Dell Data Guardian

Windows, Mac, Mobile und Web –
Administratorhandbuch v2.0

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.

Windows, Mac, Mobile und Web – Administratorhandbuch

2018 - 08

Rev. A01

Inhaltsverzeichnis

1

Einleitung

Für die Einhaltung und Überwachung von Gerätedetails, Shield-Details und Audit-Ereignissen, siehe Berichterstellung > Verwalten von Berichten.

Before You Begin

1 Installieren Sie den Dell Server vor der Bereitstellung von Clients. Machen Sie das richtige Handbuch ausfindig (siehe unten), folgen Sie den Anweisungen, und kehren Sie anschließend zu diesem Handbuch zurück.

- *Security Management Server Installations- und Migrationshandbuch*
- *Security Management Server Virtual Schnellanleitung und Installationshandbuch*
- Stellen Sie sicher, dass die Richtlinien wie gewünscht eingestellt sind. Durchsuchen Sie die AdminHilfe, die Sie über das **?** ganz rechts im Bildschirm aufrufen können. Die AdminHilfe ist eine seitenbezogene Hilfe, die eigens dafür entwickelt wurde, Sie bei der Einstellung und Änderung von Richtlinien zu unterstützten und mit den Optionen Ihres Dell Server vertraut zu machen.

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

3 Stellen Sie Clients für die Benutzer bereit.

Kontaktaufnahme mit dem Dell ProSupport

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

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

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

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

2

Anforderungen

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).

Data Guardian for 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.
- Der Computer muss für die Cloud-Verschlüsselung über ein zuweisbares Festplattenlaufwerk (Buchstabenwert) verfügen.
- Stellen Sie sicher, dass die Zielgeräte eine Verbindung zu https://sicherheitsservername.domäne.de:8443/cloudweb/register und https://sicherheitsservername.domäne.de:8443/cloudweb herstellen können.
- Vor der Implementierung von Data Guardian sollten auf den Zielgeräten möglichst keine Cloud-Speicher-Konten eingerichtet sein.

  Falls Endbenutzer ihre bereits vorhandenen Konten behalten möchten, ist darauf zu achten, dass sämtliche Dateien, die *unverschlüsselt* bleiben sollen, vor der Installation von Data Guardian aus dem Synchronisierungs-Client verschoben werden.
- Benutzer sollten beachten, dass ihre Computer nach Installation des Clients neu gestartet werden müssen.
- Data Guardian hat keinen Einfluss auf das Verhalten der Synchronisierungs-Clients. Aus diesem Grund sollten sich Administratoren und 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, Dropbox-Support unter https://www.dropbox.com/help oder 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.
- Bei Ausführung von Office 2010: Wenn Richtlinien zum Schutz von Office-Dokumenten und Dokumente mit aktivierten Makros eingerichtet wurden, müssen die Benutzer über Office 2010 Service Pack 1 oder höher verfügen (Ver. 14.0.6029 oder höher). Unter https://support.microsoft.com/en-us/kb/2121559 erfahren Sie, wie Sie feststellen können, ob ein Service Pack auf eine Microsoft Office 2010 Suite angewendet wurde. Ohne diese Aktualisierung kann nicht auf geschützte Dokumente zugegriffen werden. Neue Office-Dokumente sind unabhängig von der Richtlinie ungeschützt, es sei denn die Suchfunktion ist aktiviert. Die nächste Suche konvertiert Office-Dokumente in geschützte Dateien, aber die Benutzer können ohne eine unterstützte Office-Version nicht darauf zugreifen.
- Obwohl Dell Encryption nicht erforderlich ist, sollte, sofern verwendet, der Verschlüsselungs-Client Ver. 8.12 oder höher sein.
- Data Guardian unterstützt weder das Windows Systemwiederherstellungstool noch die Windows Insider Preview.
- Die Ordnerumleitung von Microsoft wird von Data Guardian nicht unterstützt.
- IPv6 wird bei Cloud-Verschlüsselung nicht unterstützt.
- Überprüfen Sie regelmäßig die Website dell.com/support, um stets über die neueste Dokumentation und die neuesten technischen Ratgeber zu verfügen.

Voraussetzungen

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

ANMERKUNG:

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

Microsoft .Net 4.5.2 (oder höher) ist für Data Guardian erforderlich. Auf allen von Dell werksseitig ausgelieferten Computern ist .Net 4.5.2 bereits vorinstalliert. Wenn Sie jedoch keine Dell Hardware verwenden oder Data Guardian auf älterer Dell Hardware aufrüsten, sollten Sie überprüfen, welche .Net-Version installiert ist und diese gegebenenfalls aktualisieren, bevor Sie 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

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

Betriebssysteme

In der folgenden Tabelle sind die unterstützten Betriebssysteme aufgeführt.

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

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) bis Version 1803 (Spring Creators Update/Redstone 4)

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.

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.

Cloud-Speicheranbieter

In der folgenden Tabelle sind Cloud-Speicheranbieter aufgeführt, die mit Data Guardian for Windows kompatibel sind. Updates zu den Cloud-Speicheranbietern werden häufig veröffentlicht. Dell empfiehlt, neue Versionen vor der Implementierung in die Produktionsumgebung zunächst mit Data Guardian zu testen.

Cloud-Speicheranbieter
• Dropbox • Dropbox für Unternehmen (nur Windows) **ANMERKUNG:** Je nach der von Ihrem Unternehmen verwendeten Dell Server-Version werden alle Dateien und Ordner in persönlichen Dropbox-Konten, die mit Geschäftskonten verknüpft sind, evtl. verschlüsselt. • Box® ist eine eingetragene Marke von Box. **ANMERKUNG:** Box Tools und Box Edit werden von Data Guardian nicht unterstützt. Die Verwendung von Box Tools kann zu einem BlueScreen-Zustand führen. • Google Drive **ANMERKUNG:** Google Sicherung und Synchronisierung werden nicht unterstützt. • OneDrive • OneDrive für Unternehmen • Unified OneDrive **ANMERKUNG:** Unified OneDrive ist ein einheitlicher Synchronisierungs-Client für OneDrive und OneDrive für Unternehmen.

