Dell Data Guardian

Windows, Mac, Mobile und Web – Benutzerhandbuch
v2.7

Identifier	GUID-5B8DE7B7-879F-45A4-88E0-732155904029
Status	Translated

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.

Identifier	GUID-8935090F-D61D-41F4-ABC8-F4654D88B0FA
Status	Translation Validated

Windows, Mac, Mobile und Web – Benutzerhandbuch

2019 - 06

Rev. A01

Inhaltsverzeichnis

Identifier	**GUID-1E29C798-6A65-41FB-8102-6**
Status	**Translation Validated**

1

Einleitung

Im *Dell Data Guardian-Benutzerhandbuch* finden Sie die nötigen Informationen zur Installation und Verwendung von Data Guardian auf Windows, Mac, als Mobile-Version oder Webportal.

Identifier	**GUID-6EE59323-7410-43F4-AD47-C5B7B04044E8**
Status	**Translation Validated**

Übersicht

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

- 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, .pdf.
- Einfacher Dateischutz – Zusätzliche Anwendungen und Dateitypen, z. B. Notepad.
- 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.

ANMERKUNG:
Ihr Administrator wird Ihnen mitteilen, ob Ihr Unternehmen Data Guardian nur mit Office-Dokumenten, nur mit Cloud-Speicherung oder mit beidem nutzt. Ihr Administrator teilt Ihnen auch zusätzliche Anwendungen und Dateitypen mit, die geschützt werden können.

Sie können Data Guardian auf folgenden Plattformen einsetzen:

- Windows
- iOS
- Android
- Mac
- Data Guardian-Webportal, wenn von Ihrem Administrator eingerichtet.

ANMERKUNG:
Data Guardian kann Dateien öffnen, die von anderen Plattformen verschlüsselt wurden. Einige Dateien sind möglicherweise schreibgeschützt. Die meisten Benutzer Informationen über Data Guardian für Mac stehen innerhalb der Software als Online-Hilfedatei zur Verfügung.

Identifier	GUID-C9552E05-51A1-4C2D-AADE-C078B4639CD4
Status	In Translation

Verschlüsselungsoptionen für Data Guardian

Basierend auf dem von Ihrem Unternehmen hergestellten Maß an Sicherheit legt Ihr Administrator Richtlinien zum Schutz von Daten fest, die sich im Ruhezustand oder in Bewegung befinden. Ihr Administrator wird Ihnen mitteilen, welche Richtlinien für Ihr Unternehmen gelten.

Diese Liste enthält einen Überblick über einige Verschlüsselungsoptionen und für manche Plattformen den Speicherort der Richtlinieneinstellungen.

Modi und Office-Dokumente

Richtlinie kann so eingestellt werden, dass sie Office-Dokumente schützt. Verschlüsselungsverhalten kann von Plattform und Modus abhängen. Weitere Informationen für Mac finden Sie in der Onlinehilfe.

Modi	Office-Dokumente
Modusoptionen für **Windows und Mac**: **„Abonnieren"-Modus**: Sie haben einige Optionen zur Auswahl, um festzulegen, welche Office-Dokumente geschützt werden sollen. • **Windows** und **Mac** – Ein **Sichere Dokumente**-Ordner wird zum Stammverzeichnis Ihres Dokumentenordners hinzugefügt. Dies bietet eine weitere Möglichkeit zum Verschlüsseln einer Datei. „Erzwungener Schutz"-Modus – Ihr Unternehmen benötigt eine höhere Sicherheitsstufe. Data Guardian räumt auf, um Dateien zu verschlüsseln. • **Windows** und **Mac** – Eine andere Richtlinie kann einen **Ungeschützte Dokumente**-Ordner zum Stammverzeichnis Ihres Dokumentenordners hinzufügen. Sie können geschützte Office-Dokumente oder einfache Dateischutztypen in diesem Ordner ablegen, um Sie zu entschlüsseln. • **Mac** – Schützt Dateien in **/Users**. Dieser Plattformen basieren nicht auf Modi: • Handy • Webportal	**Office-Dokumente, die unter Windows, Mac, auf Mobilgeräten und im Webportal verwendet werden** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf – Wenn mit Data Guardian geschützt, mit Adobe Acrobat Reader DC oder Microsoft Word öffnen, jedoch nicht vom Netzwerk aus.

Office-Dokumente – Windows

Ihr Administrator kann zusätzliche Data Guardian-Richtlinien festlegen, um einen Datenverlust durch diese Optionen zu kontrollieren oder zu verhindern. Verschlüsselungsverhalten kann sich je nach Modus unterscheiden.

Optionen für geschützte Office-Dokumente in Windows	Beschreibung
• Speichern – Wenn ein Office-Dokument geschützt ist, können Sie neue Inhalte speichern. (**Speichern unter** wird grau unterlegt angezeigt.) • Geschütztes „Speichern unter“ • Wenn ein Office-Dokument bereits geschützt ist, **Speichern unter** wird grau unterlegt angezeigt.	Andere Informationen für Windows: • **Ungeschütztes** Office-Dokument – Sie können **Speichern**, **Speichern unter** oder **Geschützt speichern unter** auswählen. • Ein roter Rahmen wird bei geschützten Office-Dokumenten und geschützten E-Mails angezeigt.
Kopieren/Einfügen und Zwischenablage	Sie können Inhalte von einem geschütztes Office-Dokument kopieren und in ein anderes geschütztes Office-Dokument einfügen. Sie können Daten nicht von einem geschützten Dokument kopieren und in ein ungeschütztes Dokument einfügen.
Drucken	Je nach Richtlinie kann ein geschütztes Office-Dokument gedruckt werden, über ein Wasserzeichen verfügen oder nicht gedruckt werden.
Exportieren (Windows und Office 2013 und höher, Mobilgeräte)	Sind je nach Richtlinie möglicherweise zulässig, haben ein Wasserzeichen oder sind deaktiviert. **ANMERKUNG:** Wenn ein Wasserzeichen eingestellt ist, können Office-Dokumente exportiert werden. PDF-Dateien können nicht exportiert werden.
Bildschirm drucken	Je nach Richtlinie zulässig oder blockiert.
Prozesse blockiert Beispiel: Snipping Tool	Basierend auf den von Ihrem Unternehmen festgelegten Richtlinien werden einige Prozesse blockiert, wenn ein geschütztes Office-Dokument geöffnet ist.
Wasserzeichen auf dem Bildschirm	Wenn ein geschütztes Office-Dokument geöffnet wird, zeigt der Bildschirm ein Wasserzeichen mit dem Computernamen und den Benutzernamen an.
TITUS-Klassifizierung (Windows mit „Abonnieren"-Modus)	Falls eine Richtlinie aktiviert ist, können Sie mit der rechten Maustaste auf ein Office-Dokument klicken und eine TITUS-Klassifizierung auswählen. Dies stellt für Benutzer eine andere Möglichkeit zum Schutz eines Office-Dokuments dar.
Datenklassifizierung (Windows mit „Abonnieren"-Modus)	Wenn eine Richtlinie aktiviert und konfiguriert wurde, um vertrauliche Informationen zu schützen, wie beispielsweise Sozialversicherungs- oder Kreditkartennummern, werden Office-Dokumente mit diesen Daten verschlüsselt.

Office-Dokumente – Mac, Mobilgeräte und Webportal

Verschlüsselungsverhalten kann von Plattform und Modus abhängen. Ihr Administrator wird Ihnen mitteilen, welche Richtlinien für Ihr Unternehmen gelten.

Verschlüsselungsoption	Beschreibung
Mac – Dell Data Guardian-Schnittstelle	**Mac**: Ein geschütztes Dokument zum Verschlüsseln hochladen. Ein geschütztes Dokument zum Entschlüsseln hochladen.

Verschlüsselungsoption	Beschreibung
	Nach dem Bearbeiten eines geschützten Dokuments werden die Änderungen zusammen mit der Originaldatei, entweder in der Cloud oder lokal, gespeichert.
Mobile: innerhalb der Data Guardian-App • Drucken • Wasserzeichen auf dem Bildschirm • Ausgeblendete Wasserzeichen • Exportieren	**Mobilgeräte**: Basierend auf Richtlinien: • Office-Dokumente innerhalb der Data Guardian-App sind geschützt. • Das Drucken eines geschützten Office-Dokuments ist möglicherweise zulässig, hat ein Wasserzeichen oder ist deaktiviert. • Wenn ein geschütztes Office-Dokument geöffnet wird, zeigt der Bildschirm ein Wasserzeichen mit dem Computernamen und den Benutzernamen an.
Webportal • Wasserzeichen auf dem Bildschirm	**Webportal**: Sie können geschützte oder ungeschützte Dokumente hochladen, aber jede hochgeladene Datei wird geschützt, wenn Sie auf „Herunterladen“ klicken. Wenn ein geschütztes Office-Dokument geöffnet wird, zeigt der Bildschirm ein Wasserzeichen mit dem Computernamen und den Benutzernamen an.

Zusätzliche Optionen

Verschlüsselungsverhalten kann von Plattform und Modus abhängen. Ihr Administrator wird Ihnen mitteilen, welche Richtlinien für Ihr Unternehmen gelten.

Option	Beschreibung (Modi „Abonnieren“ und „Erzwungener Schutz“)
Einfacher Dateischutz – Ermöglicht den Schutz zusätzlicher Anwendungen und Dateitypen. (Windows, Mac, Mobilgeräte und Webportal) • Beispiele: .txt oder .png **ANMERKUNG:** Derzeit wird bei diesen Dateitypen kein roter Rahmen angezeigt, selbst wenn sie geschützt sind.	Ihr Administrator kann eine Richtlinie konfigurieren, um zu verschlüsselnde Anwendungen und Dateitypen festzulegen. **Windows, Mac und Mobilgeräte**: Diese Dateien werden durchsucht und verschlüsselt. • **Mac** – für Dateierweiterungen, die vom Administrator festgelegt werden, verschlüsselt diese Dateitypen im Ordner *„/Users“*. **Webportal**: Ebenfalls basierend auf Richtlinien sind diese Dateien möglicherweise schreibgeschützt oder können nur von Benutzern bearbeitet werden.
Geben Sie geschützte Office-Dokumente für **externe Benutzer** frei. (Windows, Mac, Mobilgeräte und Webportal) Auf einer Titelseite sind Links zur Registrierung und Informationen zur Installation von Data Guardian aufgeführt.	• Externe Benutzer und **Windows**: Sie können auch eine **Datumseinschränkung (Embargo)** für geschützte Office-Dokumente und pdf.-Dateien hinzufügen. • **Webportal** – Sie können freigegebene Dateien in das Webportal hochladen. Sie können eine Datei nicht aus dem Webportal freigeben, aber Sie können sie nach dem Herunterladen freigeben.
Manipulierte Datei oder manipuliertes Deckblatt (Windows, Mac, Mobilgeräte und Web)	Bei Office-Dateien kann Data Guardian geschützte Office-Dokumente scannen, um einige Formen der Manipulation zu erkennen.
Zugriffsgruppen (intern) (Windows, Mac, Mobilgeräte und Webportal)	Sofern von Ihrem Administrator aktiviert, können nur Personen in Ihrer Zugriffsgruppe Ihre verschlüsselten Dateien anzeigen. Sie können internen und externen Benutzern Zugriff auf einzelne Dateien gewähren und sie können den Zugriff anfordern.

Option	Beschreibung (Modi „Abonnieren“ und „Erzwungener Schutz“)
	Basierend auf einer zusätzlichen Richtlinie können Sie mit der rechten Maustaste auf eine Outlook-E-Mail mit der Bezeichnung [GESCHÜTZT] klicken und den Zugriff für einzelne Benutzer entfernen.
Geofencing (Mobilgeräte)	Nur Benutzer in einer bestimmten Gegend können Dateien über ihr Mobiltelefon öffnen.
E-Mail-Verschlüsselung über Outlook (Windows)	Basierend auf einer Richtlinie ermöglicht Ihnen eine *Schutz*taste den Inhalt einer E-Mail oder eines Anhangs zu Verschlüsseln. Beim Senden an externe Benutzer werden auf einer Titelseite Links zur Registrierung und Informationen zur Installation von Data Guardian aufgeführt.

Hosted oder On-prem

Wenn Sie Data Guardian selbst installieren müssen, wird Ihr Administrator bestätigen, welche Option für Ihr Unternehmen gilt.

ANMERKUNG:

Bei mobilen Anwendungen: Wenn Workspace ONE installiert ist, können Sie sich mit einmaliger Anmeldung bei Data Guardian authentifizieren.

Hosted Dell Security Center	On-prem Dell Management Server
Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software. Wenn Ihr Unternehmen über mehrere Mandanten verfügt, stellt Ihr Administrator eine Installations-ID bereit. Wenn eine Titelseite für einen Benutzer angezeigt wird, der noch keinen Zugriff auf ein geschütztes Dokument hat, finden Sie auf der Titelseite Informationen zur Installations-ID. Alle Plattformen: Wenn ein Mandant eine bestimmte Zeit lang nicht bezahlt, kann dieser Mandant angehalten werden.	Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software. Ihr Administrator gibt den Namen der Dell Server-URL an.

Cloud-Verschlüsselung

Verschlüsselungsverhalten kann von Plattform und Modus abhängen. Ihr Administrator wird Ihnen mitteilen, welche Richtlinien für Ihr Unternehmen gelten.

Plattformen	Beschreibung
Handy	Siehe Verwenden von Cloud-Schutz mit Mobilgeräten.
Mac	Weitere Informationen finden Sie in der Online-Hilfe.
Webportal	Weitere Informationen finden Sie in der Online-Hilfe.
Windows	Der Cloud-Verschlüsselungsschutz von Data Guardian ist auf Windows-Geräten derzeit deaktiviert, um Kompatibilitätsprobleme mit neueren Funktionen von Cloud-Dienstanbietern zu vermeiden. Verwenden Sie die mobile App oder das Webportal von Data Guardian oder die Data Guardian Mac-Anwendung, um .xen-Dateien anzuzeigen, die bereits durch Cloud-Verschlüsselung geschützt sind.

Richtlinieneinstellungen

Einige Plattformen erhalten eine unvollständige Liste der Richtlinieneinstellungen für Ihr Gerät.

Plattform	Speicherort der Richtlinieneinstellungen
Mac	*Einstellungen* Fensterbereich
Handy	**Einstellungen**-Symbol > **Über**
Webportal	**Einstellungen**-Symbol > **Über**

Identifier	**GUID-DEFFD392-F513-445E-A87C-2CE7250245A2**
Status	**Translation Validated**

Zusätzlicher Support

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

Identifier	**GUID-1DE0401E-4073-46BA-95E3-**
Status	**Translation Validated**

Anforderungen

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

Identifier	**GUID-7C606C28-5532-4F36-AFA3-03126F14A6EF**
Status	**Translation Validated**

Dell Server

Data Guardian for Windows, Mac und Mobile erfordert Security Management Server oder Security Management Server Virtual v9.6 oder höher. Der Data Guardian-Web-Client erfordert Security Management Server oder Security Management Server Virtual v9.8 oder höher. Zum Zwecke dieses Dokuments werden beide Server als Dell Server bezeichnet, sofern keine konkrete Version angegeben ist (wenn z. B. bei Verwendung des Security Management Server Virtual ein anderes Verfahren notwendig ist).

Identifier	**GUID-198D0A89-3C37-4C12-87A4-1F801B60DB21**
Status	**In Translation**

Data Guardian für Windows

- Bei der Implementierung sind die bewährten IT-Verfahren zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.
- Die Installation/Aktualisierung/Deinstallation kann nur von einem lokalen Benutzer oder einem Domänenadministrator durchgeführt werden, der über ein Implementierungstool wie Microsoft SMS oder KACE vorübergehend zugewiesen werden kann. Benutzer ohne Administratorstatus, aber mit höheren Rechten, werden nicht unterstützt.
- Sichern Sie vor der Installation/Deinstallation alle wichtigen Daten.
- Nehmen Sie während der Installation oder Deinstallation keine Änderungen am Computer vor, dazu gehört auch das Einsetzen oder Entfernen von externen (USB-)Laufwerken.
- Data Guardian wird mit den spezifischen Versionen Microsoft Office 2016 sowie Microsoft Office 365 Business und Business Premium unterstützt. Es wird nicht mit Office 365 Business Essentials unterstützt.
- Data Guardian für Windows ist mit Workspace ONE kompatibel. Das Data Guardian-Installationsprogramm für Workspace ONE und eine MSI-Installation haben die Erweiterung .msi.
- Data Guardian v2.4 und höher wird auf Windows-Geräten in Air-Gap-Umgebungen unterstützt, jedoch mit einigen Einschränkungen. Derzeit werden Geolocation-Daten in Audit-Ereignissen und Embargo-Dateien nicht unterstützt. Webbeacon erfordert einige Konfigurationen.
- 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 Benutzer 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, den Abschnitt „Dropbox-Support“ unter https://www.dropbox.com/help oder den Abschnitt „OneDrive-Support“ unter http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

- Geschützte Office-Dokumente werden mit Mozy, einer Begleitlösung zu Data Guardian, unterstützt, sowie mit anderen Cloud-, E-Mail- und NFS-Speicher-Produkten.
- Obwohl Dell Encryption nicht erforderlich ist, sollte, sofern verwendet, der Verschlüsselungs-Client Ver. 8.12 oder höher sein.
- Data Guardian unterstützt weder das Windows Systemwiederherstellungstool noch die Windows Insider Preview.
- Die Ordnerumleitung von Microsoft wird von Data Guardian nicht unterstützt.
- Überprüfen Sie regelmäßig die Website dell.com/support, um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.

Voraussetzungen

.exe-Voraussetzungen

Falls noch nicht geschehen, installiert das Installationsprogramm Microsoft Visual C++ 2017 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.

.msi-Voraussetzungen

Sie müssen das Microsoft Visual Studio C++ 2017 Redistributable Package (x86 und x64) installieren.

ANMERKUNG:
Wenn Sie MSI ausführen, müssen Sie außerdem Visual Studio 2010 Tools für Office Runtime (x86 und x64) installieren.

Allgemeine Voraussetzungen

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 Data Guardian installieren, um Fehler bei der Installation/Aktualisierung zu vermeiden. Um die installierte Version von .Net zu überprüfen, folgen Sie auf dem Computer, auf dem die Installation vollzogen werden soll, den folgenden Anweisungen: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx.. Zur Installation von Microsoft .Net Framework 4.5.2 gehen Sie zu https://www.microsoft.com/en-us/download/details.aspx?id=42643.

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

Betriebssysteme

In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1703 (Creators Update/Redstone 2) bis Version 1809 (Oktober 2018 Update/ Redstone 5)

ANMERKUNG:

Der Client muss auf einem dieser Betriebssysteme installiert sein. Andernfalls wird er blockiert. Falls erforderlich, kann der Administrator durch eine Einstellung in einem Registrierungsschlüssel die Blockierung überschreiben.

Für die Unterstützung von Redstone 4 müssen Sie den Agenten aktualisieren, bevor Sie ein Upgrade des Betriebssystems durchführen. Siehe https://www.dell.com/support/article/us/en/04/sln307922.

ANMERKUNG:

Data Guardian ist nicht kompatibel mit Windows Defender Exploit Guard (WDEG) von Microsoft in Redstone 3 und höher oder mit Enhanced Mitigation Experience Toolkit (EMET) in Redstone 2 und niedriger.

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

Data Guardian bietet keine Unterstützung für mehrere Versionen von Office auf einem Computer.

Microsoft Office

Data Guardian unterstützt die folgenden Versionen von Office. Es darf jedoch nur eine Version von Office gleichzeitig installiert sein.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus: Versionen 1705, 1708 und 1803 (halbjährlicher Kanal)

Identifier	**GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4**
Status	**In Translation**

Data Guardian für Mac

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

Mac-Hardware

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

Mac-Hardware

- 10 GB freier Speicherplatz

Betriebssysteme

Nachfolgend sind die unterstützten Betriebssysteme aufgeführt.

Mac-Betriebssysteme

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.6
- macOS Mojave 10.14.4 - 10.14.5

Cloud-Speicheranbieter

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

Cloud-Speicheranbieter

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

  ANMERKUNG:
  Google Backup & Sync wird nicht unterstützt.

- OneDrive
- OneDrive für Unternehmen

Microsoft Office

Data Guardian für Mac unterstützt die folgenden Office-Versionen.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-70934847-A1D7-4AD3-8822-A1E474D4ECD6
Status	In Translation

Data Guardian für Mobile Application

Die nachfolgend aufgeführten Betriebssysteme unterstützen Data Guardian für Mobilgeräte.

Android-Betriebssysteme

- 5.0–5.1.1 Lollipop
- 6.0–6.0.1 Marshmallow
- 7.0–7.1.2 Nougat
- 8.0–8.1 Oreo
- 9.0 Pie

iOS-Betriebssysteme

- iOS 10.x–10.3
- iOS 11.x–11.4.1
- iOS 12.x–12.1.4

Chromebook-Betriebssystem

Das Betriebssystem Chrome ist in der Version M53 oder höher ist für die Ausführung von Android-Anwendungen auf Chrome erforderlich. Diese Geräte werden für die Ausführung von Android-Apps auf dem Betriebssystem Chrome validiert; bestätigen Sie allerdings Ihre Option über Ihren Vertriebsmitarbeiter:

- https://www.chromium.org/Chromium-OS/Chrome-OS-Systems-Supporting-Android-Apps

Microsoft Office

Data Guardian für Mobile Application kann Dateien öffnen, die mit den folgenden Office-Versionen erstellt wurden.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-E0E57A65-225C-46FB-9E51-60FAC92BA57A
Status	In Translation

Data Guardian für Web

Um den Data Guardian-Web-Client zu aktivieren, richtet der Administrator eine virtuelle Maschine ein, die als Host für den Web-Client dient und mit dem Dell Server v9.8 oder höher kommuniziert.

Die folgenden virtualisierten Umgebungen können zur Bereitstellung des Data Guardian-Web-Clients verwendet werden.

Virtuelle Umgebungen

- **VMware ESXi 6.7**
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-67/index.jsp

- **VMware ESXi 5.5**
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-55/index.jsp

- **Microsoft Hyper-V**
  - 64-Bit-Prozessor mit Second Level Address Translation (SLAT)
  - Mindestens 8 GB RAM empfohlen
  - Die Hardware muss die Mindestanforderungen für Hyper-V erfüllen
  - Weitere Informationen siehe https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements.

ANMERKUNG:
Diese Mindestanforderungen entsprechen fünfundzwanzig oder weniger gleichzeitigen Verbindungen zu einem einzelnen Webportal.

Cloud-Speicheranbieter

Basierend auf den Richtlinieneinstellungen kann das Data Guardian-Webportal auf diese Cloud-Speicheranbieter zugreifen.

