Anfangs- und Enddatum und -uhrzeit für die Anzeige des Dokuments durch einen externen Benutzer aus.





#### ANMERKUNG:

Startdatum und -uhrzeit können in der Zukunft liegen, falls Sie das Dokument senden möchten, aber verhindern wollen, dass der externe Benutzer es vor dem gewünschten Datum und der gewünschten Uhrzeit anzeigen kann.

3 Klicken Sie auf **OK**.

Das Dokument wird gespeichert, geschützt, geschlossen und wieder geöffnet.



#### ANMERKUNG:

Wenn Sie die Termine für ein ungeschütztes Office-Dokument ändern und dann auf „Abbrechen“ klicken, schützt Data Guardian die Datei nach wie vor.



#### ANMERKUNG:

Aktuell müssen Sie, wenn Sie Datumseinschränkungen zu einem ungeschützten Office-Dokument hinzufügen und es auf einem Netzlaufwerk speichern möchten, die Datei lokal speichern und dann in das Netzwerk kopieren.

Wenn ein externer Benutzer eine Datei nach dem Datums- und Zeitbereich öffnet, wird ein Dialogfeld angezeigt, das darauf hinweist, dass die Datei Zugriffsbeschränkungen unterliegt und der externe Benutzer sich an den Autor der Datei wenden kann. Das Dialogfeld zeigt keine Daten für den externen Benutzer an.

Wenn Sie ein Startdatum und eine Uhrzeit in der Zukunft festlegen und der externe Benutzer das Dokument vor diesem Zeitpunkt öffnet, weist ein Dialogfeld darauf hin, dass die Datei bis zu diesem Datum und dieser Uhrzeit aufgrund von Zugriffseinschränkungen nicht geöffnet werden kann.

## Erklärung der Elemente des Taskleistenmenüs von Data Guardian

Details-Bildschirm

Der Data Guardian-Details-Bildschirm stellt hilfreiche Informationen bereit, wie z. B.:

- Für technischen Support können Sie Status- oder Versionsinformationen bereitstellen.
- Um einen nicht verschleierte Dateinamen zu sehen, der einer a.xen-Datei zugeordnet ist, wählen Sie **Dateien > Dateizustand**.
- Um nach einem Dateinamen zu suchen, wählen Sie Kopieren unten rechts und fügen den Inhalt in eine Wort-Datei ein.
- Um zu sehen, wer der Eigentümer eines Ordners ist, wählen Sie Ordner und rollen zur Spalte ORDNEREIGENTÜMER.

So greifen Sie auf den Details-Bildschirm zu:

Klicken Sie auf das Data Guardian-Taskleistensymbol und anschließend auf **Details...**

Oben links auf dem Bildschirm „Details“ werden folgende Informationen angezeigt:

**Servicestatus:** Status des Windows-Service von Data Guardian. Folgende Werte sind möglich: Beendet, Start ausstehend, Beenden ausstehend, Aktiv, Fortfahren ausstehend, Unterbrechen ausstehend, Unterbrochen

**Ausführungsstatus:** Der Aktivierungsstatus des Geräts. Folgende Werte sind möglich: Aktiv, Wird erneut aktiviert, Gesperrt, Wird gesperrt

**Benutzermodus:** Interner Benutzer: ein Benutzer innerhalb dieser Domänenadresse

**Externer Benutzer:** ein Benutzer außerhalb dieser Domänenadresse

**Registrierungs-E-Mail:** Für interne Benutzer ist dies die Domänen-E-Mail-Adresse. Für externe Benutzer ist dies die E-Mail, unter der sie registriert sind.

**Server URL:** DDP EE-Server/VE-Server, der mit diesem Client kommuniziert.



**Letzte Richtlinienänderung:** Datum und Zeitstempel des Zeitpunkts, an dem die Richtlinie zuletzt geändert und vom Client verwendet wurde.

**Richtlinienversion:** Die vom DDP EE-Server/VE-Server generierte Richtlinienversion.

Die Bereiche der **Dateien** und Ordner des Details-Bildschirms zeigen folgende Informationen an:

**Name:** Name der Datei

**Cloud:** Führt den verborgenen Dateinamen auf oder zeigt an, ob die Datei *Ungeschützt* ist.

**Dateizustand:** Dieser Wert gibt den Eigentümer des Ordners an. Der Wert wird von der Schlüssel-ID festgelegt.

**Verarbeitungszustand:** Gibt an, ob die Datei einen Schlüssel braucht oder *Abgeschlossen* ist.

**Unternehmen:** Führt den Standardserver auf. Wenn in dieser Spalte die Meldung *Fehler: Schlüssel nicht von Ihrem Server* angezeigt wird, gehört der Schlüssel nicht zum Server Ihres Unternehmens. Der Schlüssel für eine verschlüsselte Datei muss zum Server Ihres Unternehmens gehören.

**Schlüssel:** Die Schlüssel-ID, die diesem Ordner zugewiesen wurde. Neue Dateien nutzen diesen Schlüssel zur Verschlüsselung.

**Ordner:** Der vollständige Pfadname des Ordners.

**Letzte Änderung:** Das Datum, an dem die Datei geändert wurde.

**Beständigkeitszustand:** Dies gibt an, ob die Datei auf der Festplatte ist.

**XEN Datei-Lesevorgang:** *Wahr* oder *Falsch*.

**Browser erstellt:** *Wahr* oder *Falsch*.

Um Protokolldateien anzuzeigen, klicken Sie auf dem Bildschirm „Details“ unten links auf **Protokoll anzeigen**.

#### ANMERKUNG:

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

Der Bereich **Ordner** auf dem Bildschirm „Details“ enthält die folgenden Informationen:

**Name:** Name des Ordners

**Schlüssel:** Die Schlüssel-ID, die diesem Ordner zugewiesen wurde. Neue Dateien nutzen diesen Schlüssel zur Verschlüsselung.

**Sync-Client:** Der letzte Sync-Client, der diesen Ordner synchronisiert hat (siehe [Cloud-Synchronisierungs-Clients](#))

**Ordneigentümer:** Dieser Wert gibt den Eigentümer des Ordners an. Der Wert wird von der Schlüssel-ID festgelegt.

**Überschreiben:** Die Optionen sind *Keine* und *Bereits vorhandene*. Zuvor vorhandene Dateien sind nicht geschützt. Falls Sie den Zugriff auf die Ordnerverwaltung und den Schutz einiger Dateien aufgehoben haben, gibt diese Spalte außerdem an, dass sie nicht geschützt sind.

