

Dell Data Protection | Dell Data Guardian for Mac

管理者ガイド v1.2



メモ、注意、警告

① **メモ:** 製品を使いやすくするための重要な情報を説明しています。

△ **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

⚠ **警告:** 物的損害、けが、または死亡の原因となる可能性があることを示しています。

© 2017 Dell Inc. 無断転載を禁じます。Dell、EMC、およびその他の商標は、Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である場合があります。

Dell Data Protection Encryption、Endpoint Security Suite、Endpoint Security Suite Enterprise、および Dell Data Guardian のスイートのドキュメントに使用されている登録商標および商標 (Dell™、Dell のロゴ、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS®、および KACE™)は、Dell Inc. の商標です。Cylance®、CylancePROTECT、および Cylance のロゴは、米国およびその他の国における Cylance, Inc. の登録商標です。McAfee® および McAfee のロゴは、米国およびその他の国における McAfee, Inc. の商標または登録商標です。Intel ®、Pentium ®、Intel Core Inside Duo®、Itanium®、および Xeon ® は米国およびその他の国における Intel Corporation の登録商標です。Adobe®、Acrobat®、および Flash® は、Adobe Systems Incorporated の登録商標です。Authen Tec® および Eikon® は、Authen Tec の登録商標です。AMD® は、詳細設定 Micro Devices, Inc. の登録商標です。Microsoft®、Windows®、および Windows Server®、Internet Explorer®、MS-DOS®、Windows Vista®、MSN®、ActiveX®、Active Directory®、Access®、ActiveSync®、BitLocker®、BitLocker To Go®、Excel®、Hyper-V®、Silverlight®、Outlook®、PowerPoint®、Skydrive®、SQL Serve®、および Visual C++® は、米国および / またはその他の国における Microsoft Corporation の商標または登録商標です。VMware® は、米国およびその他の国における VMware, Inc. の登録商標または商標です。Box® は、Box の登録商標です。DropboxSM は、Dropbox, Inc. のサービスマークです。Google™、Android™、Google™ Chrome™、Gmail™、YouTube®、および Google™ Play は、米国およびその他の国における Google Inc. の商標または登録商標のいずれかです。Apple®、Aperture®、App StoreSM、Apple Remote Desktop™、Apple TV®、Boot Camp™、FileVault™、 iCloud®SM、iPad®、iPhone®、iPhoto®、iTunes Music Store®、Macintosh®、Safari®、および Siri® は、米国またはその他の国あるいはその両方における Apple, Inc. のサービスマーク、商標、または登録商標です。GO ID®、RSA®、および SecurID® は Dell EMC の登録商標です。EnCase™ および Guidance Software® は、Guidance Software の商標または登録商標です。Entrust® は、米国およびその他の国における Entrust®, Inc. の登録商標です。InstallShield® は、米国、中国、欧州共同体、香港、日本、台湾、および英国における Flexera Software の登録商標です。Micron® および RealSSD® は、米国およびその他の国における Micron Technology, Inc. の登録商標です。Mozilla® Firefox® は、米国およびその他の国における Mozilla Foundation の登録商標です。IOS ® は同社の商標または米国およびその他の特定の国で Cisco Systems, Inc. の登録商標であり、ライセンスに使用されます。Oracle® および Java® は、Oracle および / またはその関連会社の登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。SAMSUNG™ は、米国およびその他の国における SAMSUNG の商標です。Seagate® は、米国および / またはその他の国における Seagate Technology LLC の登録商標です。Travelstar® は、米国およびその他の国における HGST, Inc. の登録商標です。UNIX® は、The Open Group の登録商標です。VALIDITY™ は、米国およびその他の国における Validity Sensors, Inc. の商標です。VeriSign® およびその他の関連標章は、米国およびその他の国における VeriSign, Inc. またはその関連会社あるいは子会社の商標または登録商標であり、Symantec Corporation にライセンス供与されています。KVM on IP® は、Video Products の登録商標です。Yahoo!® は、Yahoo! Inc. の登録商標ですこの製品は、7-Zip プログラムの一部を使用しています。このソースコードは、7-zip.org に掲載されています。ライセンス供与は、GNU LGPL ライセンス + unRAR 制限 (7-zip.org/license.txt) の対象です。