Cloud-Speicheranbieter
• OneDrive für Unternehmen

Microsoft Office

Data Guardian für Web kann Dateien öffnen, die mit den folgenden Office-Versionen erstellt wurden.

Microsoft Office
• Office 2013 SP1
• Office 2016
• Office 2019

Identifier	**GUID-F414365D-DE5B-4703-88AB-FCB73F3BD14D**
Status	**Translation Validated**

Weitere Anforderungen

Derzeit wird die Multi-Faktor-Authentifizierung (MFA) von Amazon Cognito nicht von Data Guardian-Plattformen nicht unterstützt.

Identifier	**GUID-E2815EA1-85AF-4049-B317-DF016FBA39EE**
Status	**Translation Validated**

Webbrowser

Sie können Data Guardian mit Internet Explorer, Mozilla Firefox oder Google Chrome und Microsoft Edge verwenden.

Bei einem Mac wird auch Safari unterstützt.

Identifier	**GUID-582A5665-D2A2-4B98-A51D-5F14376D98BA**
Status	**Translation Validated**

Adobe Acrobat

Für Windows und Mac lassen sich geschützte pdf-Dateien mit Adobe Acrobat Reader und 72 öffnen

ANMERKUNG:
Nicht unterstützt werden: Adobe Acrobat *Standard* DC, Adobe Acrobat *Pro* DC und Adobe Acrobat DC.

Identifier	GUID-36045ECC-D303-4A63-9ABA
Status	In Translation

Data Guardian auf Windows installieren oder deinstallieren

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

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

Identifier	GUID-D0717325-F700-400C-BC03-5FD8190A81A9
Status	In Translation

Überblick über die Installationsaufgaben für Windows

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

Data Guardian installieren

Aufgabe	Beschreibung	Weitere Informationen
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 Data Guardian interaktiv auf Windows installieren. Starten Sie das System neu, und fahren Sie mit dem nächsten Schritt fort.
Aktivierungsstatus überprüfen	Bestätigen Sie im Benachrichtigungsbereich, dass das Data Guardian-Symbol mit einem grünen Häkchen  versehen ist.	Wenn das Symbol mit einem orangefarbenen Ausrufezeichen versehen ist, siehe Mögliche Probleme mit der Aktivierung: Cloud und geschützte Office-Dokumente. **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.

Optionen für Windows

Aufgabe	Beschreibung	Weitere Informationen
Benachrichtigungsbereich-Menü anzeigen	Bietet hilfreiche Informationen zu Dateien, Ordnern und Fehlerbehebung.	Erklärung der Menüelemente des Benachrichtigungsbereichs von Data Guardian

Identifier	GUID-B54EDFCA-AFBB-4BD0-8427-515A3E052962
Status	In Translation

Zuvor vorhandene Ordner mit nicht verschlüsselten Dateien

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

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

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

Identifier	GUID-7BBFA9B6-C19E-44E8-908C-F5AF181462C8
Status	In Translation

Data Guardian interaktiv auf Windows installieren

Sie müssen ein lokaler Administrator sein, um Data Guardian zu installieren. Wenn Benutzer das Produkt installieren, dann geben Sie ihnen den Speicherort des Installationsmediums bekannt.

Vorbereitung

Bestimmen Sie abhängig von Ihrer Umgebung und dem Data Guardian-Produkt, welche der Folgenden Sie benötigen:

Hosted Dell Security Center	On-prem Dell Management Server
Wenn Ihre gehostete Umgebung über mehrere Mandanten verfügt, benötigen Sie eine Installations-ID.	Stellen Sie sicher, dass Sie den Namen des Dell Server wissen.

Data Guardian installieren

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 und kopieren es auf den lokalen Computer. Hier sind Beispiele für Installationsprogrammnamen:
   - Hosted Dell Security Center: Die Namen des Installationsprogramms haben die Dateierweiterung .exe.
   - On-prem: Die Namen des Installationsprogramms haben die:
     - Dateierweiterung .exe
     - Dateierweiterung .msi für Workspace ONE und eine Installation per MSI-Datei
3. Starten Sie das Installationsprogramm per Doppelklick.
4. Falls Sie eine Sicherheitswarnung erhalten, klicken Sie auf **Ausführen**.
5. Wählen Sie eine Sprache aus und klicken Sie auf **OK**.
6. Klicken Sie auf **OK**, wenn Sie zur Installation von Microsoft Visual C++ 2015 Redistributable Package oder Microsoft .NET Framework 4.5.2 Client Profile aufgefordert werden.
7. Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.

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

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

Installieren Sie Data Guardian niemals in den Ordnern C:\Users oder C:\Windows oder im Stammverzeichnis eines Laufwerks.

10 Wählen Sie eine dieser Optionen aus:

Hosted Dell Security Center	On-prem Dell Management Server
Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software.	Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software.
a Wählen Sie **Hosted Dell Security Center** aus. b Optional, wenn das Unternehmen über mehrere Mandanten verfügt, geben Sie eine Installations-ID ein. **ANMERKUNG:** Wenn Ihr Unternehmen über mehrere Mandanten verfügt und Sie keine Installations-ID eingeben, kann der Administrator sie später zur Registrierung hinzufügen. c Klicken Sie auf **Weiter**. d Fahren Sie mit Schritt 11 fort.	a Wählen Sie **On-prem Dell Management Server**. b Geben Sie im Feld `Dell Management Servername` den Namen des Dell Server 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. **ANMERKUNG:** Deaktivieren Sie das Kontrollkästchen *SSL-Trust-Prüfung aktivieren* nicht, es sei denn, Ihr Administrator fordert Sie dazu auf. c Klicken Sie auf **Weiter**. d Bestätigen Sie auf dem Bildschirm „Dell Management Serverdaten“, dass die Dell Server-URL-Adresse korrekt ist. Das Installationsprogramm fügt www oder http(s) und den Port hinzu. Klicken Sie auf **Weiter**. e Fahren Sie mit Schritt 11 fort.

11 Wählen Sie im Fenster „Verwaltungstyp“ diese Option aus:

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

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

Der Installationsfortschritt wird in einem Statusfenster angezeigt.

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

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

Die Installation von Data Guardian ist abgeschlossen.

15 Benutzer müssen die Aktivierung bestätigen. Das Data Guardian-Benachrichtigungsbereich-Symbol sollte ein grünes Häkchen anzeigen.

ANMERKUNG:

Abhängig davon, wie Data Guardian innerhalb des Unternehmens bereitgestellt wird, erfolgt die Aktivierung möglicherweise nicht sofort. Wenn die Aktivierung jedoch nicht erfolgt, muss der Benutzer manuell aktivieren.

Identifier	**GUID-AF4BEC71-F3FB-43E9-A588-FA2C2BC7E4BD**
Status	**Translation Validated**

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

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

Data Guardian-Option	Mögliches Problem
Geschütztes Office	• 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.
Cloud-Verschlüsselung	• 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.

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.

Identifier	**GUID-10DDD78A-61B2-4AE9-9DF4-0527FEE42D0D**
Status	**In Translation**

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.

Im Benachrichtigungsbereich wird ein Shield-Symbol mit einem orangefarbenen Ausrufezeichen angezeigt.

2 Klicken Sie auf das **Data Guardian**-Symbol im Benachrichtigungsbereich 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 im Data Guardian-Benachrichtigungsbereich angezeigt  .

4 Bestätigen Sie Ihren Benutzermodusstatus. Klicken Sie auf das Benachrichtigungsbereich-Symbol 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 Verwenden von Data Guardian als externen Benutzer.

> **ANMERKUNG:**
> Wenn der Benutzermodus **Aufgehobene Registrierung** auflistet, ist Data Guardian noch nicht aktiviert.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Hosted Dell Security Center und angehaltene Mandanten

Wenn bei einem Hosted Dell Security Center ein Mandant für einen bestimmten Zeitraum keine Zahlungen leistet, kann dieser Mandant angehalten werden. Dies gilt für Windows, Mac, Mobile und das Webportal.

Interne und externe Benutzer von Data Guardian können Folgendes erfahren:

- Alle Plattformen: Wenn Sie versuchen, Data Guardian zu installieren, zu aktivieren oder sich anzumelden, wird ein Dialogfeld mit der Meldung angezeigt, dass der Mandant angehalten wurde.
- Mac: Wenn Ihr Mandant angehalten wurde, während Data Guardian geöffnet ist, wird das Dialogfeld "Angehaltener Mandant" angezeigt, nachdem Sie den Explorer und alle Dateien geschlossen haben und dann versuchen, eine geschützte Datei zu öffnen.
- Webportal:
  - Wenn Sie bereits angemeldet sind und eine verschlüsselte Datei hochladen, wird eine Meldung angezeigt, dass der Upload fehlgeschlagen ist.
  - Wenn eine verschlüsselte oder unverschlüsselte Datei hochgeladen wurde und der Mandant angehalten wurde, wird die Meldung "Download fehlgeschlagen" angezeigt.
  - Wenn Sie sich abmelden und versuchen, sich erneut anzumelden, wird in einem Dialogfeld angezeigt, dass der Mandant angehalten wurde.

Wenden Sie sich an Ihren Administrator.

Identifier	**GUID-43BA606D-3F31-4E67-97B4-039DE9CEBC65**
Status	**In Translation**

Erklärung der Data Guardian-Menüelemente des Benachrichtigungsbereich

Details-Bildschirm

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

- Für technischen Support können Sie Status- oder Versionsinformationen bereitstellen.
- 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 Ordner ist, wählen Sie Ordner und rollen zur Spalte ORDNEREIGENTÜMER.

So greifen Sie auf den Details-Bildschirm zu:

Klicken Sie mit der rechten Maustaste auf den Data Guardian-Benachrichtigungsbereich 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
- **Aufgehobene Registrierung** – ein interner oder externer Benutzer, dessen Data Guardian nicht aktiviert wurde.

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: Der Dell 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 Dell Server erzeugte Richtlinienversion.

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

Name: Name der Datei

Cloud: Diese Funktion wurde deaktiviert, sodass keine Daten mehr verfügbar sind.

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 lesen: Diese Funktion wurde deaktiviert.

Browser erstellt: *Wahr* oder *Falsch*.

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

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

Zuvor verfügte die Cloud-Verschlüsselung von Data Guardian über einen **Ordner**-Bereich auf dem Details-Bildschirm. Die Cloud-Verschlüsselung ist derzeit deaktiviert.

Identifier	**GUID-5726752F-D15C-479E-8E8E-6BBE27B23F90**
Status	**Translation Validated**

Richtlinien auf Aktualisierungen überprüfen

Falls Ihr Administrator eine Richtlinie ändert und Sie über eine Richtlinienaktualisierung unterrichtet, gehen Sie zum Windows-Benachrichtigungsbereich, klicken Sie auf das Symbol **Dell 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.

Identifier	**GUID-62C18A73-A619-46BF-BE3A-76911412C43A**
Status	**Translation Validated**

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.

Identifier	**GUID-E67381E8-70C7-46BE-A822-9B5C48B0FFC3**
Status	**Translation Validated**

Data Guardian aufrüsten

Als bewährtes Verfahren gilt die Deinstallation der früheren Version mit anschließender Installation der aktuellen Version. Siehe Data Guardian deinstallieren.

Identifier	**GUID-CC8C1B76-3E85-415F-AAE0-3C20521D70A6**
Status	**In Translation**

Data Guardian auf Windows deinstallieren

Wenn der Administrator Data Guardian installiert hat, darf nur Ihr 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.

Identifier	**GUID-FB8AEF07-F76C-4E52-9920-B56A973DB1E6**
Status	**In Translation**

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 in das lokale Laufwerk.

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. Sie können sie alternativ im Data Guardian-Webportal anzeigen.

Data Guardian deinstallieren

1 Deinstallieren Sie das Programm über die Windows-Systemsteuerung.
2 Wählen Sie **Dell** 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 die Deinstallation von Data Guardian zu bestätigen. 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 Wenn in einem Dialogfeld der Hinweis erscheint, dass ein Office-Dokument geöffnet ist, dann klicken Sie auf **OK**, schließen das Office-Dokument und beginnen die Deinstallation erneut.
9 Klicken Sie auf **Fertigstellen**, wenn der Bildschirm „Abgeschlossen“ angezeigt wird.
10 Klicken Sie auf **Ja**, um neu zu starten.

Die Deinstallation von Data Guardian ist abgeschlossen.

Identifier	**GUID-05F5667F-C3BE-4C5E-B64D-5629C60C049D**
Status	**Translation Validated**

Dell Feedback geben

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

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

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

Identifier	GUID-E68E0B8D-7519-4C11-A918-
Status	In Translation

Verwenden von Data Guardian mit Windows

Ihr Administrator hat bereits Richtlinien zum Schutz von Dokumenten konfiguriert und wird Ihnen mitteilen, welche dieser Optionen für Ihr Unternehmen gelten.

Identifier	GUID-162A20CF-D1AD-4701-9A28-1000DB2FE1D4
Status	In Translation

Übersicht über Optionen

Diese Übersicht fasst möglichen Optionen für Data Guardian basierend auf den Richtlinien zusammen, die von Ihrem Administrator festgelegt wurden. Diese Dateien sind sicher, wenn Sie sie für andere freigeben oder auf Wechselmedien speichern.

Option	Beschreibung	Weitere Informationen
Office und Dokumente mit Makros	Dazu gehören: .docx, .pptx, .xlsx, .pdf, .docm, .pptm, .xlsm und .pdf.	Siehe Datei-Menüoptionen befolgen, um die Sicherheitsebene für Office-Dokumente zu bestimmen. Sie verfügen über einen dieser Modi: • Abonnieren • Erzwungener Schutz
Einfacher Dateischutz	Hierbei handelt es sich um zusätzlichen Anwendungen und Dateitypen, die Ihr Unternehmen verschlüsseln möchte und Ihr Administrator konfiguriert hat.	Siehe Schützen weiterer Anwendungen und Dateitypen mit einfachem Dateischutz.
Zusätzliche Optionen	Dies kann für Office-Dokumente, einfache Dateien oder beides gelten.	Siehe Weitere Optionen für Data Guardian.
Eine Datei für einen externen Benutzer freigeben	Benutzer, der eine E-Mail-Adresse außerhalb der Domäne hat (entweder jemand aus einem anderen Unternehmen oder ein interner Benutzer, der von einer E-Mail-Adresse außerhalb der Domäne auf geschützte Dateien zugreifen möchte).	Siehe Verwenden von Data Guardian als externen Benutzer.

Online mit geschützten Dokumenten arbeiten

Beim Erstellen von geschützten 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 Dokumente offline erstellt haben, teilen Sie dies unbedingt Ihrem Administrator mit.

Registerkarte Dateieigenschaften > Dell Data Guardian

Bei geschützte Office-Dokumente können Sie mit der rechten Maustaste klicken und **Eigenschaften** auswählen. Die Registerkarte **Dell Data Guardian** wird mit Informationen angezeigt, z. B. mit der Schlüssel-ID der Datei und Zugriffs- und Embargodaten.

Overlaysymbole für Windows

Bei Data Guardian 2.2 und höher werden Overlaysymbole für geschützte Dateien im Datei-Explorer angezeigt. Wenn Sie mit der rechten Maustaste auf diese geschützte Datei klicken, enthält eine Registerkarte von Dell Data Guardian weitere Informationen.

Ausgeblendete Wasserzeichen

Basierend auf den von Ihrem Administrator festgelegten Richtlinien sind geschützte Office-Dokumente möglicherweise mit einem verborgenen Wasserzeichen versehen, das den Benutzer identifiziert. Wenn Sie das Dokument drucken oder freigeben, bleibt das Wasserzeichen erhalten.

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.

Identifier	**GUID-E88C0771-29BE-4292-AD26-F913747EE0FC**
Status	**Translation Validated**

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
- .pdf

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 haben ein geschütztes Office-Dokument in der Cloud geöffnet.
- 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.

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* 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* 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.
  - **Dokumente > Ungeschützt**-Ordner – Wenn von Richtlinie im „Erzwungener Schutz“-Modus (aber nicht im „Abonnieren“-Modus) geöffnet, wird zum Stammverzeichnis des Dokumentenordners ein „Ungeschützt“-Ordner hinzugefügt. Office-Dokumente in diesem Ordner sind verschlüsselt. Wenn Sie den Ordner löschen, wird er neu erstellt.

- Wenn Sie **Geschützt Speichern unter** auswählen, 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.

Identifier	GUID-077EC2B6-61AD-4F13-95D0-CF91EF0143AF
Status	In Translation

Abonnierten Modus zum Schutz von Office-Dokumenten verwenden

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

- Arbeiten mit Datei-Menüoptionen für „Abonnieren“-Modus
- Weitere Optionen für Data Guardian

Arbeiten mit Datei-Menüoptionen für „Abonnieren“-Modus

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
Öffnen Sie die Datei mit der	Dateien werden wie gewohnt geöffnet.
Speichern	• Optionen: Bereits geschütztes Dokument: Speicherung als geschützt. Ungeschützt: Speicherung als ungeschützt. Um es zu schützen, klicken Sie auf **Geschütztes „Speichern unter“**. • 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.
Speichern unter	Hat die Standardoptionen (aber nicht „Geschützter Modus“)
Geschütztes „Speichern unter“	Einzige Option im Feld „Speichertyp“ ist „Office geschützt“
Drucken	**Aktiviert** Bei geschützten Office-Dokumenten können Sie, wenn ein Administrator das Drucken per Richtlinie deaktiviert, jedoch weiterhin „Drucken“ auswählen. Es wird aber eine Warnung angezeigt, die besagt, dass das geschützte Dokument nicht gedruckt werden kann. Wenn Ihr Administrator das Drucken zulässt, kann eine andere Richtlinie ein Wasserzeichen mit dem Benutzernamen, dem Domänennamen und der Computer-ID auf jeder Seite platzieren, wenn Sie drucken.
Freigeben	**Aktiviert** für geschützte Office-Dokumente

Dateimenü	Abonnierter Modus und geschützte Office-Dokumente
	Deaktiviert für ungeschützte Dokumente
Exportieren (Office 2013 und höher)	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 Domänennamen und die Computer-ID enthält. Wenn Sie ein Dokument im geschützten Modus für einen externen Benutzer exportieren, kann dieser es öffnen und anzeigen, jedoch nicht exportieren oder drucken.

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.

TITUS Klassifizierung und „Abonnieren“-Modus

Falls eine Richtlinie aktiviert ist, konfiguriert Ihr Administrator einige TITUS-Klassifizierung, um ein Dokument mit dieser Klassifizierung zu verschlüsseln. Sie können mit der rechten Maustaste auf ein ungeschütztes Office-Dokument klicken und diese TITUS-Klassifizierung auswählen. Dies stellt eine andere Möglichkeit zum Schutz eines Office-Dokuments dar.

Datenklassifizierung und „Abonnieren“-Modus

Wenn diese Richtlinie aktiviert ist, kann Ihr Administrator Klassifikationen für einen bestimmten Inhalt festlegen, so wie Sozialversicherungs- oder Kreditkartennummern oder andere vertrauliche Informationen. Ihr Administrator wird Sie darüber in Kenntnis setzen, welche Informationen klassifiziert wurden. Wenn Sie ein Dokument speichern, welches Informationen enthält, die auf diesen Klassifizierungsregeln basieren, wird dieses Dokument verschlüsselt.

Wenn Sie Tags in einem Office-Dokument verwenden, um eine Datenklassifizierung auszulösen, die in Metadaten von Dateitags der Richtlinie verwendet wird, wird bei dem Tag, den Sie im Office-Dokument verwenden, die Groß- und Kleinschreibung beachtet und er muss so viele Zeichen haben, wie Ihr Administrator in der Richtlinie verwendet hat.

ANMERKUNG:

Wenn diese Richtlinie aktiviert ist, bewirkt ein Aufräumprozess, dass Dateien, die die Klassifizierungsregeln erfüllen, verschlüsselt sind. Wenn Sie jedoch die Datei erstellen, können Sie mit der rechten Maustaste darauf klicken und **Datei schützen** auswählen.

Siehe auch Outlook-E-Mail-Verschlüsselung mit Data Guardian

Richtlinie für den abonnierten Modus

Wenn durch eine Data Guardian-Richtlinie das Drucken für geschützte Office-Dokumente deaktiviert wurde, können Sie nach wie vor unter **Datei > Info** oder durch Klicken mit der rechten Maustaste auf eine geschützte Office-Datei in Windows Explorer „Drucken“ auswählen. 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

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.

ANMERKUNG:
Im erzwungenen geschützten Modus werden alle Office-Dokumente geschützt.

Identifier	GUID-5E368002-F3BB-48A7-9A30-B4591019B21F
Status	In Translation

Erzwungenen geschützten Modus zum Schutz von Office-Dokumenten verwenden

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

- Für „Erzwungenen Schutz“-Modus mit Datei-Menüoptionen arbeiten
- Weitere Optionen für Data Guardian

Für „Erzwungenen Schutz“-Modus mit Datei-Menüoptionen arbeiten

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	Erzwungener geschützter Modus für geschützte und ungeschützte Office-Dokumente
Öffnen Sie die Datei mit der	Nicht geschützte Dokumente werden im schreibgeschützten Modus geöffnet.
Speichern	• Das Dokument ist geschützt. • 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. • 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. **ANMERKUNG:** 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).
Speichern unter	**Deaktiviert**
Geschütztes „Speichern unter“	Einzige Option im Feld „Speichertyp“ ist „Office geschützt“

Dateimenü	Erzwungener geschützter Modus für geschützte und ungeschützte Office-Dokumente
Drucken	**Aktiviert** Bei geschützte Office-Dokumente können Sie, wenn ein Administrator das Drucken per Richtlinie deaktiviert, jedoch weiterhin „Drucken“ auswählen. Es wird aber eine Warnung angezeigt, die besagt, dass das geschützte Dokument nicht gedruckt werden kann. Wenn Ihr Administrator das Drucken zulässt, kann eine andere Richtlinie ein Wasserzeichen mit dem Benutzernamen, dem Domänennamen und der Computer-ID auf jeder Seite platzieren, wenn Sie drucken.
Freigeben	**Deaktiviert**
Exportieren (Office 2013 und höher)	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 Domänennamen und die Computer-ID enthält. **ANMERKUNG:** Wenn Sie ein Dokument im geschützten Modus für einen externen Benutzer exportieren, kann dieser es öffnen und anzeigen, jedoch nicht exportieren oder drucken.

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.

Identifier	GUID-669244A9-0658-46A3-A9EB-A5D349D7EDBC
Status	In Translation

Weitere Optionen für Data Guardian

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.

Einfügen

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

- Sie können ungeschützte oder geschützte Daten in das ursprüngliche geschützte Dokument oder in eine geschützte PDF kopieren und einfügen. Dennoch können keine ungeschützten PDFs in Adobe Acrobat Reader DC geöffnet werden.
- 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.