**Verschleierungstyp:** Wenn Ihr Unternehmen Ihre Cloud-Speicherung verwaltet, ist dies eine Richtlinie, die für jeden Ordner festgelegt ist und angibt, welche Art von .xen-Dateien in der Cloud erstellt wird. Dies ist eine von Ihrem Administrator festgesetzte Richtlinie. Wenn Ihr Administrator *Nur Erweiterung* auswählt, wird der tatsächliche Dateiname mit der Erweiterung „.xen“ angezeigt. Falls Ihr Administrator *Guid* auswählt, wird ein verschlüsselter Dateiname mit der Erweiterung „.xen“ angezeigt. Diese Richtlinieneinstellung gilt nur für neue Ordner. Die Standardeinstellung ist *Nur Erweiterung*.

# Ordner verwalten – Menü

Einige Manager oder Administratoren müssen möglicherweise vorübergehend Fehler in von mehr als einem Benutzer gemeinsam genutzten Ordnern beheben. Sie können bei Ihrem Administrator die Genehmigung für die Option „Ordner verwalten“ anfordern. Normalerweise ist dies eine temporäre Option.

## Protokolldateien ausfindig machen

Zu Fehlerbehebungszwecken kann es sein, dass Ihr Administrator Protokolldateien von Ihnen anfordert.

So können Sie Protokolldateien ausfindig machen:

- 1 Navigieren Sie zu
- 2 Wählen Sie **Xendow.Service.log** aus.

### ① ANMERKUNG:

Nachdem die Datei Xendow.Service.log eine Größe von 3 MB erreicht hat, wird sie als Xendow.Service1.log und dann als Xendow.Service2.log gespeichert.

## Richtlinien auf Aktualisierungen überprüfen

Falls Ihr Administrator eine Richtlinie ändert und Sie über eine Richtlinienaktualisierung unterrichtet, gehen Sie zur Windows-Taskleiste, klicken Sie auf das Symbol **Dell Data Protection | Data Guardian** und wählen Sie **Auf Richtlinienaktualisierungen überprüfen**.

Wenn Ihr Administrator eine Richtlinie zum Schutz von in Microsoft Word erstellten Dateien ändert, müssen Sie Word schließen, damit diese Aktualisierung angewendet werden kann.

## Data Guardian aufrüsten

Als bewährtes Verfahren gilt die Deinstallation der früheren Version mit anschließender Installation der aktuellen Version. Siehe [Data Guardian deinstallieren](#).

## Dell Feedback geben

Falls Ihr Administrator eine Feedback-Richtlinie aktiviert hat, können Sie Dell Feedback zu diesem Produkt geben. Das kurze Formular enthält zwei Fragen zu Ihrem Zufriedenheitsgrad mit einer Bewertungsskala (wobei 10 die höchste Kundenzufriedenheit bedeutet) und einem Kommentarfeld.

Um das Formular aufzurufen, klicken Sie auf das Data Guardian-Taskleistensymbol und wählen Sie **Feedback senden** aus.

Ist diese Funktion gemäß Richtlinie deaktiviert, wird die Option nicht angezeigt.

## Mögliche Probleme mit der Aktivierung: geschützte Office-Dokumente

Wenn Sie Data Guardian installiert haben, aber das Data Guardian-Symbol in der Taskleiste nicht mit einem grünen Häkchen  versehen ist, beachten Sie Folgendes:

- Data Guardian kann vorhandene Office-Dokumente vor der Aktivierung in den geschützten Modus konvertieren. Wenn dies der Fall ist, wird ein Deckblatt mit Informationen zur Aktivierung angezeigt, wenn Sie ein Office-Dokument öffnen.




Führen Sie einen der folgenden Schritte aus:

- Starten Sie das System neu und melden Sie sich erneut mit einem UPN-Suffix, z. B. user\_name@domain.com, an.
- Fragen Sie Ihren Administrator, ob Sie das Kontrollkästchen **SSL-Prüfung aktivieren** nach der Installation von Data Guardian aktivieren sollten.
- Klären Sie mit Ihrem Systemadministrator, ob Sie Ihren Computer für die manuelle Aktivierung konfigurieren müssen. Siehe [Data Guardian aktivieren](#).

## Data Guardian aktivieren

Normalerweise wird Data Guardian nach Installation und Neustart automatisch aktiviert. Wenn der Systemadministrator Sie bittet, die Aktivierung manuell vorzunehmen, führen Sie die folgenden Schritte aus:

- 1 Melden Sie sich bei Windows an.  
In der Taskleiste wird ein Shield-Symbol mit einem orangefarbenen Ausrufezeichen angezeigt.
- 2 Klicken Sie in der Taskleiste auf das **Data Guardian**-Symbol und wählen Sie **Benutzeraktivierung** aus.
- 3 Geben Sie Ihre Domänen-E-Mail-Adresse und Ihr Domänenpasswort ein, und klicken Sie auf **Aktivieren**.  
Falls Sie ein interner Benutzer sind (also über eine E-Mail-Adresse innerhalb der Domäne verfügen), ignorieren Sie die Schaltfläche „Registrieren“. Nur externe Benutzer müssen sich registrieren.

Nach Abschluss der Aktivierung wird ein grünes Häkchen auf dem Data Guardian-Taskleistensymbol  angezeigt

- 4 Bestätigen Sie Ihren Benutzermodusstatus. Klicken Sie auf die Registerkarte -Taskleistensymbol und wählen Sie **Details** aus.
- 5 Bestätigen Sie oben den Benutzermodus:

**Intern:** Ein Benutzer mit einer E-Mail-Adresse innerhalb der Domäne des Unternehmens.

**Extern:** Ein Benutzer mit einer E-Mail-Adresse außerhalb der Domäne. Weitere Informationen finden Sie unter [Verwendung von Data Guardian als externer Benutzer](#).

# Data Guardian Mobile mit iOS oder Android verwenden

Dieser Abschnitt enthält grundlegende Informationen zur Verwendung von Data Guardian Mobile mit iOS- oder Android-Geräten. Wenn Ihr Administrator eine Richtlinie zur Aktivierung von Data Guardian festgelegt hat, werden Ihre Dateien verschlüsselt und sind in der Cloud sicher. Sie können jedoch die Data Guardian Mobile-App verwenden, um sie auf Ihrem mobilen Gerät anzuzeigen.

## Voraussetzungen

Bevor Sie die Data Guardian-Anwendung nutzen, benötigen Sie den Namen des Dell Data Protection Servers Ihres Unternehmens, z. B. server.domain.com. Diese Informationen werden von Ihrem Administrator bereitgestellt.

## Erste Schritte mit Data Guardian Mobile

Verwenden Sie die folgende Sequenz bei der Nutzung von Data Guardian Mobile.