Dell Data Guardian for Mac 管理者ガイド

2017 - 04

Rev. A01

1 Dell Data Guardian for Mac の概要	4
概要.....	4
Dell ProSupport へのお問い合わせ.....	4
2 Dell Data Guardian for Mac の要件	6
サーバー.....	6
Mac クライアントハードウェア.....	6
オペレーティングシステム.....	6
クラウドストレージプロバイダ.....	7
3 Data Guardian インストールタスク	8
前提条件.....	8
ポリシー.....	8
Dell Enterprise Server タスク.....	8
クラウドクライアントのダウンロードを許可する Security Server の設定.....	8
フルアクセスリストのユーザーの許可 / ブラックリストのユーザーの拒否.....	9
Dropbox Business チームメンバーアカウントのリモートワイブ.....	11
クライアント関連の作業.....	12
前提条件.....	12
ベストプラクティス.....	12
クライアントのインストール.....	12
4 Data Guardian のアクティブ化とユーザーエクスペリエンス	14
エンドユーザーのアクティブ化.....	14
ユーザーインタフェース.....	14
ウェブサイトでの チェックアウト オプションの回避.....	15
アプリケーションプリファレンス.....	16
Data Guardian およびクラウド同期クライアントに関するセキュリティおよびその他の考慮事項.....	17
Google Drive.....	17
OneDrive for Business.....	17
この製品に関するフィードバック.....	17
5 Data Guardian アンインストールタスク	18
前提条件.....	18
Data Guardian のアンインストール.....	18
6 用語集	19

Dell Data Guardian for Mac の概要

このガイドでは、Mac 向けクラウドクライアントソフトウェアを管理するのに必要な情報を提供します。

GUID-DC805DCF-88A3-4694-B120-B1ED63272AA5

概要

Dell Data Guardian for Mac は、クラウドベースのファイル共有システムのデータを保護します。Data Guardian を使用する Mac OS X コンピュータは、セキュアストレージ用のクラウドベースのファイル共有システムのファイルを暗号化します。

Data Guardian for Mac および Data Guardian for windows ではどちらも、もう一方で暗号化されたファイルを開くことができます。

Data Guardian for Mac は以下から構成されます。

- Data Guardian :
 - **クラウドの暗号化** - .xen ファイルとしてクラウドベースのファイル共有システム内のデータを保護します。
 - **保護されている Office 文書** - クラウド内の Office 文書 (.docx、.pptx、.xlsx、.docm、.pptm、.xlsm) を保護します。元のファイル名および拡張子を表示します。保護されている場合、ファイルは Data Guardian クライアントでのみ開くことができます。別の場所で開いた場合は、文書が保護されていることを示すカバーページが表示されます。そこには、認証済みのユーザーが暗号化されたファイルへのアクセスを要求する方法も説明されています。

クラウド暗号化のみ、または両方のポリシーグループのポリシーを設定できます。詳細については、Admin ヘルプを参照してください。

Data Guardian for Mac は、クラウド暗号化プロバイダ内でのファイル共有用に設計されています。ただし、Mac に対して「保護されている Office 文書」ポリシーが有効になっている場合、ファイルがエンドユーザーによってローカル Mac に保存されると、すべてのファイル監査およびトレサビリティは失われます。厳密なファイル監査およびトレサビリティが組織で必要な場合は、Mac Data Guardian アクティベーションの許可ポリシーを「未選択」に設定し、Data Guardian が Mac 上でアクティブ化されないようにします。

- Security Server - Data Guardian for Mac を管理するデルサーバのコンポーネントです。Security Server は、データの共有相手にかかわらず、クラウド内のデータが安全であることを確実にします。また Security Server は、機密データを伝達しないように社内デバイスを保護します。
- リモート管理コンソール - 一元化されたセキュリティポリシー管理を提供し、既存のエンタープライズディレクトリを統合して、レポートを作成します。

これらのデルコンポーネントはシームレスに相互動作し、ユーザーエクスペリエンスを損なうことなく、セキュアな環境を提供します。

GUID-B47CD81A-486F-43A5-816B-86A247C276EA

Dell ProSupport へのお問い合わせ

Dell Data Protection 製品向けの 24 時間 365 日対応電話サポート (877-459-7304、内線 431003) に電話をかけてください。

さらに、dell.com/support で Dell Data Protection 製品のオンラインサポートもご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザー、よくあるご質問 (FAQ)、および緊急の問題を取り扱っています。

米国外の電話番号については、[Dell ProSupport](#) の国際電話番号をチェックしてください。



Dell Data Guardian for Mac の要件

本章では、クライアントのハードウェアとソフトウェアの要件を説明します。導入タスクを続行する前に、導入環境が要件を満たしていることを確認してください。

① メモ:

IPv6 はサポートされていません。

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

サーバー

Data Guardian for Mac では、クライアントを Dell Enterprise Server または Dell Enterprise Server - VE、v9.6 以降に接続する必要があります。

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

Mac クライアントハードウェア

以下に Mac クライアント向けの対応ハードウェアを示します。

Mac ハードウェア

- Intel Core 2 Duo、Core i3、Core i5、Core i7、または Xeon プロセッサ
- 2 GB RAM
- 10 GB の空きディスク容量