Microsoft Office

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

Microsoft Office
• Office 2010 SP2 • Office 2013 SP1

Microsoft Office

- Office 2016
- Office 365 ProPlus: Deferred 1705, Semi-Annual 1708 und Monthly 1803

Data Guardian for 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
- 10 GB freier Speicherplatz

Betriebssysteme

Nachfolgend sind die unterstützten Betriebssysteme aufgeführt.

Mac-Betriebssysteme

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

Cloud-Speicheranbieter

Je nach Richtlinieneinstellungen kann Folgendes auf der Oberfläche von Data Guardian for 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
- OneDrive
- OneDrive für Unternehmen

Data Guardian for Mobile Application

Die nachfolgend aufgeführten Betriebssysteme unterstützen Data Guardian für Mobilgeräte.

Android-Betriebssysteme

- 4.4-4.4.4 KitKat
- 5.0-5.1.1 Lollipop
- 6.0–6.0.1 Marshmallow
- 7.0-7.1.2 Nougat
- 8.0-8.1 Oreo

iOS-Betriebssysteme

- iOS 9.x
- iOS 10.x-10.3
- iOS 11-11.3

Data Guardian for 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 6.0
  - 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-60/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

Virtuelle Umgebungen

- 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

Webbrowser

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

Bei einem Mac wird auch Safari unterstützt.

Sprachunterstützung

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

Sprachunterstützung

- EN: Englisch
- ES: Spanisch
- FR: Französisch
- IT: Italienisch
- DE: Deutsch
- JA: Japanisch
- KO: Koreanisch
- PT-BR: Portugiesisch, Brasilien
- PT-PT: Portugiesisch, Portugal

3

Konfiguration und Installation von Data Guardian auf Windows

Data Guardian Client – Registry-Einstellungen

In diesem Abschnitt werden alle vom Dell ProSupport genehmigten Registrierungseinstellungen für lokale Client-Computer beschrieben, unabhängig vom Grund für Registrierungseinstellung. Falls eine Registrierungeinstellung für zwei Produkte gilt, wird sie in beiden Kategorien aufgeführt.

Diese Registrierungsänderungen sollten nur von Administratoren ausgeführt werden und sind möglicherweise nicht für alle Szenarios geeignet oder funktionieren nicht in allen Szenarios.

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

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

  „LogVerbosity“=dword:0x1f (31)

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

  Mögliche Werte:

  Aus= 0x0 (0)

  Kritisch= 0x1 (1)

  Fehler= 0x3 (3)

  Warnung= 0x7 (7)

  Information= 0xf (15)

  Debuggen= 0x1f (31)

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

  DWORD-Wert: DisableAutomaticActivation=1

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

Konfiguration von Servern für Data Guardian

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

- Lokal gespeicherte Office-Dokumente, die gemeinsam mit anderen Benutzern auf verschiedene Weise genutzt oder auf einem Wechselmedium gespeichert werden. Folgende Office-Dokumente können geschützt werden: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- 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.

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

Konfiguration von Dell Security Management Server Virtual für Data Guardian

Um Dell Security Management Server Virtual zur Unterstützung von Data Guardian zu konfigurieren, setzen Sie in der Verwaltungskonsole eine oder beide Data Guardian-Richtlinien auf **Ein**:

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

Konfiguration von Dell Security Management Server für Data Guardian

Um Dell Security Management Serverzur Unterstützung von Data Guardian zu konfigurieren, setzen Sie in der Verwaltungskonsole eine oder beide Data Guardian-Richtlinien auf **Ein**:

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

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

Security Management Server so einrichten, dass Data Guardian-Downloads zugelassen werden

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

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

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

download.deviceWin.mode=remote

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

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

3 Bearbeiten Sie die Einträge wie folgt:

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

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

4 Speichern und schließen Sie die Datei.

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

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

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

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

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

Security Management Server für einen automatischen Download des Windows-Data Guardian-Client konfigurieren (optional)

Für automatische Downloads müssen die Datei „versions.xml“ und die Binärdateien sich am gleichen Speicherort befinden. Der Speicherort muss für den Client zugänglich sein, es könnte daher IIS sein, oder Sie könnten den **Security Server\Download\Cloudweb**-Ordner verwenden, den Sie erstellt haben. Bei Verwendung des cloudweb-Ordners befolgen Sie diese Beispielkonfiguration.

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

2 Erstellen Sie darunter einen Ordner mit dem Namen DataGuardianUpdate.

ANMERKUNG:

Sie können diesem Ordner auch einen anderen Namen als „DataGuardianUpdate“ geben.

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

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

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

Beispiel:

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Version: Dateiversion der aktualisierten ausführbaren Dateien

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

6 Speichern und schließen Sie die Datei.

7 Fügen Sie die Binärdateien zu diesem Ordner hinzu.

8 Wenn Sie IIS verwenden, starten Sie IIS neu.

9 Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.

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

11 Klicken Sie in der Data Guardian-Technologiegruppe auf **Cloud-Verschlüsselung** > **Erweiterte Einstellungen anzeigen**.

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

ANMERKUNG:

DataGuardianUpdate ist dabei der oben verwendete Beispielname.

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

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

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

Erneutes Abbilden eines Computers mit dem installierten Data Guardian

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

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

2 Überprüfen Sie, ob ein Ordner mit Offline-Schlüsseln vorhanden ist, bevor ein erneutes Abbild des Computers erstellt wird.

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

Exploit Guard oder EMET von Microsoft für verwaltete Anwendungen deaktivieren

In Windows 10 sind folgende Funktionen möglicherweise im Betriebssystem aktiviert oder in diesem integriert:

- Redstone 3 und höher – Windows Defender Exploit Guard (WDEG)
- Redstone 2 und niedriger – Enhanced Mitigation Experience Toolkit (EMET)

Wenn diese Funktionen aktiviert oder integriert sind, müssen Sie die Einstellungen konfigurieren, um diese verwalteten Anwendungen für Data Guardian zu deaktivieren:

- winword.exe
- powerpnt.exe
- excel.exe
- acrord32.exe

Windows Defender Exploit Guard (WDEG)

So deaktivieren Sie die verwalteten Anwendungen:

1 Navigieren Sie zum **Windows Defender Security Center**.

2 Klicken Sie auf **App- und Browsersteuerung**.

3 Scrollen Sie an das Ende des Bildschirms und klicken Sie auf **Exploit-Schutzeinstellungen**.

4 Wählen Sie **Programmeinstellungen**.

5 Klicken Sie auf **+**, um jede oben aufgeführte verwaltete Anwendung hinzuzufügen.

6 Wählen Sie in den Eigenschaften jeder verwalteten Anwendung das Kontrollkästchen *Überschreiben* für alle Optionen aus, die auf *Ein* gesetzt sind, und schalten Sie die Option dann auf **Aus**.