Eine geschützte PDF-Datei mit Adobe Acrobat Reader DC öffnen und bearbeiten

Bei der Verwendung von Acrobat Reader DC:

- Sie können Anmerkungen zu einer geschützten .pdf-Datei hinzufügen oder ein Formular ausfüllen. Wenn Sie die Datei speichern, wird eine neue geschützte .pdf-Datei erstellt, die die Änderungen beinhaltet. Das ist Acrobat Reader DC Funktionalität.
- Um die Sicherheit zu verbessern, wird der Internetzugang blockiert wenn eine geschützte .pdf-Datei in Acrobat Reader DC geöffnet ist, bis Acrobat Reader DC geschlossen ist.
- Um die Sicherheit zu verbessern, wenn eine geschützte PDF geöffnet ist, kann ein Benutzer von dieser Instanz keine E-Mail versenden.

ANMERKUNG:
Sie können keine geschützte .pdf-Datei über das Netzwerk öffnen. Sie können Word verwenden, um eine geschützte .pdf-Datei über das Netzwerk zu öffnen.

Drucken für Umschläge und Etiketten

Wenn der Administrator eine Richtlinie zum Hinzufügen eines Wasserzeichens beim Drucken eines geschütztes Office-Dokument 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.

Zusätzliche Optionen

Prozesse gesperrt

Je nach den von Ihrem Administrator festgelegten Richtlinien sind einige Vorgänge, z. B. Snipping Tool, möglicherweise gesperrt. Ihr Administrator kann Sie über diese Prozesse informieren. Darüber hinaus werden Sie in einem Dialogfeld darüber informiert, dass der Prozess gesperrt ist.

- **„Erzwungener Schutz"-Modus** – Wenn Ihr Administrator eine Richtlinie festlegt, um die Schaltfläche *PrtScr* zu blockieren, kann dies auch die Möglichkeit blockieren, den Touchscreen oder Tablets zum Drucken zu verwenden.
- Windows mit RS5 verfügt über eine Screen Sketch-App (zuvor das Snipping Tool). Mit Data Guardian kann Ihr Administrator eine Richtlinie aktivieren, die diese App blockiert, um die Sicherheit zu verbessern.

Anhängen eines geschützten Dokuments an eine Outlook-E-Mail

Wenn Sie ein geschütztes 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.

Sie können ein geschütztes Office-Dokument, einen zusätzlichen geschützten Dateityp, der auf Richtlinien basiert, oder eine .xen-Datei anhängen.

Wenn Sie unter Windows mit Data Guardian ein geschütztes Dokument anhängen, fügt Data Guardian Informationen für den Zugriff auf die verschlüsselte Datei dieser E-Mail hinzu.

- Interne Benutzer: Informationen werden mit einem Link zum Herunterladen eines Clients angezeigt.
- Externe Benutzer: Informationen werden mit einem Link zum Registrieren und Herunterladen eines Clients angezeigt.

ANMERKUNG:
Damit die angefügten Informationen angezeigt werden, müssen Sie die E-Mail aus Microsoft Office Outlook senden, nicht aus der webbasierten Version von Outlook.

Outlook-E-Mail-Verschlüsselung mit Data Guardian

Basierend auf der Richtlinie von Data Guardian v2.0.1 und höher, verfügen interne Benutzer oben links in Outlook zum Verschlüsseln von E-Mails und Anhängen über eine *Schützen*-Option. Es müssen sowohl Sender als auch Empfänger Data Guardian installiert und aktiviert haben.

Die Outlook-E-Mail-Verschlüsselung von Data Guardian wird mit Office 2013 und höher unterstützt, aber nicht mit Web-Mail.

Um diese zu verwenden:

1 Klicken Sie oben links auf **Schützen**.
2 Für eine externe E-Mail-Adresse klicken Sie auf **Ja**, um die Schlüsselfreigabe zu bestätigen oder auf **Nein**, wenn Sie sich entscheiden, die E-Mail nicht zu versenden.

Es hat sich bewährt, immer nur eine E-Mail geöffnet zu haben. Wenn Sie mehr als eine geöffnet haben, klicken Sie auf die E-Mail, um sie hervorzuheben, bevor Sie auf die Schaltfläche „Schützen“ klicken. Die Schaltfläche „Schützen“ sollte grau sein, wenn sich der Mauszeiger nicht auf der Option befindet.

Daten in Bewegung sind sicher. In dieser Vorschau-Version wird Data Loss Prevention (DLP) für ruhende Daten teilweise unterstützt. Zukünftige Versionen werden die Sicherheit weiter verbessern.

Um DLP bei geöffneten verschlüsselten E-Mails zu minimieren, sind einige Aktionen deaktiviert oder blockiert:

- Outlook *QuickSteps*
- *Verschieben*, *In Ordner verschieben* und zusätzliche Ordneraktionen
- Pfeile *Nächste* und *Zurück*
- *Weiter*
- Einige Optionen mit der rechten Maustaste

Um DLP zu minimieren, wenn eine verschlüsselte E-Mail geöffnet ist, werden diese Aktionen gesteuert:

- *Kopieren/Einfügen*
- *Drucken* und *Exportieren* von Daten
- Einige Optionen mit der rechten Maustaste
- Entwurfsordner und *automatisches Speichern*

Für Empfänger von Outlook-E-Mails

Wenn Sie eine verschlüsselte Outlook-E-Mail öffnen, zeigt ein Warnhinweis an, dass das Dokument geschützt ist und der Benutzer die Datei mit einem Doppelklick öffnen muss. Es wir in der Vorschau nur das Deckblatt angezeigt und nicht der Inhalt der E-Mail. Auf der Titelseite wird entweder der Dell Servername für On-prem oder eine Installations-ID für diesen bestimmten Mandanten aufgeführt, wenn Ihr Hosted Dell Security Center über mehrere Mandanten verfügt. Auf der Titelseite befinden sich auch Links zum Herunterladen des Data Guardian-Clients.

E-Mail-Klassifikation

Lokaler Bericht für geschützte Office-Dokumente mit verschlüsselter Datenklassifizierung („Abonnieren“-Modus)

Um vertrauliche Informationen in Office-Dokumenten und PDFs zu schützen, wird Ihr Administrator möglicherweise eine Richtlinie festlegen, um Dateien aufzuräumen und zu verschlüsseln, basierend auf der Datenklassifizierung. Vertrauliche Informationen beinhalten möglicherweise Sozialversicherungsnummern, Kreditkartennummern, Adressen in den vereinigten Staaten oder unternehmensspezifische Daten. Ihr Administrator wird Sie informieren durch welche vertraulichen Informationen Ihre Dateien verschlüsselt werden.

So können Sie lokale Berichte von Dateien ansehen, die aufgrund von Datenklassifizierung verschlüsselt wurden und den Grund für die Verschlüsselung:

1 Navigieren Sie zu **C:\Users\<username>\AppData\Local\Dell\Data Guardian**.
2 Öffnen Sie die **Protokollberichte der Klassifizierung**.

> **ANMERKUNG:**
> Wenn die Datei gerade verschlüsselt wird, kann der Eintrag möglicherweise aus mehreren Zeilen bestehen, bis die Verschlüsselung abgeschlossen ist.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Schützen von weiteren Anwendungen und Dateitypen mit einfachem Dateischutz

Ihr Administrator wird Sie darüber informieren, ob Richtlinien es zulassen, zusätzliche Anwendungen und Dateitypen zu verschlüsseln. Wenn jemand eine Datei öffnet, die mit einfachem Dateischutz verschlüsselt ist, aber Data Guardian nicht installiert hat, ist der Inhalt nicht mehr lesbar.

Überblick über den einfachen Dateischutz

Anwendungen

Dies sind Beispiele für Anwendungen, die Ihr Administrator möglicherweise verschlüsseln möchte:

- Notepad
- Wordpad
- Visio
- MS Paint

> **ANMERKUNG:**
> Einige Anwendungen werden nur teilweise von Data Guardian unterstützt. Ihr Administrator wird Sie über diese informieren.

Dateitypen

Dies sind Beispiele für zusätzliche Dateitypen, die konfiguriert werden können: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac und Mobilgeräte

Wenn der einfache Dateischutz konfiguriert ist, räumt Data Guardian die Computer des Benutzers auf und verschlüsselt alle lokalen Dateien mit diesen Erweiterungen. Mit einfachem Dateischutz verschlüsselte Dateien können nur mithilfe der Anwendung eingesehen und bearbeitet werden, die im Zusammenhang mit der Dateierweiterung steht.

ANMERKUNG:
Dateien in bestimmten Systemordnern werden nicht verschlüsselt, z. B. AppData. Dies gilt auch für Ordner, die in Zusammenhang mit geschützte Office-Dokumente stehen, z. B. der Ordner „Sichere Dokumente“.

Overlaysymbole für Windows

Bei Data Guardian 2.2 und höher werden Overlaysymbole für geschützte Dateien im Datei-Explorer angezeigt. Wenn Sie mit der rechten Maustaste auf diese geschützte Datei klicken, enthält eine Registerkarte von Dell Data Guardian weitere Informationen.

Schließen Sie einige Dateien aus dem Aufräumen auf Windows oder Mac aus (bevor das Aufräumen aktiviert wird).

Wenn Ihr Unternehmen entscheidet, einen weiteren Dateityp, wie. txt, zu verschlüsseln, möchten Sie möglicherweise nicht, dass alle Dateien mit dieser Erweiterung aufgeräumt und verschlüsselt werden.

Vor der Aktivierung des einfachen Dateischutzes für diese Erweiterung kann Ihr Administrator eine andere Richtlinie festlegen, die es Ihnen ermöglicht, einen Ordner zu Ihrem lokalen Computer hinzuzufügen. Die Dateien in diesem Ordner werden daraufhin nicht aufgeräumt. Ihr Administrator kann eine Richtlinie festlegen, einen Ordnernamen erstellen, den Namen des Ordners bereitstellen und vorschlagen, wo Sie diesen Ordner hinzufügen können. Dabei kann es sich um Dateien handeln, die von Ihrem System benötigt werden, oder um Dateien, die nicht geschützt werden müssen.

WICHTIG:
Sie müssen den Ordner erstellen, bevor der Administrator die grundlegende Richtlinie zum Dateischutz aktiviert.

1 Verwenden Sie den Ordnernamen und den Pfad, die Sie von Ihrem Administrator erhalten haben.
   - Navigieren Sie bei Verwendung von Mac zum **Fensterbereich „Einstellungen“ > Ausschlüsse für den einfachen Dateischutz**. Der zu erstellende Ordnername und der Pfad werden hier angezeigt.

2 Fügen Sie Dateien mit der angegebenen Erweiterung, wie. txt, hinzu, die nicht verschlüsselt werden müssen. Optional können Sie Unterordner mit von Benutzern erstellten Namen hinzufügen.

   ANMERKUNG:
   Wenn Sie Dateien mit dieser Erweiterung haben, die zuvor verschlüsselt waren, werden sie durch das Hinzufügen zu diesem Ordner nicht entschlüsselt. Sie bleiben verschlüsselt. Wenn Sie einen Ordner mit **ungeschützten Dokumenten** haben, den Ihr Administrator über eine andere Richtlinie erstellen kann, können Sie grundlegende Dateischutztypen in diesem Ordner ablegen, um Sie zu entschlüsseln.

3 Wenn der grundlegende Dateischutz aktiviert ist und Sie ungeschützte Dateien mit dieser Erweiterung auf einem Netzwerk oder einem externen Laufwerk haben, können Sie diese in den ausgeschlossenen Ordner kopieren. Er bleibt unverschlüsselt. Andernfalls werden sie verschlüsselt.

Wenn Ihr Computer mehr als einen Benutzer hat, kann nur der aktuell angemeldete Benutzer Dateien in diesem Ordner ablegen und sie vom Aufräumen ausschließen. Alle Dateien, die von einem anderen Benutzer in diesem Ordner abgelegt werden, werden durchsucht und verschlüsselt.

Entfernen einer Dateiendung unter Windows oder Mac

Ihr Administrator kann beschließen, eine Dateierweiterung zu löschen. Wenn ja, wird Ihr Computer überprüft, um diese Dateitypen zu entschlüsseln.

- Die Registerkarte Properties > Dell Data Guardian der verschlüsselten Datei wird nicht mehr angezeigt.

- Wenn Sie Dateiüberlagerungssymbole hatten, werden diese nicht mehr angezeigt.
- Die Entschlüsselung der Datei kann mehrere Minuten in Anspruch nehmen. Wenn eine Datei mit dieser Erweiterung noch verschlüsselt ist, kann sie während des Suchvorgangs geöffnet oder auf einem Dateiserver oder einem anderen Speicherort gespeichert worden sein.

Wenden Sie sich an Ihren Administrator, um die Wiederherstellung von Dateien mit dieser Erweiterung zu beantragen, die nicht entschlüsselt werden können.

Office-Anwendungen

Sie können mit einer Office-Anwendung eine Datei öffnen, die mit einfachem Dateischutz verschlüsselt ist, aber der Inhalt ist schreibgeschützt.

Webportal

Wenn der einfache Dateischutz unter "Einstellungen > Richtlinien" auf "Wahr" gesetzt ist, hat Ihr Administrator Nicht-Office-Dateitypen hinzugefügt, die Data Guardian beim Herunterladen aus dem Webportal verschlüsselt. Ihr Administrator muss Ihnen die Dateitypen mitteilen.

ANMERKUNG:
Wenn Sie einen Dateitypen hochladen, der noch nicht unterstützt wird, ist der Inhalt im Web-Portal nicht lesbar.

Sie können Nicht-Office-Dateitypen unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind, hochladen. Wenn Sie jedoch die Nicht-Office-Datei herunterladen, weicht die Dateierweiterung ab.

Nicht-Office-Dateien (wie .txt oder .png)	Beschreibung herunterladen
Vor dem Hochladen verschlüsselt Beispiel: Nicht-Office-Dateien, die bereits von Windows oder Mac verschlüsselt wurden.	Beim Herunterladen aus dem Webportal wird diese Dateierweiterung beibehalten, z. B. .txt oder .png.
Unverschlüsselte Dateien	Beim Herunterladen vom Webportal hängt die Dateierweiterung davon ab, ob Ihr Administrator die Erweiterung einer Richtlinie hinzufügt. Sie sind jedoch verschlüsselt. Beispiele für eine vom Webportal heruntergeladene TXT-Datei: • **Dateiname.txt**: Ihr Administrator hat den Dateityp .txt zu einer Richtlinie hinzugefügt. • **Dateiname.txt.xen**: Der Dateityp .txt ist nicht in der Richtlinie enthalten. Die Datei ist verschlüsselt, fügt jedoch die Erweiterung .xen hinzu.

Wenn die *Bearbeitung*srichtlinie für das Webportal aktiviert ist, können Benutzer die Nicht-Office-Dateien bearbeiten.

Identifier	**GUID-801B897D-9A0F-48C0-B46C-A3726B8BD9E4**
Status	**Translation Validated**

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.

Identifier	**GUID-A8209D75-E380-4809-A55A-CF89E3FBE29A**
Status	**In Translation**

Ordner und Dateien des Synchronisierungs-Clients in der Cloud anzeigen

Wenn Sie einen Synchronisierungs-Client-Ordner auf Ihrem Computer haben und Data Guardian diesen verschlüsselt, werden diese Dateien in der Cloud verschlüsselt.

Wenn Sie das Data Guardian-Webportal zum Verschlüsseln von Dateien verwenden, können Sie diese als. xen-Dateien verschlüsseln. Sie können keine verschlüsselten .xen-Dateien auf Windows öffnen. Sie können sie auf einem mobilen Gerät mit Data Guardian oder dem Webportal anzeigen.

Identifier	**GUID-7A2816C4-2882-4B5B-B2C6-A8032B1C4508**
Status	**Translation Validated**

Geschützte Office-Dokumente für externe Benutzer freigeben

Mit Data Guardian können Sie ein geschütztes Office-Dokument über E-Mail, Wechselmedien oder eine Netzwerkfreigabe freigeben oder in die Cloud hochladen und freigeben:

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

Wenn Sie das Dokument anhängen und auf *Senden* klicken, wird ein Bestätigungsdialogfeld angezeigt, das darauf hinweist, dass der Schlüssel für dieses geschützte Dokument für den externen Benutzer freigegeben wird.

Verbesserte Sicherheit durch Hinzufügen von Datumseinschränkungen

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 dem Dropdown-Menü 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 dann 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 geschütztes 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 eine Meldung darauf hin, dass die Datei bis zu diesem Datum und dieser Uhrzeit aufgrund von Zugriffseinschränkungen nicht geöffnet werden kann.

Identifier	GUID-FFED5E16-B72A-4858-A64D-
Status	Translation Validated

Data Guardian installieren und mit Mac verwenden

Data Guardian für Mac verfügt für bestimmte Bildschirme über integrierte Hilfeseiten, die Informationen enthalten zu:

- Dell Data Guardian-Schnittstelle, auf der Benutzer Dateien zum Verschlüsseln hochladen können
- Cloud-Verschlüsselung
- Externe Benutzer und Zugriffsbeschränkungen
- Manipulation

Klicken Sie auf der Dell Data Guardian-Schnittstelle für Mac auf das Hilfesymbol.

Identifier	GUID-0DB59561-F614-4FEB-9265-6F2711737741
Status	Translated

Installationsclient für Mac

Wenn Ihr Administrator Sie zur Whitelist Ihres Unternehmens hinzugefügt hat, können Sie sich unter folgender Adresse registrieren: https://IhrSicherheitsservername.domain.com:8443/cloudweb/register.

Nach der Registrierung erhalten Sie eine E-Mail, die Sie an https://IhrSicherheitsservername.domain.com:8443/cloudweb weiterleitet, um sich anzumelden und den entsprechenden Client herunterzuladen.

Sie müssen ein lokaler Administrator sein.

So installieren Sie Data Guardian für Mac:

1 Für den Data Guardian-Client suchen Sie das Installationsprogramm in **Dell Data Guardian-Mac-0.x.x.xxxx.dmg.**
2 Verwenden Sie die **.pkg**-Datei in Dell-Data-Guardian-0.x.x.xxxx.dmg für Installationen oder Upgrades.
3 Doppelklicken Sie auf das **Dell-Data-Guardian-x.x.x**-Paket.
4 Klicken Sie auf **Weiter**.
5 Klicken Sie im Fenster „Einführung“ auf **Fortfahren**.
6 Klicken Sie im Fenster „Softwarelizenzvereinbarung“ auf **Fortfahren**.
7 Klicken Sie auf **Zustimmen**, um fortzufahren.
8 Führen Sie im Fenster „Konfigurationstyp“ einen der folgenden Schritte aus:

Hosted Dell Security Center	On-prem Dell Management Server
Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software. a Wählen Sie **Hosted Dell Security Center** aus. b Klicken Sie auf **Weiter**.	Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software. a Wählen Sie **On-prem Dell Management Server**.

Hosted Dell Security Center	On-prem Dell Management Server
c Fahren Sie mit Schritt 9 fort.	b Geben Sie im Feld *Dell Management Servername* den Dell 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. c Klicken Sie auf **Weiter**. d Fahren Sie mit Schritt 9 fort.

9 Führen Sie im Fenster „Installationstyp“ einen der folgenden Schritte aus:

- Klicken Sie auf **Installieren** und dann fahren Sie mit Schritt 10 fort.
- Klicken Sie auf **Speicherort ändern**.
  1 Wählen Sie im Fenster "Zielauswahl" die Option "alle Benutzer" aus. Derzeit ist dies die einzige Option.
  2 Klicken Sie auf **Weiter**.
  3 Klicken Sie auf **Installieren** und dann fahren Sie mit Schritt 10 fort.

10 Geben Sie Ihren Namen und Ihr Passwort in das Dialogfeld ein, und klicken Sie auf **Software installieren**.

11 Klicken Sie im Fenster „Zusammenfassung“ auf **Schließen**.

12 Wenn Sie dazu aufgefordert werden, behalten Sie die .pkg-Datei bei, oder verschieben Sie sie in den *Papierkorb*.

13 Führen Sie einen der folgenden Schritte aus:

Hosted Dell Security Center	On-prem Dell Management Server
Das Anmeldeinformationsfenster wird nach der Installation automatisch geöffnet. Wenn Ihr Unternehmen über mehrere Mandanten verfügt, benötigen Sie eine Installations-ID. 1 Geben Sie im Fenster „Anmeldeinformationen“ Ihre E-Mail-Adresse für das Anmeldekonto ein und klicken Sie auf **Weiter**. 2 Führen Sie einen der folgenden Schritte aus: • Wenn Ihr Unternehmen über mehrere Mandanten verfügt, geben Sie eine Installations-ID ein, klicken Sie auf **Weiter** und fahren Sie mit Schritt 3 fort. **ANMERKUNG:** Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die Anmeldeinformationen. Wenn Sie eine falsche E-Mail-Adresse oder Installations-ID bemerken, klicken Sie auf **Initialisierung neu starten**, um die Zugangsdaten erneut einzugeben. • Fahren Sie für Einzelmandanten mit Schritt 3 fort. 3 Geben Sie im Microsoft Fenster Ihr Kennwort ein und klicken Sie auf **Anmelden**. 4 Geben Sie im Azure-Fenster Ihr Kennwort ein. 5 Klicken Sie auf **Anmelden**. **ANMERKUNG:** Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die Anmeldeinformationen. Wenn Sie eine falsche E-Mail-Adresse bemerken, klicken Sie auf **Initialisierung neu starten**, um die Zugangsdaten erneut einzugeben. 6 Die Dell Data Guardian-Benutzeroberfläche wird geöffnet. Siehe Dell Data Guardian-Anwendung.	1 Schließen Sie das .dmg-Fenster, um den Finder zu öffnen. 2 Siehe Endbenutzer-Aktivierung.

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

Identifier	GUID-839E9A73-4125-4A28-84A6-4F5CC4D734AC
Status	In Translation

Endbenutzer-Aktivierung (On-prem)

Aktivierung für On-prem Dell Management Server

Bei On-prem müssen Sie sich nach dem erstmaligen Öffnen von Dell Data Guardian anmelden:

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

2 Wenn das Anmeldeinformationen-Fenster geöffnet wird, geben Sie die Dell Server-Adresse, zum Beispiel „company.server.com“, ein. Diese Informationen werden von Ihrem Administrator bereitgestellt. Standardmäßig ist die Portnummer 8443. Wenn Ihr Unternehmen den Standardport in eine benutzerdefinierte Portnummer ändert, werden Sie von Ihrem Administrator darüber informiert.

ANMERKUNG:
Wählen Sie nicht das Kontrollkästchen „SSL-Fehler“ aus, es sei denn, Ihr Administrator fordert Sie dazu auf.