Aufgabe	Beschreibung	Siehe diesen Abschnitt
Data Guardian installieren	Überprüfen Sie Folgendes:  Installation durch Administrator bereits erfolgt  Installation durch Benutzer erforderlich	Administrator-installiert: Tippen Sie auf die Data Guardian-App und melden Sie sich an.  Benutzer installiert: Siehe eine der folgenden Anleitungen:  <a href="#">Installieren auf einem iOS-Gerät</a>  <a href="#">Installieren auf einem Android-Gerät</a>
Auf das Konto Ihres Cloud-Speicher-Anbieters zugreifen	Navigieren Sie auf dem Gerät zur Startseite der Data Guardian-App und tippen Sie auf Ihren Cloud-Speicheranbieter.	Lesen Sie einen der folgenden Abschnitte:  <a href="#">Zugriff auf Ihr Cloud-Speicheranbieter-Konto für iOS</a>  <a href="#">Zugriff auf Ihr Cloud-Speicheranbieter-Konto für Android</a>

Die App Data Guardian Mobile führt den von Ihrem Unternehmen verwendeten Cloud-Synchronisierungs-Client auf und ermöglicht Ihnen den Download.

### ANMERKUNG:

Wenn Sie die Cloud-Synchronisierungs-Client-App auf Ihr Gerät herunterladen, verschlüsselt Data Guardian keine Ordner oder Dateien, die Sie direkt von dieser App hochladen. Um Dateien zu verschlüsseln und zu schützen, müssen Sie sie mithilfe der Data Guardian-App in hochladen.

Zum Schutz Ihrer Daten in der Cloud verschlüsselt Data Guardian sie. Aus diesem Grund muss die Data Guardian-App auf Ihrem Mobilgerät installiert sein, um verschlüsselte Dateien anzuzeigen.

- Geschützte Office-Dateien (.docx, .pptx, .xlsx) behalten ihren Dateierweiterung.
- Die Office-fremden Dateien in der Cloud verfügen über die Dateierweiterung „.xen“.

Wenn eine nicht befugte Person auf Ihr Cloud-Speicherkonto zugreift und eine Datei auf ein mobiles Gerät herunterlädt, auf dem Data Guardian **nicht** installiert ist, kann die Person Ihre Dateien nicht öffnen oder anzeigen. Wenn Sie eine geschützte Office-Datei öffnen, wird



nur ein Deckblatt angezeigt, das darauf hinweist, dass die Person das Dokument nicht ohne Data Guardian anzeigen kann. Dies sorgt für mehr Sicherheit für Ihre Daten.

Auf Mobilgeräten können Sie folgende Aktionen durchführen:

- Ordner erstellen
- Dateien hochladen und herunterladen

**ANMERKUNG:**

Bei Data Guardian müssen Sie Uploads und Downloads auf dem Gerät starten. Wenn Sie möchten, dass Ihre Dateien beim Hochladen in die Cloud verschlüsselt werden, müssen Sie sie über die Data Guardian-Startseite hochladen und nicht über eine Cloud-Synchronisierungs-Client-App. Wenn Sie eine Datei antippen, entschlüsselt Data Guardian sie automatisch und zeigt sie in der App in Klartext an. In der Cloud ist diese Datei jedoch nach wie vor als .xen-Datei geschützt.

- Datei zu Favoriten hinzufügen
  - Bei Verwendung von iOS, siehe Schublade „Navigation“. Bei Verwendung von Android halten Sie den Dateinamen gedrückt.
- Ordner und Dateien löschen
- Freigegebenen Ordner eines internen Benutzers annehmen

**ANMERKUNG:**

Wenn ein interner Benutzer einen Ordner über Data Guardian für Sie freigibt, müssen Sie ihn von der Cloud-Speicher-Website in den Stammordner verschieben oder den freigegebenen Ordner herunterladen, um ihn auf dem Gerät anzuzeigen.

- Ein Dokument für einen externen Benutzer freigeben (falls die Richtlinie für externe Betrachter aktiviert ist): siehe [Data Guardian Cloud-Speicherungsrichtlinien für Ihr iOS-Gerät](#).
- Bearbeiten von .docx- und .ppt-Office-Dateien.

**ANMERKUNG:**

Derzeit ist die Bearbeitung von .csv- und .csv.xen-Dateien auf mobilen Geräten nicht möglich.

## Geschützte Office-Dokumente im Offline-Modus

Wenn Sie ein geschütztes Office-Dokument oder ein geschütztes Dokument mit aktivierten Makros erstellen und offline sind, wird ein Schlüssel für dieses Dokument erstellt. Wenn das Gerät online geschaltet wird, werden die Schlüssel auf den Dell Server hochgeladen. Wenn ein Gerät drei Tage offline ist, gibt eine Benachrichtigung an, dass Data Guardian keine Verbindung mit dem Dell Server herstellen konnte. Die Benachrichtigung wird täglich angezeigt, bis Sie eine Verbindung mit dem Netzwerk herstellen. Um die verschlüsselten Dateien anzuzeigen, muss das mobile Gerät online sein.

## Zusätzlichen Schutz durch Geofencing

Basierend auf vom Administrator festgelegten Richtlinien können mobile Geräte einem zusätzlichen Schutz unterliegen, sodass geschützte Office-Dokumente und .xen-Dateien außerhalb einer bestimmten Region nicht geöffnet werden können. Sie müssen sich in einer zugelassenen Region befinden, um geschützte Dateien zu öffnen. Derzeit sind die Regionen USA und Kanada. Sie müssen die Ortungsdienste auf dem Gerät aktivieren, damit Geofencing funktioniert. Wenn die Geofencing-Funktion vom Administrator aktiviert wurde und die Ortungsdienste auf Aus gesetzt sind, wird der Dateizugriff verweigert.

## Verwenden einer PIN

Ihr Administrator kann eine Richtlinie festlegen, die eine PIN voraussetzt.

# Data Guardian auf einem iOS-Gerät

## Installieren auf einem iOS-Gerät

- 1 Tippen Sie auf Ihrem Gerät auf **App Store** und suchen Sie nach **Data Guardian Mobile**.
- 2 Wählen Sie und installieren Sie die **Data Guardian**-App.



- 3 Geben Sie für das Serverfeld auf dem Anmeldebildschirm den Hostnamen des Dell Data Protection Servers Ihres Unternehmens ein, z. B. server.domain.com.
- 4 Geben Sie Ihren Benutzernamen und Ihr Passwort ein.
- 5 Tippen Sie auf **Anmelden**.