   ANMERKUNG:
   Wenn eine verwaltete Anwendung geöffnet ist und ein Dialogfeld angibt, dass Sie die .exe neu starten müssen, starten Sie sie nach Abschluss dieser Schritte neu.

7 Klicken Sie auf **Anwenden**.

8 Klicken Sie auf **Ja**.

   In den Programmeinstellungen führt die verwaltete Anwendung die Überschreibungen basierend auf den Optionen auf, die Sie geändert haben.

Enhanced Mitigation Experience Toolkit (EMET)

So deaktivieren Sie die verwalteten Anwendungen:

1 Navigieren Sie zur **Anwendungskonfiguration**.

2 Deaktivieren Sie in den Optionen **ROP-Anruferprüfung** und **Adressenfilter der Adressentabelle exportieren (EAF)** die Kontrollkästchen für die oben genannten verwalteten Anwendungen.

Profile für Cloud-Speicherschutz-Anbieter verwalten

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

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

Weitere Informationen finden Sie in der *AdminHelp*, auf die Sie über die Dell Server Remote Management Console zugreifen können.

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

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

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

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

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

2 Klicken Sie auf **Hinzufügen**.

3 Wählen Sie den Typ des Registrierungszugriffs aus:

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

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

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

ⓘ **ANMERKUNG: Für externe mobile Benutzer in einer gehosteten Umgebung muss die E-Mail-Adresse in Kleinbuchstaben angegeben werden.**

5 Klicken Sie auf **Hinzufügen**.

Weitere Informationen zur Verwendung der Full Access-Liste/Blacklist finden Sie in der *Administrator-Hilfe*, die über die Verwaltungskonsole zugänglich ist.

Data Guardian installieren

Es gibt zwei Möglichkeiten, Data Guardian zu installieren:

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

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

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

  oder

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

Zuvor vorhandene Ordner mit nicht verschlüsselten Dateien

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

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

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

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

  oder

  Für große Datenmengen kann ein Manager oder Administrator vorübergehend das Menü „Ordner verwalten“ anfordern.

Ordner verwalten – Menü

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

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

Je nach Server und Data Guardian Produkt gehen Sie wie folgt vor:

Dell Security Center in einer gehosteten Umgebung	On-prem (für Dell Management Server	Cloud-Verschlüsselung
Für eine zukünftige Version.	Stellen Sie sicher, dass Sie den Namen des Dell Security Management Server wissen.	Auf dem Computer muss ein Buchstabe verfügbar sein, der einem Festplattenlaufwerk zugewiesen werden kann.

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 (in der Regel **setup32.exe** oder **Setup64.exe**) und kopieren es auf den lokalen Computer.

3 Starten Sie das Installationsprogramm per Doppelklick.

4 Falls Sie eine Sicherheitswarnung erhalten, klicken Sie auf **Ausführen**.

5 Wählen Sie eine Sprache aus und klicken Sie auf **OK**.

6 Klicken Sie auf **OK**, wenn Sie zur Installation von Microsoft Visual C++ 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.

Unter C:\ sollten Sie Data Guardian niemals im Ordner „Benutzer“ oder „Windows“ oder im Stammverzeichnis eines Laufwerks installieren. Anderenfalls wird ein Fehler ausgegeben.

10 Wählen Sie **On-prem Dell Management Server**:

Dell Security Center in einer gehosteten Umgebung	On-prem Dell Management Server
Für eine zukünftige Version.	Geben Sie im Feld `Dell Management Servername` den Servernamen ein, mit dem dieser Computer kommunizieren wird, wie z. B. server.domain.com. Sie müssen www oder http(s) nicht einschließen. Diese Informationen werden von Ihrem Administrator bereitgestellt. Deaktivieren Sie das Kontrollkästchen *SSL-Trust-Prüfung aktivieren* nicht, es sei denn, Ihr Administrator fordert Sie dazu auf.

11 Klicken Sie auf **Weiter**.

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

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

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

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

Der Installationsfortschritt wird in einem Statusfenster angezeigt.

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

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

Die Installation von Data Guardian ist abgeschlossen.

17 Beauftragen Sie die Endbenutzer, die Aktivierung zu bestätigen. Das Data Guardian-Taskleistensymbol sollte ein grünes Häkchen anzeigen. Abhängig davon, wie Data Guardian innerhalb des Unternehmens bereitgestellt wird, erfolgt die Aktivierung möglicherweise nicht sofort. Ist dies nicht der Fall, muss der Endbenutzer die Aktivierung manuell durchführen. In einer gehosteten Umgebung muss ein Benutzer, der die Aktivierung manuell durchführt, jedes Mal reaktivieren, wenn er seinen Computer oder den Data Guardian-Service neu startet. Siehe hierzu *Data Guardian User Guide* (Data Guardian-Benutzerhandbuch).

Data Guardian mit der Befehlszeile installieren

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

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

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

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

Parameter
SERVER= <Servername> (Vollqualifizierter Domänenname des Dell Server zur Aktivierung)
ENTERPRISE=1 (Interner Benutzer)
ENABLESSLTRUST=0 (SSL Trust-Validierung deaktivieren)
REBOOT=SUPPRESS (Null ermöglicht automatische Neustarts, SUPPRESS deaktiviert Neustart)

Beispiel für eine Befehlszeile

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

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

Set GPO on Domain Controller to Enable Entitlements

- Wenn Sie für Ihre Clients Berechtigungen für Dell Digital Delivery festlegen möchten, folgen Sie den Anweisungen zum Einrichten eines Gruppenrichtlinienobjekts (GPO) auf dem Domänencontroller (das muss nicht der Server sein, auf dem der Dell Server ausgeführt wird), um diese Berechtigungen zu aktivieren.
- Die Workstation muss Mitglied der Organisationseinheit sein, für die das Gruppenrichtlinienobjekt angewendet wird.
- Achten Sie bitte darauf, dass der ausgehende Port 443 für die Kommunikation mit dem Dell Server verfügbar ist. Falls der Port 443 (aus irgendeinem Grund) gesperrt ist, funktioniert die Berechtigungsfunktion nicht.

