Dell Data Guardian

Windows、Mac、モバイル、Web ユーザー ガイド v2.7

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

メモ、注意、警告

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。

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

Windows、Mac、Mobile、Web ユーザーガイド

2019 - 06

Rev. A01

目次

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

はじめに

Dell Data Guardian ユーザーガイドでは、Windows、Mac、Mobile、Web ポータルでの Data Guardian のインストールと使用について説明します。

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

概要

管理者が設定したポリシーに基づき、Data Guardian は次のようなデータを保護します。

- ローカルに保存されている、さまざまな方法で他のユーザーと共有されている、またはリムーバブルメディアに保存されている Office ドキュメント。これらの Office ドキュメント（ .docx、.pptx、.xlsx、.docm、.pptm、.xlsm、.pdf ）は保護されます。
- 基本ファイル保護 - 追加のアプリケーションとファイルタイプ（ メモ帳など ）。
- クラウドベースのファイル共有システム - Windows コンピュータまたはモバイルデバイスはクラウドストレージ用のデータを取得し、そのデータを暗号化してクラウドに暗号化データをアップロードします。

メモ:
会社が Data Guardian を Office ドキュメントのみで使用しているか、クラウドストレージのみで使用しているか、または両方使用しているかは、管理者により通知されます。また、保護できるその他のアプリケーションとファイルタイプについても、管理者から通知されます。

Data Guardian は、次のプラットフォームでお使いいただけます。

- Windows
- iOS
- Android
- Mac
- Data Guardian Web ポータル（ 管理者が設定している場合 ）

メモ:
Data Guardian は他のプラットフォームで暗号化されたファイルを開くことができます。一部のファイルは読み取り専用になる場合があります。Mac 用 Data Guardian に関するユーザー情報のほとんどは、ソフトウェア内のオンラインヘルプとして提供されています。

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

Data Guardian の暗号化オプション

会社が確立したセキュリティレベルに基づいて、管理者はポリシーを設定し、保存データと移動中のデータを保護します。管理者は、会社に適用されるポリシーを通知します。

次のリストにはいくつかの暗号化オプションの概要を説明しています。また、一部のプラットフォームについては、ポリシーを設定する場所について説明しています。

モードと Office ドキュメント

Office ドキュメントを保護するようにポリシーを設定できます。暗号化の動作は、プラットフォームとモードによって異なる場合があります。Mac の場合は、オンラインヘルプを参照してください。

モード	Office 文書
Windows および Mac のモードオプション： **オプトインモード** - 保護する Office ドキュメントを決定する際、いくつかのオプションがあります。 • **Windows** と **Mac** - **セキュアドキュメント** フォルダが、ドキュメントフォルダのルートに追加されます。この場合、ファイルを暗号化する別の方法が提供されます。 **Force-Protected モード** - 企業に高レベルのセキュリティが必要です。Data Guardian は、スイープを実行してファイルを暗号化します。 • **Windows** および **Mac** - 別のポリシーでは、**保護されていないドキュメント** フォルダをドキュメントフォルダのルートに追加できます。保護された Office ドキュメントまたは基本ファイル保護のファイル タイプをこのフォルダーに入れて復号化します。 • **Mac** - **/Users** にあるファイルを保護します。 次のプラットフォームはモードに基づきません。 • Mobile • Web ポータル	**Windows、Mac、Mobile、Web ポータルで使用される Office ドキュメント** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf - Data Guardian で保護されている場合、Adobe Acrobat Reader DC または Microsoft Word を使用して開くことができます(ネットワークからは開かない)。

Office ドキュメント - Windows

管理者は、追加の Data Guardian ポリシーを設定し、これらのオプションを使用してデータの損失を制御または防止できます。暗号化の動作は、モードによって異なる場合があります。

Windows の保護された Office ドキュメントのオプション	説明
• 保存 - Office ドキュメントが保護されている場合、新しいコンテンツを保存することができます。(**名前を付けて保存** はグレー表示になります)。 • 名前を付けて保存 (保護付き)	Windows 向けのその他の情報： • **保護されていない** Office ドキュメント - **保存**、**名前を付けて保存**、または **名前を付けて保存 (保護付き)** を選択できます。 • 保護された Office ドキュメントと保護された E メールには、赤い境界線が表示されます。

Windows の保護された Office ドキュメントのオプション	説明
• Office ドキュメントがすでに保護されている場合、**名前を付けて保存** はグレー表示になります。	
コピー/貼り付け と クリップボード	保護された Office ドキュメントをコピーして、別の保護された Office ドキュメントに貼り付けられます。保護されたドキュメントの内容を保護されていないドキュメントに貼り付けることはできません。
印刷	ポリシーに基づいて、保護された Office ドキュメントの印刷を許可（ウォーターマーク付き）したり、無効にしたりできます。
エクスポート （Windows および Office 2013 以降、Mobile）	ポリシーに基づいて、許可（ウォーターマーク付き）したり、無効にしたりすることができます。 **メモ:** ウォーターマークが設定されている場合は、Office ドキュメントをエクスポートできます。PDF をエクスポートすることはできません。
印刷 画面	ポリシーに基づいて、許可またはブロックされます。
プロセスのブロック 例：切り取りツール	会社で設定されたポリシーに基づいて、保護された Office ドキュメントが開いているときには、一部のプロセスがブロックされます。
オンスクリーンウォーターマーク	保護された Office ドキュメントが開くと、コンピュータ名とユーザー名のウォーターマークが表示されます。
TITUS 分類 （オプトインモードの Windows）	ポリシーが有効になっている場合、Office ドキュメントを右クリックして TITUS 分類を選択できます。これは、ユーザーの Office ドキュメントを保護するためのもうひとつの方法といえます。
データの分類 （オプトインモードの Windows）	ポリシーが有効になっていて、社会保障番号やクレジットカード番号などの機密情報を保護するように設定されている場合、該当データが含まれる Office ドキュメントが暗号化されます。

Office ドキュメント - Mac、Mobile、および Web ポータル

暗号化の動作は、プラットフォームとモードによって異なる場合があります。管理者が、会社に適用されるポリシーを通知します。

暗号化オプション	説明
Mac - Dell Data Guardian インタフェース	**Mac** - 保護されたドキュメントをアップロードして暗号化します。 保護されたドキュメントをダウンロードして復号化します。 保護されたドキュメントを編集した後、変更はクラウドまたはローカルのいずれかにある元のファイルに保存されます。
Mobile - Data Guardian アプリ内 • 印刷 • オンスクリーンウォーターマーク • 非表示のウォーターマーク • エクスポート	**Mobile** - 次のポリシーに基づきます。 • Data Guardian アプリ内の Office ドキュメントは保護されます。 • 保護された Office ドキュメントの印刷を許可（ウォーターマーク付き）したり、無効にしたりすることができます。 • 保護された Office ドキュメントが開くと、コンピュータ名とユーザー名のウォーターマークが表示されます。

暗号化オプション	説明
Web ポータル • オンスクリーンウォーターマーク	**Web ポータル** - 保護された / 保護されていないドキュメントをアップロードできますが、ダウンロード をクリックしたとき、アップロードしたすべてのファイルが保護対象となります。 保護された Office ドキュメントが開くと、画面にコンピュータ名とユーザー名のウォーターマークが表示されます。

追加のオプション

暗号化の動作は、プラットフォームとモードによって異なる場合があります。管理者が、会社に適用されるポリシーを通知します。

オプション	説明（オプトインと Force Protect モード）
基本的なファイルの保護 - 追加のアプリケーションやファイルタイプを保護することができます。 （Windows、Mac、Mobile、および Web ポータル） • 例：.txt または .png **メモ:** 現在、これらのファイル タイプでは、保護されていても赤い境界線は表示されません。	管理者は、暗号化するアプリケーションとファイルタイプを指定するようにポリシーを設定できます。 **Windows、Mac、Mobile** - これらのファイルはスイープされて暗号化されます。 • **Mac** - 管理者が設定したファイル拡張子の場合、*/Users* フォルダー内でこれらのファイル タイプを暗号化します。 **Web ポータル** - ポリシーに基づいて、これらのファイルは読み取り専用にするか、編集可能できます。
保護された Office ドキュメントを**外部ユーザー**と共有します （Windows、Mac、Mobile、および Web ポータル） カバー ページには、登録用のリンクと Data Guardian のインストール情報へのリンクが記載されています。	• 外部ユーザーおよび **Windows** - 保護された Office ドキュメントと.pdf ファイルに、**日付制限（禁止）**機能も追加できます。 • **Web ポータル** - 共有ファイルを Web ポータルにアップロードすることができます。Web ポータルからファイルを共有することはできませんが、ダウンロードすると共有することができます。
改ざんされたファイルまたは表紙 （Windows、Mac、Mobile、および Web）	Office ファイルの場合、Data Guardian は保護されたドキュメントをスキャンして、改ざんされているかどうかを検出できます。
アクセス グループ（オンプレミス） （Windows、Mac、Mobile、および Web ポータル）	有効にすると、アクセス グループのユーザーのみが暗号化されたファイルを表示できます。所有者が個々のファイルについて、内部および外部ユーザーにアクセス権を付与することもできれば、ユーザーがアクセス権を要求することもできます。 その他のポリシーに基づいて、[保護] とラベルが付いた Outlook E メールを右クリックし、個々のユーザーのアクセスを削除することができます。
Geofipulation（Mobile）	指定されたエリア内にいるユーザーのみが、携帯電話からファイルにアクセスできます。
Outlook 電子メールの暗号化（Windows）	ポリシーに基づいて、保護 ボタンを使用すると、電子メールと添付ファイルのコンテンツを暗号化することができます。外部ユーザーに送信する場合、カバー ページには、登録用のリンクと Data Guardian のインストール情報へのリンクが記載されます。

Hosted または オンプレミス

ユーザーが自分で Data Guardian をインストールする必要がある場合、会社に適用するオプションは管理者が指定します。

メモ:
モバイル アプリケーションの場合、Workspace ONE がインストールされていれば、シングル サインオンで Data Guardian の認証を受けることができます。

Hosted Dell Security Center	On-prem Dell Management Server
Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（ SaaS ）ソリューション。	Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。
会社がマルチテナントの場合、インストール ID は管理者が入力します。保護されたドキュメントにまだアクセスできないユーザーにカバーページが表示される場合、インストール ID に関する情報がカバーページに含まれています。	Dell Server URL の名前は管理者が入力します。
すべてのプラットフォーム - テナントが指定された期間内に支払いを行わない場合、そのテナントを一時停止できます。	

クラウド暗号化

暗号化の動作は、プラットフォームとモードによって異なる場合があります。管理者が、会社に適用されるポリシーを通知します。

プラットフォーム	説明
Mobile	「Mobile でのクラウド保護の使用」を参照してください。
Mac	オンラインヘルプを参照してください。
Web ポータル	オンラインヘルプを参照してください。
Windows	現在、クラウド サービス プロバイダーの新機能との互換性に関する問題を防止するため、Windows では Data Guardian のクラウド暗号化保護機能は無効になっています。クラウド暗号化で保護されている.xen ファイルを表示するには、Data Guardian のモバイル アプリ、Web ポータル、Mac の Data Guardian 機能を使用してください。

ポリシー設定

一部のプラットフォームには、デバイスのポリシー設定の部分的なリストが表示されます。

プラットフォーム	ポリシー設定の場所
Mac	環境設定 ペイン
Mobile	**設定** アイコン > **バージョン情報**
Web ポータル	**設定** アイコン > **バージョン情報**

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

追加サポート

本書に記載された内容以上のサポートが必要な場合は、管理者にお問い合わせください。

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

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。

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

Dell Server

Windows、Mac、モバイル用の Data Guardian には Security Management Server または Security Management Server Virtual の v9.6 以上が必要です。Data Guardian ウェブクライアントには Security Management Server または Security Management Server Virtual の v9.8 以上が必要です。ここでは、特定のバージョンに言及する必要（Security Management Server Virtual を使用する場合は手順が異なる場合など）がない限り、両方のサーバとも Dell Server と呼びます。

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

Data Guardian for Windows

- 導入中は、IT ベストプラクティスに従う必要があります。これには、初期テスト向けの管理されたテスト環境や、ユーザーへの時間差導入が含まれますが、それらに限定されるものではありません。
- インストール、アップグレード、アンインストールを実行するユーザーアカウントは、ローカルまたはドメイン管理者ユーザーである必要があります。これは、Microsoft SMS または Dell KACE などの導入ツールによって一時的に割り当てることができます。昇格された権限を持つ非管理者ユーザーはサポートされません。
- インストールまたはアンインストールを開始する前に、重要なデータをすべてバックアップします。
- インストール中は、外付け（USB）ドライブの挿入や取り外しを含め、コンピュータに変更を加えないでください。
- Data Guardian は、Microsoft Office 2016 の特定のバージョンならびに Microsoft Office 365 Business および Business Premium でサポートされます。Office 365 Business Essentials ではサポートされていません。
- Data Guardian for Windows は、Workspace ONE と互換性があります。Workspace ONE 用 Data Guardian インストーラと MSI のインストールには .msi 拡張子が付いています。
- Air Gap 環境では、Windows で Data Guardian v2.4 以降がサポートされますが、一部制限があります。現在、監査イベントおよび輸出禁止ファイルの位置情報データがサポートされていません。Web ビーコンにいくつかの設定が必要です。
- ターゲットデバイスが https://yoursecurityservername.domain.com:8443/cloudweb/register および https://yoursecurityservername.domain.com:8443/cloudweb にアクセスできることを確認します。
- Data Guardian の導入前は、ターゲットデバイスでクラウドストレージのアカウントセットアップが行われていない状態にしておくことが最善です。ユーザーが既存のアカウントを引き続き使用する場合は、Data Guardian をインストールする前に、暗号化しないままにするファイルが同期クライアントから移動されていることを確認する必要があります。
- ユーザーは、クライアントをインストールした後に、コンピュータを再起動する必要があります。
- Data Guardian は、同期クライアントの動作と競合しません。したがって、管理者とユーザーは、Data Guardian を導入する前に、これらのアプリケーションの動作を理解しておく必要があります。詳細については、Box のサポート（https://support.box.com/home）、Dropbox のサポート（https://www.dropbox.com/help）、または OneDrive のサポート（http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other）を参照してください。

- 保護された Office ドキュメントは、Data Guardian のコンパニオンソリューションである Mozy、ならびに他のクラウド製品、電子メール製品、および NFS ストレージ製品でサポートされます。
- Dell Encryption は必須ではありませんが、使用する場合は、Encryption クライアントを v8.12 以降にする必要があります。
- Data Guardian は、Windows システムの復元ツールまたは Windows インサイダープレビューをサポートしていません。
- Microsoft のフォルダリダイレクトは、Data Guardian ではサポートされません。
- 最新のマニュアルや技術アドバイザリーについて、dell.com/support を定期的に確認してください。

前提条件

.exe の前提条件

まだインストールされていなければ、インストーラーは Microsoft Visual C++ 2017 再頒布可能パッケージ（x86 および x64）をインストールします。

メモ:
Windows 7 および Windows 8.1 の場合、Windows Update でコンピュータが最新の状態になっている必要があります。詳細については、https://support.microsoft.com/ja-jp/help/2919355 および https://support.microsoft.com/ja-jp/help/2999226 を参照してください。

.msi の前提条件

Microsoft Visual Studio C++ 2017 再頒布可能パッケージ（x86 および x64）をインストールする必要があります。

メモ:
また、MSI を実行している場合、Visual Studio 2010 Tools for Office Runtime（x86 および x64）もインストールする必要があります。