GUID-3F5F8005-9FEE-46AE-8400-336215F15DB2

オペレーティングシステム

以下に、対応オペレーティングシステムを示します。

Mac オペレーティングシステム

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

Android オペレーティングシステム

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

iOS オペレーティングシステム

- iOS 8.x
- iOS 9.x
- iOS 10.x ~ 10.3

GUID-C4B25B4F-15E5-42AF-8493-D09F2473A534

クラウドストレージプロバイダ

Dell Data Guardian インタフェースでは、ポリシー設定に基づいて次のプロバイダを表示できます。ユーザーは、クラウド同期クライアントをダウンロード、またはインストールする必要はありません。

クラウドストレージプロバイダ

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business



Data Guardian インストールタスク

GUID-168A18C7-0D8D-43F2-9A99-08FC43099963

前提条件

これらのタスクを実行する前に、次の事柄を確認してください。

- デルサーバおよびそのコンポーネントをインストールします。次のいずれかを参照してください。
 - 『Enterprise Server インストールおよびマイグレーションガイド』
 - 『Virtual Edition Quick Start Guide and Installation Guide』(Virtual Edition クイックスタートガイドおよびインストールガイド)
- リモート管理コンソールで、適切なデル管理者役割を割り当てます。

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

ポリシー

Data Guardian はデフォルトでユーザーのファイルを暗号化して、DDP EE Server/VE Server に監査イベントを送信します。ここでは、特定のバージョンに言及する必要がない限り（たとえば、Dell Enterprise Server - VE を使用する場合は手順が異なります）、両方のサーバともデルサーバと呼びます。

監査イベントに地理位置情報データを含める場合は、Wifi を有効にする必要があります。地理位置情報と監査イベントの詳細については、AdminHelp を参照してください。

サポートされている各クラウドストレージプロバイダのデフォルト動作を変更するには、クラウドストレージプロテクションプロバイダポリシーを設定してください。企業が特定のクラウドストレージプロバイダを希望する場合は、他のプロバイダに対するこのポリシーを**ブロック**に設定してください。ポリシーについては、Dell サーバのリモート管理コンソールからアクセスできる AdminHelp を参照してください。

① メモ:

このポリシーのバイパスオプションは Windows 向けです。Mac に対してバイパスを選択すると、エンドユーザーに許可と表示されます。

GUID-EE401419-8E85-45A9-8775-2C165EE3FD80

Dell Enterprise Server タスク

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

クラウドクライアントのダウンロードを許可する Security Server の設定

DDP Enterprise Server

- 1 DDP Enterprise Server で <Security Server install dir>\webapps\cloudweb\brand\dell\resources\ に移動します。

- 2 テキストエディタで **messages.properties** ファイルを開きます。
- 3 エントリが次のようになっていることを確認します。

ローカル インストールの場合 :

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

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

リモート インストールの場合 :

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

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

- 4 ファイルを保存して閉じます。
- 5 <Security Server install dir> に移動し、Download という名前のフォルダを作成します (Security Server\Download)。
- 6 ダウンロードフォルダ内に、CloudWeb フォルダ (Security Server\Download\CloudWeb) を作成します。
- 7 Dell Data Guardian インストーラを作成したフォルダに追加します。

Virtual Edition : 異なるクラウドクライアントバージョンの手動インストール

ユーザーによる最新 Dell Data Guardian インストーラのダウンロードを許可するためのアクションは不要です。最新のインストーラは、VE Security Server に事前インストールされています。

VE Security Server 上に異なる Data Guardian インストーラのバージョンを手動でインストールするには、message.properties ファイルをアップデートします。

- 1 次の場所に移動します。
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
- 2 テキストエディタで **messages.properties** ファイルを開きます。

ローカル インストールの場合 :

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

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

リモート インストールの場合 :

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

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

- 3 ファイルを保存して閉じます。
- 4 そのファイルを /opt/dell/server/security-server/download/cloudweb にコピーします。
- 5 このフォルダに Data Guardian インストーラを追加します。

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

フルアクセスリストのユーザーの許可 / ブラックリストのユーザーの拒否

フルアクセスリストとブラックリストのエントリは、Data Guardian の使用のためにデルサーバに登録できるユーザーを決定します。

フルアクセスリスト

フルアクセスリストは、特定のユーザーまたはユーザーグループによるデルサーバへの登録と Data Guardian の利用を許可します。



外部ユーザーは、登録を許可するためにフルアクセスリストに配置する必要があります。次の例を参照して、ユーザーの登録を許可します。

ユーザータイプ	入力内容
すべての organization.com 電子メールアドレス	organization.com
特定のユーザー	jdoe@organization.com
すべての Gmail ユーザー	gmail.com