1 Klicken Sie auf dem Domänencontroller, auf dem die Clients verwaltet werden sollen, auf **Start** > **Verwaltung** > **Gruppenrichtlinienverwaltung**.

2 Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, für die Sie die Richtlinie anwenden möchten, und wählen Sie **Gruppenrichtlinienobjekt in dieser Domäne erstellen** und **Hier verknüpfen** aus.

3 Geben Sie einen Namen für das neue Gruppenrichtlinienobjekt ein, wählen Sie unter „Anfangs-GPO-Quelle“ „(keine)“ aus, und klicken Sie auf **OK**.

4 Klicken Sie mit der rechten Maustaste auf das neu erstellte Gruppenrichtlinienobjekt, und wählen Sie **Bearbeiten** aus.

5 Der Group Policy Management Editor wird geladen. Rufen Sie **Computerkonfiguration** > **Einstellungen** > **Windows-Einstellungen** > **Registrierung** auf.

6 Klicken Sie mit der rechten Maustaste auf die Registrierung und wählen Sie **Neu** > **Registrierungseintrag** aus. Nehmen Sie die folgenden Einstellungen vor:

   Action: Create

   Hive: HKEY_LOCAL_MACHINE

   Key Path: SOFTWARE\Dell\Dell Data Protection

   Value name: Server

   Value type: REG_SZ

   Wertedaten: <IP-Adresse des Dell Server>

7 Klicken Sie auf **OK**.

8 Melden Sie sich von der Workstation ab und dann wieder an, oder führen Sie **gpupdate /force** aus, um die Gruppenrichtlinie zu übernehmen.

Data Guardian deinstallieren

- Wenn ein **Endbenutzer** über ein lokales Administratorkonto verfügt, kann er Data Guardian selbst deinstallieren. Weitere Informationen finden Sie im *Benutzerhandbuch* für Data Guardian. In diesem Abschnitt wird beschrieben, wie Administratoren Data Guardian deinstallieren.

> **WICHTIG: Nicht-Office Dateien auf dem DDG VDisk Virtual Drive**
> Verschieben Sie vor dem Deinstallieren von Data Guardian alle wichtigen Dateien an einen Speicherort außerhalb des DDG VDisk Virtual Drive. Wenn Data Guardian auf Endbenutzercomputern deinstalliert wird, sind die Ordner und Dateien in der Cloud verschlüsselt und nicht lesbar. Falls dieser Endbenutzer das Unternehmen verlässt und kein anderer Benutzer den Ordner oder die Datei über eine Freigabe verwendet, können die Daten nicht mehr gelesen werden; sie sind jedoch sicher (um die Dateien anzuzeigen, können Sie Data Guardian erneut installieren).
>
> Geschützte Office-Dokumente bleiben verschlüsselt, wenn Sie Data Guardian deinstallieren. Für die Entschlüsselung finden Sie im *Wiederherstellungshandbuch > Wiederherstellung von Data Guardian* weitere Informationen.

Deinstallation über die Befehlszeile

- Nach der Extraktion aus dem Master-Installationsprogramm befindet sich das Data Guardian-Client-Installationsprogramm unter **C:\Dell\DataGuardian_XXbit_setup.exe**.
- Im folgenden Beispiel wird der Data Guardian-Client im Hintergrund deinstalliert.

```
setup.exe /x /s /v" /qn"
```

Führen Sie einen Neustart durch, wenn Sie dazu aufgefordert werden.

Data Guardian mit Dropbox für Business verwenden

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

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

Richtlinie für Unternehmens- und persönliche Konten

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

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

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

Verschlüsselung	Richtlinieneinstellung	Bereitstellungsüberlegungen
Verschlüsseln Sie alle Unternehmens- und persönlichen Dateien und Ordner.	Richtlinie > Dropbox verschlüsselt persönliche Ordner > auf **Ausgewählt**eingestellt (standardmäßig)	Bevor Data Guardian bereitgestellt wird, sollten die Benutzer bereits bestehende Unternehmensdateien, die sich in Cloud-Speicher-Synchronisierungsordnern befinden, an einem Speicherort außerhalb der Synchronisierungsordner sichern. Benutzer mit persönlichen Dateien, die unverschlüsselt bleiben sollen, müssen die Dateien aus den geschäftlichen Synchronisierungsordnern entfernen oder Verlinkungen von persönlichen Konten von den Unternehmens-Synchronisierungs-Clients entfernen. Nachdem Data Guardian bereitgestellt wurde, können die Cloud-Dateien und -Ordner nur auf Computern die Data Guardian ausführen, angezeigt werden. Lesen Sie für den Fall, dass ein persönlicher Ordner versehentlich verschlüsselt wurde, den Abschnitt „Ordner eines persönlichen Kontos entschlüsseln“ im Dell Data Guardian-Benutzerhandbuch.
Verschlüsseln Sie alle Unternehmenskonten-Dateien und Ordner. Erlauben Sie, dass persönliche Kontendateien und Ordner unverschlüsselt bleiben.	Richtlinie > Dropbox verschlüsselt persönliche Ordner > auf **Nicht ausgewählt** eingestellt	Sie können die optionale Richtlinie „Meldung über das Verschlüsseln persönlicher Dropbox-Ordner“ verwenden, um eine benutzerdefinierte Meldung anzuzeigen, die die Benutzer daran erinnert, **keine** Unternehmensdateien in persönlichen Konten zu speichern, da diese Dateien nicht geschützt werden. Diese Meldung wird in den folgenden Fällen angezeigt. • Jedes mal wenn sich der Benutzer anmeldet • Wenn der Benutzer neue Dateien erstellt oder eine neue Datei oder einen neuen Ordner zu einem persönlichen Dropbox-Konto hinzufügt Wenn Sie die Richtlinie „Dropbox verschlüsselt persönliche Ordner“ für

einen Endpunkt oder eine Endpunktgruppe auf **Falsch** stellen, verbleiben alle persönliche Konten aller Benutzer dieser Endpunkte unverschlüsselt.