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

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

5 Siehe *Dell Data Guardian-Anwendung* unten.

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

Dell Data Guardian-Anwendung

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

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

Falls die Authentifizierung für die Data Guardian-Anwendung widerrufen wurde oder abgelaufen ist, ist der Name des Cloud-Speicheranbieters ausgegraut.

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

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

Wenn sie authentifiziert wurden, wird der Name des Cloud-Speicheranbieters aktiviert.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Hosted Dell Security Center und angehaltene Mandanten

Wenn bei einem Hosted Dell Security Center ein Mandant für einen bestimmten Zeitraum keine Zahlungen leistet, kann dieser Mandant angehalten werden. Dies gilt für Windows, Mac, Mobile und das Webportal.

Interne und externe Benutzer von Data Guardian können Folgendes erfahren:

- Alle Plattformen: Wenn Sie versuchen, Data Guardian zu installieren, zu aktivieren oder sich anzumelden, wird ein Dialogfeld mit der Meldung angezeigt, dass der Mandant angehalten wurde.
- Mac: Wenn Ihr Mandant angehalten wurde, während Data Guardian geöffnet ist, wird das Dialogfeld "Angehaltener Mandant" angezeigt, nachdem Sie den Explorer und alle Dateien geschlossen haben und dann versuchen, eine geschützte Datei zu öffnen.
- Webportal:
  - Wenn Sie bereits angemeldet sind und eine verschlüsselte Datei hochladen, wird eine Meldung angezeigt, dass der Upload fehlgeschlagen ist.
  - Wenn eine verschlüsselte oder unverschlüsselte Datei hochgeladen wurde und der Mandant angehalten wurde, wird die Meldung "Download fehlgeschlagen" angezeigt.
  - Wenn Sie sich abmelden und versuchen, sich erneut anzumelden, wird in einem Dialogfeld angezeigt, dass der Mandant angehalten wurde.

Wenden Sie sich an Ihren Administrator.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

Schützen von weiteren Anwendungen und Dateitypen mit einfachem Dateischutz

Ihr Administrator wird Sie darüber informieren, ob Richtlinien es zulassen, zusätzliche Anwendungen und Dateitypen zu verschlüsseln. Wenn jemand eine Datei öffnet, die mit einfachem Dateischutz verschlüsselt ist, aber Data Guardian nicht installiert hat, ist der Inhalt nicht mehr lesbar.

Überblick über den einfachen Dateischutz

Anwendungen

Dies sind Beispiele für Anwendungen, die Ihr Administrator möglicherweise verschlüsseln möchte:

- Notepad
- Wordpad
- Visio
- MS Paint

> **ANMERKUNG:**
> Einige Anwendungen werden nur teilweise von Data Guardian unterstützt. Ihr Administrator wird Sie über diese informieren.

Dateitypen

Dies sind Beispiele für zusätzliche Dateitypen, die konfiguriert werden können: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac und Mobilgeräte

Wenn der einfache Dateischutz konfiguriert ist, räumt Data Guardian die Computer des Benutzers auf und verschlüsselt alle lokalen Dateien mit diesen Erweiterungen. Mit einfachem Dateischutz verschlüsselte Dateien können nur mithilfe der Anwendung eingesehen und bearbeitet werden, die im Zusammenhang mit der Dateierweiterung steht.

ANMERKUNG:
Dateien in bestimmten Systemordnern werden nicht verschlüsselt, z. B. AppData. Dies gilt auch für Ordner, die in Zusammenhang mit geschützte Office-Dokumente stehen, z. B. der Ordner „Sichere Dokumente“.

Overlaysymbole für Windows

Bei Data Guardian 2.2 und höher werden Overlaysymbole für geschützte Dateien im Datei-Explorer angezeigt. Wenn Sie mit der rechten Maustaste auf diese geschützte Datei klicken, enthält eine Registerkarte von Dell Data Guardian weitere Informationen.

Schließen Sie einige Dateien aus dem Aufräumen auf Windows oder Mac aus (bevor das Aufräumen aktiviert wird).

Wenn Ihr Unternehmen entscheidet, einen weiteren Dateityp, wie. txt, zu verschlüsseln, möchten Sie möglicherweise nicht, dass alle Dateien mit dieser Erweiterung aufgeräumt und verschlüsselt werden.

Vor der Aktivierung des einfachen Dateischutzes für diese Erweiterung kann Ihr Administrator eine andere Richtlinie festlegen, die es Ihnen ermöglicht, einen Ordner zu Ihrem lokalen Computer hinzuzufügen. Die Dateien in diesem Ordner werden daraufhin nicht aufgeräumt. Ihr Administrator kann eine Richtlinie festlegen, einen Ordnernamen erstellen, den Namen des Ordners bereitstellen und vorschlagen, wo Sie diesen Ordner hinzufügen können. Dabei kann es sich um Dateien handeln, die von Ihrem System benötigt werden, oder um Dateien, die nicht geschützt werden müssen.

WICHTIG:
Sie müssen den Ordner erstellen, bevor der Administrator die grundlegende Richtlinie zum Dateischutz aktiviert.

1 Verwenden Sie den Ordnernamen und den Pfad, die Sie von Ihrem Administrator erhalten haben.
   - Navigieren Sie bei Verwendung von Mac zum **Fensterbereich „Einstellungen“ > Ausschlüsse für den einfachen Dateischutz**. Der zu erstellende Ordnername und der Pfad werden hier angezeigt.

2 Fügen Sie Dateien mit der angegebenen Erweiterung, wie. txt, hinzu, die nicht verschlüsselt werden müssen. Optional können Sie Unterordner mit von Benutzern erstellten Namen hinzufügen.

   ANMERKUNG:
   Wenn Sie Dateien mit dieser Erweiterung haben, die zuvor verschlüsselt waren, werden sie durch das Hinzufügen zu diesem Ordner nicht entschlüsselt. Sie bleiben verschlüsselt. Wenn Sie einen Ordner mit **ungeschützten Dokumenten** haben, den Ihr Administrator über eine andere Richtlinie erstellen kann, können Sie grundlegende Dateischutztypen in diesem Ordner ablegen, um Sie zu entschlüsseln.

3 Wenn der grundlegende Dateischutz aktiviert ist und Sie ungeschützte Dateien mit dieser Erweiterung auf einem Netzwerk oder einem externen Laufwerk haben, können Sie diese in den ausgeschlossenen Ordner kopieren. Er bleibt unverschlüsselt. Andernfalls werden sie verschlüsselt.

Wenn Ihr Computer mehr als einen Benutzer hat, kann nur der aktuell angemeldete Benutzer Dateien in diesem Ordner ablegen und sie vom Aufräumen ausschließen. Alle Dateien, die von einem anderen Benutzer in diesem Ordner abgelegt werden, werden durchsucht und verschlüsselt.

Entfernen einer Dateiendung unter Windows oder Mac

Ihr Administrator kann beschließen, eine Dateierweiterung zu löschen. Wenn ja, wird Ihr Computer überprüft, um diese Dateitypen zu entschlüsseln.

- Die Registerkarte Properties > Dell Data Guardian der verschlüsselten Datei wird nicht mehr angezeigt.
- Wenn Sie Dateiüberlagerungssymbole hatten, werden diese nicht mehr angezeigt.
- Die Entschlüsselung der Datei kann mehrere Minuten in Anspruch nehmen. Wenn eine Datei mit dieser Erweiterung noch verschlüsselt ist, kann sie während des Suchvorgangs geöffnet oder auf einem Dateiserver oder einem anderen Speicherort gespeichert worden sein.

Wenden Sie sich an Ihren Administrator, um die Wiederherstellung von Dateien mit dieser Erweiterung zu beantragen, die nicht entschlüsselt werden können.

Office-Anwendungen

Sie können mit einer Office-Anwendung eine Datei öffnen, die mit einfachem Dateischutz verschlüsselt ist, aber der Inhalt ist schreibgeschützt.

Webportal

Wenn der einfache Dateischutz unter "Einstellungen > Richtlinien" auf "Wahr" gesetzt ist, hat Ihr Administrator Nicht-Office-Dateitypen hinzugefügt, die Data Guardian beim Herunterladen aus dem Webportal verschlüsselt. Ihr Administrator muss Ihnen die Dateitypen mitteilen.

ANMERKUNG:
Wenn Sie einen Dateitypen hochladen, der noch nicht unterstützt wird, ist der Inhalt im Web-Portal nicht lesbar.

Sie können Nicht-Office-Dateitypen unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind, hochladen. Wenn Sie jedoch die Nicht-Office-Datei herunterladen, weicht die Dateierweiterung ab.

Nicht-Office-Dateien (wie .txt oder .png)	Beschreibung herunterladen
Vor dem Hochladen verschlüsselt Beispiel: Nicht-Office-Dateien, die bereits von Windows oder Mac verschlüsselt wurden.	Beim Herunterladen aus dem Webportal wird diese Dateierweiterung beibehalten, z. B. .txt oder .png.
Unverschlüsselte Dateien	Beim Herunterladen vom Webportal hängt die Dateierweiterung davon ab, ob Ihr Administrator die Erweiterung einer Richtlinie hinzufügt. Sie sind jedoch verschlüsselt. Beispiele für eine vom Webportal heruntergeladene TXT-Datei: • **Dateiname.txt**: Ihr Administrator hat den Dateityp .txt zu einer Richtlinie hinzugefügt. • **Dateiname.txt.xen**: Der Dateityp .txt ist nicht in der Richtlinie enthalten. Die Datei ist verschlüsselt, fügt jedoch die Erweiterung .xen hinzu.

Wenn die *Bearbeitung*srichtlinie für das Webportal aktiviert ist, können Benutzer die Nicht-Office-Dateien bearbeiten.

Identifier	GUID-FC539BCB-1939-4E0A-8A36-
Status	Translation Validated

Installieren und Verwenden von Data Guardian für Mobilgeräte mit iOS oder Android

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 geschützt. Die Data Guardian-App muss auf Ihrem Mobilgerät installiert sein, um verschlüsselte Dateien anzeigen oder damit arbeiten zu können.

Identifier	GUID-116F412E-15BE-4E29-A886-5A308BA693ED
Status	Translated

Voraussetzungen

Vor der Verwendung der Data Guardian-App, stellen Sie fest, welche dieser Optionen Sie im Hinblick auf Ihre Umgebung benötigen:

Hosted Dell Security Center	On-prem Dell Management Server
Wenn Ihre gehostete Umgebung über mehrere Mandanten verfügt, benötigen Sie eine Installations-ID.	Stellen Sie sicher, dass Sie den Namen des Dell Server wissen, zum Beispiel „server.domain.com“. Diese Informationen werden von Ihrem Administrator bereitgestellt.

Identifier	GUID-A802F8F9-1B8F-47DD-8525-518A4C004221
Status	Translation Validated

Erste Schritte mit Data Guardian Mobile

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

Aufgabe	Beschreibung	Siehe diesen Abschnitt
Installieren von Data Guardian – Legen Sie eine Option fest:	Installation durch Administrator bereits erfolgt	Administrator-installiert: Tippen Sie auf die Data Guardian-App und melden Sie sich an.
	Installation durch Benutzer erforderlich	Benutzer installiert: Siehe eine der folgenden Anleitungen: • Installieren auf einem iOS-Gerät • Installieren auf einem Android-Gerät
Legen Sie fest, welche Regeln für Mobilgeräte gelten	Ihr Administrator wird Ihnen mitteilen, welche Richtlinien gelten.	Sie können über Folgende verfügen: • Geschützte Office-Dokumente • Cloud-Schutz • Zusätzliche Optionen

Aufgabe	Beschreibung	Siehe diesen Abschnitt
Im Dateiverwalter navigieren	Siehe Data Guardian-Optionen.	Im Dateiverwalter navigieren
Wenn die Cloud-Schutz-Richtlinie aktiviert ist, greifen Sie auf Ihr Cloud-Speicher-Anbieter-Konto zu.	Navigieren Sie auf dem Gerät zum Datei-Manager-Bildschirm der Data Guardian-App und tippen Sie auf Ihren Cloud-Speicheranbieter.	Siehe Zugreifen auf das Konto Ihres Cloud-Speicher-Anbieters.

Basierend auf den Data Guardian-Richtlinien können Sie folgende haben:

- Geschützte Office-Dateien (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) behalten ihre Dateierweiterung.
- Zusätzlichen Anwendungen und Dateitypen, wie z. B. .txt.
- Die Office-fremden Dateien in der Cloud verfügen über die Dateierweiterung „.xen“.

Auf Mobilgeräten mit Data Guardian können Sie Folgendes tun:

- Ordner und Dateien erstellen
- Ordner und Dateien löschen
- Dokument für einen externen Benutzer freigeben (falls Richtlinie für externe Betrachter aktiviert ist)

Identifier	**GUID-618A6EAF-794D-4077-A675-AC9ACA624CC3**
Status	**In Translation**

Installieren oder Deinstallieren von Data Guardian auf einem iOS-Gerät über den App Store

Installieren auf einem iOS-Gerät

Voraussetzung: Wenn Ihr Gerät einen Fingerabdruckscanner mit Touch-ID unterstützt und Sie diesen anstelle einer PIN verwenden möchten, müssen Sie das Gerät für die Touch-ID vor der Installation von Data Guardian konfigurieren.

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 Tippen Sie auf das Kontrollkästchen, um die Lizenzvereinbarung zu akzeptieren.
4 Wählen Sie eine der folgenden Optionen aus:

Hosted Dell Security Center	On-prem
Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software. a Tippen Sie auf Hosted Dell Security Center. b Geben Sie Ihre E-Mail-Adresse ein. c Tippen Sie auf **Senden**. **ANMERKUNG:** Wenn sich Ihre E-Mail-Adresse in mehreren Mandanten befindet, geben Sie Ihre Installations-ID ein. d Geben Sie im Microsoft Azure-Fenster Ihr Kennwort ein.	Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software. a Tippen Sie auf **On-prem**. b Geben Sie für das Serverfeld auf dem Anmeldebildschirm den Namen des Dell Server Ihres Unternehmens ein, z. B. server.domain.com. c Geben Sie Ihren Benutzernamen und Ihr Passwort ein. d Tippen Sie auf **Anmelden**.

Hosted Dell Security Center	On-prem

e Tippen Sie auf **Anmelden**.

5 Tippen Sie, wenn Sie dazu aufgefordert werden, entweder auf den Fingerabdrucksensor oder erstellen Sie eine PIN.

Ihr Konto ist nun aktiviert und der Bildschirm Data Guardian Dateiverwalter wird angezeigt.

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**.

Identifier	GUID-7247F5B1-D730-4DE6-97BA-7E88AD40B7E4
Status	In Translation

Installieren oder Deinstallieren von Data Guardian auf einem iOS-Gerät mit Workspace ONE

Wenn Workspace ONE auf Ihrem Gerät installiert ist, können Sie sich mit einmaligem Anmelden bei Data Guardian authentifizieren. Diese Schritte sind identisch für Hosted Dell Security Center oder On-prem Dell Management Server.

Ihr Administrator wird die Data Guardian-App mithilfe von Push auf Ihr Gerät übertragen.

1 Wenn Sie gefragt werden, ob Sie die **Data Guardian**-App installieren möchten, tippen Sie auf **OK**.
2 Starten Sie die **Data Guardian**-App.
3 Tippen Sie bei der Lizenzvereinbarung auf **Annehmen**.
4 Tippen Sie bei der Auswahl zwischen Workspace ONE oder Data Guardian auf **Workspace ONE**, um das einmalige Anmelden zu verwenden.
5 Geben Sie Ihr Kennwort ein.
6 Wenn Sie dazu aufgefordert werden, erstellen Sie eine PIN.

> **ANMERKUNG:**
> Wenn Sie sich bei Workspace ONE anmelden, müssen Sie für Data Guardian nur Ihre PIN eingeben.

Ihr Konto ist nun aktiviert und der Bildschirm Data Guardian Dateiverwalter wird angezeigt.

Identifier	GUID-D045F8A7-9124-4843-BAF6-E0BB27CE1046
Status	In Translation

Installieren oder Deinstallieren von Data Guardian auf einem Android-Gerät über Google Play

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 Tippen Sie auf das Kontrollkästchen, um die Lizenzvereinbarung zu akzeptieren.
4 Wählen Sie eine der folgenden Optionen aus:

Hosted Dell Security Center	On-prem Dell Management Server
Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software. a Tippen Sie auf **Hosted**. b Geben Sie Ihre E-Mail-Adresse ein. c Tippen Sie auf **Senden**. **ANMERKUNG:** Wenn sich Ihre E-Mail-Adresse in mehreren Mandanten befindet, geben Sie Ihre Installations-ID ein. d Geben Sie im Microsoft Azure-Fenster Ihr Kennwort ein. e Tippen Sie auf **Anmelden**.	Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software. a Tippen Sie auf **On-prem**. b Geben Sie für das Serverfeld auf dem Anmeldebildschirm den Namen des Dell Server Ihres Unternehmens ein, z. B. server.domain.com. c Geben Sie Ihren Benutzernamen und Ihr Passwort ein. d Tippen Sie auf **Anmelden**.

5 Wenn Sie dazu aufgefordert werden, erstellen Sie eine PIN.

Ihr Konto ist nun aktiviert und der Bildschirm Data Guardian Dateiverwalter wird angezeigt.

Deinstallieren Sie die Data Guardian-App

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

Identifier	**GUID-37A6FDB2-CD4D-4EB3-BDE1-EC151BC08814**
Status	**In Translation**

Installieren oder Deinstallieren von Data Guardian auf einem Android-Gerät mit Workspace ONE

Wenn Workspace ONE auf Ihrem Gerät installiert ist, können Sie sich mit einmaligem Anmelden bei Data Guardian authentifizieren. Diese Schritte sind identisch für Hosted Dell Security Center oder On-prem Dell Management Server.

1 Tippen Sie auf Ihrem Gerät auf **Hub**.
2 Tippen Sie auf **App-Katalog**.
3 Tippen Sie in der Dell Data Guardian-App auf **Installieren**.
4 Tippen Sie im Menü *Installation bestätigen* auf **Installieren**.
5 Tippen Sie im Menü *Google Play Protect* auf **Zulassen**.
6 Tippen Sie bei der Meldung „App installiert“ auf **Fertig**.
7 Tippen Sie auf **Öffnen**, um die Data Guardian-App zu starten.
8 Bei der Auswahl, ob Sie sich über Workspace One oder Data Guardian authentifizieren möchten, tippen Sie auf **Workspace ONE**, um das einmalige Anmelden zu verwenden.
9 Tippen Sie bei der Lizenzvereinbarung auf das Kontrollkästchen.
10 Tippen Sie auf **Einmaliges Anmelden**.
11 Wenn Sie dazu aufgefordert werden, erstellen Sie eine PIN.

ANMERKUNG: Wenn Sie sich bei Workspace ONE anmelden, müssen Sie für Data Guardian nur Ihre PIN eingeben.

Ihr Konto ist nun aktiviert und der Bildschirm Data Guardian Dateiverwalter wird angezeigt.

Deinstallieren Sie die Data Guardian-App

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

Identifier	GUID-5B8DFEFC-DC7C-42AE-A662-627068964BC8
Status	In Translation

Im Datei-Manager navigieren

Im Datei-Manager von Data Guardian können Sie den lokalen Speicher oder die Cloud verwenden. Der Datei-Manager wird geöffnet, wenn Sie Data Guardian öffnen.

„Dateiverwalter“-Bildschirm

Standardordner für den „Dateiverwalter“-Bildschirm umfassen:

- Documents
- Downloads
- Fotos

„Neu erstellen“-Bildschirm

Tippen Sie auf das Hinzufügen-Symbol (**+**) und der Bildschirm *Neu erstellen* wird mit diesen Optionen angezeigt:

- Dokument
- Kalkulationstabelle
- Präsentation (PowerPoint)
- Foto
- Ordner
- Cloudservice

Optionen in der Navigationsschublade

Tippen Sie auf das Symbol in der Navigationsschublade. Folgende Optionen stehen zur Auswahl:

- **Browser**
- **Datei-Manager**
- **Einstellungen**-Symbol:
  - **PIN ändern**-Schaltfläche (falls von Richtlinie aktiviert)
  - **Browser**
  - **Datei-Manager (Einstellungen)**: Verwenden Sie diese Optionen
    - **Aktualisierungsintervall**: Wie häufig Data Guardian Ihre Cloud-Services synchronisiert. Dell empfiehlt *Manuell* oder *Täglich*. Andere Optionen sind *Stündlich* oder *Wöchentlich*.

    - **10 MB Download-Warnung**: Aktivieren oder deaktivieren. Verwenden Sie diese Option, wenn Sie kein WLAN nutzen und die Downloadgröße 10 MB überschreitet.
    - **Cache Löschen**: Löscht temporäre Dateien.
  - (iOS): **Touch-ID** oder **Face-ID**, je nach iOS-Version und vorkonfigurierter Fingerabdruck- oder Gesichtserkennung. Tippen Sie zum Aktivieren oder Deaktivieren, wenn Sie Data Guardian verwenden.
  - **Info**: siehe Richtlinien und Version von Data Guardian
  - **Data Guardian verlassen**-Schaltfläche
  - **Cloud-Konten**: Gibt an, ob sie verknüpft oder nicht verknüpft sind.
- **Browser**
- **Datei-Manager**: Um zum Bildschirm „Datei-Manager“ zurückzukehren.
- **Data Guardian sperren**

Zusätzliche Optionen

- Datei zu Favoriten hinzufügen
  - Bei Verwendung von iOS, siehe Schublade „Navigation“.
  - Bei Verwendung von Android halten Sie den Dateinamen gedrückt.

Identifier	**GUID-8826272C-679E-40FF-B0A9-D1C9888AF6E5**
Status	**Translation Validated**

Richtlinien für Data Guardian Mobile festlegen

Ihr Administrator wird Ihnen mitteilen, welche Richtlinien für Ihr Unternehmen festgelegt sind.

Identifier	**GUID-4C1E2DAD-C0CA-4E6F-96D4-0297C01CE8B2**
Status	**Translation Validated**

Anzeigen von Data Guardian-Richtlinien und -Version

Einige Data Guardian-Richtlinien sind in **Über** aufgeführt. So zeigen Sie diese Richtlinien oder die Data Guardian-Version an:

1 Tippen Sie in der Data Guardian-Navigationsschublade auf **Einstellungen -> Info**.

2 Tippen Sie auf **Richtlinie**.

Je nach den von Ihrem Administrator festgelegten Richtlinien kann die Liste Folgendes umfassen:

- PIN-Länge
- Inaktivitätszeitlimit
- Fehler bei der Anmeldung
- Kopieren und einfügen – Ermöglicht das Kopieren aus einem geschützten Dokument und das Einfügen in ein geschütztes Dokument.