### Zugriff auf Ihr Cloud-Speicheranbieter-Konto für iOS

Nach der Anmeldung bei Data Guardian wird durch eine Data Guardian-Richtlinie ermittelt, welche Cloud-Speicher-Anbieter auf der Startseite angezeigt werden. Ihr Administrator kann einen bestimmten Cloud-Speicher-Anbieter angeben, der in Ihrem Unternehmen verwendet werden soll.

Die Schublade „Navigation“ enthält zusätzliche Optionen.

So greifen Sie auf ein Konto zu:

- 1 Tippen Sie auf der Data Guardian-Startseite auf Ihren Cloud-Speicher-Anbieter.
- 2 Führen Sie eine der folgenden Aktionen aus, indem Sie die Online-Anweisungen befolgen:
  - Erstellen Sie ein Konto bei dem jeweiligen Cloud-Speicher-Anbieter.
  - Melden Sie sich bei einem bereits vorhanden Konto eines Cloud-Speicher-Anbieters an.



#### ANMERKUNG:

Weitere Informationen finden Sie in der Hilfe Ihres Cloud-Speicher-Anbieters.

### Verlinkung eines Cloud-Speicher-Anbieters aufheben

Wenn Sie mehrere Konten bei ein und demselben Cloud-Speicher-Anbieter haben, können Sie immer nur bei einem Konto gleichzeitig angemeldet sein. Sie müssen zuerst das Kontrollkästchen deaktivieren und sich vom aktuellen Konto abmelden, und sich dann mit den entsprechenden Anmeldeinformationen an einem der anderen Konten anmelden.

- 1 Öffnen Sie die Data Guardian-Navigationsschublade und tippen Sie auf **Einstellungen**.
- 2 Tippen Sie auf **Verknüpfung aufheben**.

### Anzeigen der Data Guardian-Cloud-Speicherungsrichtlinien für Ihr iOS-Gerät

- 1 Tippen Sie in der Data Guardian-Navigationsschublade auf **Einstellungen**.
- 2 Tippen Sie auf **Richtlinie**.  
In der Liste kann Folgendes enthalten sein:
  - Überprüfung – Anzahl der Richtlinien, die überprüft wurden.
  - Dateinamen verbergen: Die Standardeinstellung lautet **Nein**.
  - Cloud-Synchronisierungs-Client: Die Richtlinie sollte auf **Verschlüsseln** eingestellt sein.
  - Externe Betrachter: Wenn die Einstellung **Ja** lautet, ist die Freigaberichtlinie aktiviert. Wenn Sie ein Dokument in der App öffnen, können Sie die Datei mithilfe einer Menüoption freigeben.

### Deinstallieren Sie die Data Guardian-App

- 1 Tippen und halten Sie in der iOS Apps-Schublade das Symbol für **Data Guardian**.
- 2 Tippen Sie auf **x**.
- 3 Tippen Sie auf **Löschen**.

## Fehlerbehebung bei iOS und Data Guardian

Wenn Sie auf einem iOS-Gerät ein geschütztes Office-Dokument öffnen, das größer als 25 MB ist und ein Dialogfeld wegen niedrigem Speicher angezeigt wird, stammt die Warnung von Polaris Office, nicht von Data Guardian. Wenn das Gerät über ausreichend Speicherplatz verfügt, schließen Sie die Datei und öffnen Sie sie dann erneut.



Wenn Sie bei Dropbox für Unternehmen eine Datei als offline verfügbar markieren und die Datei dann auf der Dropbox-Website umbenennen, lässt sich die Datei auf dem iOS-Gerät mit der Data Guardian-App nicht öffnen.

# Data Guardian auf einem Android-Gerät

## Installieren auf einem Android-Gerät

- 1 Greifen Sie auf Ihrem Gerät auf **Google Play** zu und suchen Sie nach Data Guardian **Mobile**.
- 2 Wählen Sie und installieren Sie die **Data Guardian-App**.
- 3 Geben Sie für das Serverfeld auf dem Anmeldebildschirm den Namen des Dell Data Protection Servers Ihres Unternehmens ein, z. B. server.domain.com.
- 4 Geben Sie Ihren Benutzernamen und Ihr Passwort ein.
- 5 Tippen Sie auf **Anmelden**.

Ihr Konto ist jetzt aktiviert.

## Zugriff auf Ihr Cloud-Speicheranbieter-Konto für Android

Nach der Anmeldung bei Data Guardian wird durch eine Data Guardian-Richtlinie ermittelt, welche Cloud-Speicher-Anbieter angezeigt werden. Ihr Administrator kann einen bestimmten Cloud-Speicher-Anbieter vorgeben, der in Ihrem Unternehmen verwendet werden soll, und andere Anbieter sperren.

So greifen Sie auf ein Konto zu:

- 1 Tippen Sie auf der Data Guardian-Startseite auf Ihren Cloud-Speicher-Anbieter.
- 2 Führen Sie eine der folgenden Aktionen aus, indem Sie die Anweisungen im Bildschirm befolgen:
  - Erstellen Sie ein Konto bei dem jeweiligen Cloud-Speicher-Anbieter.
  - Melden Sie sich bei einem bereits vorhanden Konto eines Cloud-Speicher-Anbieters an.

### ANMERKUNG:

Weitere Informationen finden Sie in der Hilfe Ihres Cloud-Speicher-Anbieters.

- 3 Greifen Sie auf Ihr Konto zu, öffnen Sie die Navigationsschublade, und tippen Sie auf **Einstellungen**. Wenn Sie den Zugriff auf einen Cloud-Speicher-Anbieter gewähren, wird das Kontrollkästchen markiert.

### ANMERKUNG:

Wenn Sie mehrere Konten bei ein und demselben Cloud-Speicher-Anbieter haben, können Sie immer nur bei einem Konto gleichzeitig angemeldet sein. Sie müssen zuerst das Kontrollkästchen deaktivieren und sich vom aktuellen Konto abmelden, und sich dann mit den entsprechenden Anmeldeinformationen an einem der anderen Konten anmelden.

### ANMERKUNG:

Wenn Sie in OneDrive und Dropbox eine Datei von „Anwendungen“ nicht freigeben können und die Datei einen Link mit der Data Guardian-App gemeinsam verwendet, geben Sie die Datei über den Dateibrowser auf dem Gerät frei.

## Deinstallieren Sie die Data Guardian-App

- 1 Tippen Sie in der Android Apps-Schublade auf **Einstellungen**.
- 2 Tippen Sie in **Einstellungen** auf **Apps**.
- 3 Drücken Sie auf das **Data Guardian**-Symbol.
- 4 Ziehen Sie das Symbol auf die Option „Deinstallieren“.
- 5 Klicken Sie auf **OK**.