Unternehmens- und persönliche Ordner

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

Berichte anzeigen

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

Für die Einhaltung und Überwachung von Gerätedetails, Shield-Details und Audit-Ereignissen, siehe **Berichterstellung > Verwalten von Berichten**.

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

Data Guardian – Fehlerbehebung

Verwenden Sie den Bildschirm „Details“

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

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

Verwenden Sie den Bildschirm „Erweiterte Details“

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

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

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

  Richtlinie: Listet alle Richtliniennamen und -werte auf.

Protokolldateien anzeigen

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

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

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

Fehlerbehebung bei Problemen mit der automatischen Aktivierung

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

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

Temporäre Ordnerverwaltungsrechte gewähren

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

So stellen Sie Ordnerverwaltungsrechte bereit:

1 Klicken Sie in der Verwaltungskonsole auf **Bestückungen** > **Endpunkte**.
2 Suchen Sie oder klicken Sie auf einen Endpunkt und anschließend auf die Registerkarte **Sicherheitsrichtlinien**.
3 Wählen Sie **Cloud-Verschlüsselung** aus, und klicken Sie dann auf **Erweiterte Einstellungen anzeigen**.
4 Klicken Sie auf das Kontrollkästchen neben dem *Ordnerverwaltung aktiviert,* um die Richtlinie auszuwählen.
5 Klicken Sie auf **Speichern**.
6 Klicken Sie im linken Fensterbereich auf **Verwaltung** > **Festlegen**.
7 Geben Sie eine Anmerkung ein und klicken Sie auf **Richtlinien festlegen**.

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

So verwalten Sie Ordner am Endpunkt:

1 Erstellen Sie einen Ordner innerhalb des Synchronisierungs-Client-Ordners und fügen Sie Dateien hinzu, sodass die Dateien in der Cloud verschlüsselt werden.
2 Klicken Sie auf die Data Guardian-Taskleistensymbol und wählen Sie **Ordner verwalten** aus.

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

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

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

Häufig gestellte Fragen

Häufig gestellte Fragen zur Ordnerverwaltung

Frage

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

Antwort

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

Lösung

1 Erstellen Sie einen neuen Ordner.

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

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

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

Frage

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

Antwort

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

Lösung

Fügen Sie die Dateien zum Synchronisierungsordner hinzu.

Frage

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

Antwort

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

Lösung

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

Verschiedene Häufig gestellte Fragen

Frage

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

Antwort

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

Lösung

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

Frage

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

Antwort

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

Lösung

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

4

Konfiguration und Installation von Data Guardian auf Mac

Data Guardian für Mac ist auf die Freigabe von Dateien innerhalb von Cloud-Verschlüsselungsanbietern ausgelegt. Wenn jedoch „Geschützte Office-Dokumente“-Richtlinien für Macs aktiviert sind, gehen alle Überwachungs- und Rückverfolgbarkeitsdaten verloren, wenn die Datei vom Benutzer auf dem lokalen Mac gespeichert wird. Wenn in Ihrer Organisation eine strikte Datei-Überwachung und -Rückverfolgbarkeit benötigt wird, legen Sie die *Data Guardian-Richtlinie Mac zulassen* auf **Nicht ausgewählt** fest, um zu verhindern, dass Data Guardian auf Macs aktiviert wird.

Servertasks

Voraussetzungen

Stellen Sie Folgendes sicher, bevor Sie diese Aufgaben durchführen:

- Installieren Sie den Dell Server und die dazugehörigen Komponenten. Lesen Sie einen der folgenden Abschnitte:
  - *Security Management Server Installation and Migration Guide (Installations- und Migrationshandbuch für Security Management Server)*
  - *Security Management Server Virtual Quick Start Guide and Installation Guide (Schnellanleitung und Installationshandbuch für Security Management Server Virtual)*
- Weisen Sie in der Verwaltungskonsole eine geeignete Dell Administratorrolle zu.

Richtlinien

Per Standardeinstellung verschlüsselt Data Guardian Benutzerdateien und sendet Überprüfungsereignisse an Security Management Server Virtual. Zum Zwecke dieses Dokuments werden beide Server als „Dell Server“ bezeichnet, sofern keine konkrete Version angegeben ist (wenn z. B. bei Verwendung von Security Management Server Virtual ein anderes Verfahren notwendig ist).

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

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

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

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

Stellen Sie Folgendes sicher, bevor Sie diese Aufgaben durchführen:

- Installieren Sie den Dell Server und die dazugehörigen Komponenten. Lesen Sie einen der folgenden Abschnitte:
  - *Installations- und Migrationshandbuch für Security Management Server*
  - *Schnellanleitung und Installationshandbuch für Security Management Server Virtual*
- Weisen Sie in der Verwaltungskonsole eine geeignete Dell Administratorrolle zu.

Security Management Server

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

download.deviceWin.mode=local

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

Für die **Remote**-Installation:

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

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

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

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

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

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

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

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

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

Für die **Remote**-Installation:

download.deviceWin.mode=remote

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

3 Speichern und schließen Sie die Dateien.

4 Kopieren Sie die Dateien in den Ordner /opt/dell/server/security-server/download/cloudweb.

5 Fügen Sie die Data Guardian-Installationsprogramme zu diesem Ordner hinzu.

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

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

Full Access-Liste

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

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

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

Negativliste

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

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

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

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

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

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

2 Klicken Sie auf **Hinzufügen**.

3 Wählen Sie den Typ des Registrierungszugriffs aus:

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

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

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

5 Klicken Sie auf **Hinzufügen**.

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

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

1 Wählen Sie **Verwaltung > Schlüsselanforderungsverwaltung**.

2 Weitere Informationen erhalten Sie durch Klicken auf **?.** (Hilfe).

Client-Aufgaben

Voraussetzungen

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

Bewährte Verfahren

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

- Kontrollierte Testumgebungen für anfängliche Tests
- Stufenweise Bereitstellungen für Benutzer

Client-Installation

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

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

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

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

Upgrade von früheren Versionen von Cloud Edition

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

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

Installationsoptionen

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

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

  oder

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

Interaktive Installation

1. Für den Data Guardian-Client suchen Sie das Installationsprogramm in **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Verwenden Sie die .**pkg-** Datei in DDPSL-Explorer-0.x.x.xxxx.dmg für Installationen oder Upgrades. Sie können dafür eine skriptgesteuerte Installation, Batchdateien oder eine andere in Ihrem Unternehmen verfügbare Push-Technologie nutzen.
3. Doppelklicken Sie auf das **Dell-Data-Guardian-x.x.x**-Paket.
4. Klicken Sie auf **Weiter**.
5. Klicken Sie im Fenster „Einführung“ auf **Fortfahren**.
6. Klicken Sie im Fenster „Softwarelizenzvereinbarung“ auf **Fortfahren**.
7. Klicken Sie auf **Zustimmen**, um fortzufahren.
8. Wählen Sie im Fenster „Konfigurationstyp“ **On-prem Dell Management Server** aus.