Version

3 Weitere Richtlinienoptionen festlegen.

Diese können Folgendes umfassen:

- Geschützte Office-Dokumente
- Cloud-Schutz
- Zusätzliche Richtlinien

Identifier	**GUID-3613C9F0-10DE-4A67-9158-1964C8D2D77E**
Status	**Translation Validated**

Verwenden von geschützten Office-Dokumenten mit dem Mobiltelefon

Ihr Administrator wird Ihnen mitteilen, welche Optionen für Ihr Unternehmen aktiviert sind. Wenn Sie Data Guardian installiert haben und ein geschütztes Office-Dokument öffnen, wird eine Meldung angezeigt, dass das Dokument entschlüsselt wird.

Data Guardian Optionen für Office-Dokumente

Diese Data Guardian-Optionen werden angezeigt.

- **Erstellen** – Je nach Richtlinieneinstellung wird das Dokument geschützt, wenn Sie es erstellen. Im Kopf dieser Datei wird *Geschütztes Dokument* angezeigt.
- **Kopieren/Einfügen** – Bei einem geschütztes Office-Dokument können Sie Inhalte nur in ein anderes geschütztes Office-Dokument kopieren.
- **Drucken** – Je nach zusätzlichen Richtlinieneinstellungen haben Sie ein Wasserzeichen, wenn Sie drucken.
- **Exportieren** – Je nach zusätzlichen Richtlinieneinstellungen haben Sie ein Wasserzeichen, wenn Sie exportieren.

Wenn ein Office-Dokument geöffnet ist, tippen Sie auf das Symbol links oben für diese Optionen:

- **Speichern**
- **Speichern unter**
- **Exportieren**
- **Beenden**

Zusätzliche Office-Optionen basierend auf Richtlinie:

- **Bearbeiten** – Sie können .docx- und .ppt-Office-Dateien bearbeiten.

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

- **Ausgeblendetes Wasserzeichen** – Je nach Richtlinie verfügen geschützte Office-Dokumente möglicherweise über ein verborgenes Wasserzeichen, das den Benutzer identifiziert. Wenn Sie das Dokument drucken oder freigeben, bleibt das Wasserzeichen erhalten.
- **Wasserzeichen auf dem Bildschirm** – Wenn ein geschütztes Office-Dokument geöffnet ist, wird auf dem Client-Bildschirm ein Wasserzeichen angezeigt.

Zusätzliche Informationen für Office-Dokumente

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.

Troubleshooting für geschützte Office-Dokumente

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.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Schützen von weiteren Anwendungen und Dateitypen mit einfachem Dateischutz

Ihr Administrator wird Sie darüber informieren, ob Richtlinien es zulassen, zusätzliche Anwendungen und Dateitypen zu verschlüsseln. Wenn jemand eine Datei öffnet, die mit einfachem Dateischutz verschlüsselt ist, aber Data Guardian nicht installiert hat, ist der Inhalt nicht mehr lesbar.

Überblick über den einfachen Dateischutz

Anwendungen

Dies sind Beispiele für Anwendungen, die Ihr Administrator möglicherweise verschlüsseln möchte:

- Notepad
- Wordpad
- Visio
- MS Paint

> **ANMERKUNG:**
> Einige Anwendungen werden nur teilweise von Data Guardian unterstützt. Ihr Administrator wird Sie über diese informieren.

Dateitypen

Dies sind Beispiele für zusätzliche Dateitypen, die konfiguriert werden können: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac und Mobilgeräte

Wenn der einfache Dateischutz konfiguriert ist, räumt Data Guardian die Computer des Benutzers auf und verschlüsselt alle lokalen Dateien mit diesen Erweiterungen. Mit einfachem Dateischutz verschlüsselte Dateien können nur mithilfe der Anwendung eingesehen und bearbeitet werden, die im Zusammenhang mit der Dateierweiterung steht.

> **ANMERKUNG:**
> Dateien in bestimmten Systemordnern werden nicht verschlüsselt, z. B. AppData. Dies gilt auch für Ordner, die in Zusammenhang mit geschützte Office-Dokumente stehen, z. B. der Ordner „Sichere Dokumente“.

Overlaysymbole für Windows

Bei Data Guardian 2.2 und höher werden Overlaysymbole für geschützte Dateien im Datei-Explorer angezeigt. Wenn Sie mit der rechten Maustaste auf diese geschützte Datei klicken, enthält eine Registerkarte von Dell Data Guardian weitere Informationen.

Schließen Sie einige Dateien aus dem Aufräumen auf Windows oder Mac aus (bevor das Aufräumen aktiviert wird).

Wenn Ihr Unternehmen entscheidet, einen weiteren Dateityp, wie. txt, zu verschlüsseln, möchten Sie möglicherweise nicht, dass alle Dateien mit dieser Erweiterung aufgeräumt und verschlüsselt werden.

Vor der Aktivierung des einfachen Dateischutzes für diese Erweiterung kann Ihr Administrator eine andere Richtlinie festlegen, die es Ihnen ermöglicht, einen Ordner zu Ihrem lokalen Computer hinzuzufügen. Die Dateien in diesem Ordner werden daraufhin nicht aufgeräumt. Ihr Administrator kann eine Richtlinie festlegen, einen Ordnernamen erstellen, den Namen des Ordners bereitstellen und vorschlagen, wo Sie diesen Ordner hinzufügen können. Dabei kann es sich um Dateien handeln, die von Ihrem System benötigt werden, oder um Dateien, die nicht geschützt werden müssen.

WICHTIG:

Sie müssen den Ordner erstellen, bevor der Administrator die grundlegende Richtlinie zum Dateischutz aktiviert.

1 Verwenden Sie den Ordnernamen und den Pfad, die Sie von Ihrem Administrator erhalten haben.
   - Navigieren Sie bei Verwendung von Mac zum **Fensterbereich „Einstellungen“ > Ausschlüsse für den einfachen Dateischutz**. Der zu erstellende Ordnername und der Pfad werden hier angezeigt.

2 Fügen Sie Dateien mit der angegebenen Erweiterung, wie. txt, hinzu, die nicht verschlüsselt werden müssen. Optional können Sie Unterordner mit von Benutzern erstellten Namen hinzufügen.

   ANMERKUNG:

   Wenn Sie Dateien mit dieser Erweiterung haben, die zuvor verschlüsselt waren, werden sie durch das Hinzufügen zu diesem Ordner nicht entschlüsselt. Sie bleiben verschlüsselt. Wenn Sie einen Ordner mit **ungeschützten Dokumenten** haben, den Ihr Administrator über eine andere Richtlinie erstellen kann, können Sie grundlegende Dateischutztypen in diesem Ordner ablegen, um Sie zu entschlüsseln.

3 Wenn der grundlegende Dateischutz aktiviert ist und Sie ungeschützte Dateien mit dieser Erweiterung auf einem Netzwerk oder einem externen Laufwerk haben, können Sie diese in den ausgeschlossenen Ordner kopieren. Er bleibt unverschlüsselt. Andernfalls werden sie verschlüsselt.

Wenn Ihr Computer mehr als einen Benutzer hat, kann nur der aktuell angemeldete Benutzer Dateien in diesem Ordner ablegen und sie vom Aufräumen ausschließen. Alle Dateien, die von einem anderen Benutzer in diesem Ordner abgelegt werden, werden durchsucht und verschlüsselt.

Entfernen einer Dateiendung unter Windows oder Mac

Ihr Administrator kann beschließen, eine Dateierweiterung zu löschen. Wenn ja, wird Ihr Computer überprüft, um diese Dateitypen zu entschlüsseln.

- Die Registerkarte Properties > Dell Data Guardian der verschlüsselten Datei wird nicht mehr angezeigt.
- Wenn Sie Dateiüberlagerungssymbole hatten, werden diese nicht mehr angezeigt.
- Die Entschlüsselung der Datei kann mehrere Minuten in Anspruch nehmen. Wenn eine Datei mit dieser Erweiterung noch verschlüsselt ist, kann sie während des Suchvorgangs geöffnet oder auf einem Dateiserver oder einem anderen Speicherort gespeichert worden sein.

Wenden Sie sich an Ihren Administrator, um die Wiederherstellung von Dateien mit dieser Erweiterung zu beantragen, die nicht entschlüsselt werden können.

Office-Anwendungen

Sie können mit einer Office-Anwendung eine Datei öffnen, die mit einfachem Dateischutz verschlüsselt ist, aber der Inhalt ist schreibgeschützt.

Webportal

Wenn der einfache Dateischutz unter "Einstellungen > Richtlinien" auf "Wahr" gesetzt ist, hat Ihr Administrator Nicht-Office-Dateitypen hinzugefügt, die Data Guardian beim Herunterladen aus dem Webportal verschlüsselt. Ihr Administrator muss Ihnen die Dateitypen mitteilen.

ANMERKUNG:
Wenn Sie einen Dateitypen hochladen, der noch nicht unterstützt wird, ist der Inhalt im Web-Portal nicht lesbar.

Sie können Nicht-Office-Dateitypen unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind, hochladen. Wenn Sie jedoch die Nicht-Office-Datei herunterladen, weicht die Dateierweiterung ab.

Nicht-Office-Dateien (wie .txt oder .png)	Beschreibung herunterladen
Vor dem Hochladen verschlüsselt Beispiel: Nicht-Office-Dateien, die bereits von Windows oder Mac verschlüsselt wurden.	Beim Herunterladen aus dem Webportal wird diese Dateierweiterung beibehalten, z. B. .txt oder .png.
Unverschlüsselte Dateien	Beim Herunterladen vom Webportal hängt die Dateierweiterung davon ab, ob Ihr Administrator die Erweiterung einer Richtlinie hinzufügt. Sie sind jedoch verschlüsselt. Beispiele für eine vom Webportal heruntergeladene TXT-Datei: • **Dateiname.txt**: Ihr Administrator hat den Dateityp .txt zu einer Richtlinie hinzugefügt. • **Dateiname.txt.xen**: Der Dateityp .txt ist nicht in der Richtlinie enthalten. Die Datei ist verschlüsselt, fügt jedoch die Erweiterung .xen hinzu.

Wenn die *Bearbeitung*srichtlinie für das Webportal aktiviert ist, können Benutzer die Nicht-Office-Dateien bearbeiten.

Identifier	**GUID-36644E42-9324-479F-8128-F89D438E8F17**
Status	**Translation Validated**

Verwenden von Cloud-Schutz mit Mobiltelefon

Wenn Ihr Administrator den Cloud-Schutz aktiviert, benötigen Sie zwei Anwendungen:

- Cloud-Sync-Client-App – Siehe Online-Hilfe für diesen Cloud-Sync-Client.
- Die mobile Data Guardian-App führt den von Ihrem Unternehmen verwendeten Cloud-Synchronisierungs-Client auf und ermöglicht Ihnen den Download.

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 ein geschütztes Office-Dokument 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.

Zugreifen auf das Konto Ihres Cloud-Speicher-Anbieters

So greifen Sie auf das Konto Ihres Cloud-Speicher-Anbieters zu:

1 Tippen Sie auf dem Datei-Manager-Bildschirm auf das Symbol „Hinzufügen (**+**)“.

2 Tippen Sie auf **Cloud-Service**.
Eine Data Guardian-Richtlinie bestimmt, welche Cloud-Speicheranbieter angezeigt werden. Ihr Administrator kann einen oder mehrere bestimmte Cloud-Speicher-Anbieter vorgeben, der oder die in Ihrem Unternehmen verwendet werden sollen, und andere Anbieter sperren.

3 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.

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.

Verwenden von Cloud-Schutz

Auf Mobilgeräten mit Data Guardian können Sie Folgendes tun:

- 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.

- 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.

- **Datei > Kopieren** – Je nach den von Ihrem Administrator festgelegten Richtlinien können Sie eine Datei von einem Cloud-Anbieter zu einem anderen kopieren.
- Wenn Sie bei Android mit 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.

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 -> Datei-Manager -> Cloud-Service**. Wenn Sie den Zugriff auf einen Cloud-Speicher-Anbieter gewähren, wird das Kontrollkästchen markiert.

2 Führen Sie einen der folgenden Schritte aus:

Android

a Tippen Sie auf **Verknüpft**.

b Tippen Sie auf **Ja**.

iOS

a Tippen Sie auf **Verknüpfung aufgehoben**.

Dies entfernt den Zugriff auf und Dateien von Data Guardian. Dateien werden jedoch nicht aus der Cloud entfernt.

Troubleshooting bei Cloud-Schutz

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.

Identifier	**GUID-19337C15-12E9-4E8D-B908-29416128B500**
Status	**Translation Validated**

Zusätzliche Richtlinien mit Mobiltelefon verwenden

Ihr Administrator wird Ihnen mitteilen, welche dieser Richtlinien für Ihr Unternehmen eingerichtet wurden.

Verwenden einer PIN

Ihr Administrator kann eine Richtlinie festlegen, die eine PIN einer vorgegebenen Länge voraussetzt.

Manipulation

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

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.

Identifier	**GUID-21086952-1999-4F9B-A47C-C57073C7C715**
Status	**Translation Validated**

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 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.

ANMERKUNG:
Google Backup & Sync wird nicht unterstützt.

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.

Identifier	**GUID-46C6144D-AF30-4559-96AC-39DB1738D2D8**
Status	**Translation Validated**

Protokolle

Aus Sicherheitsgründen sind auf Mobilgeräten keine Protokolldateien verfügbar.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Hosted Dell Security Center und angehaltene Mandanten

Wenn bei einem Hosted Dell Security Center ein Mandant für einen bestimmten Zeitraum keine Zahlungen leistet, kann dieser Mandant angehalten werden. Dies gilt für Windows, Mac, Mobile und das Webportal.

Interne und externe Benutzer von Data Guardian können Folgendes erfahren:

- Alle Plattformen: Wenn Sie versuchen, Data Guardian zu installieren, zu aktivieren oder sich anzumelden, wird ein Dialogfeld mit der Meldung angezeigt, dass der Mandant angehalten wurde.
- Mac: Wenn Ihr Mandant angehalten wurde, während Data Guardian geöffnet ist, wird das Dialogfeld "Angehaltener Mandant" angezeigt, nachdem Sie den Explorer und alle Dateien geschlossen haben und dann versuchen, eine geschützte Datei zu öffnen.
- Webportal:
  - Wenn Sie bereits angemeldet sind und eine verschlüsselte Datei hochladen, wird eine Meldung angezeigt, dass der Upload fehlgeschlagen ist.
  - Wenn eine verschlüsselte oder unverschlüsselte Datei hochgeladen wurde und der Mandant angehalten wurde, wird die Meldung "Download fehlgeschlagen" angezeigt.
  - Wenn Sie sich abmelden und versuchen, sich erneut anzumelden, wird in einem Dialogfeld angezeigt, dass der Mandant angehalten wurde.

Wenden Sie sich an Ihren Administrator.

Identifier	**GUID-66FB1CE0-6669-4DDD-80E8-BCBAA27D4E13**
Status	**Translation Validated**

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.

Identifier	GUID-BDAC1DD8-21C2-4ED1-B0A
Status	In Translation

Geschützten Dateien auf einem Webclient anzeigen oder bearbeiten

Wenn Ihr Administrator ein Data Guardian-Webportal einrichtet, können Sie einen Link zu einer URL für diesen Webclient nutzen und verschlüsselte Dateien ohne Installieren eines Data Guardian-Clients aufrufen. Basierend auf den Richtlinien können Sie auch eine Datei bearbeiten.

Basierend auf den von Ihrem Administrator festgelegten Richtlinien können Sie Folgendes aufrufen:

- Geschützte Office-Dokumente: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- .xen-Dateien – Office- oder nicht-Office-Dateien, die Data Guardian beim Hochladen in die Cloud verschlüsselt hat.
- Zusätzliche Dateitypen, z. B. Notepad.

Basierend auf den von Ihrem Administrator festgelegten Richtlinien können Sie auf einen Cloud-Speicheranbieter zugreifen.

Identifier	GUID-C468D78F-0ADF-45FC-B5A2-44B933EB2497
Status	Translation Validated

Zugreifen auf das Webportal für Data Guardian

Die Schritte können je nach Browser, den Sie verwenden, leicht abweichen.

1 Fordern Sie von Ihrem Administrator die URL für den Zugriff auf das Webportal an.
2 Klicken Sie auf die URL.
Wenn Sie eine Warnmeldung erhalten, klicken Sie auf **Weiter** oder **Fortfahren**.
3 Klicken Sie im Fenster der Lizenzvereinbarung auf **Einverstanden**.
Wenn Sie eine Warnmeldung erhalten, klicken Sie auf **Weiter** oder **Fortfahren**.
4 Geben Sie die Anmeldeinformationen für Ihre Domäne ein.
5 Klicken Sie auf **Anmelden**.
6 Wenn Sie dazu aufgefordert werden, Ihren Standort nachzuverfolgen, wählen Sie eine Option aus.
7 Zum Anzeigen oder Bearbeiten von Dateien finden Sie in der Online-Hilfe, die Sie über das Data Guardian-Webportal aufgerufen können, weitere Informationen.

> **ANMERKUNG:**
> Für Mac müssen Sie Safari so konfigurieren, dass es Pop-up-Fenster zulässt.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Schützen von weiteren Anwendungen und Dateitypen mit einfachem Dateischutz

Ihr Administrator wird Sie darüber informieren, ob Richtlinien es zulassen, zusätzliche Anwendungen und Dateitypen zu verschlüsseln. Wenn jemand eine Datei öffnet, die mit einfachem Dateischutz verschlüsselt ist, aber Data Guardian nicht installiert hat, ist der Inhalt nicht mehr lesbar.

Überblick über den einfachen Dateischutz

Anwendungen

Dies sind Beispiele für Anwendungen, die Ihr Administrator möglicherweise verschlüsseln möchte:

- Notepad
- Wordpad
- Visio
- MS Paint

> **ANMERKUNG:**
> Einige Anwendungen werden nur teilweise von Data Guardian unterstützt. Ihr Administrator wird Sie über diese informieren.

Dateitypen

Dies sind Beispiele für zusätzliche Dateitypen, die konfiguriert werden können: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac und Mobilgeräte

Wenn der einfache Dateischutz konfiguriert ist, räumt Data Guardian die Computer des Benutzers auf und verschlüsselt alle lokalen Dateien mit diesen Erweiterungen. Mit einfachem Dateischutz verschlüsselte Dateien können nur mithilfe der Anwendung eingesehen und bearbeitet werden, die im Zusammenhang mit der Dateierweiterung steht.

> **ANMERKUNG:**
> Dateien in bestimmten Systemordnern werden nicht verschlüsselt, z. B. AppData. Dies gilt auch für Ordner, die in Zusammenhang mit geschützte Office-Dokumente stehen, z. B. der Ordner „Sichere Dokumente“.

Overlaysymbole für Windows

Bei Data Guardian 2.2 und höher werden Overlaysymbole für geschützte Dateien im Datei-Explorer angezeigt. Wenn Sie mit der rechten Maustaste auf diese geschützte Datei klicken, enthält eine Registerkarte von Dell Data Guardian weitere Informationen.

Schließen Sie einige Dateien aus dem Aufräumen auf Windows oder Mac aus (bevor das Aufräumen aktiviert wird).

Wenn Ihr Unternehmen entscheidet, einen weiteren Dateityp, wie. txt, zu verschlüsseln, möchten Sie möglicherweise nicht, dass alle Dateien mit dieser Erweiterung aufgeräumt und verschlüsselt werden.

Vor der Aktivierung des einfachen Dateischutzes für diese Erweiterung kann Ihr Administrator eine andere Richtlinie festlegen, die es Ihnen ermöglicht, einen Ordner zu Ihrem lokalen Computer hinzuzufügen. Die Dateien in diesem Ordner werden daraufhin nicht aufgeräumt. Ihr

Administrator kann eine Richtlinie festlegen, einen Ordnernamen erstellen, den Namen des Ordners bereitstellen und vorschlagen, wo Sie diesen Ordner hinzufügen können. Dabei kann es sich um Dateien handeln, die von Ihrem System benötigt werden, oder um Dateien, die nicht geschützt werden müssen.

WICHTIG:
Sie müssen den Ordner erstellen, bevor der Administrator die grundlegende Richtlinie zum Dateischutz aktiviert.

1 Verwenden Sie den Ordnernamen und den Pfad, die Sie von Ihrem Administrator erhalten haben.
   - Navigieren Sie bei Verwendung von Mac zum **Fensterbereich „Einstellungen“ > Ausschlüsse für den einfachen Dateischutz**. Der zu erstellende Ordnername und der Pfad werden hier angezeigt.

2 Fügen Sie Dateien mit der angegebenen Erweiterung, wie. txt, hinzu, die nicht verschlüsselt werden müssen. Optional können Sie Unterordner mit von Benutzern erstellten Namen hinzufügen.

   ANMERKUNG:
   Wenn Sie Dateien mit dieser Erweiterung haben, die zuvor verschlüsselt waren, werden sie durch das Hinzufügen zu diesem Ordner nicht entschlüsselt. Sie bleiben verschlüsselt. Wenn Sie einen Ordner mit **ungeschützten Dokumenten** haben, den Ihr Administrator über eine andere Richtlinie erstellen kann, können Sie grundlegende Dateischutztypen in diesem Ordner ablegen, um Sie zu entschlüsseln.

3 Wenn der grundlegende Dateischutz aktiviert ist und Sie ungeschützte Dateien mit dieser Erweiterung auf einem Netzwerk oder einem externen Laufwerk haben, können Sie diese in den ausgeschlossenen Ordner kopieren. Er bleibt unverschlüsselt. Andernfalls werden sie verschlüsselt.

Wenn Ihr Computer mehr als einen Benutzer hat, kann nur der aktuell angemeldete Benutzer Dateien in diesem Ordner ablegen und sie vom Aufräumen ausschließen. Alle Dateien, die von einem anderen Benutzer in diesem Ordner abgelegt werden, werden durchsucht und verschlüsselt.

Entfernen einer Dateiendung unter Windows oder Mac

Ihr Administrator kann beschließen, eine Dateierweiterung zu löschen. Wenn ja, wird Ihr Computer überprüft, um diese Dateitypen zu entschlüsseln.

- Die Registerkarte Properties > Dell Data Guardian der verschlüsselten Datei wird nicht mehr angezeigt.
- Wenn Sie Dateiüberlagerungssymbole hatten, werden diese nicht mehr angezeigt.
- Die Entschlüsselung der Datei kann mehrere Minuten in Anspruch nehmen. Wenn eine Datei mit dieser Erweiterung noch verschlüsselt ist, kann sie während des Suchvorgangs geöffnet oder auf einem Dateiserver oder einem anderen Speicherort gespeichert worden sein.