全体的な前提条件

Data Guardian には、Microsoft .Net 4.5.2 以降が必要です。デルの工場から出荷されるすべてのコンピュータには、.Net 4.5.2 が事前インストールされています。ただし、Dell ハードウェア上にインストールしていない、または旧型の Dell ハードウェア上で Data Guardian をアップグレードしている場合は、インストール / アップグレード失敗を防ぐため、Data Guardian をインストールする前に、インストールされている .Net のバージョンを検証し、必要に応じてバージョンをアップデートするようにしてください。インストールされている .NET のバージョンを検証するには、インストール対象のコンピュータで http://msdn.microsoft.com/ja-jp/library/hh925568(v=vs.110).aspx に記載されている手順を実行します。Microsoft .Net Framework 4.5.2 をインストールするには、https://www.microsoft.com/en-us/download/details.aspx?id=42643 に移動してください。

ハードウェア

最小限のハードウェア要件は、オペレーティングシステムの最小要件を満たしている必要があります。次の表では、Windows クライアント向けの対応ハードウェアが詳しく説明されています。

Windows ハードウェア
• 200 MB の空きディスク容量（オペレーティングシステムに応じて異なります）
• 10/100/1000 または Wi-Fi ネットワークインタフェースカード
• TCP/IP がインストールされアクティブ化されている

オペレーティングシステム

次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 7 SP1：Enterprise、Professional、Ultimate
- Windows 8.1 Update 0 ~ 1：Enterprise Edition、Pro Edition
- Windows 10：Education、Enterprise、Pro バージョン 1703（Creators Update/Redstone 2）からバージョン 1809（October 2018 Update/Redstone 5）

メモ:
クライアントは、これらのオペレーティングシステムのいずれかを実行している必要があります。それ以外の場合はブロックされます。必要に応じて、レジストリキーを設定し、管理者がブロックを上書きできるようにします。

Redstone 4 サポートでは、オペレーティングシステムをアップグレードする前に、エージェントをアップグレードする必要があります。https://www.dell.com/support/article/us/en/04/sln307922 を参照してください。

メモ:
Data Guardian は、Microsoft の Windows Defender Exploit Guard（WDEG）（Redstone 3 以降の場合）または Enhanced Mitigation Experience Toolkit（EMET）（Redstone 2 以前の場合）に対応していません。

Windows 7 では、Data Guardian 監査イベントの位置情報ポリシーはサポートされません。

Data Guardian では、1 台のコンピュータに複数バージョンの Office がインストールされている場合はサポートされません。

Microsoft Office

Data Guardian は、次のバージョンの Office をサポートしています。ただし、インストールされている Office のバージョンは 1 つだけである必要があります。

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus：バージョン 1705、1708、1803（半期チャネル）

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

Data Guardian for Mac

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

Mac ハードウェア

- 10 GB の空きディスク容量

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

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

クラウドストレージプロバイダ

Data Guardian for Mac のインタフェースでは、ポリシー設定に基づいて以下が表示されます。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

  メモ:
  Google Backup and Sync はサポートされません。

- OneDrive
- OneDrive for Business

Microsoft Office

Data Guardian for Mac は、次のバージョンの Office をサポートしています。

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

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

Data Guardian for Mobile Application

以下に、Data Guardian for Mobile をサポートするオペレーティングシステムの一覧を示します。

Android オペレーティングシステム

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

iOS オペレーティングシステム

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

Chromebook オペレーティング システム

Chrome OS で Android アプリケーションを実行するには、Chrome OS のバージョン M53 以降が必要です。Chrome OS で Android アプリを実行できることは検証済みですが、販売代理店に選択肢を確認してください。

- https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps

Microsoft Office

Data Guardian for Mobile Application は、次のバージョンの Office で作成されたファイルを開けます。

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

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

Data Guardian for Web

Data Guardian Web クライアントを有効にするには、管理者が Web クライアントをホストする仮想マシンをセットアップして、Dell Server v9.8 以降と通信します。

次の仮想環境は、Data Guardian Web クライアントの展開に使用できます。

仮想環境

- **VMware ESXi 6.7**
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-67/index.jsp を参照してください。

- **VMware ESXi 5.5**
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-55/index.jsp を参照してください。

- **Microsoft Hyper-V**
  - SLAT（Second Level Address Translation）搭載の 64 ビット プロセッサー
  - 最小 8 GB RAM（推奨）
  - ハードウェアは Hyper-V 最小要件を満たしている必要があります
  - 詳細については、https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements を参照してください。

メモ:
これらの最小値では、1 つの Web ポータルへの同時接続数は 25 以下になります。

クラウドストレージプロバイダ

Data Guardian の Web ポータルは、ポリシー設定に基づいて、次のクラウド ストレージ プロバイダーにアクセスできます。

クラウドストレージプロバイダ

- OneDrive for Business

Microsoft Office

Data Guardian for Web は、次のバージョンの Office で作成されたファイルを開くことができます。

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

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

その他の要件

現在、Amazon Cognito のマルチファクタ認証（MFA）は、どの Data Guardian プラットフォームでもサポートされていません。

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

ウェブブラウザ

Data Guardian は、Internet Explorer、Mozilla Firefox、Google Chrome、および Microsoft Edge で使用できます。

Mac では、Safari もサポートされます。

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

Adobe Acrobat

Windows および Mac では、保護された .pdf ファイルは Adobe Acrobat Reader DC で開くことができます。

メモ:
Adobe Acrobat *Standard* DC、Adobe Acrobat *Pro* DC、および Adobe Acrobat DC はサポートされません。

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

Windows での Data Guardian のインストール/アンインストール

Data Guardian をインストールするには、コンピュータのローカル管理者である必要があります。

Data Guardian をインストールした後に、コンピュータを再起動する準備をしておきます。

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

Windows でのインストール作業の概要

この概要では、Data Guardian のインストール手順を説明します。

Data Guardian のインストール

タスク	説明	詳細
Data Guardian のインストール	次の点について確認してください。 ユーザーは Data Guardian をインストールする必要があります。 管理者がすでに Data Guardian をインストールしている場合 - 次の手順に進みます。	ユーザーのインストール：「Windows での Data Guardian のインストール」を参照してください。再起動し、次の手順に進みます。
アクティブ化状態を確認する	通知エリアで、Data Guardian アイコンに緑色のチェックマーク  が表示されているか確認します。	このアイコンに橙色の感嘆符が表示されている場合、「クラウドおよび保護された Office のアクティブ化で起こりうる問題」を参照してください。 **メモ:** Office ドキュメントを開いたときに、カバーページにインストールとアクティブ化に関する情報が表示された場合、管理者が Office ドキュメントを保護するためのポリシーを設定している可能性があります。Data Guardian がインストールされてアクティブになっていることを確認します。

Windows のオプション

タスク	説明	詳細
通知エリアのメニューを表示する	ファイル、フォルダ、およびトラブルシューティングに関する有用な情報が得られます。	Data Guardian 通知エリアメニュー項目について

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

非暗号化ファイルがある既存フォルダ

Data Guardian の導入時には、ターゲットデバイスで、クラウドストレージプロバイダのアカウントセットアップが行われていない状態にしておくことが最善です。

Data Guardian をインストールする前に、ローカルコンピュータと同期されているフォルダで、クラウドストレージプロバイダのアカウントが設定されている場合：

- クラウドと同期している既存のファイルとフォルダは、平文のままになります。
- それらの既存のフォルダにファイルを追加すると、それらのファイルも平文のままになります。
- クラウドから同期したファイルは、暗号化されます。

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

Windows への Data Guardian の対話形式によるインストール

Data Guardian をインストールするには、ローカル管理者である必要があります。ユーザーが製品をインストールする場合は、インストールメディアの場所を通知します。

作業を開始する前に

使用環境と Data Guardian 製品に応じて、次の中から必要なものを判断してください。

Hosted Dell Security Center	On-prem Dell Management Server
ホスティング環境がマルチテナントである場合、インストール ID が必要になります。	Dell Server 名がわかっていることを確認します。

Data Guardian のインストール

Data Guardian をインストールした後に、コンピュータを再起動する準備をしておきます。

1 Data Guardian のインストーラをダウンロードするには、管理者に指定された場所に移動します。
2 オペレーティングシステムに応じて、32 ビットまたは 64 ビットのいずれかを選択してローカルコンピュータにコピーします。次にインストーラ名の例を示します。
   - Hosted Dell Security Center：インストーラ名には.exe 拡張子が付いています
   - オンプレミス：インストーラ名には次の拡張子が付いています
     - .exe
     - .msi（Workspace ONE および MSI インストールの場合）
3 ファイルをダブルクリックしてインストーラを起動します。
4 セキュリティ警告が表示された場合は、**実行** をクリックします。

5 言語を選択し、**OK** をクリックします。

6 Microsoft Visual C++ 2015 再頒布可能パッケージ、または Microsoft .NET Framework 4.5.2 Client Profile をインストールするプロンプトが表示された場合は、**OK** をクリックします。

7 ようこそ 画面で **次へ** をクリックします。

8 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

9 宛先フォルダ 画面で、**次へ** をクリックして、**C:\Program Files\Dell\Data Guardian** のデフォルトの場所にインストールします。

Data Guardian は、**C:\Users**、**C:** フォルダ、またはどのドライブのルートにもインストールしないでください。

10 以下のいずれかを選択します。

Hosted Dell Security Center	On-prem Dell Management Server
Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（SaaS）ソリューション。	Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。
a **Hosted Dell Security Center** を選択します。 b （オプション）会社がマルチテナントの場合は、インストール ID を入力します。 **メモ:** 会社がマルチテナントの場合に、インストール ID を入力しなかったとしても、管理者が後からレジストリに追加することができます。 c **続行** をクリックします。 d 手順 11 に進みます。	a **On-prem Dell Management Server** を選択します。 b *Dell Management Server 名：* フィールドに、このコンピュータが通信する Dell Server 名（例：server.domain.com）を入力します。www または http（https）を含める必要はありません。この情報は管理者によって提供されます。 **メモ:** 管理者に指示されない限り、*SSL Trust* 検証の有効化 チェックボックスをクリアしないでください。 c **次へ** をクリックします。 d Dell Management Server 情報の確認画面で、Dell Server の URL アドレスが正しいことを確認します。インストーラが www または http（https）、およびポートを追加します。**次へ** をクリックします。 e 手順 11 に進みます。

11 管理タイプ ウィンドウでは、次のオプションを選択します。

- 内部使用：会社のドメイン内の電子メールアドレスを持つユーザー。

12 **インストール** をクリックしてインストールを開始します。

ステータスウィンドウにインストールの進捗状況が表示されます。

13 インストール完了 画面が表示されたら、**終了** をクリックします。

14 **はい** をクリックして再起動します。

Data Guardian のインストールが完了します。

15 ユーザーはアクティベーションを確認する必要があります。Data Guardian 通知エリア アイコンに緑色のチェックマーク  が表示されます。

メモ:

企業内で Data Guardian を導入した方法によっては、すぐにアクティブにならないことがあります。ただし、アクティベーションされない場合は、ユーザーが手動でアクティブ化する必要があります。

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

クラウドおよび保護された Office のアクティブ化で起こりうる問題

Data Guardian をインストールしたが、通知エリアの Data Guardian アイコンに緑色のチェックマーク  が表示されていない場合、クラウド暗号化、保護された Office（またはその両方）の有無に応じて次の点に注意してください。

Data Guardian オプション	起こりうる問題
保護対象 Office	• アクティブ化する前に、Data Guardian が既存の Office ドキュメントを保護モードに変換することがあります。その場合、Office ドキュメントを開いたときに、カバーページにアクティブ化する方法が表示されます。
クラウド暗号化	• クラウド同期 Web サイトへのアクセスはブロックされます。 • クラウド同期アプリケーションは、それらの Web サービスへの接続がブロックされます。 • ローカル同期フォルダは、この間は更新されません。

以下のいずれかを行ってください。

- 再起動して UPN サフィックス (user_name@domain.com など) を使用して再度ログインします。
- Data Guardian をインストールしたときに、*SSL Trust* 検証の有効化 チェックボックスを選択する必要があるかどうかを管理者に確認してください。
- コンピュータを手動でアクティブ化するよう設定する方法についてはシステム管理者にお問い合わせください。「Data Guardian のアクティブ化」を参照してください。

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

Data Guardian のアクティブ化

通常、インストールして再起動すると Data Guardian は自動的にアクティブ化します。管理者から手動でアクティブ化するよう指示された場合は、次の手順を実行します。

1 Windows にログインします。
通知エリアに、橙色の感嘆符の付いたシールドアイコンが表示されます。
2 通知エリアの **Data Guardian** アイコンをクリックして、**ユーザーのアクティブ化** を選択します。
3 お使いの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、**アクティブ化** をクリックします。
内部ユーザー(ドメイン電子メールアドレスを持っている)の場合、登録 ボタンは無視します。外部ユーザーの場合のみ、登録する必要があります。

アクティブ化が完了すると、Data Guardian 通知エリア アイコンに緑色のチェックマーク  が表示されます。
4 ユーザーモードステータスを確認してください。通知エリア アイコンをクリックし、[**詳細**] を選択します。
5 最上部でユーザーモードを確認します。
内部：会社のドメイン内の電子メールアドレスを持つユーザー。

外部：ドメイン電子メールアドレス以外のアドレスを持つユーザー。詳細については、「外部ユーザーとして Data Guardian を使用」を参照してください。

> **メモ:**
> ユーザーモードに **未登録** と表示されている場合、Data Guardian はまだアクティブになっていません。

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

Hosted Dell Security Center および一時停止されたテナント

Hosted Dell Security Center では、指定された期間内に支払いを行わないテナントを一時停止にできます（ Windows、Mac、Mobile、Web ポータル ）。

Data Guardian の内部 / 外部ユーザーには、以下が発生する場合があります。

- すべてのプラットフォーム - Data Guardian をインストール、アクティブ化、または Data Guardian にログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。
- Mac - Data Guardian が開いているときにテナントが一時停止されている場合、エクスプローラとすべてのファイルを閉じた後に一時停止されているテナントのダイアログが表示され、保護されたファイルを開こうとします。
- Web ポータル：
  - すでにログインしていて暗号化されたファイルをアップロードした場合、アップロードに失敗したことを示すメッセージが表示されます。
  - 暗号化されたファイルまたは非暗号化ファイルがアップロードされてテナントが一時停止された場合、ダウンロードに失敗したことを示すメッセージが表示されます。
  - ログアウト後に再度ログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。

管理者に連絡してください。

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

Data Guardian 通知エリアメニュー項目について

詳細画面

Data Guardian 詳細画面では、役に立つ情報が提供されます。例えば、次のとおりです。

- テクニカルサポートに対して、ステータスまたはバージョン情報を提供することができます。
- ファイル名を検索するには、右下にある コピー を選択して、内容を Word ファイルに貼り付けます。
- フォルダの所有者を表示するには、フォルダ を選択してから フォルダ所有権 列にスクロールします。

詳細画面にアクセスするには、次の手順を実行します。

Data Guardian 通知エリア アイコンを右クリックしてから、**詳細** をクリックします。

詳細画面の左上角に、次の情報が表示されます。

サービスステータス：Data Guardian Windows Service のステータスです。値：停止、開始保留中、停止保留中、実行中、継続保留中、一時停止保留中、一時停止