# Sicherheitsüberlegungen für die Verwendung von Data Guardian mit Synchronisierungs-Clients

Data Guardian verschlüsselt Ordner und Dateien, um Daten zu sichern. Da Data Guardian mit Synchronisierungs-Clients arbeitet, sollten Sie folgende Überlegungen berücksichtigen.

## Google Drive

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 nicht auf dem Dell Data Protection EE-Server/VE-Server. Die Dateien werden daher nicht verschlüsselt. Bei Android- und iOS-Geräten mit Data Guardian ist der Zugriff auf diese Google Docs blockiert. Je nach Plattform reagiert das System etwas anders:

- Android
- iOS – Es wird eine Meldung angezeigt.

## OneDrive und OneDrive für Unternehmen

Bei Verwendung von OneDrive für Unternehmen geschieht Folgendes: Wenn Sie mehrere Dateien herunterladen und den Herunterladevorgang abbrechen, storniert OneDrive für Unternehmen die Dateien, die noch nicht heruntergeladen wurden, und setzt den Vorgang für die Datei fort, die sich derzeit noch im Herunterladevorgang befindet. Dies ist ein Microsoft-Problem. Laden Sie daher zunächst alle Dateien vollständig herunter, bevor Sie den Vorgang abbrechen.

## Protokolle

Aus Sicherheitsgründen sind auf Mobilgeräten keine Protokolldateien verfügbar.

## Dell Feedback geben

Falls Ihr Administrator eine Feedback-Richtlinie aktiviert hat, können Sie Dell Feedback zu diesem Produkt geben. Ist diese Funktion gemäß Richtlinie deaktiviert, wird die Option nicht angezeigt.

So können Sie Feedback senden:

- 1 Tippen Sie in der Data Guardian-Navigationsschublade auf **Feedback**.
- 2 Die kurzen Fragen bieten Ihnen die Möglichkeit, Ihren Zufriedenheitsgrad anhand einer Skala zu bewerten (wobei 10 für die höchste Kundenzufriedenheit steht) und einen Kommentar einzugeben.



# Verwendung von Data Guardian als externer Benutzer

Auch externe Benutzer, die über eine domänenfremde E-Mail-Adresse verfügen, können Data Guardian verwenden. Beispiele:

- Sie haben Data Guardian in Ihrem Unternehmen installiert und aktiviert, möchten jedoch die geschützten Dateien freigeben oder gemeinsam mit einem Benutzer außerhalb des Unternehmens an geschützten Dateien arbeiten.
- Ihre E-Mail-Adresse ist Teil der Domäne Ihres Unternehmens, Sie möchten Data Guardian jedoch auf einem Computer oder einem Mobilgerät mit Ihrer persönlichen, domänenfremden E-Mail-Adresse installieren und aktivieren. Auf diese Weise können Sie mit Ihren geschützten Dateien von einer domänenfremden E-Mail-Adresse aus interagieren.

Für externe Benutzer siehe [Serveranforderungen](#). Außerdem darf sich die Domäne oder der Benutzer nicht auf der Blacklist des Unternehmens befinden.

## ANMERKUNG:

Externe Benutzer, die mit Secure Lifecycle 1.0 oder höher registriert wurden, werden migriert, wenn das Unternehmen ein Upgrade durchführt.

## Aufgaben interner Benutzer

Um sichere Dateien für einen externen Benutzer freizugeben, können Sie ein geschütztes Office-Dokument oder eine .xen-Datei über eine Outlook-E-Mail senden. Eine Bestätigungsaufforderung erinnert Sie daran, dass der Schlüssel für die geschützte Datei freigegeben wird.

## ANMERKUNG:

Wenn ein externer Benutzer eine geschützte Datei per E-Mail sendet, werden die Schlüssel nicht freigegeben.

Sie können auch über die Option „Zugriff gewähren“ sichere Dateien für einen externen Benutzer freigeben. Dazu müssen Sie Folgendes ausführen:

- Machen Sie eine oder mehrere sichere Dateien für den externen Benutzer verfügbar.
  - Geschützte Office-Dokumente: Zugang zu einer oder mehreren sicheren Dateien gewähren Sie durch:
    - Lokaler Ordner oder Netzlaufwerk
    - E-Mail
    - Wechselmedien
    - Netzwerkfreigabe
  - .xen-Dateien (nicht Office): Erstellen Sie einen Ordners für die Freigabe auf dem Synchronisierungs-Client und fügen Sie die Dateien hinzu.
- Erteilen Sie dem externen Benutzer den Zugriff auf eine oder mehrere Dateien.

Wenn Sie vorhaben, eine Office-fremde .xen-Dateien freizugeben, müssen Sie sie zu einem Ordner auf dem Synchronisierungs-Client hinzufügen und anschließend den Zugang gewähren. Für geschützte Office-Dateien müssen Sie Zugang gewähren. Die folgenden Schritte können je nach der Methode oder dem Synchronisierungs-Client, die bzw. den Sie verwenden, variieren.

### Einen Ordner auf dem Synchronisierungs-Client freigeben, um .xen-Dateien freizugeben

- 1 Greifen Sie über Windows Explorer auf Ihren Synchronisierungs-Client zu, erstellen Sie einen Ordner, und laden Sie eine Datei hoch, die Sie für einen externen Benutzer freigeben möchten. Siehe [Ordner und Dateien auf dem lokalen Computer und in der Cloud anzeigen](#).

Geschützte Office-Dokumente können sich auf dem DDG VDisk Virtual Drive, im Data Guardian-Ordner oder auf dem Desktop befinden.

**ANMERKUNG:**

Bei geschützten Office-Dateien können Sie keinen Ordner auswählen.

Eine Seite für die *Freigabe für Zugriff auf geschützte Dokumente* wird geöffnet, auf der in einer Spalte die ausgewählten Dateien angezeigt werden.

- Bestätigen Sie auf der Synchronisierungs-Client-Website, dass der Ordner und die Datei erstellt und verschlüsselt wurden. Beim Hinzufügen einer .xen-Datei zu einem neuen Ordner auf dem DDG VDisk Virtual Drive fügt Data Guardian ein Dokument mit dem Namen *Zugriff auf sichere Dateien.html* zum Ordner auf der Website hinzu. Diese Datei kommt nur dann zum Einsatz, wenn der Ordner gemeinsam mit einem externen Benutzer verwendet wird.
- Klicken Sie auf der Synchronisierungs-Client-Website mit der rechten Maustaste auf den Ordner, den Sie erstellt haben, und klicken Sie dann auf **Freigeben**. Daraufhin wird ein Fenster geöffnet, in das Sie das E-Mail-Konto für einen externen Benutzer eingeben können. Die jeweiligen Schritte können je nach verwendetem Synchronisierungs-Client abweichen. Links zu Informationen zu Ihrem Synchronisierungs-Client finden Sie unter [Arbeit mit dem Cloud-Synchronisierungs-Client auf dem virtuellen DDG VDisk-Laufwerk](#).
- [Gewähren Sie Zugriff](#) auf die einzelnen Dateien in dem Ordner, den Sie freigeben möchten.