ブラックリスト

ブラックリストでは、特定のユーザーまたはユーザーグループのデルサーバへの登録と Data Guardian の利用を禁止します。ブラックリストに電子メールアドレスを入力されたユーザーは、Data Guardian に登録できないと通知するメッセージを受信します。

① メモ:

ユーザーがすでに登録されている場合、このリストはこれらのユーザーの Data Guardian の利用を禁止しません。

フルアクセスリストで承認グループのメンバーになっている特定のユーザーを除外する場合は、このブラックリストを使用することができます。さらに、ドメイン全体をブラックリストに指定できます。この指定では、そのドメインの電子メールアドレスを持つすべてのユーザーが登録できなくなります。次の例を参照して、ユーザーまたはグループによるデルサーバへの登録を禁止します。

ユーザータイプ	入力内容
すべての organization.com 電子メールアドレス	organization.com
特定のユーザーおよびその電子メールアドレス	jdoe@organization.com
すべての Gmail ユーザー	gmail.com

フルアクセスリスト / ブラックリストを変更するには、次の手順に従ってください。

- 1 リモート管理コンソールの左ペインで、**管理 > 外部ユーザー管理** とクリックします。
- 2 **追加** をクリックします。
- 3 登録アクセスタイプを選択します：

ブラックリスト - ユーザーまたはドメインの登録をブロックします。ユーザーは、保護されている Office 文書または .xen ファイルを開けません。

フルアクセスリスト - ユーザーまたはドメインの登録およびすべてのファイルアクセスを許可します。ユーザーまたはドメインがブラックリストにも含まれている場合は、アクセスは許可されません。

- 4 ドメイン / 電子メールの入力 フィールドで、ドメイン全体のアクセスを設定するためにユーザーのドメインを入力するか、そのユーザーに対するアクセスのみを設定するために電子メールアドレスを入力します。
- 5 **追加** をクリックします。

フルアクセスリスト / ブラックリストの使用の詳細については、デルサーバのリモート管理コンソールからアクセスできる *AdminHelp* を参照してください。

外部ユーザーは、保護されているファイルへのキーのため、内部ユーザーからのアクセスを要求することができます。内部ユーザーが利用できない場合は、リモート管理コンソールを使用してアクセスをへのアクセスを許可または拒否することができます。

- 1 **管理 > キー要求管理** の順に選択します。
- 2 詳細については、**?** (ヘルプ) を選択してください。

Dropbox Business チームメンバーアカウントのリモートワイプ

企業が Dropbox Business を使用している場合、チームメンバーが退職した場合などに、企業の Dropbox のチームアカウントからそのユーザーをリモートで削除することができます。チームメンバーのアカウントに関連付けられたファイルおよびフォルダが、該当のアカウントで使用されているすべてのデバイスから削除されます。これにより、当該ユーザーからこれらファイルへのアクセスが無効になります。

前提条件

① メモ:

この手順を実施する前に、企業またはその他の Dropbox Business チームメンバーが必要とする可能性があるファイルまたはフォルダのすべてを、チームメンバーアカウントからバックアップする必要があります。

Dropbox Business の管理者のみが、Dropbox Business アカウントをリモートワイプすることができます。

エンドユーザーは、Dell Data Guardian をアクティブ化し、ビジネス向け Dropbox に接続する必要があります。

リモート管理コンソールでの登録

登録する必要があるのは Dropbox Business の管理者 1 名のみです。

- 1 リモート管理コンソールの左ペインで、**管理 > Dropbox 管理** を選択します。
- 2 ビジネス向け Dropbox のページで、**登録** をクリックします。
Dropbox Business サイトがブラウザで開きます。
- 3 プロンプトが表示されたら、Dropbox Business 管理者アカウントで Dropbox にログインします。
- 4 Dell Data Guardian へのアクセスを許可するには、**許可する** をクリックします。
確認ページに、Dropbox で DDP Enterprise Server - VE への認証が許可されたことが示されます。
- 5 リモート管理コンソールで、**管理 > Dropbox 管理** に戻り、**更新** をクリックします。
管理者名が表示されます。

① メモ:

基本的に、ベストプラクティスは、登録を解除しないことです。ただし、チームメンバーをビジネス向け Dropbox チームから削除するためにビジネス向け Dropbox 管理者の権限を取り消す場合は、**登録解除** をクリックします。

チームメンバーアカウントのリモートワイプ

① メモ:

リモートワイプオプションを使用できるのは、登録済みの Dropbox Business チームメンバーアカウントのみです。リモートワイプオプションがユーザーアカウントで表示されない場合、そのユーザーは Dropbox Business アカウントに登録されていません。

- 1 リモート管理コンソールの左ペインで、**ポピュレーション > ユーザー** の順に選択します。
- 2 指定したユーザーを検索します。
- 3 **ユーザー詳細** ページにアクセスします。
- 4 コマンド列で、**リモートワイプ** をクリックします。
リモートワイプが実行されます。