実行状態：デバイスのアクティブ化状態です。値：アクティブ、再アクティブ化中、サスペンド、サスペンド中

ユーザーモード：

- **内部ユーザー** - このドメインアドレス内のユーザー

- **外部ユーザー** - このドメインアドレス外のユーザー
- **未登録** - Data Guardian がアクティブになっていない、内部または外部ユーザー

登録メール：内部ユーザーの場合は、これはドメイン電子メールアドレスです。外部ユーザーの場合は、ユーザー登録先の電子メールです。

サーバ URL：このクライアントと通信する Dell Server です。

ポリシー最終変更：ポリシーが最後に変更され、クライアントによって実行されたときの日付とタイムスタンプです。

ポリシーバージョン：Dell Server によって生成されたポリシーバージョンです。

詳細画面の **ファイル** エリアには、次の情報が表示されます。

名前：ファイルの名前です。

クラウド：この機能は無効になっているため、データはありません。

ファイル状態：この値はフォルダの所有者を示します。値はキー ID によって決定されます。

プロセスの状態：ファイルにキーが必要か、完了しているかがリストされます。

企業：デフォルトサーバをリストします。メッセージ *Error: Key Not From Your Server*（エラー：お使いのサーバのキーではありません）がこの列に表示された場合、キーが企業のサーバに属していません。暗号化されたファイルのキーは、企業のサーバーに属している必要があります。

キー：フォルダに割り当てられたキー ID です（新しいファイルは暗号化のためにこのキーを使用します）。

フォルダー：フォルダーの完全パス名です。

最終変更：ファイルが最後に変更された日付です。

永続性状態：ファイルがディスク上にあるかどうかを示します。

XEN ファイルの読み取り：この機能は無効になっています。

ブラウザの作成：正 または 誤 になります。

ログファイルを表示するには、詳細画面の右下隅から **ログの表示** をクリックします。

メモ:
ログファイルは、**C:\ProgramData\Dell\Data Guardian** でも確認できます。

Data Guardian の場合、以前は、クラウド暗号化の［詳細］画面に［**フォルダー**］領域がありました。現在、クラウド暗号化は無効になっています。

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

ポリシーアップデートのチェック

管理者がポリシーを変更し、ポリシーの更新を通知する場合、Windows 通知エリアに移動して **Dell Data Guardian** アイコンをクリックし、**ポリシーアップデートのチェック** を選択します。

管理者が Microsoft Word で作成したファイルを保護するようポリシーを変更した場合、その更新が適用されるまで Word を閉じておく必要があります。

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

ログファイルの場所

トラブルシューティングのために、管理者はログファイルを要求することがあります。

ログファイルを見つけるには、次の手順を実行します。

1 次の場所に移動します。

2 **Xendow.Service.log** を選択します。

> **メモ:**
> Xendow.Service.log は、サイズが 3 MB に達すると、Xendow.Service1.log、Xendow.Service2.log の順に名前を変更して保存されます。

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

Data Guardian のアップグレード

ベストプラクティスは、以前のバージョンをアンインストールして最新バージョンをインストールすることです。「Data Guardian のアンインストール」を参照してください。

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

Windows での Data Guardian のアンインストール

管理者が Data Guardian をインストールした場合、その管理者のみがインストールした Data Guardian をアンインストールできます。外部コンピュータ上で管理者権限を持っている外部ユーザーも、フォルダの共有への招待を受けていれば、Data Guardian のアンイストール作業をその外部コンピュータから行うことができます。

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

Data Guardian のアンインストール

Data Guardian をアンインストールするには、コンピュータのローカル管理者である必要があります。

ローカルドライブへのファイルのコピー

コンピュータまたはデバイスから Data Guardian をアンインストールする場合、同期クライアントのウェブサイト上のファイルを安全に保存して、暗号化状態を維持するようにする必要があります。

1 アンインストールを行う前に、ファイルにアクセスする必要があるかどうかを決定します。

2 これらのファイルをローカル ドライブにコピーします。

同期クライアントウェブサイト上のフォルダおよびファイルは暗号化され、それらをダウンロードしても暗号化されています。ファイルを表示するには、Data Guardian を再インストールする必要があります。また、ファイルを Data Guardian Web ポータルで表示することもできます。

Data Guardian のアンインストール

1 プログラムのアンインストールには、Windows コントロールパネルを使用します。
2 **DellData Guardian** を選択して、上部メニューの **変更** をクリックします。
3 ようこそ 画面が表示されたら **次へ** をクリックします。
4 **削除** を選択して、**次へ** をクリックします。
5 Dell Data Guardian のアンインストールを確認する警告が表示されます。アンインストールする場合は、**次へ** をクリックします。
6 プログラムの削除 画面で、**削除** をクリックします。
ステータスウィンドウに進捗状況が表示されます。
7 同期クライアントからのエラーダイアログが表示される場合は、**続行** をクリックします。
8 Office ドキュメントを開いているダイアログ状態が表示された場合は、**OK** をクリックしてから Office ドキュメントを閉じ、アンインストールを再開します。
9 完了 画面が表示されたら、**終了** をクリックします。
10 **はい** をクリックして再起動します。

Data Guardian のアンインストールが完了します。

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

デルについてのご意見をお聞かせください

管理者がフィードバックを有効にしていた場合、この製品に関するフィードバックをデルに提供できます。この簡単なフィードバックは、記入欄と評価スケール（最高ご満足度 = 10）によるお客様のご満足度レベルについての 2 つの質問で構成されています。

アクセスするには、通知エリアの Data Guardian アイコンをクリックして、**フィードバックの送信** を選択します。

この機能がポリシーによって有効化されていない場合、このオプションは表示されません。

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

Windows での Data Guardian の使用

管理者はドキュメントを保護するポリシーを設定しており、企業にどのオプションが適用されているかを通知します。

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

オプションの概要

この概要では、管理者によって設定されたポリシーに基づいて、Data Guardian で使用可能なオプションを説明します。これらのドキュメントは、他のユーザーと共有したり、リムーバブルメディアに保存したりする場合、保護されます。

オプション	説明	詳細
Office とマクロに対応したドキュメント	これらのドキュメントには、.docx、.pptx、.xlsx、.pdf、.docm、.pptm、.xlsm、.pdf などがあります。	「Office ドキュメント用のセキュリティレベルを決定するためのファイルメニューオプションの確認」を参照してください。 次のいずれかのモードを使用できます。 • オプトイン • Force-Protected
基本ファイル保護	これらは、会社が暗号化し、管理者が設定した追加のアプリケーションとファイルタイプです。	「基本的なファイル保護による追加のアプリケーションとファイル タイプ」を参照してください。
追加のオプション	これらのオプションは、Office ドキュメント、基本ファイル、またはその両方に適用されます。	「Data Guardian の追加オプション」を参照してください。
外部ユーザーとのファイル共有	非ドメイン メール アドレスを持つユーザー（別の企業の誰か、または非ドメイン メール アドレスで保護対象ファイルにアクセスしようとする内部ユーザー ）。	「外部ユーザーとして Data Guardian を使用」を参照してください。

保護されたドキュメントのオンラインでの作業

保護されたドキュメントを作成する際、それらのドキュメントにキーが生成されるためオンラインで作業することをお勧めします。コンピュータを再イメージ化して保護されたドキュメントを作成した場合、管理者にお問い合わせください。

ファイルのプロパティ > *Dell Data Guardian* タブ

保護された Office ドキュメントを右クリックして、**プロパティ** を選択できます。**Dell Data Guardian** タブには、ファイルのキー ID、アクセス、および禁止データなどの情報が表示されます。

Windows のオーバーレイアイコン

Data Guardian 2.2 以降のファイルエクスプローラでは、保護されたファイルにはオーバーレイアイコンが表示されます。保護されたファイルを右クリックすると、詳細が Dell Data Guardian タブに表示されます。

非表示のウォーターマーク

管理者が設定したポリシーによっては、保護された Office ドキュメントには、ユーザーを識別する非表示のウォーターマークが使われていることがあります。ドキュメントを印刷または共有してもウォーターマークは残ります。

メモ:
Office ドキュメントを開いたときに、カバーページにインストールとアクティブ化に関する情報が表示された場合、管理者が Office ドキュメントを保護するためのポリシーを設定している可能性があります。Data Guardian がインストールされてアクティブになっていることを確認します。「クラウドおよび保護された Office のアクティブ化で起こりうる問題」を参照してください。

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

Data Guardian の保護モードでの Office ドキュメントの使用

企業のセキュリティ強化のために、管理者は、次の Office アプリケーション用のファイルを保護するポリシーを有効にすることがあります。

- .docx、.pptx、.xlsx
- .docm、.pptm、.xlsm
- .pdf

権限のないユーザーが保護されたファイルにアクセスした場合、次のような操作をしてもファイルは暗号化された状態を保ちます。

- 電子メールへの添付
- ブラウザへの移動 - 一部のクラウド同期クライアントでは、ファイル名を右クリックして、**移動** をクリックします。
- ネットワークでの共有
- クラウドストレージプロバイダへのアップロード
- リムーバブルメディアへの保存

Office ドキュメントの場合、Data Guardian のインストールまたは有効化の方法が記載された、次のようなカバーページが表示されます。

- Data Guardian をインストールする必要があります。
- Data Guardian をアクティブ化する必要があります。
- クラウド内で保護された Office ドキュメントを開いています。
- Data Guardian がインストールされているコンピュータから Data Guardian がインストールされていない個人のデバイスに Office ファイルがダウンロードされました。
- 権限のないユーザーが Office ファイルの 1 つにアクセスしています - カバーページに企業固有のメッセージが表示されますが、ユーザーはファイルのコンテンツを表示できません。

Office ドキュメント用のセキュリティレベルを決定するためのファイルメニューオプションの確認

管理者が Data Guardian ポリシーを有効にしているか確認するには、Office ドキュメントを開いて **ファイル** を選択します。左ペインに 名前を付けて保存（保護付き）が表示されている場合、Office ドキュメントに追加の保護を設定できます。

セキュリティレベルを決定するには、次のオプションが有効か無効かを確認します。

- **オプトインモード** - 保護する Office ドキュメントを決定する際、いくつかのオプションがあります。
  - 名前を付けて保存 と 名前を付けて保存（保護付き）が有効になっている場合 - Office ドキュメントを保護する場合は、**名前を付けて保存（保護付き）** を選択します。

  - 印刷 および エクスポート は、ポリシーに応じて有効または無効にできます。
  - 共有 が有効になっています。
  - **ドキュメント > セキュアドキュメント** フォルダ - オプトインモード (ただし Force-protected モードではない) では、セキュアドキュメント フォルダが、ドキュメント フォルダのルートに追加されます。このフォルダの Office ドキュメントは暗号化されます。このフォルダから保護された Office ドキュメントを削除すると、そのドキュメントは暗号化された状態を保ちます。フォルダの名前を変更する場合、名前が変更されたフォルダのコンテンツが暗号化されます。フォルダを削除すると、フォルダが再作成されます。
- **Force-Protected モード** - 企業に高レベルのセキュリティが必要です。
  - 名前を付けて保存 が無効で 名前を付けて保存 *(* 保護付き *)* が有効 - すべての Office ドキュメントを保護モードで保存する必要があります。
  - 印刷 および エクスポート は、ポリシーに基づいて有効または無効にできます。
  - 共有 が無効になっています。

    メモ:
    Force-Protected モードでは、ポリシーも、コンピュータをスイープする特定の回数を有効にして、保護されていないすべての Office ファイルを見つけて保護モードに変更します。保護されていないすべての Office ファイルをスイープするには Data Guardian のネットワークにログインし、接続している必要があります。
  - **ドキュメント > 保護なし** フォルダ - Force-Protected モード (オプトインモードはない) のポリシーによって有効にされている場合は、保護されていないフォルダがドキュメントフォルダのルートに追加されます。このフォルダの Office ドキュメントは復号化されます。フォルダを削除すると、フォルダが再作成されます。

- **名前を付けて保存 (保護付き)** を選択した場合、保存ファイルの種類 フィールドでは、保護されている *Office* オプションのみが表示されます。

- **ファイル > 情報** は次のようになります。
  - オプトインモードおよび Force-Protected モード：日付制限の追加 が表示されます (管理者がそのポリシーを有効にしている場合)「日付制限を追加したセキュリティの強化」を参照してください。
  - オプトインモードおよび Force-Protected モード：セキュリティを高めるために、この Office ドキュメントのプロパティ情報 (作成者、日付など) が非表示になります。
  - 読み取り専用ステータス：詳細については、次を参照してください。

    メモ:
    ファイル > 情報 の ドキュメントの保護 オプションは、Microsoft Office に関連しています (Data Guardian の保護モードではありません)。

Office ドキュメントを読み取り専用モードで開いた場合、次のことを確認します。

- 左ペインに 名前を付けて保存 *(* 保護付き *)* が表示されない場合、読み取り専用であることは、Data Guardian のポリシーとは関連していません。
- 管理者がポリシーを Force-protected モードに設定し、高レベルのセキュリティを追加すると、保護されていない Office ドキュメントが読み取り専用モードで開きます。

  メモ:
  OneDrive では、**ファイル > 開く > OneDrive** から開いた保護されている Office ドキュメントが読み取り専用モードの場合、OneDrive 同期クライアントをインストールし設定しているか確認します。

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

オプトインモードによる Office ドキュメントの保護

会社が Data Guardian の保護モードを使用している場合、次を参照してください。

- オプトインモードのファイルメニューオプションで作業する

オプトインモードのファイルメニューオプションで作業する

この表には Office ドキュメントのファイルメニューオプションがリストされています。セキュリティのレベルに応じて、一部のオプションがグレー表示されます。

メモ:
現在、組み込みの Office ドキュメントは保護された Office モードでサポートされません。

ファイルメニュー	オプトインモードおよび保護された Office ドキュメント
テキストエディタで	ファイルは通常どおりに開きます。
保存	• オプション： すでに保護されたドキュメント - 保護付きで保存されます。 保護なし - 保護なしで保存されます。保護するには、**名前を付けて保存（保護付き）** をクリックします。 • 読み取り専用のドキュメント - ダイアログに、保護されていないドキュメントは保存できないと表示されます。名前を付けて保存 ウィンドウが開き、ファイルを別名で保存する必要があります。
名前を付けて保存	標準のオプションあり（ただし、保護モードではない）
名前を付けて保存（保護付き）	保存ファイルの種類 フィールドには、保護された Office オプションのみが表示されます。
印刷	**有効** ただし、保護された Office ドキュメントについては、ポリシーを使って管理者が印刷を無効にしている場合、印刷 メニューを選択することはできますが、保護されたドキュメントを印刷できないことを示すトースト通知が表示されます。 管理者が印刷を許可した場合、別のポリシーによりユーザー名、ドメイン名、コンピュータ ID を含むウォーターマークが各ページに適用された状態で印刷されます。
共有	保護された Office ドキュメントの場合、**有効** です。 保護されていない Office ドキュメントの場合、**無効** です。
エクスポート （Office 2013 以降）	管理者が設定したポリシーに基づいて有効化またはグレー表示されます。
保護エクスポート （Office 2013 以降）	エクスポート メニューオプションがグレー表示され、保護エクスポート が有効な場合、各ページにユーザー名、ドメイン名、およびコンピュータの ID を含むウォーターマークが適用されてドキュメントがエクスポートされます。 外部ユーザーに保護モードのドキュメントをエクスポートする場合、外部ユーザーはそのドキュメントを開いて表示できますが、エクスポートや印刷をすることはできません。