### Zugriff auf eine oder mehrere geschützte Office-Dateien gewähren

Für alle Dateien, die Sie für externe Benutzer freigeben, müssen Sie Zugriff gewähren.

- Klicken Sie mit der rechten Maustaste auf eine sichere Datei und wählen Sie **Zugriff auf geschützte Datei gewähren**. Sie können eine oder mehrere Dateien (bis zu 50) auswählen.
- Geben Sie im Feld *E-Mail für Freigabe* die E-Mail-Adresse des Benutzers außerhalb der Domäne ein, und klicken Sie auf **Hinzufügen**.
- Wiederholen Sie diesen Schritt, um bis zu zehn E-Mail-Adressen hinzuzufügen.
- Klicken Sie auf **OK**. Ein Dialogfeld zeigt entweder an, dass die Freigabe erfolgreich war, oder dass die E-Mail-Adresse nicht zum Empfang geschützter Dateien berechtigt ist.
- Es hat sich bewährt, den externen Benutzer darüber zu informieren, dass er oder sie eine E-Mail von Ihnen erhalten werden, in der Anweisungen für die Registrierung bei einem Dell Server, den Download und die Aktivierung von Dell Data Protection | Data Guardian sowie die anschließende Anzeige der freigegebenen geschützten Dateien enthalten sind.

### Genehmigen oder Verweigern des Zugriffs, wenn ein externer Benutzer Zugriff anfordert

Eine externe Benutzer, der Data Guardian installiert hat, kann den Zugriff auf ein geschütztes Dokument anfordern, wenn er oder sie nicht über einen Schlüssel für dieses Dokument verfügt.

- Wenn Sie eine E-Mail mit einer Zugriffsanforderung von einem externen Benutzer für ein geschütztes Dokument erhalten, wird Ihnen der Name des externen Benutzers und der angeforderten Datei angezeigt.
- Klicken Sie auf **Genehmigen** oder **Ablehnen**. Eine E-Mail wird an den externen Benutzer gesendet. Wenn Sie die Genehmigung erteilen, wird der Schlüssel für das geschützte Dokument freigegeben.

Wenn Sie nicht verfügbar sind, hat Ihr Administrator außerdem die Möglichkeit, den Zugriff zu genehmigen oder zu verweigern.



# Aufgaben externer Benutzer

Zum Öffnen und Anzeigen eines Data Guardian-Dokuments muss der externe Benutzer:

- sich bei Data Guardian anmelden.
- Data Guardian installieren: der externe Benutzer muss über Administratorrechte auf dem eigenen Computer verfügen.
- Wenn der interne Benutzer einen Ordner über einen Synchronisierungs-Client freigibt, muss der externe Benutzer über ein Synchronisierungs-Client-Konto verfügen. Siehe [Installieren eines Cloud-Synchronisierungs-Clients](#) und dann [Arbeit mit dem Cloud-Synchronisierungs-Client auf dem virtuellen DDG VDisk-Laufwerk](#).

## Registrierung von Data Guardian

Wenn ein interner Benutzer eine Datei zum ersten Mal freigibt, muss sich der externe Benutzer registrieren.

So registrieren Sie Data Guardian:

- 1 Klicken Sie auf den Hyperlink in der Kontoverifikations-E-Mail vom Dell Enterprise Server.
- 2 Wechseln Sie zur Webseite.
- 3 Klicken Sie auf der Seite „Bestätigung“ auf **Weiter zur Anmeldung**.
- 4 Klicken Sie auf der Anmeldeseite auf **Kennwort vergessen**.

### ANMERKUNG:

Der Dell Server hat ein zufälliges Kennwort zugewiesen, das Sie zurücksetzen müssen.

- 5 Geben Sie auf der Seite „Kennwort zurücksetzen“ Ihr Kennwort ein, bestätigen Sie es und klicken Sie dann auf **Registrieren**. Daraufhin wird ein Bestätigungsdialogfeld für die Registrierung angezeigt, außerdem wird eine E-Mail an die vom internen Benutzer angegebene E-Mail-Adresse gesendet.
- 6 Öffnen Sie die Konto-Aktivierungs-E-Mail und klicken Sie auf den Link.  
Die E-Mail führt auch den Servernamen auf, den Sie verwenden müssen, wenn Sie die Data Guardian installieren.
- 7 Geben Sie auf der Anmeldeseite die E-Mail-Adresse und das Passwort ein, die bzw. das Sie für die Registrierung verwendet haben.
- 8 Klicken Sie auf **Anmelden**.  
Eine Data Guardian-Download-Seite wird geöffnet.
- 9 Laden Sie Data Guardian herunter und installieren Sie die Anwendung.  
Eine Download-Seite mit Optionen für Windows, iOS, Android, und Mac OS X wird geöffnet. Bei einem Enterprise Server wird die Download-Seite geöffnet. Bei einem Dell Enterprise Server: VE werden Sie durch Klicken auf „Windows“ zur Website [dell.com/support](http://dell.com/support) weitergeleitet.

Diese Schritte beschreiben die Installation von Data Guardian auf Windows. Siehe auch [Benutzeraufgaben: geschützte Office-Dokumente ohne Cloud-Verschlüsselung](#).

### ANMERKUNG:

Auf der Download-Seite wird außerdem der Servername angezeigt, den Sie in diesen Schritten benötigen.


- 10 Unter Windows klicken Sie auf **Herunterladen (32-Bit)** oder **Herunterladen (64-Bit)**, je nach dem, welches Betriebssystem auf dem Computer ausgeführt wird.
- 11 Laden Sie die Setup-Datei in ein Verzeichnis auf Ihrem Computer herunter.
- 12 Doppelklicken Sie zum Starten des Installationsprogramms auf die Setup-Datei.
- 13 Wählen Sie eine Sprache aus und klicken Sie auf **OK**.
- 14 Klicken Sie auf **OK**, wenn Sie zur Installation von Microsoft Visual C++ 2010 Redistributable Package aufgefordert werden.
- 15 Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.
- 16 Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen, und klicken Sie auf **Weiter**.
- 17 Klicken Sie auf dem Bildschirm des Zielordners auf **Weiter**, um die Installation am Standardort von **C:\Program Files\Dell\Dell Data Protection\Dell Data Guardian\** auszuführen.