① メモ:

リモートワイプを選択する前に、企業またはその他の Dropbox Business チームメンバーが必要とする可能性があるファイルまたはフォルダのすべてを、チームメンバーアカウントからバックアップする必要があります。



- 5 リモートワイブの確認画面で、**はい** をクリックします。
ユーザー詳細ページに、リモートワイブが実行される日付がリストされています。
- 6 お使いの Dropbox Business 管理者コンソールメンバー ページで、チームメンバーのリストを更新します。
ユーザーがリストから削除されます。**削除済みメンバー** タブを選択すると、削除されたメンバーを表示できます。

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

クライアント関連の作業

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

前提条件

- ターゲットデバイスが次にアクセスできることを確認します。
 - <https://yoursecurityservername.domain.com:8443/cloudweb/register>
 - <https://yoursecurityservername.domain.com:8443/cloudweb>
- インストールを実行しているユーザーが、インストールのためのローカル管理者アカウントを持っていることを確認します。
- コマンドラインを使用してインストールしている場合、ユーザーがアクティブ化を行う Dell Security Server の完全修飾ドメイン名を把握しておくようにしてください。

GUID-5A15F45E-2F97-4EB4-90CD-66CD732758AB

ベストプラクティス

導入中は、IT のベストプラクティスに従ってください。ベストプラクティスには以下が挙げられますが、これらに限定されません。

- 初期テストのために制御されたテスト環境
- ユーザーへのスタッガ化された導入

GUID-CF4B86F3-D8AF-4834-B159-8813EEA72B9D

クライアントのインストール

ホワイトリストに追加済みのユーザーは、この時点で <https://yoursecurityservername.domain.com:8443/cloudweb/register> で登録することができます。

ユーザーは登録後に、ログインして適切なクライアントをダウンロードするために <https://yoursecurityservername.domain.com:8443/cloudweb> に誘導する電子メールを受信します。

エンドユーザーは通常、<https://yoursecurityservername.domain.com:8443/cloudweb> で登録後、ユーザー自身で Mac クライアントをインストールするため、管理者の Mac クライアントのインストールはオプションです。

ただし、組織から Mac クライアントのインストールを求められる場合にはインストールすることもできます。ユーザーインターフェースを使用して、または組織で利用可能なプッシュテクノロジーを使用するコマンドラインによって Data Guardian クライアントをインストールします。エンドユーザーによる登録およびアクティブ化は、どちらも引き続き必須です。

旧バージョンの Cloud Edition からのアップグレード

企業に旧バージョンの Cloud Edition があり、Data Guardian にアップグレードする場合、旧バージョンの Cloud Edition は削除されます。



① メモ:

企業が Cloud Edition から Data Guardian にアップグレードする場合、ユーザーは Data Guardian をクラウドストレージプロバイダと再リンクする必要があります。認証の詳細については、オンラインの Dell Data Guardian ヘルプを参照してください。

インストールオプション

クライアントのインストール / アップグレードを行うには、次のいずれかを選択します。

- **インタラクティブなインストール** - これは Data Guardian for Mac をインストールする最も簡単な方法です。ただし、この方法は、1 台のコンピュータごとにクライアントをインストールする計画の場合にのみ使用してください。

または

- **コマンドラインでのインストール** - この高度なインストール方法については、管理者がコマンドラインの構文を使用して実行する必要があります。この方法は、スクリプト形式のインストール、バッチファイルの使用、または組織で利用できる任意のプッシュテクノロジーに活用できます。

インタラクティブなインストール

- 1 Data Guardian クライアントの場合、**Dell-Data-Guardian--0.x.x.xxxx.dmg** にインストーラがあります。
- 2 インストールまたはアップグレードするには、DDPSL-Explorer-0.x.x.xxxx.dmg 内の **.pkg** ファイルを使用します。これには、スクリプト形式のインストール、バッチファイル、または組織で利用できる任意のプッシュテクノロジーを使用できます。
- 3 **Dell-Data-Guardian-x.x.x** パッケージをダブルクリックします。
- 4 **続行** をクリックします。
- 5 はじめに ウィンドウで、**続行** をクリックします。
- 6 ソフトウェアライセンス契約 ウィンドウで、**続行** をクリックします。
- 7 **同意する** をクリックして続行します。
- 8 インストールの種類 ウィンドウで、次のいずれかを実行します。
 - **インストール** をクリックして、手順 9 に進みます。
 - 宛先の選択 ウィンドウで、以下のオプションを選択し、**インストールの続行** をクリックして、**手順 9** に進みます。
 - このコンピュータのすべてのユーザーにインストール
 - このユーザーにのみインストール
- 9 ダイアログにユーザーの名前とパスワードを入力し、**ソフトウェアのインストール** をクリックします。
- 10 サマリ ウィンドウで、**閉じる** をクリックします。
- 11 「**エンドユーザーのアクティブ化**」を参照してください。