   ANMERKUNG:
   Hosted Dell Security Center ist für eine zukünftige Version.

9. Führen Sie im Fenster „Installationstyp“ einen der folgenden Schritte aus:
   - Klicken Sie auf **Installieren** und dann fahren Sie mit Schritt 9 fort.
   - Klicken Sie auf **Speicherort ändern**.
     1. Wählen Sie im Fenster für die Zielauswahl alle Benutzer oder einzelner Benutzer aus.
     2. Klicken Sie auf **Weiter**.
     3. Klicken Sie auf **Installieren** und dann fahren Sie mit Schritt 9 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. Siehe Endbenutzer-Aktivierung.

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

13 Schließen Sie das .dmg Fenster, um den Finder zu öffnen.

Installation über die Befehlszeile

1 Laden Sie die .dmg.
2 Führen Sie eine Installation über die Befehlszeile durch, indem Sie den folgenden Installationsbefehl ausgeben:
```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```
3 Leiten Sie die Benutzer bei der Aktivierung von Data Guardian an. Siehe Endbenutzer-Aktivierung.

Endbenutzer-Aktivierung

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

1 Wählen Sie im Finder **Anwendungen** aus, und doppelklicken Sie auf **Dell Data Guardian**.
2 Wenn das Dell Server-Fenster geöffnet wird, geben Sie die Dell Server-Adresse ein und klicken Sie auf **Speichern**.
Das Fenster „Anmeldeinformationen“ wird angezeigt.
3 Geben Sie Ihre Domänen-E-Mail-Adresse und Ihr Domänenpasswort ein.
4 Klicken Sie auf **Anmelden**, um Dell Data Guardian zu aktivieren.
Nachdem die Dell Data Guardian-Anwendung geöffnet und erfolgreich aktiviert wurde, wird im linken Bereich der 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 Dell Data Guardian-Anwendung widerrufen wurde oder abgelaufen ist, ist der Name des Cloud-Speicheranbieters ausgegraut.

5 Wählen Sie den Cloud-Speicheranbieter im linken Fensterbereich aus.
Es wird ein Fenster angezeigt, in dem Sie zur Eingabe Ihrer Anmeldeinformationen aufgefordert werden. Wenn sie authentifiziert wurden, wird der Name des Cloud-Speicheranbieters aktiviert.

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

Data Guardian deinstallieren

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

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

Finder

1 Halten Sie die Taste <Option> gedrückt, und wählen Sie **Gehe zu** aus der Menüleiste aus.
2 Öffnen Sie den Ordner **~/Library/Application Support/Dell**.
3 Klicken Sie mit der rechten Maustaste auf den Ordner **DellDataGuardian** und wählen Sie **in Papierkorb verschieben** aus.
4 Öffnen Sie über **Gehe zu** in der Menüleiste den Ordner "Applications", und verschieben Sie die **Dell Data Guardian**-Anwendung in den Papierkorb.
5 Klicken Sie auf **OK**.

6 Geben Sie bei entsprechender Aufforderung das Administrator-Kennwort ein.

Terminal

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

1 Verwenden Sie diese Befehle:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Entfernen Sie den Ordner **DellDataGuardian**.

Konfiguration und Installation von Data Guardian für den Web-Client

Dieser Web-Client ermöglicht es Benutzern, ein geschütztes Office-Dokument oder eine .xen-Datei ohne vorherige Installation des Data Guardian-Clients anzuzeigen. Als allgemeine Regel empfiehlt Dell zuerst die Installation von Security Management Server oder Security Management Server Virtual.

Herunterladen der OVA-Datei

Bei der Erstinstallation wird Data-Guardian-Web als OVA-Datei bereitgestellt. Das Open Virtual Application-Format wird zur Bereitstellung von Software für die Ausführung auf virtuellen Maschinen verwendet.

So laden Sie die OVA-Datei herunter:

1 Navigieren Sie zur Produktsupportseite Data Guardian.
2 Klicken Sie auf **Treiber und Downloads**.
3 Klicken Sie zum „Anzeigen verfügbarer Aktualisierungen für <OS-Version>“ auf **OS ändern** und wählen Sie entweder **VMware ESXi 6.0** oder **VMware ESXi 5.5** aus.
4 Wählen Sie unter „Anzeige nach:“ **Alle anzeigen** aus.
5 Wählen Sie unter Dell Data Security **Herunterladen** aus.

Installation von Data Guardian for Web

Data Guardian Web installieren und konfigurieren

Stellen Sie vor Beginn sicher, dass alle Anforderungen an die Systeme und die virtuelle Umgebung erfüllt sind.

1 Suchen Sie die Data Guardian-Dateien auf dem Installationsmedium und doppelklicken Sie auf **Data-Guardian-Web-1.x.x.ova** für den Import in VMware.
2 Schalten Sie Data-Guardian-Web ein.
3 Wählen Sie die Sprache für die Lizenzvereinbarung aus und wählen Sie dann **EULA anzeigen** aus.
4 Lesen Sie die Vereinbarung durch und wählen Sie **EULA akzeptieren**.
5 Falls eine Aktualisierung verfügbar ist, klicken Sie auf **Annehmen**.
6 Wenn Sie aufgefordert werden, das Standardkennwort zu ändern, wählen Sie **Ja** aus.
7 Geben Sie auf dem Bildschirm *ddguser-Kennwort einstellen* das aktuelle (Standard-)Passwort **ddguser** und dann ein eindeutiges Kennwort ein. Wiederholen Sie es und wählen Sie **OK** aus.

   Passwörter müssen folgende Elemente enthalten:

   - Mindestens 8 Zeichen
   - Mindestens 1 Großbuchstaben
   - Mindestens 1 Ziffer
   - Mindestens 1 Sonderzeichen

8 Wiederholen Sie den vorherigen Schritt für die Konten *ddgconsole* und *ddgsupport*.

ANMERKUNG:
Um das Standardkennwort zu behalten, das das gleiche ist wie der Name, klicken Sie auf **Abbrechen**. Um das Kennwort zu ändern, geben Sie **ddgconsole** oder **ddgsupport** in das Feld „Aktuelles Kennwort“ ein.

9 Verwenden Sie im Dialogfeld *Hostname konfigurieren* die Zurücktaste, um den Standardhostnamen zu entfernen. Geben Sie einen FQDN-Hostnamen ein und wählen Sie **OK** aus.

10 Wenn Sie über mehrere Knoten und einen Load Balancer verfügen, geben Sie einen Load Balancer-Hostnamen ein.

11 Wählen Sie im Dialogfeld *Netzwerkeinstellungen konfigurieren* eine der nachstehenden Optionen aus und wählen Sie dann **OK** aus.

- (Standard) DHCP verwenden.
- (Empfohlen) Drücken Sie im Feld „DHCP verwenden“ die Leertaste, um das X zu entfernen, und geben Sie manuell die zutreffenden folgenden Adressen ein: Statische IP-Netzwerkmaske Standard-Gateway DNS-Server 1 DNS-Server 2 DNS-Server 3

ANMERKUNG:
Bei Verwendung einer statischen IP-Adresse müssen Sie auch einen Host-Eintrag auf dem DNS-Server erstellen.

12 Wenn der SCP-Bildschirm angezeigt wird, klicken Sie nicht auf OK. Sie müssen zuerst die .cer- und .key-Dateien zur Anwendung hinzufügen oder sie aus der pfx- oder .p7b-Datei der Zertifizierungsstelle extrahieren. Siehe WinSCP-Tool verwenden.

ANMERKUNG:
Wenn Sie auf OK auf dem SCP-Bildschirm klicken, bevor Sie sie extrahieren, müsse Sie Data-Guardian-Web neustarten und zu dem Dialogfeld *Konfiguration von Netzwerkeinstellungen* navigieren.

WinSCP-Tool verwenden

Unter Windows verwenden Sie Ihr ddgconsole-Konto, um die SSL-Zertifikatsdatei und die SSL-Schlüsseldatei sicher zu kopieren.

1 Unter Windows öffnen Sie das WinSCP-Tool.

2 Geben Sie auf der Seite WinSCP den Hostnamen ein.

3 Geben Sie den standardmäßigen ddgconsole-Benutzernamen und das Standardkennwort ein (oder Ihren geänderten Benutzernamen und das geänderte Kennwort).

4 Klicken Sie auf **Anmelden**.

5 Ziehen Sie das Zertifikat und den Schlüssel, die .pfx-Datei oder die .p7b-Datei von Ihrem lokalen Laufwerk in das Verzeichnis **opt/dell/files**.

6 Wenn Sie eine .pfx-Datei oder .p7b-Datei hinzugefügt haben, geben Sie ein Kennwort ein, wenn Sie dazu aufgefordert werden. Das Zertifikat und der Schlüssel werden aus der Zertifizierungsstelle extrahiert und zu **apache2/ssl/folder** hinzugefügt.

Anstatt die .pfx- oder .p7b-Datei zu ziehen, können Sie das Zertifikat manuell extrahieren. Hier ist Beispielcode:

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
```