- 18 Geben Sie im Feld *Servername*: den Servernamen ein, mit dem dieser Computer kommunizieren wird. Dieser Name ist in der Aktivierungs-E-Mail enthalten, die Sie erhalten haben. Alternativ finden Sie den Namen auch oben auf der Download-Seite.
- 19 Klicken Sie auf **Weiter**.
- 20 Bestätigen Sie auf dem Bildschirm „Aktivierungsserver bestätigen“, dass die Server-URL-Adresse korrekt ist. Das Installationsprogramm fügt www oder http(s) und den Port hinzu. Klicken Sie auf **Weiter**.
- 21 Wählen Sie im Fenster „Management Type“ (Verwaltungstyp) diese Option aus:
  - Externe Verwendung: Ein Benutzer mit einer E-Mail-Adresse außerhalb der Domäne.
- 22 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.  
Der Installationsfortschritt wird in einem Statusfenster angezeigt.
- 23 Klicken Sie auf **Fertigstellen**, wenn der Bildschirm „Installation abgeschlossen“ angezeigt wird.
- 24 Klicken Sie auf **Ja**, um neu zu starten.  
Die Installation von Data Guardian ist abgeschlossen.
- 25 Siehe [Data Guardian aktivieren](#).

## Data Guardian aktivieren

Nach der Installation von Data Guardian und dem Neustart des Computers führen Sie zur Aktivierung folgende Schritte durch:

- 1 Melden Sie sich bei Windows an.  
In der Taskleiste wird ein Cloud-Symbol mit einem orangefarbenen Ausrufezeichen angezeigt.
- 2 Wenn in der Taskleiste ein Dialogfeld angezeigt wird, klicken Sie auf **Zur Aktivierung hier klicken**.  
Wenn das Dialogfeld nicht angezeigt wird, klicken Sie auf das **Data Guardian**-Taskleistensymbol und wählen Sie **Benutzeraktivierung** aus.
- 3 Geben Sie Ihre E-Mail-Adresse und das Passwort ein, die bzw. das Sie für die Registrierung verwendet haben, und klicken Sie dann auf **Aktivieren**.

Nach Abschluss der Aktivierung wird ein grünes Häkchen auf dem Data Guardian-Taskleistensymbol  angezeigt

- 4 Bestätigen Sie Ihren Benutzermodusstatus. Klicken Sie auf die Registerkarte -Taskleistensymbol und wählen Sie **Details** aus.  
Oben lautet der Benutzermodus:

**Extern:** Ein Benutzer mit einer E-Mail-Adresse außerhalb der Domäne.

Wenn Sie bereits auf einem Synchronisierungs-Client installiert und angemeldet sind, wird das DDG VDisk Virtual Drive in Windows Explorer angezeigt.

## Zugriff von einem internen Benutzer anfordern

Bei Windows und Mobile kann ein externer Benutzer, der Data Guardian installiert und aktiviert hat, Zugriff auf eine Datei von einem internen Benutzer anfordern. Der externe Benutzer muss für jede Datei eine separate Anforderung stellen.

- 1 Wenn Sie eine geschützte Office-Datei öffnen und die Meldung angezeigt wird, dass Sie Zugriff anfordern müssen, klicken Sie auf **Ja** oder **Nein**.  
Ein Dialogfeld weist darauf hin, dass die Anforderung erfolgreich gesendet wurde. Der interne Benutzer kann den Zugriff genehmigen oder verweigern und der externe Benutzer erhält eine E-Mail mit dem Ergebnis. Wenn der externe Benutzer die geschützte Datei öffnet, bevor der interne Benutzer den Zugriff genehmigt, wird eine Meldung angezeigt, dass die Anforderung sich im Wartezustand befindet.
- 2 Nach 48 Stunden kann der externe Benutzer erneut Zugriff anfordern.  
In der Taskleiste kann der externe Benutzer mit der rechten Maustaste auf das Data Guardian-Symbol klicken und die Seite **Details** auswählen. Klicken Sie auf die Registerkarte **Sicherheit**. Wenn die Zeit für eine Anforderung wieder *Keine* beträgt, kann der externe Benutzer erneut Zugriff anfordern.



# Anzeigen eines geschützten Office-Dokuments

Wenn ein Unternehmen eine Richtlinie zum Schutz von Office-Dokumenten aktiviert und ein interner Benutzer eine geschützte Datei an einem externen Benutzer sendet, muss der externe Benutzer beim ersten Öffnen dieses Dokuments mit dem Dell Server verbunden sein. Anschließend kann er oder sie das Dokument für einen bestimmten Zeitraum, z. B. eine Woche, offline anzeigen. Der externe Benutzer muss dann eine Verbindung zum Server herstellen und das geschützte Dokument erneut öffnen.

Aus Sicherheitsgründen kann ein externer Benutzer folgende Aktionen nicht mit einem geschützten Office-Dokument durchführen.

- Drucken
- Exportieren
- Speichern unter
- Freigeben



# Synchronisierungs-Client oder Data Guardian deinstallieren

Wenn der Administrator Data Guardian installiert hat, kann nur der Administrator das Produkt deinstallieren. Ein externer Benutzer, der zur Freigabe eines Ordners eingeladen wurde und über Administratorrechte auf einem externen Computer verfügt, kann Data Guardian auf diesem externen Computer deinstallieren.

## Einen Cloud-Synchronisierungs-Client deinstallieren

Wenn Sie Ihren Cloud-Synchronisierungs-Client deinstallieren, aber immer noch über Data Guardian auf Ihrem Computer verfügen, können Sie Ihre Dateien auf dem DDG VDisk Virtual Drive nach wie vor in Klartext anzeigen.

Wenn Sie jedoch den gleichen Cloud-Synchronisierungs-Client erneut installieren, benötigen Sie einen neuen Schlüssel, um ihn auf dem DDG VDisk Virtual Drive zu öffnen und müssen Ihre Dateien von der Synchronisierungs-Client-Website herunterladen.

## Data Guardian deinstallieren

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

### Dateien auf das lokale Laufwerk kopieren

Wenn Sie Data Guardian von Ihrem Computer oder Gerät deinstallieren, müssen Dateien auf der Synchronisierungs-Client-Website immer noch geschützt sein. Daher bleiben sie verschlüsselt.

- 1 Bevor Sie mit der Deinstallation beginnen, überprüfen Sie, ob Sie Zugriff auf bestimmte Dateien benötigen.
- 2 Kopieren Sie diese Dateien aus dem DDG VDisk Virtual Drive auf Ihre lokale Festplatte.