① メモ:

企業が Cloud Edition から Data Guardian にアップグレードする場合、ユーザーは Data Guardian をクラウドストレージプロバイダと再リンクする必要があります。認証の詳細については、オンラインの Dell Data Guardian ヘルプを参照してください。

コマンドラインでのインストール

- 1 .dmg をマウントします。
- 2 次の installer コマンドを使用して、パッケージのコマンドラインでのインストールを実行します。

```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```
- 3 エンドユーザーに Data Guardian をアクティブ化するよう指示します。「**エンドユーザーのアクティブ化**」を参照してください。



Data Guardian のアクティブ化とユーザーエクスペリエンス

GUID-FC07AF63-06D4-4D0C-8FA3-369265AB00E2

エンドユーザーのアクティブ化

初めて Mac 上で Dell Data Guardian を開いた後で、次の手順に従います。

- 1 Finder で、**アプリケーション** を選択し、**Dell Data Guardian** をダブルクリックします。
- 2 デルサーバウィンドウが開いたら、DDP サーバアドレスを入力し、**保存** をクリックします。
資格情報 ウィンドウが開きます。
- 3 ドメイン電子メールアドレスとドメインパスワードを入力します。
- 4 **ログイン** をクリックして、Dell Data Guardian をアクティブ化します。
Dell Data Guardian アプリケーションが開き、アクティブ化が成功すると、クラウドストレージプロバイダの名前が左側のペインでアクティブ化されます。

すべてのユーザーが同じクラウドプロバイダを使用して共同作業することを企業が希望している場合、管理者は、そのプロバイダのみを有効にして、他のプロバイダが表示されないようにするポリシーを設定できます。

アクティブ化が成功しなかった場合、または Dell Data Guardian アプリケーションの認証が取り消されたか期限切れになった場合は、クラウドストレージプロバイダの名前がグレー表示されます。

- 5 左ペインでクラウドストレージプロバイダを選択します。
ウィンドウが開き、資格情報のためのプロンプトが表示されます。
- 6 認証の詳細については、オンラインの Dell Data Guardian ヘルプを参照してください。

GUID-9317238E-00E5-4F56-909D-C76F09426D53

ユーザーインターフェイス

Dell Data Guardian インタフェースは、OS X Finder のカラム表示インタフェースと似ています。各カラムは、選択されたクラウドストレージプロバイダ上の 1 つのフォルダを表します。

① メモ:

タイトルバーは、お使いのオペレーティングシステムによって異なる場合があります。

ファイルの暗号化および復号化を行うには、クラウドストレージプロバイダのウェブサイトではなく、Dell Data Guardian インタフェースを使用する必要があります。

以下は、Dell Data Guardian ウィンドウで実行できるタスクです。

- **ファイル > 新規フォルダ** - 新しいフォルダを作成します。

メモ:

Google Drive と OneDrive では共有フォルダが自動的に追加されます。ただし、OneDrive for Business でのデータ共有はサポートされていません。

- **コンテキストメニュー** - メインウィンドウで 1 つまたは複数のフォルダまたはファイルを選択します。次に、Control キーを押しながらクリック (または右クリック) して、メニューオプションを選択します。

- **ダウンロード**

- **名前の変更** - Dell Data Guardian インタフェースでファイルの名前を変更すると、Dell Data Guardian は、クラウドストレージプロバイダのウェブサイトに変更を同期します。クラウドストレージプロバイダウェブサイトでは、.xen ファイルの名前を変更しないでください。変更が同期されません。

- **削除**

メモ:

Data Guardian を使用する Google Drive には **移動 オプション** (ゴミ箱に移動) がありません。他の Data Guardian 機能と一致するように、削除 オプションのみとなります。

- **リンク解除** - Dell Data Guardian をクラウドストレージプロバイダからリンク解除するには、左側のペインでプロバイダを選択し、Ctrl キーを押しながらクリック (または右クリック) して、メニューから **リンク解除** を選択します。

ファイルとフォルダに関する追加情報 :

- Dell Data Guardian ユーザーインタフェースに表示されているフォルダにファイルおよびフォルダを追加するには、OS X Finder からドラッグするか、またはドラッグアンドドロップをサポートする他のアプリケーションからドラッグします。ファイルは、現在のポリシーに基づいて暗号化されます。
- アプリケーションでファイルを復号化して開くには、Dell Data Guardian ウィンドウでそのファイルをダブルクリックします。そのファイルが外部アプリケーションで変更された場合、変更されたファイルがそのときに暗号化されて、クラウドストレージプロバイダ上に新しいリビジョンとしてアップロードされます。
- 暗号化されていないローカル コピーを作成するには、Dell Data Guardian ウィンドウから Finder にファイルまたはフォルダをドラッグします。