Hier ist Beispielcode zum Extrahieren des privaten Schlüssels aus PFX-Datei:

```
openssl pkcs12 -in domain.pfx -nocerts -nodes -out domain.key
```

7 Kehren Sie zum SCP-Bildschirm der Administration Console zurück.

Administration Console

Gehen Sie auf dem SCP-Bildschirm der Administration Console wie folgt vor:

1 Klicken Sie auf **OK**. Der Bildschirm *Apache2 Reverse Proxy Zertifikatinstallation* wird geöffnet und führt das Zertifikat auf.

2 Wählen Sie ein Zertifikat aus und drücken Sie die **Eingabetaste**.

3 Führen Sie einen der folgenden Schritte aus:

- Wenn Sie einen Schlüssel im WinSCP-Tool hinzugefügt haben, wählen Sie den Schlüssel auf dem nächsten Bildschirm aus und drücken Sie die **Eingabetaste**.

- Wenn Sie ein Kennwort im WinSCP-Tool für eine .pfx-Datei oder .p7b-Datei eingegeben haben, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden, und klicken Sie auf **OK**.

4 Geben Sie auf dem Bildschirm zur Festlegung des Dell Server den Hostnamen Ihres Servers ein und klicken Sie auf **OK**. Ein Dialogfeld mit URL wird angezeigt, die bei der Bereitstellung zu verwenden ist. Die URL hat das Format: **https://node.domain.com/edap-admin-ui/provision_node**.

ANMERKUNG:

node.domain.com ist der Name, den Sie unter *Hostnamen konfigurieren* eingegeben haben. Die URL führt Sie zu diesem Knoten.

5 Öffnen Sie einen Browser und geben Sie die URL ein.

6 Wenn sich die Seite zur Bereitstellung des Dell Data Guardian-Knotens öffnet, klicken Sie auf **Bereitstellung des Knotens starten**.

7 Geben Sie auf der Anmeldeseite die E-Mail-Adresse und das Kennwort Ihrer Domain ein und klicken Sie auf **Anmelden**. Das Dialogfeld des Dell Data Guardian gibt an, dass die Bereitstellung erfolgreich war.

8 Kehren Sie zum Bildschirm der Administration Console zurück, auf dem Ihre URL aufgeführt wird, und klicken Sie auf **OK**. Der Anwendungsserver wird neu gestartet und das Administration Console > Hauptmenü wird geöffnet.