Wenden Sie sich an Ihren Administrator, um die Wiederherstellung von Dateien mit dieser Erweiterung zu beantragen, die nicht entschlüsselt werden können.

Office-Anwendungen

Sie können mit einer Office-Anwendung eine Datei öffnen, die mit einfachem Dateischutz verschlüsselt ist, aber der Inhalt ist schreibgeschützt.

Webportal

Wenn der einfache Dateischutz unter "Einstellungen > Richtlinien" auf "Wahr" gesetzt ist, hat Ihr Administrator Nicht-Office-Dateitypen hinzugefügt, die Data Guardian beim Herunterladen aus dem Webportal verschlüsselt. Ihr Administrator muss Ihnen die Dateitypen mitteilen.

ANMERKUNG:
Wenn Sie einen Dateitypen hochladen, der noch nicht unterstützt wird, ist der Inhalt im Web-Portal nicht lesbar.

Sie können Nicht-Office-Dateitypen unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind, hochladen. Wenn Sie jedoch die Nicht-Office-Datei herunterladen, weicht die Dateierweiterung ab.

Nicht-Office-Dateien (wie .txt oder .png)	Beschreibung herunterladen
Vor dem Hochladen verschlüsselt Beispiel: Nicht-Office-Dateien, die bereits von Windows oder Mac verschlüsselt wurden.	Beim Herunterladen aus dem Webportal wird diese Dateierweiterung beibehalten, z. B. .txt oder .png.
Unverschlüsselte Dateien	Beim Herunterladen vom Webportal hängt die Dateierweiterung davon ab, ob Ihr Administrator die Erweiterung einer Richtlinie hinzufügt. Sie sind jedoch verschlüsselt. Beispiele für eine vom Webportal heruntergeladene TXT-Datei: • **Dateiname.txt**: Ihr Administrator hat den Dateityp .txt zu einer Richtlinie hinzugefügt. • **Dateiname.txt.xen**: Der Dateityp .txt ist nicht in der Richtlinie enthalten. Die Datei ist verschlüsselt, fügt jedoch die Erweiterung .xen hinzu.

Wenn die *Bearbeitung*srichtlinie für das Webportal aktiviert ist, können Benutzer die Nicht-Office-Dateien bearbeiten.

Identifier	**GUID-932E973E-B2CD-4305-B50F-F85231243FA4**
Status	**In Translation**

Verwenden eines Cloud-Speicheranbieters

Basierend auf den Richtlinien kann das Webportal auf einen Cloud-Speicheranbieter zugreifen. Weitere Informationen finden Sie in der Online-Hilfe des Webportals.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Hosted Dell Security Center und angehaltene Mandanten

Wenn bei einem Hosted Dell Security Center ein Mandant für einen bestimmten Zeitraum keine Zahlungen leistet, kann dieser Mandant angehalten werden. Dies gilt für Windows, Mac, Mobile und das Webportal.

Interne und externe Benutzer von Data Guardian können Folgendes erfahren:

- Alle Plattformen: Wenn Sie versuchen, Data Guardian zu installieren, zu aktivieren oder sich anzumelden, wird ein Dialogfeld mit der Meldung angezeigt, dass der Mandant angehalten wurde.
- Mac: Wenn Ihr Mandant angehalten wurde, während Data Guardian geöffnet ist, wird das Dialogfeld "Angehaltener Mandant" angezeigt, nachdem Sie den Explorer und alle Dateien geschlossen haben und dann versuchen, eine geschützte Datei zu öffnen.
- Webportal:
  - Wenn Sie bereits angemeldet sind und eine verschlüsselte Datei hochladen, wird eine Meldung angezeigt, dass der Upload fehlgeschlagen ist.
  - Wenn eine verschlüsselte oder unverschlüsselte Datei hochgeladen wurde und der Mandant angehalten wurde, wird die Meldung "Download fehlgeschlagen" angezeigt.
  - Wenn Sie sich abmelden und versuchen, sich erneut anzumelden, wird in einem Dialogfeld angezeigt, dass der Mandant angehalten wurde.

Wenden Sie sich an Ihren Administrator.

Identifier	GUID-FF3D5442-1632-454D-8787-1
Status	Translation Validated

8

Verwenden von Data Guardian als externen 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.

Externe Benutzer müssen die Server-Anforderungen erfüllen. Außerdem darf sich die Domäne oder der Benutzer nicht auf der Blacklist des Unternehmens befinden.

In einer gehosteten Umgebung können externe Benutzer jeweils nur für einen Mandanten aktiviert werden.

Zu den Optionen für externe Benutzer gehören:

- **Windows**: Laden Sie einen Data Guardian-Client herunter und installieren Sie ihn. Siehe Aufgaben interner Benutzer unter Windows und Aufgaben externer Benutzer.
- **Mac**: Siehe Externe Benutzer unter Mac.
- **Handy**
- **Webportal**: Anstatt einen Data Guardian-Client herunterzuladen, verwenden Sie das Data Guardian-Webportal. Externe Benutzer können ein geschütztes Office-Dokument oder eine .pdf- oder .xen-Datei anzeigen. Je nach Richtlinien kann der externe Benutzer die Datei bearbeiten. Siehe Externe Benutzer und Webportal.

Identifier	GUID-EBDBAE23-A90F-4603-934B-6B40EE93C248
Status	In Translation

Aufgaben interner Benutzer in Windows

Um geschützte Dateien für einen externen Benutzer freizugeben, haben Sie folgende Möglichkeiten:

- Verwenden Sie die Option *Zugriff auf geschützte Datei* für geschützte Office-Dokumente.
- Genehmigen oder Verweigern des Zugriffs, wenn ein externer Benutzer Zugriff anfordert
- Senden Sie ein geschütztes Office-Dokument als Outlook-E-Mail.

Zugriff auf eine oder mehrere geschützte Office-Dateien gewähren

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

1 Klicken Sie mit der rechten Maustaste auf eine geschützte Datei und wählen Sie **Zugriff auf geschützte Datei**. Sie können eine oder mehrere Dateien (bis zu 50) auswählen. Das Fenster „Zugriff auf geschützte Dokumente freigeben“ wird geöffnet. Dateien können sich an folgenden Speicherorten befinden:
   - Lokaler Ordner oder Netzlaufwerk
   - E-Mail
   - Wechselmedien
   - Netzwerkfreigabe
2 Geben Sie oben rechts im Feld *E-Mail für Freigabe* die E-Mail-Adresse des Benutzers außerhalb der Domäne ein und klicken Sie auf **Hinzufügen**.
3 Wiederholen Sie diesen Schritt, um bis zu zehn E-Mail-Adressen hinzuzufügen.
4 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.
5 Informieren Sie externe Benutzer, die noch nicht registriert sind, am besten darüber, dass Sie eine E-Mail mit Anweisungen erhalten, mit der sie sich bei einem Dell Server registrieren, Data Guardian herunterladen und aktivieren sowie freigegebene geschützte Dateien anzeigen können.

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

Ein externer 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.

1 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.
2 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.

Senden einer geschützten Datei als Outlook-E-Mail

Wenn Sie eine geschützte Datei anhängen und auf *Senden* klicken, werden Sie durch eine Bestätigungsaufforderung daran erinnert, 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.

Identifier	**GUID-967BF32F-F6F1-4C5A-BA0B-34CA9F73A438**
Status	**In Translation**

Aufgaben externer Benutzer in Windows

Ein interner Benutzer kann entscheiden, Ihnen Zugriff auf geschützte Dateien zu gewähren. Möglicherweise erhalten Sie Folgendes:

- E-Mail mit Anweisungen zur Registrierung
- Geschützte Datei mit einer Titelseite, die einen Link zum Registrieren einer gültigen E-Mail-Adresse enthält

ANMERKUNG:
Auf der Titelseite wird entweder der Dell Servername für On-prem oder eine Installations-ID für diesen bestimmten Mandanten aufgeführt, wenn Ihr Hosted Dell Security Center über mehrere Mandanten verfügt. Auf der Titelseite befinden sich auch Links zum Herunterladen des Data Guardian-Clients.

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

- sich bei Data Guardian anmelden.
- Data Guardian herunterladen und installieren: der externe Benutzer muss über Administratorrechte auf dem eigenen Computer verfügen.

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 Führen Sie einen der folgenden Schritte aus:
   - E-Mail: Klicken Sie auf **Akzeptieren**.
   - Geschütztes Dokument mit einer Warnung auf der Titelseite: Klicken Sie auf den angegebenen Link, um eine gültige E-Mail-Adresse zu registrieren.

2 Folgen Sie einer Reihe von Schritten, die auf der Umgebung Ihres Unternehmens basieren:

Hosted Dell Security Center

Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software.

a Geben Sie beim Öffnen des Dell Data Guardian-Webportals Ihre E-Mail-Adresse ein.

b Scrollen Sie nach unten und klicken Sie auf **Zustimmen**.

c Scrollen Sie im Dell Security Center-Fenster nach unten zu *Benötigen Sie ein Konto?* und klicken Sie auf **Registrieren**.

d Geben Sie auf der Seite für das neue Konto eine E-Mail-Adresse, einen Vornamen, einen Nachnamen und ein Kennwort ein. Das Kennwort muss mindestens acht Zeichen lang sein und aus Kleinbuchstaben, Großbuchstaben, Sonderzeichen und Ziffern bestehen.

e Klicken Sie auf **Anmelden**.

f Navigieren Sie zu der E-Mail-Adresse, die Sie zum Registrieren verwendet haben, und rufen Sie den Bestätigungscode ab. Geben Sie ihn ein.

ANMERKUNG:
Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

g Klicken Sie auf **Konto bestätigen**. Wenn Ihr Konto bestätigt ist, wird das Webportal geöffnet.

h Ziehen Sie die geschützte Datei in das Webportal und klicken Sie auf **Jetzt hochladen**.

i Sie erhalten nach der Registrierung eine Willkommens-E-Mail. Diese E-Mail enthält einen Link zum Herunterladen eines Windows-Clients.

ANMERKUNG:
Wenn Ihr Hosted Dell Security Center über mehrere Mandanten verfügt, enthält die E-Mail auch die Installations-ID, die Sie benötigen.

On-prem Dell Management Server

Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software.

ANMERKUNG:
Für On-prem können Sie Data Guardian vor der Registrierung installieren. Klicken Sie nach der Aktivierung auf den Link **Registrieren**.

a Wenn sich das Dell Data Guardian-Fenster öffnet, geben Sie Ihre E-Mail-Adresse ein.

b Klicken Sie auf **Registrieren**.

c Geben Sie auf der Seite „Registrieren“ Ihr Kennwort ein, bestätigen Sie es und klicken Sie dann auf **Anmelden**.

Daraufhin wird ein Bestätigungsdialogfeld für die Registrierung angezeigt, außerdem wird eine E-Mail an die vom internen Benutzer angegebene E-Mail-Adresse gesendet. Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

d Klicken Sie auf den Hyperlink in der Kontoverifikations-E-Mail vom Dell Server.

ANMERKUNG:
Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

e Wechseln Sie zur Webseite.

f Klicken Sie auf der Seite „Bestätigung“ auf **Weiter zur Anmeldung**.

g Klicken Sie auf der Anmeldeseite auf **Kennwort vergessen**.

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

Hosted Dell Security Center	On-prem Dell Management Server
	h 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.
	i Öffnen Sie die Konto-Aktivierungs-E-Mail und klicken Sie auf den Link. Die E-Mail führt auch den Dell Server-Namen auf, den Sie verwenden müssen, wenn Sie die Data Guardian installieren.
	j Geben Sie auf der Anmeldeseite die E-Mail-Adresse und das Passwort ein, die bzw. das Sie für die Registrierung verwendet haben.
	k Klicken Sie auf **Anmelden**. Eine Data Guardian-Download-Seite wird geöffnet.

Laden Sie Data Guardian für Windows herunter und installieren Sie es

Nach der Registrierung können Sie auf einen Link klicken, um einen Windows-Client herunterzuladen. Abhängig davon, was der interne Benutzer anfangs angegeben hat, sind die Links hier verfügbar:

- Bei einem Security Management Server wird eine Download-Seite mit Optionen für den Windows-Client geöffnet.
- Bei einem Security Management Server Virtual: Durch Klicken auf „Windows“ werden Sie zur Website dell.com/support weitergeleitet.
- Wenn Sie eine geschützte Datei erhalten haben, enthält die Titelseite Links zum Herunterladen eines Clients.
- Sie erhalten möglicherweise eine Willkommens-E-Mail mit Links zum Herunterladen eines Clients.

Diese Schritte beschreiben die Installation von Data Guardian auf Windows.

1 Unter Windows klicken Sie auf **Herunterladen (32-Bit)** oder **Herunterladen (64-Bit)**, je nach dem, welches Betriebssystem auf dem Computer ausgeführt wird.
2 Laden Sie die Setup-Datei in ein Verzeichnis auf Ihrem Computer herunter.
3 Doppelklicken Sie zum Starten des Installationsprogramms auf die Setup-Datei.
4 Wählen Sie eine Sprache aus und klicken Sie auf **OK**.
5 Klicken Sie auf **OK**, wenn Sie zur Installation von Microsoft Visual C++ 2010 Redistributable Package aufgefordert werden.
6 Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.
7 Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen, und klicken Sie auf **Weiter**.
8 Klicken Sie auf dem Bildschirm des Zielordners auf **Weiter**, um die Installation am Standardort von **C:\Programme\Dell\Dell Data Guardian** auszuführen.
9 Wählen Sie im Bildschirm „Konfigurationstyp“ eine der folgenden Optionen aus:

Hosted Dell Security Center	On-prem Dell Management Server
a Wählen Sie Hosted Dell Security Center aus. b Wenn Ihr Unternehmen über mehrere Mandanten verfügt, geben Sie die Installations-ID ein, die Sie auf der Titelseite oder in der Begrüßungs-E-Mail finden. c Klicken Sie auf **Weiter**. d Fahren Sie mit Schritt 10 fort.	a Wählen Sie On-prem Dell Management Server. b Geben Sie im Feld *Servername:* den Namen des Dell Server 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. c Klicken Sie auf **Weiter**. d Bestätigen Sie auf dem Bildschirm „Aktivierungsserver bestätigen“, dass die Dell Server-URL-Adresse korrekt ist. Das Installationsprogramm fügt www oder http(s) und den Port hinzu. Klicken Sie auf **Weiter**. e Fahren Sie mit Schritt 10 fort.

10 Wählen Sie im Fenster „Verwaltungstyp“ diese Option aus:

- Externe Verwendung: Ein Benutzer mit einer E-Mail-Adresse außerhalb der Domäne.

11 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.
Der Installationsfortschritt wird in einem Statusfenster angezeigt.

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

13 Klicken Sie auf **Ja**, um neu zu starten.
Die Installation von Data Guardian ist abgeschlossen.

14 Siehe Data Guardian aktivieren.

ANMERKUNG:
Achten Sie auf Hinweise und Ausnahmen in Use Data Guardian with Windows (Use Data Guardian mit Windows), beispielsweise können Sie eine geschützte .pdf-Datei vom Netzwerk nicht öffnen. Sie können Word verwenden, um eine geschützte .pdf-Datei über das Netzwerk zu öffnen.

Identifier	**GUID-92B941BF-52D2-4302-AFA1-3D348E260E03**
Status	**In Translation**

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.
Im Benachrichtigungsbereich wird ein Cloud-Symbol mit einem orangefarbenen Ausrufezeichen angezeigt.

2 Wenn Im Benachrichtigungsbereich ein Dialogfeld angezeigt wird, klicken Sie auf **Zur Aktivierung hier klicken**.
Wenn das Dialogfeld nicht angezeigt wird, klicken Sie auf das **Data Guardian**-Symbol im Benachrichtigungsbereich und wählen Sie **Benutzeraktivierung** aus.

ANMERKUNG:
In einer gehosteten Umgebung können externe Benutzer jeweils nur für einen Mandanten aktiviert werden. Wenn Sie bereits einen Mandanten aktiviert haben, müssen Sie Data Guardian deinstallieren und mit der anderen Installations-ID erneut installieren. Optional können Sie das Webportal verwenden, um geschützte Dokumente hochzuladen und anzuzeigen.

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**.

ANMERKUNG:
Für On-prem: Wenn Sie vor der Registrierung Data Guardian installiert haben, klicken Sie auf den Link **Registrieren**.

Nach Abschluss der Aktivierung wird ein grünes Häkchen im Data Guardian-Benachrichtigungsbereich angezeigt  .

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

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

Identifier	**GUID-55AD51F6-9437-4B64-9A9F-E598A3BBDC74**
Status	**Translation Validated**

Zugriff von einem internen Benutzer anfordern

Wenn ein externer Benutzer Data Guardian installiert und aktiviert hat, kann der Benutzer unter Windows, Mac und Mobile den Zugriff auf ein geschütztes Office-Dokument oder eine PDF-Datei von einem internen Benutzer anfordern. Der externe Benutzer muss für jede Datei eine separate Anforderung stellen.

1 Wenn Sie ein geschütztes Office-Dokument 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.

Im Benachrichtigungsbereich 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.

Identifier	**GUID-1DB6F793-018B-4F14-AA95-63980FCDD713**
Status	**Translation Validated**

Externe Benutzer- und Mac-Aufgaben

Interne Benutzeraufgaben für Mac

Führen Sie einen der folgenden Schritte aus:

- Geschützte Dokumente – Senden an externe Benutzer per E-Mail, Netzwerkfreigabe oder Wechselspeicher.
- Wenn die Cloud-Verschlüsselung von Data Guardian aktiviert ist – Ziehen Sie in der Dell Data Guardian-Benutzeroberfläche geschützte Dateien in die Spalte neben der Spalte des Cloud-Speicheranbieters.

Externe Benutzeraufgaben für Mac

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 Beim Öffnen eines geschützten Dokuments, bei dem eine Titelseitenwarnung angezeigt wird, klicken Sie auf den zur Verfügung gestellten Link, um eine gültige E-Mail-Adresse zu registrieren.

> **ANMERKUNG:**
> Auf der Titelseite wird entweder der Dell Servername für On-prem oder eine Installations-ID für diesen bestimmten Mandanten aufgeführt, wenn Ihr Hosted Dell Security Center über mehrere Mandanten verfügt. Auf der Titelseite befinden sich auch Links zum Herunterladen des Data Guardian-Clients.

2 Führen Sie je nach Umgebung eine der folgenden Aktionen aus:

Hosted Dell Security Center

Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software.

a Geben Sie beim Öffnen des Dell Data Guardian-Webportals Ihre E-Mail-Adresse ein.

b Scrollen Sie nach unten und klicken Sie auf **Zustimmen**.

c Scrollen Sie im Dell Security Center-Fenster nach unten zu *Benötigen Sie ein Konto?* und klicken Sie auf **Registrieren**.

d Geben Sie auf der Seite für das neue Konto eine E-Mail-Adresse, einen Vornamen, einen Nachnamen und ein Kennwort ein. Das Kennwort muss mindestens acht Zeichen lang sein und aus Kleinbuchstaben, Großbuchstaben, Sonderzeichen und Ziffern bestehen.

e Klicken Sie auf **Anmelden**.

f Navigieren Sie zu der E-Mail-Adresse, die Sie zum Registrieren verwendet haben, und rufen Sie den Bestätigungscode ab. Geben Sie ihn ein.

> **ANMERKUNG:**
> Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

g Klicken Sie auf **Konto bestätigen**. Wenn Ihr Konto bestätigt ist, wird das Webportal geöffnet.

h Laden Sie die geschützte Datei hoch, um sie anzuzeigen.

Sie erhalten eine E-Mail mit Links zum Herunterladen des Mac-Clients. Oder klicken Sie auf den Link auf der Titelseite. Siehe unten.

On-prem Dell Management Server

Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software.

a Wenn sich das Dell Data Guardian-Fenster öffnet, geben Sie Ihre E-Mail-Adresse ein.

b Klicken Sie auf **Registrieren**.

c Geben Sie auf der Seite „Registrieren“ Ihr Kennwort ein, bestätigen Sie es und klicken Sie dann auf **Anmelden**.

Daraufhin wird ein Bestätigungsdialogfeld für die Registrierung angezeigt, außerdem wird eine E-Mail an die vom internen Benutzer angegebene E-Mail-Adresse gesendet. Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

d Öffnen Sie die Konto-Aktivierungs-E-Mail und klicken Sie auf den Link.

Die E-Mail führt auch den Dell Server-Namen auf, den Sie verwenden müssen, wenn Sie die Data Guardian installieren.

e Klicken Sie auf der Registrierungsbestätigungsseite auf **Zurück zur Anmeldung**.

Sie können auf der Titelseite auf einen Link klicken, um einen Client herunterzuladen und zu installieren. Siehe unten.

Laden Sie einen Data Guardian-Client herunter und installieren Sie ihn (optional).

1 Geben Sie auf der Anmeldeseite von Dell Data Guardian die E-Mail-Adresse und das Passwort ein, die bzw. das Sie für die Registrierung verwendet haben.

2 Klicken Sie auf **Anmelden**.

Eine Data Guardian-Download-Seite mit Optionen für Windows, iOS, Android und Mac OS X wird geöffnet.

3 Klicken Sie unter Mac OS X auf **Herunterladen**.

4 Wählen Sie auf der Seite *Treiber und Downloads* **Apple Mac OS** aus und klicken Sie auf **Herunterladen**.

5 Laden Sie die .dmg in ein Verzeichnis auf Ihrem Computer herunter und führen Sie die .pkg-Datei aus.

6 Führen Sie eine der folgenden Aktionen aus, um sich anzumelden/zu aktivieren:

Hosted Dell Security Center

a Verwenden Sie die E-Mail-Adresse, die Sie bei der Registrierung verwendet haben.

b Die Anmeldeinformationen sind die Daten, die Sie zum Anmelden bei .dmg verwendet haben.

c Klicken Sie auf **Anmelden**.

On-prem Dell Management Server

a Weitere Informationen finden Sie in der integrierten Online-Hilfe für Data Guardian. Geben Sie den Namen des Dell Server ein, der in der E-Mail zur Kontobestätigung aufgeführt ist.

b Geben Sie auch Ihre E-Mail-Adresse und Ihr Kennwort ein. Die Anmeldeinformationen haben Sie zur Registrierung verwendet.

c Klicken Sie auf **Anmelden**.

Identifier	GUID-B2D2A78A-86B7-4D46-A530-C531CE3B706A
Status	Translation Validated

Externe Benutzer und Mobilgeräte

Wenn ein interner Benutzer einen Link über die Cloud zu einer geschützten Datei freigibt, wird in der Datei eine Titelseite angezeigt, die einen Link zum Registrieren einer gültigen E-Mail-Adresse enthält.