- Data Guardian のクラウド暗号化では、拡張子のないファイルの編集は許可されません。これらのファイルは、読み取り専用ファイルとして扱われます。拡張子のないファイルを編集するには、クラウドストレージプロバイダウェブサイトからこのファイルをダウンロードして編集し、Dell Data Guardian インタフェースを使用してアップロードします。
- 拡張属性はクラウドにコピーされません。

GUID-12885ECF-2D63-4BD1-8719-280F247D161E

ウェブサイトでの チェックアウト オプションの回避

Data Guardian は、OneDrive for Business ウェブサイトまたは任意のクラウドストレージプロバイダウェブサイト上の **開く / チェックアウト オプション** を指定して使用するファイルを保護または暗号化しません。ファイルが開かれ、チェックアウトされている場合は、自動アップロードがブロックされるため、Dell Data Guardian インタフェースで Open コマンドを使用しないでください。

ファイルを Data Guardian を使用して保護する場合、Dell Data Guardian インタフェースを使用してファイル进行操作します。

特定のプロパティを持つファイルをクラウドストレージプロバイダウェブサイトから操作する場合は、次の手順を実行します。

- 1 Dell Data Guardian インタフェースで、ファイルを Control を押しながらクリック (またはファイルを右クリック) し、**ダウンロード** を選択します。
- 2 ファイルを選択し、編集します。
- 3 Dell Data Guardian インタフェースから、ファイルをアップロードします。



アプリケーションプリファレンス

プリファレンスを起動するには、次の手順を実行します。

- 1 Dell Data Guardian を起動します。
- 2 Dell Data Guardian メニューバーから、**プリファランス** を選択します。

① メモ:

この情報は ヘルプ アイコンからも入手できます。

以下の設定を変更できます。

- 「ドット (.)」で開始するファイルを非表示にする - デフォルトで、このボックスはオンになっており、これらのファイルが非表示になっています。非表示ファイルを表示するには、このチェックボックスのチェックを外します。

① メモ:

通常、OS X Finder ではドット区切り文字で始まるファイルは非表示になっています。

- **クラウドストレージプロバイダのリンク解除** - Data Guardian によって認証されたクラウドストレージプロバイダが表示されます。Data Guardian からクラウドストレージプロバイダを削除するには、プロバイダ名を選択して、プリファレンス ウィンドウの左下にあるマイナス (-) ボタンをクリックします。

サーバポリシー - DDP Server 管理者は、Data Guardian がファイルとフォルダをどのように管理するかを制御する次のポリシーを設定します。

- **DDP Server** - サーバの URL をリストします。
- **ポーリング間隔** - クライアントソフトウェアがポリシーアップデートのポーリングを行う間隔を分単位でリストします。
- **暗号化** - クラウドストレージウェブサイトでのフォルダおよびファイルの暗号化を許可するマスター暗号化ポリシーです。
- **拡張子のみ** または **難読化**

拡張子のみ (デフォルトのポリシー設定) は、ウェブサイトに表示するファイル名を表示します。

企業がファイルに対して追加保護を必要とする場合、このポリシーを **難読化** に設定して、クラウドウェブサイト上のファイル名を GUID 名として非表示にします。

① メモ:

ポリシーが最初に 拡張子のみ に設定されており、ユーザーがクラウドウェブサイト上にファイルを所有している場合にポリシーが 難読化 に変更されると、ウェブサイト上にある既存のファイル名は難読化されません。既存のファイル名を難読化するには、ユーザーがファイルをダウンロードし、それらを Data Guardian インタフェース経由で再度アップロードする必要があります。または、ユーザーがファイルを編集すると、難読化されたファイル名でアップロードされます。

- **保護されている Office 文書** - クラウド内の Office 文書 (.docx、.pptx、.xlsx、.docm、.pptm、.xlsm) を保護しますが、.xen 拡張子ではなく、ファイル拡張子を表示します。

このポリシーが有効になっている場合、クラウド内の Office 文書 (.docx、.pptx、.xlsx、.docm、.pptm、.xlsm) は、.xen 拡張子ではなく、ファイル拡張子を表示します。ただし、クラウド内のファイルを開くことはできません。ダウンロードした場合も同様です。開いた場合は、文書が保護されていることを示す、カバーページのみが表示されます。Data Guardian をインストールしたが、認証されていない場合、カバーページはそれを示します。

- **監査イベント** - 有効になっている場合、監査イベントをデルサーバに送信します。
- **地理位置情報** - 有効になっている場合、デルサーバに送信される監査イベントには地理位置情報データ (緯度と経度) が含まれます。
- **コールバックビーコン** - 有効になっている場合、保護されたすべての Office ファイルにコールバックビーコンを送信します。
- **コールバックビーコンの URL** - 有効になっている場合、コールバックビーコンが Office に保護されたファイルに挿入されたときに使用する URL を指定します。