保護されたマクロ有効ドキュメントのオンラインでの作業

保護されたマクロ有効ドキュメントにはマクロが設定されていますがブロックされます。ただし現在、Data Guardian は新しく保護されたドキュメント（.docm、.pptm、.xlsm）を閉じて再度開いた場合のみ、マクロ有効ドキュメントを制御できます。また、マクロを含む保護されたドキュメントを保護なしで保存する場合、マクロを実行するにはそのドキュメントを閉じて再度開く必要があります。

TITUS 分類とオプトインモード

ポリシーが有効になっている場合、管理者はいくつかの TITUS 分類を設定して、その分類に応じてドキュメントを暗号化します。保護されていない Office ドキュメントを右クリックすると、TITUS 分類を選択できます。これは、Office ドキュメントを保護するためのもうひとつの方法といえます。

データ分類とオプトインモード

このポリシーが有効になっている場合、管理者は社会保障番号、クレジットカード番号、その他の機密情報など、特定のコンテンツの分類を設定できます。管理者は、どの情報が分類されたかを通知します。これらの分類ルールに基づく情報が含まれているドキュメントを保存すると、ドキュメントは暗号化されます。

Office ドキュメントでタグを使用して、ポリシーのファイルタグのメタデータで使用されているデータの分類をトリガーする場合、Office ドキュメントで使用するタグは大文字と小文字が区別され、管理者がポリシーで使用している大文字 / 小文字と一致する必要があります。

メモ:
このポリシーが有効な場合にスイープすると、分類ルールを満たすファイルが暗号化されます。ただし、ファイルを作成する場合は、右クリックして **ファイルの保護** を選択します。

また「Data Guardian による Outlook メールの暗号化」を参照してください。

オプトインモードのトラブルシューティング

保護された Office ドキュメントの印刷が Data Guardian のポリシーによって無効になっている場合、**ファイル > 情報** の順に選択するか、Windows エクスプローラで保護された Office ファイルを右クリックすると、印刷を選択できます。ただし、印刷 を選択すると、次のような動作になります。

- Word - ダイアログボックスに Word の動作が停止したことを表示されます。
- Excel - ダイアログボックスにポリシーにより 印刷 が無効になっていることが表示されます。
- PowerPoint - ダイアログボックスにポリシーにより印刷が無効になっていることが表示されます。OK をクリックすると、ドキュメントが保護されていることを示すカバーページが印刷されます。

保護されているオプトインモードドキュメントの特定

オプトインモードで、ドキュメントが保護されているかどうか確認する場合、ドキュメントを開いてタイトルバーに保護されていると表示されているか確認します。

メモ:
Force-protected モードの場合、すべての Office ドキュメントが保護されます。

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

Force-Protected モードによる Office ドキュメントの保護

企業が Data Guardian の保護モードを使用している場合、次を参照してください。

- Force Protected モードのファイルメニューオプションで作業する
- Data Guardian の追加オプション

Force Protected モードのファイルメニューオプションで作業する

この表には Office ドキュメントのファイルメニューオプションがリストされています。セキュリティのレベルに応じて、一部のオプションがグレー表示されます。

メモ:
現在、組み込みの Office ドキュメントは保護された Office モードでサポートされません。

ファイルメニュー	保護および非保護のドキュメントの Force-protected モード
テキストエディタで	保護対象でない文書は読み取り専用モードで開きます。
保存	• ドキュメントが保護されます。 • 読み取り専用文書 - 編集できますが、元のドキュメントは保存できません。保存 をクリックすると、名前を付けて保存 (保護付き) ウィンドウが開き、新しい名前を付けて保護モードで保存する必要があります。 • リモートドキュメント - リモートの場所で開いたドキュメントが保護されていない場合、変更して保存するにはローカルドライブに保存する必要があります。リモートの場所に保存することはできません。 **メモ:** 保存 をクリックすると、名前を付けて保存 ウィンドウが開き、保存ファイルの種類 フィールドには、保護された Office オプションのみが表示されます(ドキュメント、プレゼンテーション、またはワークブック)。
名前を付けて保存	**無効**
名前を付けて保存 (保護付き)	保存ファイルの種類 フィールドには、保護された Office オプションのみが表示されます。
印刷	**有効** ただし、保護された Office ドキュメントについては、ポリシーを使って管理者が印刷を無効にしている場合、印刷メニューを選択できますが、保護されたドキュメントを印刷できないことを示すトースト通知が表示されます。 管理者が印刷を許可した場合、別のポリシーによりユーザー名、ドメイン名、コンピュータ ID を含むウォーターマークが各ページに適用された状態で印刷されます。
共有	**無効**
エクスポート (Office 2013 以降)	管理者が設定したポリシーに基づいて有効化またはグレー表示されます。
保護エクスポート (Office 2013 以降)	エクスポート メニューオプションがグレー表示され、保護エクスポート が有効な場合、各ページにユーザー名、ドメイン名、およびコンピュータの ID を含むウォーターマークが適用されてドキュメントがエクスポートされます。 **メモ:** 外部ユーザーに保護モードのドキュメントをエクスポートする場合、外部ユーザーはそのドキュメントを開いて表示できますが、エクスポートや印刷をすることはできません。

保護されたマクロ有効ドキュメントのオンラインでの作業

保護されたマクロ有効ドキュメントにはマクロが設定されていますがブロックされます。ただし現在、Data Guardian は新しく保護されたドキュメント (.docm、.pptm、.xlsm) を閉じて再度開いた場合のみ、マクロ有効ドキュメントを制御できます。また、マクロを含む保護されたドキュメントを保護なしで保存する場合、マクロを実行するにはそのドキュメントを閉じて、再度開く必要があります。

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

Data Guardian の追加オプション

保護されている Office ドキュメント用の追加のメニューオプション

Office ドキュメントの種類やドキュメントが保護されているかどうかにより、次の操作が影響を受けます。

右クリック > 保護

Office ドキュメントを右クリックして、**保護** を選択できます。表示するメニューオプションのコンテンツを追加する必要があります。空のドキュメントを保護できません。

貼り付け

管理者が Office ドキュメントを保護するポリシーを設定している場合：

- 元の保護されたドキュメントまたは保護された PDF には、保護されない / 保護されたデータをコピーして貼り付けることができます。ただし、保護対象外の PDF は、Adobe Acrobat Reader DC で開くことができます。
- 保護されたドキュメントから保護されていないドキュメントにデータをコピーまたは貼り付けることはできません。クリップボードには何も表示されず、企業固有のテキストメッセージで、保護されていない、または管理されていないドキュメントに貼り付けることはできないことが通知されます。

> **メモ:**
> 保護されたドキュメントからテキストを切り取り、保護されていないドキュメントにメッセージが表示された場合、保護されたドキュメントで **元に戻す** をクリックしてテキストを取得します。

保護モードでのドラッグアンドドロップ

保護された Word ドキュメントにコンテンツをドラッグアンドドロップすることができます。現在、保護された Power Point および Excel ファイルではドラッグアンドドロップが無効になっています。

保護された PDF を Adobe Acrobat Reader DC で開いて編集する

Acrobat Reader DC を使用する場合：

- 保護された .pdf ファイルに注釈を追加するか、フォームに入力できます。ファイルを保存すると、変更が反映された、保護された .pdf ファイルが新しく作成されます。これは Acrobat Reader DC の機能です。
- セキュリティを強化するため、1 つの保護されている .pdf ファイルを Acrobat Reader DC で開くと、Acrobat Reader DC が終了するまでインターネットアクセスがブロックされます。
- セキュリティを強化するため、保護された .pdf が開いている場合、このインスタンスからメールを送信できません。

> **メモ:**
> 保護された .pdf ファイルはネットワークからは開けません。Word を使用すると、保護されている .pdf ファイルをネットワークから開くことができます。

封筒とラベルの印刷

保護された Office ドキュメントを印刷する際、管理者がウォーターマークを追加するポリシーを設定している場合、封筒またはラベルを印刷するには次の手順に従います。

1 Word ドキュメントで **差し込み文書** タブを選択します。
2 **封筒** または **ラベル** オプションを選択します。

3 アドレスまたは差出人住所を入力したら、**印刷** をクリックします。

メモ:
印刷に別のオプションを使用する際、管理者が印刷された Office ドキュメントにウォーターマークを追加するポリシーを設定している場合、ウォーターマークが封筒またはラベルに表示されます。

追加のオプション

プロセスのブロック

管理者が設定したポリシーに基づいて、切り取りツールなどの一部のプロセスがブロックされる場合があります。該当するプロセスについては、管理者から通知されます。また、ダイアログによってそのプロセスがブロックされていることが通知されます。

- **Force-Protected モード** - 管理者が *PrtScr* ボタンをブロックするようポリシーを設定している場合、タッチスクリーンまたはタブレットを使用して画面を印刷する機能もブロックすることができます。
- RS5 版の Windows には、スクリーンスケッチアプリ（旧スニッピングツール）が付属しています。Data Guardian を使用すると、管理者はこのアプリをブロックするポリシーを有効にして、セキュリティを高めることができます。

保護されたドキュメントの Outlook の電子メールへの添付

Outlook の電子メールに保護されたドキュメントを添付する場合、テキストとして挿入 ではなく **挿入** を選択します。テキストとして挿入 ではドキュメントのコンテンツを電子メールの本文に直接貼り付けるため、保護されなくなります。

ポリシーに基づいた追加の保護ファイルタイプ保護された Office ドキュメントまたは .xen 形式のファイルを添付できます。

Data Guardian を搭載した Windows では、保護されたドキュメントを添付すると、Data Guardian がその電子メールの暗号化されたファイルにアクセスするための情報を追加します。

- 内部ユーザー - クライアントをダウンロードするためのリンクを含む情報を表示します。
- 外部ユーザー - クライアントを登録してダウンロードするためのリンクを含む情報を表示します。

メモ:
追加された情報を表示するには、ウェブベースのバージョンの Outlook ではなく Microsoft Office Outlook から電子メールを送信する必要があります。

Data Guardian による Outlook メールの暗号化

Data Guardian v2.0.1 以降のポリシーに基づき、内部ユーザーにはメールと添付ファイルの両方を暗号化する 保護 オプションが Outlook の左上にあります。送信者と受信者のいずれも、Data Guardian がインストールされアクティブ化されている必要があります。

Data Guardian の Outlook メールの暗号化は Office 2013 移行でサポートされていますが、Web メールではサポートされていません。

使用するには、次を実行します。

1 左上の **保護** をクリックします。
2 外部メールアドレスの場合は **はい** をクリックしてキーの共有を確定するか、送信しない場合は **いいえ** をクリックします。

ベストプラクティスは、一度に 1 つのメールを開くことです。メールを複数開いている場合は、保護ボタンをクリックする前にメールをクリックしてフォーカスしてください。マウスを項目に合わせないと保護ボタンはグレーになります。

移動中のデータは安全です。このプレビューリリースでは、ディスク上のデータに対する Data Loss Prevention（DLP）が部分的にサポートされています。今後のリリースで、セキュリティの向上を予定しています。

暗号化された電子メールを開いたときに DLP を最小限に抑えるため、次のような一部の操作が無効化またはブロックされます。

- Outlook の クイック操作
- 移動、フォルダへ移動、詳細フォルダ の各操作
- 次へ および 戻る の矢印
- 転送
- 一部の右クリックオプション

暗号化された電子メールを開いたときに DLP を最小限に抑えるため、次の操作が制限されます。

- コピー / 貼り付け
- データの印刷およびエクスポート
- 一部の右クリックオプション
- 下書きフォルダおよび自動保存

Outlook メールを受信する場合

暗号化された Outlook メールを開くと、ドキュメントが保護されていることを示す警告が表示されます。ユーザーはダブルクリックしてファイルを開きます。プレビューには電子メールの内容が表示されません。表紙のみが表示されます。カバーページには、オンプレミス の場合は Dell Server 名、Hosted Dell Security Center がマルチテナントの場合は特定のテナント用にインストール ID がリストされています。カバーページには、Data Guardian クライアントをダウンロードするためのリンクも含まれています。

E メールの分類

データの分類で暗号化された保護 Office ドキュメントのローカルレポート (オプトインモード)

Office ドキュメントや PDF の機密情報を保護するために、管理者はデータの分類に基づいてファイルをスイープし、暗号化するポリシーを設定する場合があります。機密情報には、社会保障番号、クレジットカード番号、米国の住所、または企業固有のデータなどがあります。どのような機密情報によってファイルが暗号化されるかは、管理者から通知されます。

暗号化されたファイルのデータの分類とその暗号化の理由のローカルレポートを表示するには、次の手順を実行します。

1 **C:\Users\<username>\AppData\Local\Dell\Data Guardian** に移動します。

2 **Classification Report.log** を開きます。

メモ:
ファイルが暗号化中の場合は、暗号化が完了するまで、エントリには複数の行が存在する可能性があります。

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

基本ファイル保護による追加のアプリケーションとファイルタイプ

管理者は、ポリシーが追加のアプリケーションとファイルタイプを暗号化することができるかどうかを通知します。何者かが Basic File Protection で暗号化されたファイルを開いても、Data Guardian がインストールされていない場合は、そのファイルのコンテンツを表示することはできません。

基本ファイル保護の概要

アプリケーション

次に、管理者が暗号化するアプリケーションの例を示します。

- メモ帳
- ワードパッド
- Visio
- MS ペイント

メモ:
一部のアプリケーションでは、Data Guardian が部分的にサポートされています。これについては、管理者が通知します。

ファイルタイプ

設定可能なファイルタイプには、.txt、.rtf、.csv、.odt、.vsdx、.png、.jpg、.jpeg、.jpe、.jfif、.gif、.tif、.tiff、.bmp などがあります。

Windows、Mac、および Mobile

基本ファイル保護ポリシーが設定されている場合、Data Guardian はユーザーのコンピューターをスイープし、これらの拡張子を持つすべてのローカル ファイルを暗号化します。基本ファイル保護で暗号化されたファイルは、ファイルの拡張子に関連付けられているアプリケーションを使用してのみ表示および編集できます。

メモ:
AppData など特定のシステムフォルダ内のファイルは、暗号化されません。また、セキュアドキュメントフォルダなどの保護された Office ドキュメントに関連するフォルダも暗号化されません。

Windows のオーバーレイアイコン

Data Guardian 2.2 以降のファイルエクスプローラでは、保護されたファイルにはオーバーレイアイコンが表示されます。保護されたファイルを右クリックすると、詳細が [Dell Data Guardian] タブに表示されます。

Windows または Mac で一部のファイルをスイープから除外する (スイープが有効になる前に)

会社が追加のファイル タイプ (.txt など) を暗号化すると決定した場合でも、必ずしも、その拡張子が付いたすべてのファイルをスイープして暗号化する必要があるとは限りません。

その拡張子に対して基本ファイル保護を有効にする前に、管理者は、ローカル コンピューターでのフォルダー追加をユーザーに許可する別のポリシーを設定し、さらにそのフォルダー内のファイルがスイープされないように設定することができます。管理者は、ポリシーを設定し、フォルダー名を設定し、フォルダー名を通知して、そのフォルダーを追加できる場所を提案できます。これらのファイルは、システムで必要されるファイルの場合もあれば、保護が不要なファイルの場合もあります。