ANMERKUNG:
Auf der Titelseite wird entweder der Dell Servername für On-prem oder eine Installations-ID für diesen bestimmten Mandanten aufgeführt, wenn Ihr Hosted Dell Security Center über mehrere Mandanten verfügt. Auf der Titelseite befinden sich auch Links zum Herunterladen des Data Guardian-Clients.

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

- sich bei Data Guardian anmelden.
- Data Guardian herunterladen und installieren: der externe Benutzer muss über Administratorrechte auf dem eigenen Computer verfügen.

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 in der Titelseitenwarnung auf den angegebenen Link, um eine gültige E-Mail-Adresse zu registrieren.

2 Folgen Sie einer Reihe von Schritten, die auf der Umgebung Ihres Unternehmens basieren:

Hosted Dell Security Center

Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software.

a Geben Sie beim Öffnen des Dell Data Guardian-Webportals Ihre E-Mail-Adresse ein.

b Scrollen Sie nach unten und klicken Sie auf **Zustimmen**.

c Scrollen Sie im Dell Security Center-Fenster nach unten zu *Benötigen Sie ein Konto?* und klicken Sie auf **Registrieren**.

d Geben Sie auf der Seite für das neue Konto eine E-Mail-Adresse, einen Vornamen, einen Nachnamen und ein Kennwort ein. Das Kennwort muss mindestens acht Zeichen lang sein und aus Kleinbuchstaben, Großbuchstaben, Sonderzeichen und Ziffern bestehen.

e Klicken Sie auf **Anmelden**.

f Navigieren Sie zu der E-Mail-Adresse, die Sie zum Registrieren verwendet haben, und rufen Sie den Bestätigungscode ab. Geben Sie ihn ein.

ANMERKUNG:
Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

g Klicken Sie auf **Konto bestätigen**. Wenn Ihr Konto bestätigt ist, wird das Webportal geöffnet.

h Ziehen Sie die geschützte Datei in das Webportal und klicken Sie auf **Jetzt hochladen**.

On-prem Dell Management Server

Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software.

ANMERKUNG:
Für On-prem können Sie Data Guardian vor der Registrierung installieren. Klicken Sie nach der Aktivierung auf den Link **Registrieren**.

a Wenn sich das Dell Data Guardian-Fenster öffnet, geben Sie Ihre E-Mail-Adresse ein.

b Klicken Sie auf **Registrieren**.

c Geben Sie auf der Seite „Registrieren“ Ihr Kennwort ein, bestätigen Sie es und klicken Sie dann auf **Anmelden**.

Daraufhin wird ein Bestätigungsdialogfeld für die Registrierung angezeigt, außerdem wird eine E-Mail an die vom internen Benutzer angegebene E-Mail-Adresse gesendet. Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

d Klicken Sie auf den Hyperlink in der Kontoverifikations-E-Mail vom Dell Server.

ANMERKUNG:
Wenn Sie keine E-Mail sehen, überprüfen Sie Ihren Spam-Ordner.

e Wechseln Sie zur Webseite.

f Klicken Sie auf der Seite „Bestätigung“ auf **Weiter zur Anmeldung**.

Hosted Dell Security Center	On-prem Dell Management Server
i Sie erhalten nach der Registrierung eine Willkommens-E-Mail. Diese E-Mail enthält einen Link zum Herunterladen eines Windows-Clients. **ANMERKUNG:** Wenn Ihr Hosted Dell Security Center über mehrere Mandanten verfügt, enthält die E-Mail auch die Installations-ID, die Sie benötigen.	g Klicken Sie auf der Anmeldeseite auf **Kennwort vergessen**. **ANMERKUNG:** Der Dell Server hat ein zufälliges Kennwort zugewiesen, das Sie zurücksetzen müssen. h 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. i Öffnen Sie die Konto-Aktivierungs-E-Mail und klicken Sie auf den Link. Die E-Mail führt auch den Dell Server-Namen auf, den Sie verwenden müssen, wenn Sie die Data Guardian installieren. j Geben Sie auf der Anmeldeseite die E-Mail-Adresse und das Passwort ein, die bzw. das Sie für die Registrierung verwendet haben. k Klicken Sie auf **Anmelden**. Eine Data Guardian-Download-Seite wird geöffnet.

Laden Sie Data Guardian für Mobile herunter und installieren Sie es

Führen Sie einen der folgenden Schritte aus:

- Installieren oder deinstallieren Sie Data Guardian auf einem Android-Gerät
- Installieren oder deinstallieren Sie Data Guardian auf einem iOS-Gerät

Identifier	**GUID-FE0A7159-E0F3-4E21-9FE6-008C831F7D44**
Status	**Translation Validated**

Externer Benutzer und Webportal

Aufgaben interner Benutzer

Ein interner Benutzer hat folgende Optionen:

- Senden Sie einem externen Benutzer die Unternehmens-URL für den Zugriff auf das Data Guardian-Webportal.
- Eine geschützte Datei an einen externen Benutzer schicken. Wenn der Benutzer die Datei öffnet, wird ein Deckblatt angezeigt.

Der externe Benutzer kann geschütztes Office-Dokument, .pdf-Dateien und .xen-Dateien nur anzeigen oder Dateien auf Grundlage von Richtlinien bearbeiten. Der externe Benutzer muss aber keinen Data Guardian-Client herunterladen.

Aufgaben externer Benutzer für Webportal

So registrieren Sie sich für das Data Guardian-Webportal:

1 Klicken Sie auf die Webportal-URL, die entweder von einem internen Benutzer empfangen oder auf der Titelseite einer geschützten Datei gefunden wurde.

2 Scrollen Sie im Fenster der Lizenzvereinbarung nach unten und klicken Sie auf **Zustimmen**.

3 Führen Sie eine dieser Optionen durch, je nachdem, ob Ihr Unternehmen eine Hosted- oder On-prem-Lösung nutzt.

Hosted Dell Security Center	On-prem Dell Management Server
Eine gehostete Software-as-a-Service(SaaS)-Lösung zur Verwaltung der Dell Data Security Software.	Ein On-prem-Server innerhalb des Unternehmensnetzwerks zur Verwaltung der Dell Data Security Software.
a Geben Sie eine E-Mail-Adresse und ein Kennwort ein. b Klicken Sie auf **Anmelden**. c Geben Sie eine E-Mail-Adresse, einen Vornamen, einen Nachnamen und das Kennwort ein. Das Kennwort muss mindestens acht Zeichen lang sein und aus Kleinbuchstaben, Großbuchstaben, Sonderzeichen und Ziffern bestehen. d Klicken Sie auf **Anmelden**. e Navigieren Sie zu der E-Mail-Adresse, die Sie zum Registrieren verwendet haben, und rufen Sie den Bestätigungscode ab. Geben Sie ihn ein. f Geben Sie den Überprüfungscode ein und klicken Sie auf **Konto bestätigen**. Das Webportal wird geöffnet.	a b Klicken Sie auf **Sie haben noch kein Konto?**. c Geben Sie eine E- Mail-Adresse ein und klicken Sie auf **Registrieren**. **ANMERKUNG:** Für interne Benutzer, die sich als externer Benutzer registrieren möchten, ist diese eine Nicht-Domänen-E-Mail-Adresse. d Geben Sie auf der Registrierungsseite ein Kennwort ein, bestätigen Sie es und klicken Sie dann auf **Registrieren**. Die Bestätigungsseite besagt, dass eine Bestätigungs-E-Mail an die von Ihnen bereitgestellte E-Mail-Adresse gesendet wurde. e Zum Abschließen der Aktivierung des Kontos öffnen Sie die E-Mail mit dem Titel *Kontoverifizierung* und klicken Sie auf den Link. f Klicken Sie auf dem Registrierungsbestätigungsbildschirm auf **Zurück zur Anmeldung**. g Geben Sie die E-Mail-Adresse und das Kennwort ein, die Sie für die Registrierung verwendet haben.

Wenn ein interner Benutzer den Schlüssel nicht teilt, können Sie auf das Webportal zugreifen, aber die Datei nicht öffnen.

4 Die Upload-Seite von Dell Data Guardian wird geöffnet.

5 Klicken Sie auf **Durchsuchen**, um zur Datei zu navigieren und sie hochzuladen, oder ziehen Sie die Datei in das Webportal und legen Sie sie dort ab.

6 Klicken Sie auf **?** zum Anzeigen der Onlinehilfe für jede Seite.

Um Dateien zu bearbeiten, muss ein Administrator eine Richtlinie für diesen Benutzer ändern. Wenn die Gewährung nach der Registrierung erfolgt, müssen Sie sich beim Webportal ab- und wieder anmelden.

Optional können Sie einen Data Guardian-Client herunterladen. Auf der Titelseite befinden sich auch Links zum Herunterladen des Data Guardian-Clients. Auf der Titelseite wird auch der Dell Servername für On-prem oder eine Installations-ID für diesen bestimmten Mandanten aufgeführt, wenn Ihr Hosted Dell Security Center mehrere Mandanten hat.

Zugriff von einem internen Benutzer anfordern

Wenn Sie ein geschütztes Office-Dokument oder eine PDF-Datei hochladen und ein fehlgeschlagener Upload-Dialog angibt, dass Sie keinen Zugriff haben, können Sie den Zugriff vom Autor der Datei anfordern:

1 Klicken Sie im Dialogfeld *Upload fehlgeschlagen* auf **Ja**.

2 Warten Sie auf eine E-Mail des internen Benutzers, um anzugeben, ob der Zugriff gewährt oder verweigert wurde.

ANMERKUNG:

Wenn Sie keine E-Mail vom internen Benutzer erhalten, müssen Sie 48 Stunden warten, bevor Sie erneut Zugriff anfordern können. Wenn Sie die geschützte Datei öffnen, bevor der interne Benutzer den Zugriff genehmigt, wird in einer Meldung angezeigt, dass die Anforderung aussteht.

Identifier	**GUID-01B874EC-88D4-4264-803C-472B65D1180F**
Status	**Translation Validated**

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 Dell Server herstellen und das geschützte Dokument erneut öffnen.

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

- Drucken
- Exportieren
- Speichern unter
- Freigeben

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Hosted Dell Security Center und angehaltene Mandanten

Wenn bei einem Hosted Dell Security Center ein Mandant für einen bestimmten Zeitraum keine Zahlungen leistet, kann dieser Mandant angehalten werden. Dies gilt für Windows, Mac, Mobile und das Webportal.

Interne und externe Benutzer von Data Guardian können Folgendes erfahren:

- Alle Plattformen: Wenn Sie versuchen, Data Guardian zu installieren, zu aktivieren oder sich anzumelden, wird ein Dialogfeld mit der Meldung angezeigt, dass der Mandant angehalten wurde.
- Mac: Wenn Ihr Mandant angehalten wurde, während Data Guardian geöffnet ist, wird das Dialogfeld "Angehaltener Mandant" angezeigt, nachdem Sie den Explorer und alle Dateien geschlossen haben und dann versuchen, eine geschützte Datei zu öffnen.
- Webportal:
  - Wenn Sie bereits angemeldet sind und eine verschlüsselte Datei hochladen, wird eine Meldung angezeigt, dass der Upload fehlgeschlagen ist.
  - Wenn eine verschlüsselte oder unverschlüsselte Datei hochgeladen wurde und der Mandant angehalten wurde, wird die Meldung "Download fehlgeschlagen" angezeigt.
  - Wenn Sie sich abmelden und versuchen, sich erneut anzumelden, wird in einem Dialogfeld angezeigt, dass der Mandant angehalten wurde.

Wenden Sie sich an Ihren Administrator.

Identifier	GUID-EF1D5890-EB47-482E-AF29-
Status	In Translation

Mit den Data Guardian von Zugriffsgruppen (intern) erhöhen Sie die Sicherheit

Die Zugriffsgruppen von Data Guardian erhöhen die Sicherheit, indem Benutzergruppen gebildet werden, die an verschlüsselten Daten zusammenarbeiten können. Benutzer außerhalb einer Gruppe können nicht auf die Daten zugreifen oder sie anzeigen, es sei denn, der Eigentümer der Datei gewährt den Zugriff. Zugriffsgruppen können interne und externe Benutzer umfassen. Sie können Zugriffsgruppen mit Windows, Mac, mobilen Geräten und dem Webportal verwenden.

Wählen Sie basierend auf Ihrem Unternehmen eine der Optionen aus:

- Im Unternehmen ist Data Guardian im Abonnementmodus installiert
- Im Unternehmen ist Data Guardian im erzwungenen geschützten Modus installiert
- Das Unternehmen setzt bislang weder Data Guardian noch den Abonnementmodus ein
- Das Unternehmen setzt bislang weder Data Guardian noch den erzwungenen geschützten Modus ein

Sie können auch Folgendes tun:

- Ändern des Eigentümers einer verschlüsselten Datei
- Widerrufen des Zugriffs auf einen Schlüssel

Identifier	GUID-F71ADE66-5107-4796-B57E-FC00340C788C
Status	In Translation

Im Unternehmen ist Data Guardian im Abonnementmodus installiert

Wenn Ihr Unternehmen Zugriffsgruppen verwendet, um die Sicherheit für sensible Daten zu erhöhen, müssen Sie wissen, wer sich in Ihrer Zugriffsgruppe befindet. Um einen reibungslosen Übergang zu gewährleisten, kann Ihr Unternehmen zunächst eine kurze Frist für die Verarbeitung bestehender gemeinsam genutzter und verschlüsselter Dateien einräumen. Nach Ablauf der Übergangsfrist können die Mitglieder Ihrer Zugriffsgruppe alle freigegebenen, verschlüsselten Dateien, die Sie erstellt haben, einsehen. Sie können Personen außerhalb Ihrer Zugriffsgruppe Zugang gewähren.

Identifizieren Sie die Personen in Ihrer Zugriffsgruppe

Ihr Administrator wird Sie darüber informieren, wer sich in einer oder mehreren Ihrer Zugriffsgruppen befindet, je nachdem, wer Zugriff auf bestimmte Dateien benötigt. Drunter fallen interne und externe Benutzer. Wenn Sie mit bestimmten Benutzern an sensiblen Daten arbeiten, können Sie Ihren Administrator bitten, eine Zugriffsgruppe für diesen Inhalt zu erstellen.

Verwenden Sie eine Übergangszeit, um freigegebene, verschlüsselte Dateien zu verarbeiten

Wenn Sie Data Guardian bereits installiert haben und bestehende Dateien verschlüsselt sind, ist die beste Vorgehensweise für Ihr Unternehmen eine kurze Übergangszeit für die verschlüsselten Dateien, die freigegeben wurden. Um einen reibungslosen Übergang zu ermöglichen, beachten Sie Folgendes für freigegebene, verschlüsselte Dateien:

- Der Eigentümer oder Autor der Datei, ob intern oder extern, hat weiterhin Zugriff auf die Datei.
- Interne oder externe Benutzer innerhalb Ihrer Zugriffsgruppe haben Zugriff auf die meisten freigegebenen Dateien. Basierend auf dem Typ des Schlüssels, der einigen Dateien zugeordnet ist, kann der Zugriff auf einige verloren gehen.
- Interne Benutzer außerhalb Ihrer Zugriffsgruppe - Benutzer sollten während der Übergangszeit alle freigegebenen Dateien öffnen, um Zugriff auf den Schlüssel zu erhalten. Wenn sie in dieser kurzen Zeitspanne keine gemeinsame, verschlüsselte Datei öffnen, verlieren sie den Zugriff auf die Datei.
- Externe Benutzer, die nicht zu Ihrer Zugriffsgruppe gehören - Wenn Sie bereits Zugang zu einer verschlüsselten Datei gewährt haben, hat der externe Benutzer auch während und nach der Übergangszeit weiterhin Zugriff.

Wenn Sie den Zugriff auf eine Datei nach der Übergangszeit verlieren, können Sie den Zugriff vom Eigentümer anfordern.

Erneuter Zugriff auf freigegebene, verschlüsselte Dateien nach Ablauf der Übergangsfrist

Für Windows und Mac im Opt-in-Modus können Sie die folgenden Schritte ausführen, um den Zugriff wiederzuerlangen:

- Geschützte Office-Dokumente – Ein Dialogfeld fordert Sie zu einer Zugriffsanforderung auf und der Eigentümer der Datei kann entscheiden, ob er den Zugriff gewähren möchte.
- Zusätzliche Dateitypen, die über einfachen Dateischutz verschlüsselt werden – keine Eingabeaufforderung nach der Freigabe vorhanden. Der Benutzer muss den Eigentümer der Datei kennen und mit der rechten Maustaste auf die verschlüsselte Datei klicken, um die Schlüssel-ID auf der Registerkarte „Data Guardian“ zu finden. Der Benutzer kann diese Informationen an den Eigentümer senden und den Zugriff anfordern.

Zusammenarbeit bei neuen verschlüsselten Dateien nach der Übergangszeit

Für neue Dateien, die Sie nach der Übergangszeit erstellen und verschlüsseln:

- Interne oder externe Benutzer innerhalb Ihrer Zugriffsgruppe - Haben Zugriff auf alle freigegebenen, verschlüsselten Dateien.
  - Jeder, der aus der Zugriffsgruppe entfernt wird, verliert den Zugriff.
  - Wenn der Eigentümer einer Datei aus der Gruppe entfernt wird, haben andere Benutzer weiterhin Zugriff.
- Interne oder externe Benutzer außerhalb Ihrer Zugriffsgruppe - Können keine verschlüsselte Datei anzeigen.
  - Ein interner Benutzer innerhalb der Zugriffsgruppe kann Zugriff gewähren.
  - Wenn ein externer Benutzer Eigentümer einer verschlüsselten Datei ist, kann er einer anderen Person Zugriff gewähren.
  - Wenn ein interner oder externer Benutzer außerhalb der Gruppe ein geschütztes Office-Dokument erhält und versucht, es zu öffnen, fordert ihn ein Dialog dazu auf, Zugriff zu beantragen.
  - Wenn ein interner oder externer Benutzer außerhalb der Gruppe einen Dateityp mit „einfachem Dateischutz“ öffnet, kann der Benutzer mit der rechten Maustaste auf die verschlüsselte Datei klicken, um die Schlüssel-ID auf der Registerkarte „Data Guardian“ zu suchen, und diese Informationen an den Eigentümer senden.

Identifier	GUID-18DE070B-862D-4CAF-8CDE-DA86552E6C57
Status	In Translation

Im Unternehmen ist Data Guardian im erzwungenen geschützten Modus installiert

Wenn Ihr Unternehmen Zugriffsgruppen verwendet, um die Sicherheit für sensible Daten zu erhöhen, müssen Sie wissen, wer sich in Ihrer Zugriffsgruppe befindet. Um einen reibungslosen Übergang zu gewährleisten, kann Ihr Unternehmen zunächst eine kurze Frist für die Verarbeitung bestehender gemeinsam genutzter und verschlüsselter Dateien einräumen. Nach Ablauf der Übergangsfrist können die Mitglieder Ihrer Zugriffsgruppe alle freigegebenen, verschlüsselten Dateien, die Sie erstellt haben, einsehen. Sie können Personen außerhalb Ihrer Zugriffsgruppe Zugang gewähren.

Identifizieren Sie die Personen in Ihrer Zugriffsgruppe

Ihr Administrator wird Sie darüber informieren, wer sich in einer oder mehreren Ihrer Zugriffsgruppen befindet, je nachdem, wer Zugriff auf bestimmte Dateien benötigt. Drunter fallen interne und externe Benutzer. Wenn Sie mit bestimmten Benutzern an sensiblen Daten arbeiten, können Sie Ihren Administrator bitten, eine Zugriffsgruppe für diesen Inhalt zu erstellen.

Verwenden Sie eine Übergangszeit, um freigegebene, verschlüsselte Dateien zu verarbeiten

Wenn Sie Data Guardian bereits installiert haben und bestehende Dateien verschlüsselt sind, ist die beste Vorgehensweise für Ihr Unternehmen eine kurze Übergangszeit für die verschlüsselten Dateien, die freigegeben wurden. Um einen reibungslosen Übergang zu ermöglichen, beachten Sie Folgendes für freigegebene, verschlüsselte Dateien:

- Der Eigentümer oder Autor der Datei, ob intern oder extern, hat weiterhin Zugriff auf die Datei.
- Interne oder externe Benutzer innerhalb Ihrer Zugriffsgruppe haben Zugriff auf die meisten freigegebenen Dateien. Basierend auf dem Typ des Schlüssels, der einigen Dateien zugeordnet ist, kann der Zugriff auf einige verloren gehen.
- Interne Benutzer außerhalb Ihrer Zugriffsgruppe - Benutzer sollten während der Übergangszeit alle freigegebenen Dateien öffnen, um Zugriff auf den Schlüssel zu erhalten. Wenn sie in dieser kurzen Zeitspanne keine gemeinsame, verschlüsselte Datei öffnen, verlieren sie den Zugriff auf die Datei.
- Externe Benutzer, die nicht zu Ihrer Zugriffsgruppe gehören - Wenn Sie bereits Zugang zu einer verschlüsselten Datei gewährt haben, hat der externe Benutzer auch nach der Übergangszeit weiterhin Zugriff.

Wenn Sie den Zugriff auf eine Datei nach der Übergangszeit verlieren, können Sie den Zugriff vom Eigentümer anfordern.

Erneuter Zugriff auf freigegebene, verschlüsselte Dateien nach Ablauf der Übergangsfrist

Für Windows und Mac im erzwungenen geschützten Modus können Sie die folgenden Schritte ausführen, um den Zugriff wiederzuerlangen:

- Geschützte Office-Dokumente – Ein Dialogfeld fordert Sie zu einer Zugriffsanforderung auf und der Eigentümer der Datei kann entscheiden, ob er den Zugriff gewähren möchte.
- Zusätzliche Dateitypen, die über einfachen Dateischutz verschlüsselt werden – keine Eingabeaufforderung nach der Freigabe vorhanden. Der Benutzer muss den Eigentümer der Datei kennen und mit der rechten Maustaste auf die verschlüsselte Datei klicken, um die Schlüssel-ID auf der Registerkarte „Data Guardian“ zu finden. Der Benutzer kann diese Informationen an den Eigentümer senden und den Zugriff anfordern.

Zusammenarbeit bei neu erstellten Dateien nach der Übergangszeit

Für neue Dateien, die Sie nach der Übergangszeit erstellen und verschlüsseln:

- Interne oder externe Benutzer innerhalb Ihrer Zugriffsgruppe - Haben Zugriff auf alle freigegebenen, verschlüsselten Dateien.
  - Jeder, der aus der Zugriffsgruppe entfernt wird, verliert den Zugriff.
  - Wenn der Eigentümer einer Datei aus der Gruppe entfernt wird, haben andere Benutzer weiterhin Zugriff.
- Interne oder externe Benutzer außerhalb Ihrer Zugriffsgruppe - Können keine verschlüsselte Datei anzeigen.
  - Ein interner Benutzer innerhalb der Zugriffsgruppe kann Zugriff gewähren.
  - Wenn ein externer Benutzer Eigentümer einer verschlüsselten Datei ist, kann er einer anderen Person Zugriff gewähren.
  - Wenn ein interner oder externer Benutzer außerhalb der Gruppe eine verschlüsselte Datei erhält und versucht, sie zu öffnen, fordert sie ein Dialog dazu auf, Zugriff zu beantragen.