- **クラウドストレージプロテクトプロバイダ** - プロバイダ名は、ポリシー設定に基づいて表示されます。オプションは、**Box / Dropbox / Google Drive / OneDrive OneDrive for Business** です。

そのクラウドストレージプロバイダにアップロードされたファイルの暗号化を有効または無効にします。次のいずれかが表示されます。

- **暗号化** - クラウドに送信されたファイルは暗号化されます。
- **許可する** - ユーザーはクラウド内のファイルにアクセスできますが、クラウドストレージプロバイダウェブサイトへ送信されたファイルは暗号化されません。
- **ブロック** - クラウドストレージプロバイダは使用不可で、現時点ではクラウドプロバイダ名がメインウィンドウに表示されないことを意味します。

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

Data Guardian およびクラウド同期クライアントに関するセキュリティおよびその他の考慮事項

GUID-ED3DC4CF-B650-4563-83F3-84FE0268BBC3

Google Drive

Data Guardian のクラウド暗号化により、クラウド内のフォルダおよびファイルが暗号化され、データを保護します。次の考慮事項に注意してください。

- **保護** に設定されている企業のセキュリティポリシーは、Google Docs と Data Guardian の併用を禁止しています。許可する に設定されている場合は、編集できます。詳細については、IT 管理者にお問い合わせください。

Google Drive には、ユーザーがドキュメントに対してリアルタイムで共同作業を行うことができる Google Docs アプリが含まれています。しかし、この共同作業は Google サーバー上で行われ、ファイルは暗号化されません。作成する Google Docs は、Google Docs クラウドストレージプロバイダフォルダに表示されますが、

そのフォルダを開くと、Data Guardian がそのドキュメントを暗号化できないことを警告するダイアログが表示されます。

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

OneDrive for Business

OneDrive for Business でのデータ共有はサポートされていません。

GUID-A6AA7EB4-EB2B-44A2-BAC2-902473A21C42

この製品に関するフィードバック

ポリシーで有効になっている場合、ユーザーは Dell Data Guardian に関するフィードバックを提供できます。このフィードバックフォームは、メニューバー、**Dell Data Protection フィードバックの提供** から利用できます。



Data Guardian アンインストールタスク

本項では、Data Guardian をアンインストールする管理者の手順について説明します。エンドユーザーがローカル管理者アカウントを持っている場合、そのユーザーは自分で Data Guardian for Mac をアンインストールできます。

GUID-0AECB4CA-AADA-41B7-A403-5D8C97FFAFD5

前提条件

アンインストールを実行するには、ローカル管理者アカウントが必要です。

GUID-C8A4F28D-6FE8-4B26-A3FB-60795DD70304

Data Guardian のアンインストール

Data Guardian を削除するには、次のいずれかを実行します。

Finder

- 1 <オプション> キーを押しながら、メニューバーから、**進む** を選択します。
- 2 **~/Library/Application Support/Dell** フォルダを開きます。
- 3 **DataGuardian** フォルダを削除します。
- 4 メニューバーの **進む** から、アプリケーションフォルダを開き、**Data Guardian** アプリケーションを削除します。

ターミナル

次のいずれか、または両方の場所に Data Guardian が存在する可能性があります。

- 1 次のいずれか、または両方のコマンドを使用してください。
 - `rm -R ~/Applications/Data\ Guardian.app`
 - `rm -R ~/Library/Application Support/Dell/DataGuardian`
- 2 **DataGuardian** フォルダを削除します。

用語集

アクティブ化 (アクティブ化済み) - コンピュータがデルサーバに登録され、少なくともポリシーの初期セットを受け取ったときにアクティブ化が実行されます。

デルサーバ - デルサーバは、コンポーネントのコレクションで構成されています。サーバ側の製品全体を指す場合は、集合的にデルサーバと呼ばれます。

リモート管理コンソール - リモート管理コンソールは、企業全体に対する導入のための管理コンソールです。リモート管理コンソールは、Dell Enterprise Server のコンポーネントの 1 つです。

Security Server - Dell Data Guardian を管理するデルサーバのコンポーネントです。Security Server は、データの共有相手にかかわらず、クラウド内のデータが安全であることを確実にします。また Security Server は、機密データを伝達しないように社内デバイスを保護します。

外部ユーザー - 組織のドメインアドレスに属さないユーザーです。