重要:
管理者が基本ファイル保護ポリシーを有効にする前に、ユーザーはフォルダーを作成する必要があります。

1 ユーザーは、管理者から通知されたフォルダー名とパスを使用します。
   - Mac の場合、**[環境設定] > [基本ファイル保護の除外]** の順に選択します。作成するフォルダーの名前とパスはここに表示されます。
2 指定された拡張子 (.txt など) が付いていて、暗号化する必要がないファイルを追加します。ユーザーは、必要に応じて、任意の名前でサブフォルダーを追加できます。

メモ:
その拡張子が付いていて、以前に暗号化されたファイルの場合、このフォルダーに入れても復号化されません。これらのファイルは、暗号化された状態に保たれます。管理者が別のポリシーを通じて作成できる**保護されていないドキュメント** フォルダーがある場合は、このフォルダーに基本ファイル保護のファイル タイプを入れて復号化できます。

3 基本ファイル保護が有効になった後、ネットワークまたは外付けドライブにその拡張子を持つ保護されていないファイルがある場合は、それらを除外フォルダーにコピーできます。これらのファイルは、暗号化されていない状態に保たれます。それ以外の場合、これらのファイルは暗号化されます。

コンピューターに複数のユーザーが存在する場合、こうしたフォルダーにファイルを置き、そのファイルをスイープされないように設定できるのは、そのときログインしているユーザーのみです。その他のユーザーがそのフォルダーに置いているファイルは、すべてスイープされて暗号化されます。

Windows または Mac でのファイル拡張子の削除

管理者はファイル拡張子の削除を決定することができます。その場合、該当するファイル タイプを復号化するために、コンピューターがスイープされます。

- 暗号化されたファイルの *[プロパティ] > [Dell Data Guardian]* タブが表示されなくなります。
- ファイル オーバーレイ アイコンがあった場合、それらは表示されなくなります。
- 復号化の完了には数分かかる場合があります。該当拡張子のファイルが暗号化されたままになっている場合、スイープの最中にファイルが開かれていたか、ファイル サーバーなどの別の場所に保存されていた可能性があります。

復号化されなかった拡張子のファイルのリカバリーを要求する場合は、管理者に連絡してください。

Office アプリケーション

Office アプリケーションを使用して、基本ファイル保護で暗号化されたファイルを開くことができます。この場合、コンテンツは読み取り専用になります。

Web ポータル

設定 > ポリシー の順に移動して基本ファイル保護が True に設定されている場合、管理者が Office 以外のファイルを追加していることを意味します。このファイルは Web ポータルからダウンロードされたときに Data Guardian により暗号化されるファイルです。管理者からファイルタイプを確認する必要があります。

メモ:
サポート対象外のファイルタイプをアップロードしても、Web ポータルで内容を読むことはできません。

暗号化されているかどうかにかかわらず、Office 以外のファイルタイプをアップロードできますただし、Office 以外のファイルをダウンロードする場合は、ファイル拡張子が異なります。

Office 以外のファイル (.txt や .png など)	ダウンロードの説明
アップロード前に暗号化済み 例 : Windows または Mac で暗号化済みの Office 以外のファイル。	Web ポータルからダウンロードした場合、ファイル固有の拡張子 (.txt や .png など) が維持されます。
非暗号化ファイル	Web ポータルからダウンロードした場合、管理者が拡張子をポリシーに追加したかどうかによってファイル拡張子は異なります。ただし、これらのファイルは暗号化されています。 Web ポータルからダウンロードした .txt ファイルの例 : • **filename.txt** - 管理者が .txt ファイルタイプをポリシーに追加しました。 • **filename.txt.xen** - .txt ファイルタイプがポリシーに含まれていません。ファイルは暗号化されていますが .xen 拡張子が付いています。

Web ポータルの 編集 ポリシーが有効になっている場合、ユーザーは Office 以外のファイルを編集できます。

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

改ざんと保護された Office 文書

Data Guardian は保護された Office ドキュメントをスキャンして、改ざんされているかどうかを検出できます。

内部ユーザーが保護された Office ドキュメントトを改ざんしている場合：

- Data Guardian は改ざんの一部を修復し復元できます。
- 修復できない改ざんがある場合、ダイアログボックスにファイルが改ざんされており、管理者に連絡するようメッセージが表示されます。

権限のないユーザーが保護された Office ドキュメントを開いた場合、カバーページのみが表示されます。権限のないユーザーがカバーページを変更した場合、認証済みのユーザーがそのファイルを保護されたものとして再度保存したときに Data Guardian がカバーページを復元します。

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

クラウド内の同期クライアントフォルダおよびファイルの表示

コンピューターに同期クライアント フォルダーがあり、Data Guardian がこのフォルダーを暗号化している場合、これらのファイルはクラウド内で暗号化されます。

Data Guardian Web ポータルを使用してファイルを暗号化すると、これらのファイルは.xen ファイルとして暗号化されます。Windows では、暗号化された.xen ファイルを開くことはできません。モバイル デバイスでは、Data Guardian または Web ポータルを使用して表示することができます。

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

保護された Office ドキュメントを外部ユーザーと共有

Data Guardian では、保護された Office ドキュメントを電子メール、リムーバブルメディア、ネットワーク共有を使用して共有したり、クラウドにアップロードして共有することができます。

- すべての内部 Data Guardian ユーザーがドキュメントを表示できます。
- ポリシーに基づいて、外部ユーザーもドキュメントを表示できます。

ドキュメントを添付して 送信 をクリックすると、確認ダイアログが表示され、保護されたドキュメントのキーが外部ユーザーと共有されることが通知されます。

日付制限を追加したセキュリティの強化

オプションとして、外部ユーザーのセキュリティ強化のため、日付制限を追加して外部ユーザーが保護された Office ドキュメントを表示できる時間を制限できます。

1 **ファイル > 情報 > 日付制限** の順に選択します。

2 ドロップダウンメニューから、外部ユーザーがドキュメントを表示できる開始日時と終了日時を選択します。

メモ:
ドキュメントを送信したいが、外部ユーザーが指定した日付と時刻までドキュメントを表示しないようにするには、開始日時を将来の日時に設定します。

3 **OK** をクリックします。
ドキュメントは保存および保護され、閉じられてから再度開かれます。

メモ:
保護されていない Office ドキュメントの日付を変更し、キャンセル をクリックすると、Data Guardian は引き続きファイルを保護します。

メモ:
現在、保護された Office ドキュメントに日付制限を追加し、ネットワークドライブに保存することを予定している場合、そのファイルをローカルに保存しネットワークにコピーする必要があります。

指定した日時範囲以降に外部ユーザーがファイルを開いた場合、ファイルにアクセス制限があること、および外部ユーザーはファイルの作成者に連絡できることがダイアログに表示されます。このダイアログには、外部ユーザーの日付は表示されません。

開始日 フィールドに将来の日時を設定し、その日時の前に外部ユーザーがファイルを開くと、ダイアログにアクセス制限のため指定された日時までファイルが開けないことが表示されます。

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

Mac に Data Guardian をインストールして使用する

Data Guardian for Mac には各画面にヘルプが組み込まれており、次のような情報が表示されます。

- Dell Data Guardian インターフェイス：ユーザーがファイルをアップロードして暗号化する
- クラウド暗号化
- 外部ユーザーとアクセス制限
- 改ざん

Mac 用の Dell Data Guardian インターフェイスで、ヘルプアイコンをクリックします。

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

Mac 用インストールクライアント

管理者によって会社のホワイトリストに追加されている場合、https://yoursecurityservername.domain.com:8443/cloudweb/register で登録できます。

登録後、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 に移動するように指示する電子メールを受信します。

ローカル管理者である必要があります。

Data Guardian for Mac をインストールするには

1 Data Guardian クライアントの場合、**Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg** にインストーラがあります。
2 Dell-Data-Guardian-0.x.x.xxxx.dmg 内の**.pkg** ファイルを使用して、インストールまたはアップグレードします。
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 構成タイプ ウィンドウで、次のいずれかを選択します。

Hosted Dell Security Center	On-prem Dell Management Server
Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（ SaaS ）ソリューション。 a **Hosted Dell Security Center** を選択します。 b **続行** をクリックします。 c 手順 9 に進みます。	Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。 a **On-prem Dell Management Server** を選択します。 b *Dell Management Server 名：* フィールドに、このコンピュータが通信する Dell Server 名（ 例：server.domain.com ）を

Hosted Dell Security Center	On-prem Dell Management Server
	入力します。www または http (https) を含める必要はありません。この情報は管理者によって提供されます。 c **続行** をクリックします。 d 手順 9 に進みます。

9 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 10 に進みます。
- **インストール場所を変更** をクリックします。
  1 インストール先の選択 ウィンドウですべてのユーザーを選択します (現在、唯一のオプションです)。
  2 **続行** をクリックします。
  3 **インストール** をクリックして、手順 10 に進みます。

10 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。

11 サマリ ウィンドウで、**閉じる** をクリックします。

12 プロンプトが表示されたら、.pkg ファイルをそのまま保持するか、ごみ箱 に移動します。

13 以下のいずれかを行ってください。

Hosted Dell Security Center	On-prem Dell Management Server
インストール後、資格情報 ウィンドウが自動的に開きます。会社がマルチテナントの場合は、インストール ID が必要になります。 1 資格情報 ウィンドウで、ログインアカウントの電子メールを入力し、**続行** をクリックします。 2 以下のいずれかを行ってください。 • 会社の環境がマルチテナントの場合、インストール ID を入力して **続行** をクリックし、手順 3 に進みます。 **メモ:** エラーが表示される場合は、認証情報を確認してください。E メール アドレスまたはインストール ID が間違っていた場合は、[**初期化を再開**] をクリックして、認証情報を再度入力してください。 • シングルテナントの場合、手順 3 に進みます。 3 Microsoft ウィンドウで、パスワードを入力して **サインイン** をクリックします。 4 Azure ウィンドウで、パスワードを入力します。 5 **ログイン** をクリックします。 **メモ:** エラーが表示される場合は、認証情報を確認してください。E メール アドレスが正しくない場合は、[**初期化を再開**] をクリックして、認証情報を再度入力してください。 6 Dell Data Guardian のインタフェースが開きます。「Dell Data Guardian アプリケーション」を参照してください。	1 .dmg ウィンドウを閉じると、Finder が開きます。 2 「エンドユーザーのアクティブ化」を参照してください。

メモ: 会社が Cloud Edition から Data Guardian にアップグレードする場合、Data Guardian を認証して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 Data Guardian ヘルプを参照してください。

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

エンドユーザーのアクティベーション（オンプレミス）

On-prem Dell Management Server のアクティベーション

オンプレミスの場合、最初に Dell Data Guardian を開いた後、ログインしてアクティブ化する必要があります。

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 [資格情報] ウィンドウが開いたら、Dell Server のアドレス（例：company.server.com ）を入力します。この情報は管理者によって提供されます。デフォルトのポート番号は 8443 です。デフォルト ポートがカスタム ポート番号に変更された場合は、管理者から通知があります。

> **メモ:**
> 管理者に指示されない限り、SSL エラー チェックボックスを選択しないでください。

3 E メール アドレスとパスワードを入力します。

4 **ログイン** をクリックして、Data Guardian をアクティブ化します。

5 下の「*Dell Data Guardian* アプリケーション」を参照してください。

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。

Dell Data Guardian アプリケーション

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薄い色で左側のペインに表示されます。

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。

Data Guardian の認証が取り消しまたは期限切れになった場合、クラウドストレージプロバイダの名前もグレー表示されます。

1 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。

2 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。資格情報を入力します。

認証されると、クラウドストレージプロバイダの名前がアクティブ化されます。

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

Hosted Dell Security Center および一時停止されたテナント

Hosted Dell Security Center では、指定された期間内に支払いを行わないテナントを一時停止にできます（Windows、Mac、Mobile、Web ポータル）。

Data Guardian の内部 / 外部ユーザーには、以下が発生する場合があります。

- すべてのプラットフォーム - Data Guardian をインストール、アクティブ化、または Data Guardian にログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。
- Mac - Data Guardian が開いているときにテナントが一時停止されている場合、エクスプローラとすべてのファイルを閉じた後に一時停止されているテナントのダイアログが表示され、保護されたファイルを開こうとします。
- Web ポータル：
  - すでにログインしていて暗号化されたファイルをアップロードした場合、アップロードに失敗したことを示すメッセージが表示されます。
  - 暗号化されたファイルまたは非暗号化ファイルがアップロードされてテナントが一時停止された場合、ダウンロードに失敗したことを示すメッセージが表示されます。
  - ログアウト後に再度ログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。

管理者に連絡してください。

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

基本ファイル保護による追加のアプリケーションとファイルタイプ

管理者は、ポリシーが追加のアプリケーションとファイルタイプを暗号化することができるかどうかを通知します。何者かが Basic File Protection で暗号化されたファイルを開いても、Data Guardian がインストールされていない場合は、そのファイルのコンテンツを表示することはできません。

基本ファイル保護の概要

アプリケーション

次に、管理者が暗号化するアプリケーションの例を示します。

- メモ帳
- ワードパッド
- Visio
- MS ペイント

> **メモ:**
> 一部のアプリケーションでは、Data Guardian が部分的にサポートされています。これについては、管理者が通知します。

ファイルタイプ

設定可能なファイルタイプには、.txt、.rtf、.csv、.odt、.vsdx、.png、.jpg、.jpeg、.jpe、.jfif、.gif、.tif、.tiff、.bmp などがあります。

Windows、Mac、および Mobile

基本ファイル保護ポリシーが設定されている場合、Data Guardian はユーザーのコンピューターをスイープし、これらの拡張子を持つすべてのローカル ファイルを暗号化します。基本ファイル保護で暗号化されたファイルは、ファイルの拡張子に関連付けられているアプリケーションを使用してのみ表示および編集できます。

> **メモ:**
> AppData など特定のシステムフォルダ内のファイルは、暗号化されません。また、セキュアドキュメントフォルダなどの保護された Office ドキュメントに関連するフォルダも暗号化されません。

Windows のオーバーレイアイコン

Data Guardian 2.2 以降のファイルエクスプローラでは、保護されたファイルにはオーバーレイアイコンが表示されます。保護されたファイルを右クリックすると、詳細が [Dell Data Guardian] タブに表示されます。

Windows または Mac で一部のファイルをスイープから除外する（スイープが有効になる前に）

会社が追加のファイル タイプ（.txt など）を暗号化すると決定した場合でも、必ずしも、その拡張子が付いたすべてのファイルをスイープして暗号化する必要があるとは限りません。

その拡張子に対して基本ファイル保護を有効にする前に、管理者は、ローカル コンピューターでのフォルダー追加をユーザーに許可する別のポリシーを設定し、さらにそのフォルダー内のファイルがスイープされないように設定することができます。管理者は、ポリシーを設定し、フォルダー名を設定し、フォルダー名を通知して、そのフォルダーを追加できる場所を提案できます。これらのファイルは、システムで必要されるファイルの場合もあれば、保護が不要なファイルの場合もあります。

重要:
管理者が基本ファイル保護ポリシーを有効にする前に、ユーザーはフォルダーを作成する必要があります。

1 ユーザーは、管理者から通知されたフォルダー名とパスを使用します。
   - Mac の場合、**[環境設定] > [基本ファイル保護の除外]** の順に選択します。作成するフォルダーの名前とパスはここに表示されます。

2 指定された拡張子（.txt など）が付いていて、暗号化する必要がないファイルを追加します。ユーザーは、必要に応じて、任意の名前でサブフォルダーを追加できます。