Zusätzliche Aufgaben:

- Stellen Sie die URL den internen Benutzern zur Verfügung, damit sie Zugang zum Data Guardian-Web-Client erhalten.
  - Für einen Einzelknoten ist die URL in diesem Format: **https://nodename/**, wobei der Knotenname den eingegebenen Hostnamen unter *Hostnamen konfigurieren* reflektiert.
  - Für mehrere Knoten ist die URL in diesem Format: **https://loadBalancerName/**, wobei der Knotenname den eingegebenen Hostnamen des Load Balancer unter *Hostnamen konfigurieren* reflektiert.
- Für den künftigen Zugriff auf den Server für Aktualisierungen dieser VM oder zur Überprüfung der Protokolle müssen Sie SSH für diese VM aktivieren. Wählen Sie **Grundlegende Konfiguration > SSH-Einstellungen** zur Aktivierung von SSH für einen ddgsupport-Benutzer.
- In der Verwaltungskonsole müssen Sie das Gerät neu starten, wenn Sie Richtlinien von Knoten-basierten Webportalen ändern. Siehe hierzu Neustart des Geräts. Nach dem Neustart müssen Sie sich mit Ihren ddguser-Anmeldeinformationen anmelden.

Öffnen der Verwaltungskonsole

Öffnen Sie die Verwaltungskonsole unter https://server.domain.com:8443/webui/.

Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

Für den Zugriff auf die Verwaltungskonsole werden die folgenden Web-Browser unterstützt:

- Internet Explorer 11.x oder höher
- Internet Explorer 41.x oder höher
- Google Chrome 46.x oder höher
- Safari

Data Guardian – Grundlegende Terminal-Konfigurationsaufgaben

Die grundlegenden Konfigurationsaufgaben werden über das Hauptmenü aufgerufen.

Hostnamen ändern

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von ist nicht erforderlich.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Hostname** aus.

2 Verwenden Sie die Zurück-Taste, um den bestehenden Data-Guardian-Web-Hostnamen zu entfernen, ersetzen Sie ihn durch einen neuen Hostnamen und wählen Sie **OK**.

Ändern der Netzwerkeinstellungen

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von ist nicht erforderlich.

1 Wählen Sie aus dem Menü *Grundkonfiguration* das **Netzwerk** aus.

2 Wählen Sie auf dem Bildschirm *Netzwerkeinstellungen konfigurieren* eine der nachstehenden Optionen aus und wählen Sie dann **OK** aus.

- (Standard) DHCP verwenden (IPv4).
- (Empfohlen) Drücken Sie in „DHCP verwenden“ die Leertaste, um das X zu entfernen, und geben Sie manuell die zutreffenden folgenden Adressen ein:

  Statische IP-Adresse

  Netzwerkmaske

  Standard-Gateway

  DNS-Server 1

  DNS-Server 2

  DNS-Server 3

  Für eine statische Konfiguration kann entweder IPv6 oder IPv4 gewählt werden.

ANMERKUNG:
Bei Verwendung einer statischen IP-Adresse müssen Sie einen Host-Eintrag auf dem DNS-Server erstellen.

Benutzerkennwörter ändern

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von ist nicht erforderlich.

Sie können die Passwörter für die folgenden Benutzer ändern:

- ddguser (Terminal-Administrator) – Dieser Benutzer hat Zugriff auf das Terminal und die Menüs von Data Guardian.
- ddgconsole (Shell-Zugriff) – Dieser Benutzer hat Zugriff auf die Shell von Data Guardian. Shell-Zugriff steht für einen Netzwerkadministrator zur Verfügung, um die Netzwerkkonnektivität zu überprüfen und allfällige Probleme zu beheben.
- ddgsupport (Dell ProSupport Administrator) – Dieser Benutzer existiert nur für die Nutzung von Dell ProSupport. Sie kontrollieren das Kennwort für dieses Konto aus Sicherheitsgründen.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Benutzerpasswörter ändern** aus.

2 Wählen Sie auf dem Bildschirm *Benutzerpasswörter ändern* das zu ändernde Benutzerpasswort aus und wählen Sie dann **Eingabe** aus.

3 Geben Sie auf dem Bildschirm *Passwort einstellen* das aktuelle Passwort ein. Dann geben Sie das neue Passwort ein, wiederholen Sie es zur Bestätigung und wählen dann **OK** aus.

Passwörter müssen folgende Elemente enthalten:

- Mindestens 8 Zeichen
- Mindestens 1 Großbuchstaben
- Mindestens 1 Ziffer
- Mindestens 1 Sonderzeichen

ANMERKUNG: Um verschiedene Benutzerkonten auszuwählen, drücken Sie zum Anzeigen der Auswahlliste die Leertaste auf der Tastatur.

Aktivierung von SSH

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von ist nicht erforderlich.

Sie können SSH für die Support-Administrator Anmeldung, Shell-Zugang und die Terminal-Befehlszeilenschnittstelle aktivieren.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **SSH** aus.
2 Markieren Sie den Benutzer, für den Sie SSH aktivieren möchten und drücken Sie die Leertaste, um ein **X** einzugeben und wählen Sie **OK** aus.

Dienste starten oder beenden

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Um alle Dienste gleichzeitig hoch- oder herunterzufahren, wählen Sie aus dem Menü *Grundkonfiguration* entweder **Anwendung starten** oder **Anwendung beenden** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.

ⓘ | **ANMERKUNG: Es kann bis zu zwei Minuten dauern, bis der Serverstatus geändert wird.**

Neustart des Geräts

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Gerät neu starten** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.
3 Nach dem Neustart melden Sie sich bei Data Guardian an.

Herunterfahren des Geräts

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Scrollen Sie im Menü *Grundkonfiguration* nach unten und wählen Sie **Gerät herunterfahren** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.
3 Nach dem Neustart melden Sie sich bei Data Guardian an.

Administratoraufgaben

Terminal-Sprache einstellen oder ändern

Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie im Hauptmenü **Sprache einstellen** aus.
2 Wählen Sie mithilfe der Pfeiltasten die gewünschte Sprache aus.

Erstellen eines Systemmomentaufnahme-Protokolls

Wenn Sie ein System-Schnappschuss-Protokoll für Dell ProSupport erstellen möchten, wählen Sie aus dem Hauptmenü **Support-Tools** aus.

1 Wählen Sie im Menü *Support-Tools* **System Schnappschuss-Protokoll erstellen** aus.
2 Wenn angezeigt wird, dass die Datei erstellt wurde, wählen Sie **OK** aus.