Identifier	**GUID-BDD3EF46-A9A1-48C2-BB76-B9D874BC37E4**
Status	**In Translation**

Das Unternehmen setzt bislang weder Data Guardian noch den Abonnementmodus ein

Wenn Ihr Unternehmen plant, Data Guardian mit Zugriffsgruppen zu verwenden, um die Sicherheit für sensible Daten zu erhöhen, ist es am besten, alle Dateien zu identifizieren, die Sie mit internen oder externen Benutzern teilen, und herauszufinden, ob diese Benutzer in einer Zugriffsgruppe sind, die Ihr Administrator für Sie erstellt. Um einen reibungslosen Übergang zu gewährleisten, kann Ihr Unternehmen zunächst eine kurze Frist für die Verarbeitung bestehender gemeinsam genutzter Dateien einräumen. Nach Ablauf der Übergangsfrist können die Mitglieder Ihrer Zugriffsgruppe alle freigegebenen, verschlüsselten Dateien, die Sie erstellt haben, einsehen. Sie können Personen außerhalb Ihrer Zugriffsgruppe Zugriff gewähren, so dass Sie mit ihnen zusammenarbeiten können, aber eine höhere Sicherheit haben.

Identifizieren Sie die Personen in Ihrer Zugriffsgruppe

Ihr Administrator wird Sie darüber informieren, wer sich in einer oder mehreren Ihrer Zugriffsgruppen befindet, je nachdem, wer Zugriff auf bestimmte Dateien benötigt. Drunter fallen interne und externe Benutzer. Wenn Sie mit bestimmten Benutzern an sensiblen Daten arbeiten, können Sie Ihren Administrator bitten, eine Zugriffsgruppe für diesen Inhalt zu erstellen.

Verwenden Sie eine Übergangszeit verschlüsselte Dateien zu verarbeiten

Wenn Data Guardian installiert ist, findet ein Suchvorgang auf Windows oder Mac statt und verschlüsselt die folgenden Dateien, wenn Ihr Administrator eine Richtlinie für sie aktiviert hat.

- Zusätzliche Dateitypen, wie z.B..txt oder.png, die für den Basis-Dateischutz konfiguriert sind.
- Daten-Klassifizierungsdateien (Windows)
- TITUS-Klassifizierungsdateien (Windows)

Wenn Sie bereits an Dateien zusammenarbeiten oder sie mit internen oder externen Benutzern teilen, gehören diese Benutzer möglicherweise zu Ihrer Zugriffsgruppe oder nicht. Die beste Vorgehensweise für einen reibungslosen Übergang ist eine kurze Übergangszeit, um eine der verschlüsselten Dateien zu verarbeiten, die mit anderen Benutzern geteilt werden. Während dieser Übergangszeit müssen Sie sich an Ihrem Computer anmelden.

Beachten Sie die folgenden Punkte, wenn Sie die Freigabe oder Zusammenarbeit an diesen Dateien fortsetzen möchten:

- Bei den oben aufgeführten, gemeinsam genutzten Dateien wird die erste Person, die sich einloggt und ihren Computer reinigen lässt, zum Eigentümer aller gemeinsam genutzten Dateien.
- Wenn eine andere Person Eigentümer der Datei wird und der ursprüngliche Autor nicht in seiner Zugriffsgruppe ist, muss der ursprüngliche Eigentümer den Zugriff vom neuen Eigentümer verlangen. Der ursprüngliche Eigentümer kann auch verlangen, dass der Administrator den Eigentümer wechselt.
- Computer externer Benutzer werden nicht bereinigt, so dass Kopien von ungeschützten freigegebenen Dateien nicht bereinigt und verschlüsselt werden.
- Wenn die Cloud-Verschlüsselung von Data Guardian aktiviert ist und Benutzer Ordner oder Dateien auf einem Cloud-Speicheranbieter freigeben, werden diese Dateien ebenfalls gelöscht.

Zusammenarbeit bei neu erstellten Dateien nach der Übergangszeit

Für neue Dateien, die Sie nach der Übergangszeit erstellen und verschlüsseln:

- Interne oder externe Benutzer innerhalb Ihrer Zugriffsgruppe - Haben Zugriff auf alle freigegebenen, verschlüsselten Dateien.
  - Jeder, der aus der Zugriffsgruppe entfernt wird, verliert den Zugriff.
  - Wenn der Eigentümer einer Datei aus der Gruppe entfernt wird, haben andere Benutzer weiterhin Zugriff.
- Interne oder externe Benutzer außerhalb Ihrer Zugriffsgruppe - Können keine verschlüsselte Datei anzeigen.
  - Ein interner Benutzer innerhalb der Zugriffsgruppe kann Zugriff gewähren.
  - Wenn ein externer Benutzer Eigentümer einer verschlüsselten Datei ist, kann er einer anderen Person Zugriff gewähren.
  - Wenn ein interner oder externer Benutzer außerhalb der Gruppe eine verschlüsselte Datei erhält und versucht, sie zu öffnen, fordert sie ein Dialog dazu auf, Zugriff zu beantragen.

Identifier	**GUID-16B7D77E-57D2-47D9-B2CC-39DB65B223E2**
Status	**In Translation**

Das Unternehmen setzt bislang weder Data Guardian noch den erzwungenen geschützten Modus ein

Wenn Ihr Unternehmen plant, Data Guardian mit Zugriffsgruppen zu verwenden, um die Sicherheit für sensible Daten zu erhöhen, ist es am besten, alle Dateien zu identifizieren, die Sie mit internen oder externen Benutzern teilen, und herauszufinden, ob diese Benutzer in einer Zugriffsgruppe sind, die Ihr Administrator für Sie erstellt. Um einen reibungslosen Übergang zu gewährleisten, kann Ihr Unternehmen zunächst eine kurze Frist für die Verarbeitung bestehender gemeinsam genutzter Dateien einräumen. Nach Ablauf der Übergangsfrist können die Mitglieder Ihrer Zugriffsgruppe alle freigegebenen, verschlüsselten Dateien, die Sie erstellt haben, einsehen. Sie können Personen außerhalb Ihrer Zugriffsgruppe Zugriff gewähren, so dass Sie mit ihnen zusammenarbeiten können, aber eine höhere Sicherheit haben.

Identifizieren Sie die Personen in Ihrer Zugriffsgruppe

Ihr Administrator wird Sie darüber informieren, wer sich in einer oder mehreren Ihrer Zugriffsgruppen befindet, je nachdem, wer Zugriff auf bestimmte Dateien benötigt. Drunter fallen interne und externe Benutzer. Wenn Sie mit bestimmten Benutzern an sensiblen Daten arbeiten, können Sie Ihren Administrator bitten, eine Zugriffsgruppe für diesen Inhalt zu erstellen.

Verwenden Sie eine Übergangszeit verschlüsselte Dateien zu verarbeiten

Wenn Data Guardian installiert ist, findet ein Suchvorgang auf Windows oder Mac statt und verschlüsselt die folgenden Dateien, wenn Ihr Administrator eine Richtlinie für sie aktiviert hat.

- Office-Dokumente
- PDFs
- Zusätzliche Dateitypen, wie z.B..txt oder.png, die für den Basis-Dateischutz konfiguriert sind.

Die beste Vorgehensweise für einen reibungslosen Übergang ist eine kurze Übergangszeit, um eine der verschlüsselten Dateien zu verarbeiten, die mit anderen Benutzern geteilt werden. Während dieser Übergangszeit müssen Sie sich an Ihrem Computer anmelden.

Beachten Sie die folgenden Punkte, wenn Sie die Freigabe oder Zusammenarbeit an diesen Dateien fortsetzen möchten:

- Bei den oben aufgeführten, gemeinsam genutzten Dateien wird die erste Person, die sich einloggt und ihren Computer reinigen lässt, zum Eigentümer aller gemeinsam genutzten Dateien.
- Wenn eine andere Person Eigentümer der Datei wird und der ursprüngliche Autor nicht in seiner Zugriffsgruppe ist, muss der ursprüngliche Eigentümer den Zugriff vom neuen Eigentümer verlangen. Der ursprüngliche Eigentümer kann auch verlangen, dass der Administrator den Eigentümer wechselt.
- Computer externer Benutzer werden nicht bereinigt, so dass Kopien von ungeschützten freigegebenen Dateien nicht bereinigt und verschlüsselt werden.
- Wenn die Cloud-Verschlüsselung von Data Guardian aktiviert ist und Benutzer Ordner oder Dateien auf einem Cloud-Speicheranbieter freigeben, werden diese Dateien ebenfalls gelöscht.

Zusammenarbeit bei neu erstellten Dateien nach der Übergangszeit

Für neue Dateien, die Sie nach der Übergangszeit erstellen und verschlüsseln:

- Interne oder externe Benutzer innerhalb Ihrer Zugriffsgruppe - Haben Zugriff auf alle freigegebenen, verschlüsselten Dateien.
  - Jeder, der aus der Zugriffsgruppe entfernt wird, verliert den Zugriff.
  - Wenn der Eigentümer einer Datei aus der Gruppe entfernt wird, haben andere Benutzer weiterhin Zugriff.
- Interne oder externe Benutzer außerhalb Ihrer Zugriffsgruppe - Können keine verschlüsselte Datei anzeigen.
  - Ein interner Benutzer innerhalb der Zugriffsgruppe kann Zugriff gewähren.
  - Wenn ein externer Benutzer Eigentümer einer verschlüsselten Datei ist, kann er einer anderen Person Zugriff gewähren.
  - Wenn ein interner oder externer Benutzer außerhalb der Gruppe eine verschlüsselte Datei erhält und versucht, sie zu öffnen, fordert sie ein Dialog dazu auf, Zugriff zu beantragen.

Identifier	**GUID-2627974A-3D0D-4075-81BC-86DFD31CF90B**
Status	**Translated**

Ändern des Eigentümers einer verschlüsselten Datei

Wenn während der Übergangszeit für Zugriffsgruppen ein anderer Benutzer als Eigentümer eines gemeinsamen, verschlüsselten Dokuments bezeichnet wurde, das Sie ursprünglich erstellt haben, können Sie verlangen, dass Ihr Administrator Sie als Eigentümer bezeichnet.

Identifier	GUID-0ED28BBC-3A7C-48F3-A1AE-A5039C39C392
Status	In Translation

Widerrufen des Zugriffs auf einen Schlüssel

Wenn Sie einem externen Benutzer Zugriff auf eine verschlüsselte Datei gewährt haben, verfügt der Benutzer über den Schlüssel zum Öffnen der Datei.

Wenn Sie nicht mehr möchten, dass der externe Benutzer Zugriff auf die Datei hat, können Sie optional den Administrator auffordern, den Schlüssel zu widerrufen. Dies gilt nur für externe Benutzer.

Identifier	GUID-8B76A529-19A6-4107-983B-707F5AB1D09C
Status	In Translation

Vorfreigabe von geschützten Dateien auf Windows

Data Guardian muss installiert und einer oder mehreren Zugriffsgruppen zugewiesen werden.
Wenn sich ein interner oder externer Benutzer nicht in Ihrer Zugriffsgruppe befindet, können Sie eine Vorfreigabe der geschützten Datei veranlassen.

1 Klicken Sie mit der rechten Maustaste auf eine geschützte Datei und wählen Sie **Zugriff auf geschützte Datei**.

   Auf der Benutzeroberfläche von *Freigabe von geschütztem Dateizugriff*, wird der Dokumentname unter„Ausgewählte Datei“ angezeigt.

2 Klicken Sie unter *E-Mail zur Freigabe* auf **Hinzufügen** und geben Sie die gültige E-Mail-Adresse eines externen Benutzers oder eines internen Benutzers ein, der sich nicht in Ihrer Zugriffsgruppe befindet.

   Sie können bis zu zehn einzelne Adressen gleichzeitig hinzufügen.

3 Zum Ändern einer E-Mail-Adresse klicken Sie auf **Ändern**.

4 Um eine E-Mail-Adresse zu löschen, wählen Sie einen Eintrag aus und klicken Sie auf **Löschen**.

> **ANMERKUNG:**
> Der Name des Dateiinhabers wird angezeigt und kann nicht ausgewählt oder gelöscht werden.

5 Unter „Verfügbare Gruppen“ werden Ihre Zugriffsgruppen angezeigt. Wählen Sie eine oder mehrere Gruppen aus und verwenden Sie die Pfeile, um sie zu *Freigegebene Gruppen* hinzuzufügen.

6 Klicken Sie auf **OK**. Eine Erfolgsmeldung wird angezeigt.

> **ANMERKUNG:**
> Externe Benutzer können das geschützte Dokument nicht für andere externe Benutzer freigeben.

Wenn ein externer Benutzer eine geschützte Data Guardian-Datei zum ersten Mal erhält, muss der Benutzer Data Guardian installieren oder das Webportal verwenden, um die geschützte Datei anzuzeigen.

Identifier	GUID-C67795A0-FA20-4E32-9A2B-89654D67DFB2
Status	In Translation

Vorfreigabe von geschützten Dateien auf Mac

Data Guardian muss installiert und einer oder mehreren Zugriffsgruppen zugewiesen werden.
Wenn sich ein interner oder externer Benutzer nicht in Ihrer Zugriffsgruppe befindet, können Sie eine Vorfreigabe der geschützten Datei veranlassen.

1 Klicken Sie mit der rechten Maustaste auf eine geschützte Datei und wählen Sie **Zugriff auf geschützte Datei**.

Auf der Benutzeroberfläche von *Freigabe von geschütztem Dateizugriff*, wird der Dokumentname unter„Ausgewählte Datei“ angezeigt.

2 Klicken Sie unter *E-Mail zur Freigabe* auf **Hinzufügen** und geben Sie die gültige E-Mail-Adresse eines externen Benutzers oder eines internen Benutzers ein, der sich nicht in Ihrer Zugriffsgruppe befindet.

Sie können bis zu zehn einzelne Adressen gleichzeitig hinzufügen.

3 Um eine E-Mail-Adresse zu löschen, wählen Sie einen Eintrag aus und klicken Sie auf **Löschen**.

ANMERKUNG:

Der Name des Dateiinhabers wird angezeigt und kann nicht ausgewählt oder gelöscht werden.

4 Unter „Verfügbare Gruppen“ werden Ihre Zugriffsgruppen angezeigt. Wählen Sie eine oder mehrere Gruppen aus und verwenden Sie die Pfeile, um sie zu *Freigegebene Gruppen* hinzuzufügen.

5 Klicken Sie auf **OK**. Eine Erfolgsmeldung wird angezeigt.

ANMERKUNG:

Externe Benutzer können das geschützte Dokument nicht für andere externe Benutzer freigeben.

Wenn ein externer Benutzer eine geschützte Data Guardian-Datei zum ersten Mal erhält, muss der Benutzer Data Guardian installieren oder das Webportal verwenden, um die geschützte Datei anzuzeigen.

Identifier	**GUID-FAF997A4-8E8E-4DCB-BA76-575F951F0799**
Status	**In Translation**

Vorfreigabe von geschützten Dateien auf iOS oder Android

Wenn sich ein interner oder externer Benutzer nicht in Ihrer Zugriffsgruppe befindet, können Sie eine Vorfreigabe der geschützten Datei veranlassen.

1 Tippen Sie auf eine geschützte Datei.

2

ANMERKUNG:

Auf der Registerkarte *Benutzer* wird der Name des Dateieigentümers angezeigt, er kann jedoch nicht ausgewählt oder gelöscht werden. Wenn Sie die Datei bereits mit internen oder externen Benutzern gemeinsam genutzt haben, werden deren Namen angezeigt.

3 Klicken Sie auf der Registerkarte *Benutzer* auf das Pluszeichen (+) unten rechts, um die E-Mail-Adresse eines externen Benutzers oder eines internen Benutzers hinzuzufügen, der sich nicht in Ihrer Zugriffsgruppebefindet.

4 Um eine E-Mail-Adresse zu löschen, wischen Sie mit dem Finger darüber und tippen Sie auf **Löschen**.

5 Tippen Sie auf die Registerkarte **Gruppen**, um Ihre Zugriffsgruppen anzuzeigen.

6 Tippen Sie auf eine Gruppe, um eine geschützte Datei freizugeben.

ANMERKUNG:

Ein Häkchen gibt eine Gruppe an, für die Sie die geschützte Datei freigeben möchten.

7 Tippen Sie oben rechts auf **Freigeben**.

Eine Erfolgsmeldung wird angezeigt. Externe Benutzer können das geschützte Dokument nicht für andere externe Benutzer freigeben.

Wenn ein externer Benutzer eine geschützte Data Guardian-Datei zum ersten Mal erhält, muss der Benutzer Data Guardian installieren oder das Webportal verwenden, um die geschützte Datei anzuzeigen.

Identifier	GUID-455BE40E-83D4-4C42-890C-18067EE3CFD5
Status	In Translation

Vorfreigabe von geschützten Dateien auf dem Webportal

Wenn sich ein interner oder externer Benutzer nicht in Ihrer Zugriffsgruppe befindet, können Sie eine Vorfreigabe der geschützten Datei veranlassen.

1 Laden Sie im Webportal ein geschütztes Dokument hoch.

Wenn Ihr Administrator Sie in eine oder mehrere Zugriffsgruppen aufgenommen hat, wird neben dem Download-Symbol das Symbol *Geschützter Dateizugriff* angezeigt.

2 Klicken Sie auf das Symbol **Geschützter Dateizugriff**.

Auf der Benutzeroberfläche von *Freigabe von geschütztem Dateizugriff*, wird der Dokumentname unter„Ausgewählte Datei“ angezeigt.

3 Klicken Sie unter *E-Mail zur Freigabe* auf **Neue hinzufügen**.

4 Geben Sie die gültige E-Mail-Adresse eines externen oder internen Benutzers ein, der nicht zu Ihrer Zugriffsgruppe gehört, und klicken Sie auf das Häkchen, um sie zu speichern. Sie können bis zu zehn einzelne Adressen gleichzeitig hinzufügen.

> **ANMERKUNG:**
> Zum Löschen einer E-Mail-Adresse klicken Sie auf **X**. Der Name der Person, die das Dokument freigibt, ist hervorgehoben und kann nicht ausgewählt oder gelöscht werden.

5 Unter „Verfügbare Gruppen“ werden Ihre Zugriffsgruppen angezeigt. Klicken Sie entweder auf **Alle auswählen** oder klicken Sie auf das Pfeilsymbol neben einer Option, um sie zu den *freigegebenen Gruppen* hinzuzufügen oder daraus zu entfernen.

6 Klicken Sie auf **OK**.

> **ANMERKUNG:**
> Externe Benutzer können das geschützte Dokument nicht für andere externe Benutzer freigeben.

Wenn ein externer Benutzer eine geschützte Data Guardian-Datei zum ersten Mal erhält, muss der Benutzer das Webportal installieren.

Identifier	GUID-5BE95524-98D7-476C-9790-CA2298568418
Status	In Translation

Vorfreigabe von geschützten Dateien als externer Benutzer

Data Guardian muss installiert und einer oder mehreren Zugriffsgruppen zugewiesen werden.
Wenn Sie der Urheber oder Eigentümer einer geschützten Datei sind, können Sie die Datei für einen internen Benutzer freigeben. Sie können das geschützte Dokument nicht für andere externe Benutzer freigeben. Wenn Sie die Datei nicht besitzen, können Sie sie nicht mehr freigeben.

- Die *freizugebende E-Mail* listet nicht die Namen anderer Benutzer auf, mit denen der geschützte dokumentierte gemeinsam genutzt wurde.
- Es werden keine Gruppen in den verfügbaren Gruppen angezeigt. Freigaben sind nur für Einzelpersonen möglich.

1 Klicken Sie mit der rechten Maustaste auf eine geschützte Datei und wählen Sie **Zugriff auf geschützte Datei**.

Auf der Benutzeroberfläche von *Freigabe von geschütztem Dateizugriff*, wird der Dokumentname unter„Ausgewählte Datei“ angezeigt.

2 Klicken Sie unter *E-Mail zur Freigabe* auf **Hinzufügen** und geben Sie die gültige E-Mail-Adresse eines externen Benutzers oder eines internen Benutzers ein, der sich nicht in Ihrer Zugriffsgruppe befindet.

Sie können bis zu zehn einzelne Adressen gleichzeitig hinzufügen.

3 Zum Ändern einer E-Mail-Adresse klicken Sie auf **Ändern**.

4 Um eine E-Mail-Adresse zu löschen, wählen Sie einen Eintrag aus und klicken Sie auf **Löschen**.

> **ANMERKUNG:**
> Als Eigentümer der Datei können Sie Ihren Namen nicht auswählen oder löschen.

5 Klicken Sie auf **OK**. Eine Erfolgsmeldung wird angezeigt.

Wenn ein Benutzer eine geschützte Data Guardian-Datei zum ersten Mal erhält, muss der Benutzer Data Guardian installieren oder das Webportal verwenden, um die geschützte Datei anzuzeigen.

Identifier	**GUID-F97CE528-0A49-4763-80D0-0F5937EAE934**
Status	**In Translation**

Ändern von Personen, die Zugriff auf geschützte E-Mails haben

Basierend auf den von Ihrem Administrator festgelegten Richtlinien können Sie mit der rechten Maustaste auf eine E-Mail klicken, die Sie geschützt und an Benutzer in ihrer Zugriffsgruppe gesendet haben. Sie können ändern, wer Zugriff auf diese E-Mail hat.

1 Klicken Sie in Outlook mit der rechten Maustaste auf eine E-Mail-Adresse mit der Bezeichnung [GESCHÜTZT].

2 Wählen Sie unten **Zugriff auf geschützte E-Mail** aus.
Eine Liste der Benutzer, mit denen Sie einen gemeinsamen Zugriff nutzen, wird angezeigt.

3 Entfernen Sie einzelne Benutzer, wenn diese keinen Zugriff auf die geschützte E-Mail mehr haben sollen.

Identifier	GUID-F553E0C3-FCF3-4782-8FD4-
Status	Translation Validated

Häufig gestellte Fragen

Identifier	GUID-D70F8E30-C205-474A-BC17-DB3867AE07AE
Status	In Translation

Verschiedene häufig gestellte Fragen

Frage

Frage

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

Antwort

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

Lösung

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

Identifier	GUID-36E78894-7902-4034-8BFA-6D63A1743855
Status	Translation Validated

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 im Benachrichtigungsbereich 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**.