   メモ:
   その拡張子が付いていて、以前に暗号化されたファイルの場合、このフォルダーに入れても復号化されません。これらのファイルは、暗号化された状態に保たれます。管理者が別のポリシーを通じて作成できる**保護されていないドキュメント** フォルダーがある場合は、このフォルダーに基本ファイル保護のファイル タイプを入れて復号化できます。

3 基本ファイル保護が有効になった後、ネットワークまたは外付けドライブにその拡張子を持つ保護されていないファイルがある場合は、それらを除外フォルダーにコピーできます。これらのファイルは、暗号化されていない状態に保たれます。それ以外の場合、これらのファイルは暗号化されます。

コンピューターに複数のユーザーが存在する場合、こうしたフォルダーにファイルを置き、そのファイルをスイープされないように設定できるのは、そのときログインしているユーザーのみです。その他のユーザーがそのフォルダーに置いているファイルは、すべてスイープされて暗号化されます。

Windows または Mac でのファイル拡張子の削除

管理者はファイル拡張子の削除を決定することができます。その場合、該当するファイル タイプを復号化するために、コンピューターがスイープされます。

- 暗号化されたファイルの *[プロパティ] > [Dell Data Guardian]* タブが表示されなくなります。
- ファイル オーバーレイ アイコンがあった場合、それらは表示されなくなります。
- 復号化の完了には数分かかる場合があります。該当拡張子のファイルが暗号化されたままになっている場合、スイープの最中にファイルが開かれていたか、ファイル サーバーなどの別の場所に保存されていた可能性があります。

復号化されなかった拡張子のファイルのリカバリーを要求する場合は、管理者に連絡してください。

Office アプリケーション

Office アプリケーションを使用して、基本ファイル保護で暗号化されたファイルを開くことができます。この場合、コンテンツは読み取り専用になります。

Web ポータル

設定 > ポリシー の順に移動して基本ファイル保護が True に設定されている場合、管理者が Office 以外のファイルを追加していることを意味します。このファイルは Web ポータルからダウンロードされたときに Data Guardian により暗号化されるファイルです。管理者からファイルタイプを確認する必要があります。

メモ:
サポート対象外のファイルタイプをアップロードしても、Web ポータルで内容を読むことはできません。

暗号化されているかどうかにかかわらず、Office 以外のファイルタイプをアップロードできますただし、Office 以外のファイルをダウンロードする場合は、ファイル拡張子が異なります。

Office 以外のファイル（ .txt や .png など ）	ダウンロードの説明
アップロード前に暗号化済み 例：Windows または Mac で暗号化済みの Office 以外のファイル。	Web ポータルからダウンロードした場合、ファイル固有の拡張子（ .txt や .png など ）が維持されます。
非暗号化ファイル	Web ポータルからダウンロードした場合、管理者が拡張子をポリシーに追加したかどうかによってファイル拡張子は異なります。ただし、これらのファイルは暗号化されています。 Web ポータルからダウンロードした .txt ファイルの例： • **filename.txt** - 管理者が .txt ファイルタイプをポリシーに追加しました。 • **filename.txt.xen** - .txt ファイルタイプがポリシーに含まれていません。ファイルは暗号化されていますが .xen 拡張子が付いています。

Web ポータルの 編集 ポリシーが有効になっている場合、ユーザーは Office 以外のファイルを編集できます。

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

iOS または Android での Data Guardian Mobile のインストールと使用

このセクションでは、iOS または Android デバイスでの Data Guardian Mobile の使用方法に関する基本情報を説明します。管理者が Data Guardian を有効にするポリシーを設定している場合、ファイルは暗号化され、安全に保管されます。暗号化したファイルを表示して作業するには、Data Guardian アプリをモバイルデバイスにインストールする必要があります。

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

前提条件

Data Guardian アプリを使用する前に、使用環境に基づいて、次のどちらが必要かを判断してください。

Hosted Dell Security Center	On-prem Dell Management Server
ホスティング環境がマルチテナントである場合、インストール ID が必要になります。	Dell Server 名（server.domain.com など）を確認しておいてください。 この情報は管理者によって提供されます。

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

Data Guardian Mobile の使用を開始するために

Data Guardian Mobile を使用する際は、この手順に従ってください。

タスク	説明	参照
Data Guardian をインストール - オプションを指定します。	管理者がインストール済み ユーザーがインストールする必要あり	インストールした管理者：Data Guardian アプリをタップしてログインします。 ユーザーのインストール：次のいずれかを参照してください。 • iOS デバイスでのインストール • Android デバイスでのインストール
モバイルに適用するポリシーを決定する	管理者は、ポリシーが適用されるかを通知します。	次のポリシーが使用できます。 • 保護対象 Office 文書 • クラウド保護 • 追加のオプション

タスク	説明	参照
ファイルマネージャの操作	Data Guardian のオプションを参照してください。	ファイルマネージャの操作
クラウド保護ポリシーが有効な場合、クラウドストレージプロバイダアカウントにアクセスできる	デバイスで、Data Guardian アプリのファイルマネージャ画面に移動し、お使いのクラウドストレージプロバイダをタップします。	「クラウドストレージプロバイダアカウントへのアクセス」を参照してください。

Data Guardian のポリシーに基づいて、以下を利用できます。

- 保護された Office ファイル（ .docx、.pptx、.xlsx、.docm、.pptm、.xlsm、.pdf ）は、個々のファイル拡張子を保持します。
- 追加のアプリケーションと .txt などのファイルの種類。
- クラウド内の Office 以外のファイルには .xen 拡張子が付きます。

Data Guardian をインストールしているモバイルデバイスでは、次のことができます。

- フォルダとファイルの作成
- フォルダとファイルの削除
- 外部ユーザーとのドキュメントの共有（ 外部ビューアに対してポリシーが有効になっている場合 ）

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

App Store からの iOS デバイスへの Data Guardian のインストール/アンインストール

iOS デバイスでのインストール

前提条件：デバイスが Touch ID 指紋スキャナーをサポートしていて、PIN の代わりにこれを使用する場合、Data Guardian をインストールする前に、Touch ID 用にデバイスを設定する必要があります。

1 お使いのデバイスで、**App Store** をタップし、**Data Guardian Mobile** を検索します。

2 **Data Guardian** アプリを選択してインストールします。

3 チェックボックスをタップして、ライセンス契約に同意します。

4 次のいずれかのオプションを選択します。

Hosted Dell Security Center	On-prem
Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（ SaaS ）ソリューション。 a **Hosted Dell Security Center** をタップします。 b 電子メールを入力します。 c **送信** をタップします **メモ:** 電子メールアドレスが複数のテナントにある場合は、インストール ID を入力します。 d Microsoft Azure ウィンドウで、パスワードを入力します。	Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。 a **On-prem** をタップします。 b ログイン画面の サーバ フィールドに、会社の Dell Server の名前（ 例：server.domain.com ）を入力します。 c ユーザー名とパスワードを入力します。 d **サインイン** をタップします。

e **サインイン** をタップします。

5 プロンプトが表示されたら、指紋センサーをタップするか PIN を作成します。

お使いのアカウントがアクティブになり、Data Guardian のファイルマネージャ画面が表示されます。

Data Guardian アプリのアンインストール

1 iOS アプリドロワーで、**Data Guardian** アイコンをタップアンドホールドします。
2 **x** をタップします。
3 **削除** をタップします。

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

Workspace ONE による iOS デバイスへの Data Guardian のインストール/アンインストール

Workspace ONE がインストールされている場合は、シングル サインオンで Data Guardian の認証を受けることができます。下記の手順は、Hosted Dell Security Center でも On-prem Dell Management Server でも同じです。

管理者が、Data Guardian アプリをデバイスにプッシュします。

1 **Data Guardian** アプリをインストールするかどうかの確認メッセージが表示されたら、[**OK**] をタップします。
2 **Data Guardian** アプリを起動します。
3 ライセンス契約画面で、[**同意する**] をタップします。
4 Workspace ONE または Data Guardian を選択するオプションで、[**Workspace One**] をタップしてシングル サインオンを設定します。
5 パスワードを入力します。
6 プロンプトが表示されたら、PIN を作成します。

> **メモ:**
> Workspace ONE にサインインすれば、Data Guardian の PIN を入力するだけで済みます。

お使いのアカウントがアクティブになり、Data Guardian のファイルマネージャ画面が表示されます。

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

Google Play からの Android デバイスへの Data Guardian のインストール/アンインストール

Android デバイスでのインストール

1 お使いのデバイスで、**Google Play** にアクセスし、**Data Guardian Mobile** を検索します。
2 **Data Guardian** アプリを選択してインストールします。
3 チェックボックスをタップして、ライセンス契約に同意します。
4 次のいずれかのオプションを選択します。

Hosted Dell Security Center	On-prem Dell Management Server
Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（SaaS）ソリューション。 a **Hosted** をタップします。 b 電子メールを入力します。 c **送信** をタップします **メモ:** 電子メールアドレスが複数のテナントにある場合は、インストール ID を入力します。 d Microsoft Azure ウィンドウで、パスワードを入力します。 e **サインイン** をタップします。	Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。 a **On-prem** をタップします。 b ログイン画面の サーバ フィールドに、会社の Dell Server の名前（例：server.domain.com）を入力します。 c ユーザー名とパスワードを入力します。 d **サインイン** をタップします。

5 プロンプトが表示されたら、PIN を作成します。

お使いのアカウントがアクティブになり、Data Guardian のファイルマネージャ画面が表示されます。

Data Guardian アプリのアンインストール

1 Android アプリドロワーで、**設定** をタップします。
2 **設定** で、**アプリ** をタップします。
3 **Data Guardian** アイコンをタップ & ホールドします。
4 このアイコンをアンインストール オプションにドラッグします。
5 **OK** をタップします。

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

Workspace ONE による Android デバイスへの Data Guardian のインストール/アンインストール

Workspace ONE がインストールされている場合は、シングル サインオンで Data Guardian の認証を受けることができます。下記の手順は、Hosted Dell Security Center でも On-prem Dell Management Server でも同じです。

1 デバイスで、[**ハブ**] をタップします。
2 [**アプリ カタログ**] をタップします。
3 Dell Data Guardian アプリで、[**インストール**] をタップします。
4 [インストールの確認] で、[**インストール**] をタップします。
5 [*Google Play* プロテクト] で、[**許可**] をタップします。
6 アプリのインストール メッセージで、[**完了**] をタップします。
7 [**開く**] をタップして、Data Guardian アプリを起動します。
8 Workspace ONE または Data Guardian による認証オプションで、[**Workspace One**] をタップしてシングル サインオンを設定します。
9 ライセンス契約のチェックボックスをタップします。
10 [**シングル サインオン**] をタップします。
11 プロンプトが表示されたら、PIN を作成します。

メモ: Workspace ONE にサインインすれば、Data Guardian の PIN を入力するだけで済みます。

お使いのアカウントがアクティブになり、Data Guardian のファイルマネージャ画面が表示されます。

Data Guardian アプリのアンインストール

1 Android アプリドロワーで、**設定** をタップします。
2 **設定** で、**アプリ** をタップします。
3 **Data Guardian** アイコンをタップ＆ホールドします。
4 アイコンをアンインストール オプションにドラッグします。
5 **OK** をタップします。

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

ファイルマネージャの操作

Data Guardian のファイルマネージャでは、ローカルストレージまたはクラウドを使用できます。Data Guardian を開くと、ファイルマネージャが開きます。

ファイルマネージャ画面

ファイルマネージャ画面のデフォルトのフォルダは、次のとおりです。

- ドキュメント
- ダウンロード
- フォト

新規作成 画面

追加（ **+** ）アイコンをタップすると、新規作成 画面が表示され、次のオプションが使用できます。

- ドキュメント
- スプレッドシート
- プレゼンテーション（ PowerPoint ）
- 写真
- フォルダ
- クラウドサービス

ナビゲーションドロワーのオプション

ナビゲーションドロワーのアイコンをタップします。次のオプションがあります。

- **ブラウザ**
- **ファイルマネージャ**
- **設定** アイコン：
  - **PIN の変更** ボタン（ ポリシーで有効になっている場合 ）
  - **ブラウザ**
  - **ファイルマネージャ（ 設定 ）** - 次のオプションを使用
    - **更新間隔** - Data Guardian とクラウドサービスの同期頻度。手動 または 毎日 を推奨します。その他のオプションには、毎時 と 毎週 があります。

    - **10 MB ダウンロード警告** - 有効 または 無効 にします。Wi-Fi に接続していないときに、ダウンロードサイズが 10 MB を超える場合に使用します。
    - **キャッシュをクリア** - 一時ファイルをクリアします。
  - (iOS) - **Touch ID** または **Face ID**。指紋または顔の認識を事前に設定してある場合、iOS のバージョンに応じて使用できます。Data Guardian の使用時には、タップして有効または無効にします。
  - **バージョン情報** - 「Data Guardian のポリシーとバージョン」を参照
  - **Data Guardian を終了** ボタン
  - **クラウドアカウント** - リンクされているか否かを示します。
- **ブラウザ**
- **ファイルマネージャ** - ファイルマネージャ画面に戻ります。
- **Data Guardian をロック**

追加のオプション

- お気に入り へのファイルの追加
  - iOS の場合は、ナビゲーションドロワーを参照してください。
  - Android の場合、ファイル名を長押しします。

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

Data Guardian Mobile のポリシーの決定

管理者は、企業に対して設定されているポリシーを通知します。

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

Data Guardian のポリシーとバージョンの表示

一部の Data Guardian ポリシーは **バージョン情報** に記載されています。これらのポリシー、または Data Guardian のバージョンを表示するには

1 Data Guardian ナビゲーションドロワーで、**設定 > バージョン情報** の順にタップします。
2 **ポリシー** をタップします
管理者が設定したポリシーに基づいて、リストには次のような項目が含まれます。
- PIN 長
- 非アクティブなタイムアウト
- ログイン失敗回数
- コピーと貼り付け - 保護されたドキュメントを保護されたドキュメントにコピーできます。

バージョン
3 追加のポリシーオプションを決定します。
次のオプションがあります。
- 保護対象 Office 文書
- クラウド保護
- 追加のポリシー

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

Mobile での保護された Office ドキュメントの使用

管理者は、自分の会社に対して有効になっているオプションを通知します。Data Guardian をインストールして、保護された Office ドキュメントを開くと、ドキュメントの復号化を行っていることを示すメッセージが表示されます。

Office ドキュメントの Data Guardian オプション

次の Data Guardian のオプションが表示されます。

- **作成** - ポリシー設定に基づいて、ドキュメントが作成時に保護されます。このファイルのヘッダに、保護されたドキュメントが表示されます。
- **コピー/貼り付け** - 保護された Office ドキュメントから別の保護された Office ドキュメントへは、コンテンツをコピーのみができます。
- **印刷** - 追加のポリシー設定に基づいて、印刷時にウォーターマークを入れることができます。
- **エクスポート** - 詳細ポリシー設定に基づいて、エクスポートの際にウォーターマークを入れることができます。

Office ドキュメントが開いている場合は、左上にあるアイコンをタップして、次のオプションを選択できます。

- **保存**
- **名前を付けて保存**
- **エクスポート**
- **終了**

ポリシーに基づく詳細オプションには、次のものがあります。

- **編集** - Office ファイル（ .docx および .ppt ）を編集できます。

  メモ:
  現在、.csv および .csv.xen ファイルは、モバイルデバイス上で編集できません。

- **非表示のウォーターマーク** - ポリシーに基づいて、保護された Office ドキュメントに、ユーザーを識別する非表示のウォーターマークを含められます。ドキュメントを印刷または共有してもウォーターマークは残ります。
- **オンスクリーンウォーターマーク** - 保護された Office ドキュメントを開くと、クライアント画面にウォーターマークが表示されます。