Diese vom DDG VDisk Virtual Drive kopierten Dateien werden in Klartext angezeigt. Die Ordner und Dateien auf der Synchronisierungs-Client-Website werden verschlüsselt, auch wenn Sie sie herunterladen möchten. Um sie anzuzeigen, müssen Sie Data Guardian neu installieren.

### Data Guardian deinstallieren

- 1 Deinstallieren Sie das Programm über die Windows-Systemsteuerung.
- 2 Wählen Sie Dell Data Protection | Data Guardian und klicken Sie auf **Ändern** im oberen Menü.
- 3 Klicken Sie auf **Weiter**, wenn der Startbildschirm angezeigt wird.
- 4 Wählen Sie **Entfernen** und klicken Sie auf **Weiter**.
- 5 Eine Warnung wird angezeigt, um zu bestätigen, dass Sie Dell Data Protection | Data Guardian deinstallieren möchten. Falls ja, klicken Sie auf **Weiter**.
- 6 Klicken Sie auf dem Bildschirm „Programme entfernen“ auf **Entfernen**.  
Ein Statusfenster zeigt den Fortschritt an.
- 7 Falls Sie einen Fehlerdialog vom Synchronisierungs-Client erhalten, klicken Sie auf **Fortfahren**.
- 8 Klicken Sie auf **Fertigstellen**, wenn der Bildschirm „Abgeschlossen“ angezeigt wird.
- 9 Klicken Sie auf **Ja**, um neu zu starten.

Die Deinstallation von Dell Data Protection |Data Guardian ist nun abgeschlossen.







# Häufig gestellte Fragen

## Verschiedene häufig gestellte Fragen

### Frage

Ich habe den Sync-Ordner des Cloud-Providers in den Ordner „Programme“ verschoben. Nun kann ich keine Dateien mehr entschlüsseln, die aus der Cloud in meinen Synchronisierungsordner heruntergeladen werden.

### Antwort

Nach Design sind der Ordner „Programme“ oder andere ausgeschlossene Ordner ungeschützt, basierend auf der Richtlinie. Data Guardian entschlüsselt daher keine Dateien, die in diesen Ordner oder dessen Unterordner heruntergeladen wurden.

### Lösung

Heben Sie die Verknüpfung des Synchronisierungs-Clients auf oder deinstallieren Sie ihn und verschieben Sie den Synchronisierungsordner wieder an den ursprünglichen Ort oder an einen anderen verwalteten Speicherort.

### ANMERKUNG:

Eine Liste der verwalteten und nicht verwalteten Speicherorte erhalten Sie bei Ihrem Administrator.

### Frage

Ich habe einige archivierte .xen-Ordner auf meinen Desktop kopiert. Einige wurden entschlüsselt, andere jedoch nicht.

### Antwort

Während der Synchronisierung entschlüsselt Data Guardian direkt in den Synchronisierungsordner, oder die Entschlüsselung erfolgt beim Herunterladen über einen Webbrowser. Für Dateien, die von einem anderen Standort kopiert wurden, verwenden Sie Windows Explorer und verschieben die .xen-Datei in das virtuelle Laufwerk zur Entschlüsselung.

### Lösung

Verschieben Sie die .xen-Dateien in den Ordner des virtuellen Laufwerks, damit sie in die Cloud hochgeladen werden. Dadurch werden sie auf lokaler Ebene entschlüsselt.

### Frage

Ich habe meinen Computer umbenannt. Nun erhalte ich keine Richtlinienaktualisierungen mehr, und Dateien werden beim Hochladen in die Cloud nicht verschlüsselt.

### Antwort

Der Server erkennt derzeit nur den Endpunkt, bei dem die ursprüngliche Aktivierung vorgenommen wurde. Wenn Sie den Endpunktnamen ändern, erfasst der Server ihn nicht mehr als Empfänger der Richtlinie, und Data Guardian funktioniert nicht wie erwartet.

### Lösung

1 Halten Sie die Synchronisation von Dateien mit dem lokalen Computer an.





#### ANMERKUNG:

Wenn Sie die Synchronisation vor der Deinstallation nicht anhalten, sind wertvolle Daten in der Cloud möglicherweise ungeschützt oder werden möglicherweise gelöscht.

2 Deinstallieren Sie Data Guardian und installieren Sie es anschließend erneut. Sie brauchen zur Deinstallation Administratorrechte.

#### Frage

Ich kann auf gesperrten Windows-Geräten keine Dateien in die Cloud hochladen. Wenn ich die bereits geöffneten Fenster schließe, erhalte ich die Fehlermeldung „Zugriff verweigert“.

#### Antwort

Die Fehlermeldung stammt nicht von Data Guardian. Sie können lokal auf die Dateien zugreifen, erhalten aber keine zukünftigen Aktualisierungen der Dateien.

## Häufig gestellte Fragen zu Office-Dokumenten und geschütztem Modus

#### Frage

Ich habe versucht, ein Office-Dokument zu öffnen ( .docx, .pptx, .xlsx, .docm, .pptm, .xlsm), und es wurde ein Deckblatt angezeigt.

#### Antwort

Wenn der Administrator eine Richtlinie zum Schutz von Office-Dokumenten festgelegt hat, müssen entweder Sie oder Ihr Administrator Data Guardian installieren. Vergewissern Sie sich, dass das Data Guardian-Symbol in der Taskleiste mit einem grünen Häkchen versehen ist, was darauf hinweist, dass es aktiviert ist.

#### Lösung

Stellen Sie fest, ob Sie Data Guardian installieren oder aktivieren müssen. Siehe [Data Guardian installieren](#) oder [Mögliche Probleme mit der Aktivierung](#).

#### Frage

Ich kann ein geschütztes Office-Dokument (Word, PowerPoint oder Excel) nicht öffnen.

#### Antwort

Überprüfen Sie Folgendes:

- Einstellungen für den Zugriffsschutz: Wenn Ihr Administrator Richtlinien zum Schutz von Office-Dokumenten festlegt, verwenden Sie diese Einstellung nicht in **Datei > Optionen**.

#### Lösung

So überprüfen Sie die Einstellungen für den Zugriffsschutz:

- 1 In einem Office-Dokument wählen Sie **Datei > Optionen**.
- 2 Wählen Sie **Trust Center** aus der Liste aus.
- 3 Klicken Sie rechts auf **Einstellungen für das Trust Center**.
- 4 Wählen Sie **Einstellungen für den Zugriffsschutz** aus der Liste aus.
- 5 Stellen Sie bei *Word/Excel/PowerPoint 2007 und späteren Dokumenten* sicher, dass das Kontrollkästchen **Öffnen** nicht markiert ist.
- 6 Klicken Sie auf **OK**.