Office ドキュメントの追加情報

オフラインのときに保護された Office ドキュメント

保護された Office ドキュメントまたは保護されたマクロ有効ドキュメントを作成し、オフラインにした場合、それらのドキュメント用のキーが作成されます。デバイスがオンラインに戻ると、それらのキーは Dell Server にアップロードされます。デバイスが 3 日間オフラインの場合、Data Guardian が Dell Server に接続していないことが通知されます。この通知はネットワークに接続するまで毎日表示されます。暗号化されたファイルを表示するには、モバイルデバイスをオンラインにする必要があります。

保護された Office ドキュメントのトラブルシューティング

iOS デバイスで、25 MB 以上の保護された Office ドキュメントを開いたときにメモリ不足のダイアログが表示された場合、この警告は、Data Guardian からのものではなく、Polaris Office からの警告です。デバイスに十分なメモリがある場合は、ファイルを閉じて、再度開きます。

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

基本ファイル保護による追加のアプリケーションとファイルタイプ

管理者は、ポリシーが追加のアプリケーションとファイルタイプを暗号化することができるかどうかを通知します。何者かが Basic File Protection で暗号化されたファイルを開いても、Data Guardian がインストールされていない場合は、そのファイルのコンテンツを表示することはできません。

基本ファイル保護の概要

アプリケーション

次に、管理者が暗号化するアプリケーションの例を示します。

- メモ帳
- ワードパッド
- Visio
- MS ペイント

> **メモ:**
> 一部のアプリケーションでは、Data Guardian が部分的にサポートされています。これについては、管理者が通知します。

ファイルタイプ

設定可能なファイルタイプには、.txt、.rtf、.csv、.odt、.vsdx、.png、.jpg、.jpeg、.jpe、.jfif、.gif、.tif、.tiff、.bmp などがあります。

Windows、Mac、および Mobile

基本ファイル保護ポリシーが設定されている場合、Data Guardian はユーザーのコンピューターをスイープし、これらの拡張子を持つすべてのローカル ファイルを暗号化します。基本ファイル保護で暗号化されたファイルは、ファイルの拡張子に関連付けられているアプリケーションを使用してのみ表示および編集できます。

> **メモ:**
> AppData など特定のシステムフォルダ内のファイルは、暗号化されません。また、セキュアドキュメントフォルダなどの保護された Office ドキュメントに関連するフォルダも暗号化されません。

Windows のオーバーレイアイコン

Data Guardian 2.2 以降のファイルエクスプローラでは、保護されたファイルにはオーバーレイアイコンが表示されます。保護されたファイルを右クリックすると、詳細が [Dell Data Guardian] タブに表示されます。

Windows または Mac で一部のファイルをスイープから除外する (スイープが有効になる前に)

会社が追加のファイル タイプ (.txt など) を暗号化すると決定した場合でも、必ずしも、その拡張子が付いたすべてのファイルをスイープして暗号化する必要があるとは限りません。

その拡張子に対して基本ファイル保護を有効にする前に、管理者は、ローカル コンピューターでのフォルダー追加をユーザーに許可する別のポリシーを設定し、さらにそのフォルダー内のファイルがスイープされないように設定することができます。管理者は、ポリシーを設定し、フォルダー名を設定し、フォルダー名を通知して、そのフォルダーを追加できる場所を提案できます。これらのファイルは、システムで必要されるファイルの場合もあれば、保護が不要なファイルの場合もあります。

重要:
管理者が基本ファイル保護ポリシーを有効にする前に、ユーザーはフォルダーを作成する必要があります。

1 ユーザーは、管理者から通知されたフォルダー名とパスを使用します。
   - Mac の場合、**[環境設定] > [基本ファイル保護の除外]** の順に選択します。作成するフォルダーの名前とパスはここに表示されます。
2 指定された拡張子（.txt など）が付いていて、暗号化する必要がないファイルを追加します。ユーザーは、必要に応じて、任意の名前でサブフォルダーを追加できます。

   メモ:
   その拡張子が付いていて、以前に暗号化されたファイルの場合、このフォルダーに入れても復号化されません。これらのファイルは、暗号化された状態に保たれます。管理者が別のポリシーを通じて作成できる**保護されていないドキュメント** フォルダーがある場合は、このフォルダーに基本ファイル保護のファイル タイプを入れて復号化できます。

3 基本ファイル保護が有効になった後、ネットワークまたは外付けドライブにその拡張子を持つ保護されていないファイルがある場合は、それらを除外フォルダーにコピーできます。これらのファイルは、暗号化されていない状態に保たれます。それ以外の場合、これらのファイルは暗号化されます。

コンピューターに複数のユーザーが存在する場合、こうしたフォルダーにファイルを置き、そのファイルをスイープされないように設定できるのは、そのときログインしているユーザーのみです。その他のユーザーがそのフォルダーに置いているファイルは、すべてスイープされて暗号化されます。

Windows または Mac でのファイル拡張子の削除

管理者はファイル拡張子の削除を決定することができます。その場合、該当するファイル タイプを復号化するために、コンピューターがスイープされます。

- 暗号化されたファイルの *[プロパティ] > [Dell Data Guardian]* タブが表示されなくなります。
- ファイル オーバーレイ アイコンがあった場合、それらは表示されなくなります。
- 復号化の完了には数分かかる場合があります。該当拡張子のファイルが暗号化されたままになっている場合、スイープの最中にファイルが開かれていたか、ファイル サーバーなどの別の場所に保存されていた可能性があります。

復号化されなかった拡張子のファイルのリカバリーを要求する場合は、管理者に連絡してください。

Office アプリケーション

Office アプリケーションを使用して、基本ファイル保護で暗号化されたファイルを開くことができます。この場合、コンテンツは読み取り専用になります。

Web ポータル

設定 > ポリシー の順に移動して基本ファイル保護が True に設定されている場合、管理者が Office 以外のファイルを追加していることを意味します。このファイルは Web ポータルからダウンロードされたときに Data Guardian により暗号化されるファイルです。管理者からファイルタイプを確認する必要があります。

メモ:
サポート対象外のファイルタイプをアップロードしても、Web ポータルで内容を読むことはできません。

暗号化されているかどうかにかかわらず、Office 以外のファイルタイプをアップロードできますただし、Office 以外のファイルをダウンロードする場合は、ファイル拡張子が異なります。

Office 以外のファイル（.txt や .png など）	ダウンロードの説明
アップロード前に暗号化済み 例：Windows または Mac で暗号化済みの Office 以外のファイル。	Web ポータルからダウンロードした場合、ファイル固有の拡張子（.txt や .png など）が維持されます。
非暗号化ファイル	Web ポータルからダウンロードした場合、管理者が拡張子をポリシーに追加したかどうかによってファイル拡張子は異なります。ただし、これらのファイルは暗号化されています。

Office 以外のファイル（ .txt や .png など）	ダウンロードの説明
	Web ポータルからダウンロードした .txt ファイルの例： • **filename.txt** - 管理者が .txt ファイルタイプをポリシーに追加しました。 • **filename.txt.xen** - .txt ファイルタイプがポリシーに含まれていません。ファイルは暗号化されていますが .xen 拡張子が付いています。

Web ポータルの 編集 ポリシーが有効になっている場合、ユーザーは Office 以外のファイルを編集できます。

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

Mobile でのクラウド保護の使用

管理者がクラウド保護を有効にするには、次の 2 つのアプリケーションが必要になります。

- クラウド同期クライアントアプリ - クラウド同期クライアントのオンラインヘルプを参照してください。
- Data Guardian Mobile アプリにより、会社で使用されているクラウド同期クライアントがリストされ、ダウンロードできるようになります。

権限のないユーザーがクラウドストレージアカウントにアクセスし、Data Guardian が**インストールされていない**モバイルデバイスにファイルをダウンロードした場合、そのユーザーはファイルを開いたり表示したりすることはできません。保護された Office ドキュメントを開いた場合、カバーページのみが表示され、Data Guardian を使用しないとドキュメントを表示できないことが通知されます。これにより、データの安全性が向上します。

クラウドストレージプロバイダアカウントへのアクセス

クラウドストレージプロバイダアカウントにアクセスするには

1 ファイルマネージャ画面で、追加（ **+** ）アイコンをタップします。

2 **クラウドサービス** をタップします。

Data Guardian ポリシーによって、表示されるクラウドストレージプロバイダが決まります。社内で使用するクラウドストレージプロバイダが管理者によって 1 つ以上指定され、それ以外のプロバイダはブロックされていることがあります。

3 画面の表示に従って、次のいずれかを実行します。

- クラウドストレージプロバイダに対してアカウントを作成します。
- 既存のクラウドストレージプロバイダアカウントにサインインします。

> **メモ:**
> 詳細については、クラウドストレージプロバイダのヘルプを参照してください。

メモ:
デバイスにクラウド同期クライアントアプリをダウンロードする場合、Data Guardian はアプリから直接アップロードしたフォルダまたはファイルを暗号化しません。ファイルを暗号化して保護するには、Data Guardian アプリを使用してファイルをアップロードする必要があります。

クラウド保護を使用する

Data Guardian をインストールしているモバイルデバイスでは、次のことができます。

- フォルダの作成
- ファイルのアップロードとダウンロード

メモ:
Data Guardian では、デバイスでアップロードとダウンロードを開始する必要があります。クラウドへのアップロード時にファイルを暗号化する場合は、クラウド同期クライアントアプリではなく、Data Guardian ホーム画面からファイルをアップロードする必要があります。ファイルをタップすると、Data Guardian が自動的にファイルを復号化し、アプリでファイルが平文で表示されます。一方、クラウド内では、そのファイルは .xen ファイルとして安全に保管されたままです。

- フォルダとファイルの削除
- 内部ユーザーの共有フォルダの受け入れ

メモ:
Data Guardian を介して内部ユーザーとフォルダを共有する場合、デバイスでフォルダを表示するには、クラウドストレージ Web サイトにアクセスしてルートフォルダにフォルダを移動するか、共有フォルダをダウンロードする必要があります。

- **ファイル > コピー** - 管理者が設定したポリシーに基づいて、特定のクラウドプロバイダから別のクラウドプロバイダにファイルをコピーすることができます。
- OneDrive または Dropbox を使用している Android で、アプリケーションからのファイルを共有できず、そのファイルが Data Guardian アプリとリンクを共有している場合、デバイスのファイルブラウザアプリからファイルを共有します。

クラウドストレージプロバイダへのリンク解除

同じクラウドストレージプロバイダに対して複数のアカウントを持っている場合、それらに同時にログインすることはできません。チェックボックスをクリアしてリンクを解除し、現在のアカウントからログアウトしてから、他の資格情報でログインする必要があります。

1 Data Guardian ナビゲーションドロワーを開き、**設定 > ファイルマネージャ > クラウドサービス** の順にタップします。クラウドストレージプロバイダにアクセスを許可している場合、チェックボックスにチェックマークが表示されます。

2 以下のいずれかを行ってください。

Android

a **リンク済み** をタップします。

b **はい** をタップします。

iOS

a **リンク解除** をタップします。

Data Guardian へのアクセスが削除され、ファイルも削除されます。ただし、クラウドのファイルは削除されません。

クラウド保護のトラブルシューティング

Dropbox for Business では、ファイルをオフラインで使用可能としてマークし、Dropbox Web サイトでファイルの名前を変更すると、そのファイルは Data Guardian アプリがインストールされている iOS デバイスで開けなくなります。

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

Mobile での追加のポリシーの使用

管理者は、どのポリシーが会社に設定されているかを通知します。

PIN の使用

管理者は、PIN を必要とするポリシーを設定し、その長さを設定することができます。

改ざん

Data Guardian は保護された Office ドキュメントをスキャンして、改ざんされているかどうかを検出できます。

Geofencing を介した追加の保護

管理者によって設定されたポリシーに基づいて、モバイルデバイスは保護された Office ドキュメントと .xen ファイルが特定の地域以外で開けないようにするよう追加の保護を設定できます。保護されたファイルを開くには、承認された地域内にいる必要があります。現在、その地域は米国およびカナダに設定されています。ジオフェンスを実行するには、デバイスでロケーションサービスを有効にする必要があります。管理者が Geofencing 機能を有効にしており、ロケーションサービスがオフに設定されている場合、ファイルへのアクセスは拒否されます。

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

Data Guardian と同期クライアントのセキュリティ上の考慮事項

Data Guardian は、フォルダとファイルを暗号化してデータを保護します。Data Guardian は同期クライアントで機能するため、次の点に注意してください。

Google Drive

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、Dell Server 上ではなく、Google サーバ上で行われます。そのため、これらのファイルは暗号化されません。Data Guardian がインストールされた Android および iOS デバイスの場合、これらの Google Docs へのアクセスはブロックされます。この動作は、プラットフォームごとにわずかに異なっています。

- Android
- iOS - メッセージが表示されます。

メモ:
Google Backup and Sync はサポートされません。

OneDrive と OneDrive for Business

OneDrive for Business の場合、複数のファイルをダウンロードしているとき、そのダウンロードをキャンセルすると、OneDrive for Business はダウンロードが完了していないファイルをキャンセルしますが、ダウンロードが進行中のファイルはダウンロードを続行します。これは、Microsoft の問題です。したがって、それらのファイルは完全にダウンロードされてからキャンセルされます。

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

ログ

セキュリティ上の理由から、モバイルデバイス上でログファイルは利用できません。

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

Hosted Dell Security Center および一時停止されたテナント

Hosted Dell Security Center では、指定された期間内に支払いを行わないテナントを一時停止にできます（ Windows、Mac、Mobile、Web ポータル ）。

Data Guardian の内部 / 外部ユーザーには、以下が発生する場合があります。

- すべてのプラットフォーム - Data Guardian をインストール、アクティブ化、または Data Guardian にログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。
- Mac - Data Guardian が開いているときにテナントが一時停止されている場合、エクスプローラとすべてのファイルを閉じた後に一時停止されているテナントのダイアログが表示され、保護されたファイルを開こうとします。
- Web ポータル：
  - すでにログインしていて暗号化されたファイルをアップロードした場合、アップロードに失敗したことを示すメッセージが表示されます。
  - 暗号化されたファイルまたは非暗号化ファイルがアップロードされてテナントが一時停止された場合、ダウンロードに失敗したことを示すメッセージが表示されます。
  - ログアウト後に再度ログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。

管理者に連絡してください。

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

デルへのフィードバックの送信

管理者がフィードバックポリシーを有効にしていた場合、この製品に関するフィードバックをデルに提供できます。この機能がポリシーによって有効化されていない場合、このオプションは表示されません。

フィードバックを送信するには、次の手順を実行します。

1 Data Guardian ナビゲーションドロワーで、**フィードバック** をタップします 。
2 簡単な質問に答えることで、満足度レベルを評価し（ 最高満足度 = 10 ）、コメントを入力することができます。

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

Web クライアント上の保護されたファイルの表示または編集

管理者が Data Guardian Web ポータルを設定している場合、その Web クライアントの URL にリンクして、Data Guardian クライアントをインストールせずに暗号化されたファイルを表示することができます。ポリシーに基づいて、ファイルを編集することもできます。
管理者が設定したポリシーに基づいて、次のファイルを表示できます。

- 保護対象 Office ドキュメント：.docx、.pptx、.xlsx、.docm、.pptm、.xlsm、.pdf。
- .xen ファイル - クラウドにアップロードされたときに Data Guardian が暗号化した Office または Office 以外のファイル。
- その他のファイルタイプ（メモ帳など）。

管理者が設定したポリシーに基づいて、クラウド ストレージ プロバイダーにアクセスできます。

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

Data Guardian の Web ポータルへのアクセス

手順は使用するブラウザによって多少異なります。

1 管理者から、Web ポータルにアクセスするための URL を教えてもらいます。
2 教えられた URL をクリックします。
警告が表示された場合は、**続行** または **進む** をクリックします。
3 ライセンス契約画面で、**同意する** をクリックします。
警告が表示された場合は、**続行** または **進む** をクリックします。
4 ドメイン資格情報を入力します。
5 **ログイン** をクリックします。
6 位置情報を追跡するよう求められた場合は、オプションを選択します。
7 ファイルを表示または編集するには、Data Guardian Web ポータルのオンラインヘルプを参照してください。

メモ:
Mac の場合は、Safari でポップアップを許可するよう設定する必要があります。

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

基本ファイル保護による追加のアプリケーションとファイルタイプ

管理者は、ポリシーが追加のアプリケーションとファイルタイプを暗号化することができるかどうかを通知します。何者かが Basic File Protection で暗号化されたファイルを開いても、Data Guardian がインストールされていない場合は、そのファイルのコンテンツを表示することはできません。

基本ファイル保護の概要

アプリケーション

次に、管理者が暗号化するアプリケーションの例を示します。

- メモ帳
- ワードパッド
- Visio
- MS ペイント

> **メモ:**
> 一部のアプリケーションでは、Data Guardian が部分的にサポートされています。これについては、管理者が通知します。

ファイルタイプ

設定可能なファイルタイプには、.txt、.rtf、.csv、.odt、.vsdx、.png、.jpg、.jpeg、.jpe、.jfif、.gif、.tif、.tiff、.bmp などがあります。

Windows、Mac、および Mobile

基本ファイル保護ポリシーが設定されている場合、Data Guardian はユーザーのコンピューターをスイープし、これらの拡張子を持つすべてのローカル ファイルを暗号化します。基本ファイル保護で暗号化されたファイルは、ファイルの拡張子に関連付けられているアプリケーションを使用してのみ表示および編集できます。

> **メモ:**
> AppData など特定のシステムフォルダ内のファイルは、暗号化されません。また、セキュアドキュメントフォルダなどの保護された Office ドキュメントに関連するフォルダも暗号化されません。

Windows のオーバーレイアイコン

Data Guardian 2.2 以降のファイルエクスプローラでは、保護されたファイルにはオーバーレイアイコンが表示されます。保護されたファイルを右クリックすると、詳細が [Dell Data Guardian] タブに表示されます。

Windows または Mac で一部のファイルをスイープから除外する (スイープが有効になる前に)

会社が追加のファイル タイプ (.txt など) を暗号化すると決定した場合でも、必ずしも、その拡張子が付いたすべてのファイルをスイープして暗号化する必要があるとは限りません。

その拡張子に対して基本ファイル保護を有効にする前に、管理者は、ローカル コンピューターでのフォルダー追加をユーザーに許可する別のポリシーを設定し、さらにそのフォルダー内のファイルがスイープされないように設定することができます。管理者は、ポリシーを設定し、フォルダー名を設定し、フォルダー

名を通知して、そのフォルダーを追加できる場所を提案できます。これらのファイルは、システムで必要されるファイルの場合もあれば、保護が不要なファイルの場合もあります。

重要:
管理者が基本ファイル保護ポリシーを有効にする前に、ユーザーはフォルダーを作成する必要があります。

1 ユーザーは、管理者から通知されたフォルダー名とパスを使用します。
   - Mac の場合、**[環境設定] > [基本ファイル保護の除外]** の順に選択します。作成するフォルダーの名前とパスはここに表示されます。

2 指定された拡張子（.txt など）が付いていて、暗号化する必要がないファイルを追加します。ユーザーは、必要に応じて、任意の名前でサブフォルダーを追加できます。

   メモ:
   その拡張子が付いていて、以前に暗号化されたファイルの場合、このフォルダーに入れても復号化されません。これらのファイルは、暗号化された状態に保たれます。管理者が別のポリシーを通じて作成できる**保護されていないドキュメント** フォルダーがある場合は、このフォルダーに基本ファイル保護のファイル タイプを入れて復号化できます。

3 基本ファイル保護が有効になった後、ネットワークまたは外付けドライブにその拡張子を持つ保護されていないファイルがある場合は、それらを除外フォルダーにコピーできます。これらのファイルは、暗号化されていない状態に保たれます。それ以外の場合、これらのファイルは暗号化されます。

コンピューターに複数のユーザーが存在する場合、こうしたフォルダーにファイルを置き、そのファイルをスイープされないように設定できるのは、そのときログインしているユーザーのみです。その他のユーザーがそのフォルダーに置いているファイルは、すべてスイープされて暗号化されます。

Windows または Mac でのファイル拡張子の削除

管理者はファイル拡張子の削除を決定することができます。その場合、該当するファイル タイプを復号化するために、コンピューターがスイープされます。

- 暗号化されたファイルの *[プロパティ] > [Dell Data Guardian]* タブが表示されなくなります。
- ファイル オーバーレイ アイコンがあった場合、それらは表示されなくなります。
- 復号化の完了には数分かかる場合があります。該当拡張子のファイルが暗号化されたままになっている場合、スイープの最中にファイルが開かれていたか、ファイル サーバーなどの別の場所に保存されていた可能性があります。

復号化されなかった拡張子のファイルのリカバリーを要求する場合は、管理者に連絡してください。

Office アプリケーション

Office アプリケーションを使用して、基本ファイル保護で暗号化されたファイルを開くことができます。この場合、コンテンツは読み取り専用になります。

Web ポータル

設定 > ポリシー の順に移動して基本ファイル保護が True に設定されている場合、管理者が Office 以外のファイルを追加していることを意味します。このファイルは Web ポータルからダウンロードされたときに Data Guardian により暗号化されるファイルです。管理者からファイルタイプを確認する必要があります。

メモ:
サポート対象外のファイルタイプをアップロードしても、Web ポータルで内容を読むことはできません。

暗号化されているかどうかにかかわらず、Office 以外のファイルタイプをアップロードできますただし、Office 以外のファイルをダウンロードする場合は、ファイル拡張子が異なります。

Office 以外のファイル（.txt や .png など）	ダウンロードの説明
アップロード前に暗号化済み	Web ポータルからダウンロードした場合、ファイル固有の拡張子（.txt や .png など）が維持されます。

Office 以外のファイル（ .txt や .png など）	ダウンロードの説明
例：Windows または Mac で暗号化済みの Office 以外のファイル。	
非暗号化ファイル	Web ポータルからダウンロードした場合、管理者が拡張子をポリシーに追加したかどうかによってファイル拡張子は異なります。ただし、これらのファイルは暗号化されています。 Web ポータルからダウンロードした .txt ファイルの例： • **filename.txt** - 管理者が .txt ファイルタイプをポリシーに追加しました。 • **filename.txt.xen** - .txt ファイルタイプがポリシーに含まれていません。ファイルは暗号化されていますが .xen 拡張子が付いています。

Web ポータルの 編集 ポリシーが有効になっている場合、ユーザーは Office 以外のファイルを編集できます。

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

クラウド ストレージ プロバイダーの使用

ポリシーに基づいて、Web ポータルはクラウド ストレージ プロバイダーにアクセスできます。詳細については、Web ポータル オンラインのヘルプを参照してください。

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

Hosted Dell Security Center および一時停止されたテナント

Hosted Dell Security Center では、指定された期間内に支払いを行わないテナントを一時停止にできます（ Windows、Mac、Mobile、Web ポータル ）。

Data Guardian の内部 / 外部ユーザーには、以下が発生する場合があります。

- すべてのプラットフォーム - Data Guardian をインストール、アクティブ化、または Data Guardian にログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。
- Mac - Data Guardian が開いているときにテナントが一時停止されている場合、エクスプローラとすべてのファイルを閉じた後に一時停止されているテナントのダイアログが表示され、保護されたファイルを開こうとします。
- Web ポータル：
  - すでにログインしていて暗号化されたファイルをアップロードした場合、アップロードに失敗したことを示すメッセージが表示されます。
  - 暗号化されたファイルまたは非暗号化ファイルがアップロードされてテナントが一時停止された場合、ダウンロードに失敗したことを示すメッセージが表示されます。
  - ログアウト後に再度ログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。

管理者に連絡してください。

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

外部ユーザーとして Data Guardian を使用

ドメイン電子メールアドレス以外のアドレスを持つ外部ユーザーでも、Data Guardian を使用することができます。例えば次のような場合です。

- 会社のシステムの一部として Data Guardian のインストールとアクティブ化を行ったが、社外のユーザーと保護対象ファイルを共有したり、保護対象ファイルに対して共同作業をしたりする必要がある。
- 使用している電子メールアドレスは会社のドメインのものだが、ドメイン電子メールアドレス以外の個人アドレスのコンピュータまたはモバイルデバイスにも Data Guardian をインストールしてアクティブ化したい。これにより、保護対象ファイルを企業のドメイン電子メールアドレスではないアドレスで扱えるようになる。

外部ユーザーはサーバ要件を満たす必要がある。また、ドメインまたはユーザーを会社のブラックリストに登録しないでください。

ホスティング環境では、外部ユーザーがアクティブ化できるテナントは 1 つだけです。

外部ユーザーは次のいずれかを選択できます。

- **Windows** - Data Guardian クライアントをダウンロードしてインストールします。「Windows の内部ユーザーのタスク」および「外部ユーザーのタスク」を参照してください。
- **Mac** - 「外部ユーザーと Mac」を参照してください。
- **Mobile**
- **Web ポータル** - Data Guardian クライアントをダウンロードしないで、Data Guardian Web ポータルを使用します。外部ユーザーは、保護された Office ドキュメントの .pdf または .xen ファイルを表示できます。ポリシーに基づいて、ファイルを編集することもできます。「外部ユーザーと Web ポータル」を参照してください。

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

Windows の内部ユーザーのタスク

保護対象ファイルを外部ユーザーと共有するには、次の操作を実行します。

- 保護された Office ドキュメントで [保護されたファイル アクセス] オプションを使用
- 外部ユーザーがアクセスを要求した場合のアクセスの承認または拒否
- 保護された Office ドキュメントを Outlook メールで送信

複数の保護された Office ファイルへのアクセス権の付与

外部ユーザーと共有するすべてのファイルにアクセス権を付与する必要があります。

1 保護対象ファイルを右クリックして、[**保護されたファイル アクセス**] を選択します。1 つから最大 50 個のファイルを選択することができます。保護されたドキュメントへのアクセスを共有 ウィンドウが開きます。次の場所にあるファイルが対象になります。

- ローカルフォルダまたはネットワークドライブ

- 電子メール
- リムーバブルメディア
- ネットワーク共有

2 右上の 共有する電子メール フィールドで、非ドメインユーザーの電子メールアドレスを入力して、**追加** をクリックします。

3 この手順を繰り返して、最大 10 件の電子メールアドレスを追加します。

4 **OK** をクリックします。
ダイアログボックスにより、共有が成功したこと、または電子メールアドレスに保護されたファイルを受信する権限がないことが通知されます。

5 未登録の外部ユーザー向けのベストプラクティスとしては、Dell Server に登録し、Data Guardian をダウンロードしてアクティブ化し、保護された共有ファイルを表示する手順を説明する電子メールを送信することを通知します。

外部ユーザーがアクセスを要求した場合のアクセスの承認または拒否

Data Guardian をインストールしている外部ユーザーは、保護されたドキュメントのキーを持っていない場合、それらのドキュメントに対するアクセスを要求できます。

1 外部ユーザーから保護されたドキュメントへのアクセスを求める電子メールを受信した場合、外部ユーザーと要求されたファイルの名前を表示できます。

2 **承認** または **拒否** をクリックします。
電子メールが、対象の外部ユーザーに送信されます。承認する場合、保護されたドキュメントのキーが共有されます。

対応できない場合、管理者はアクセスを承認または拒否することもできます。

Outlook メールで保護されたファイルを送信

保護されたファイルを添付して 送信 をクリックすると、保護されたファイルに対するキーが共有されることを確認するプロンプトが表示されます。

メモ:
外部ユーザーが保護されたファイルを電子メールで送信する場合、キーは共有されません。

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

Windows の外部ユーザーのタスク

内部ユーザーは、外部ユーザーに対して、保護対象ファイルへのアクセスの許可を与えることができます。外部ユーザーは、次のような情報を受け取ります。

- 登録手順が記載された電子メール
- 有効な電子メールアドレスを登録するためのリンクを含む、カバーページ付きの保護対象ファイル

メモ:
カバーページには、オンプレミス の場合は Dell Server 名、Hosted Dell Security Center がマルチテナントの場合は特定のテナント用にインストール ID がリストされています。カバーページには、Data Guardian クライアントをダウンロードするためのリンクも含まれています。

Data Guardian ドキュメントを開いて表示するには、外部ユーザーは次を実行する必要があります。

- Data Guardian に登録する

- Data Guardian のダウンロードおよびインストール - 外部ユーザーはコンピュータの管理者権限を持っている必要があります。

Data Guardian の登録

内部ユーザーが初めてファイルを共有する場合、外部ユーザーは登録する必要があります。

Data Guardian を登録するには：

1 以下のいずれかを行います。
- 電子メール - **承諾** をクリックします。
- カバーページの警告を表示する保護されたドキュメント - 提供されたリンクをクリックして有効な電子メールアドレスを登録します。

2 会社の環境に応じて、次の手順の中から選んでください。

Hosted Dell Security Center

Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（ SaaS ）ソリューション。

a Dell Data Guardian Web ポータルが開いたら、電子メールアドレスを入力します。
b 下にスクロールして、**同意する** をクリックします。
c Dell Security Center ウィンドウで、下の アカウントが必要ですか? までスクロールして、**サインアップ** をクリックします。
d 新規アカウント ページに、電子メール、名、姓、パスワードを入力します。パスワードは 8 文字以上で、小文字、大文字、特殊文字、数字を含める必要があります。
e **サインアップ** をクリックします。
f 確認コードの登録と取得に使用した電子メールまで移動して、入力します。

> **メモ:**
> 電子メールが表示されない場合は、スパムをチェックしてください。

g **アカウントの確認** をクリックします。確認を完了すると、Web ポータルが開きます。
h 保護されたファイルを Web ポータルにドラッグして、**今すぐアップロード** をクリックします。
i 登録後に受信するウェルカムメールには、Windows クライアントをダウンロードするためのリンクが含まれています。

> **メモ:**
> Hosted Dell Security Center がマルチテナントの場合、必要になるインストール ID もリストされます。

On-prem Dell Management Server

Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。

> **メモ:**
> オンプレミス には、登録前に Data Guardian をインストールできます。アクティブ化するには、**登録** リンクをクリックします。

a Dell Data Guardian ウィンドウが開いたら、メールアドレスを入力します。
b **登録** をクリックします。
c 登録ページでパスワードを入力して確定し、**サインイン** をクリックします。
登録の確認 ダイアログが表示され、内部ユーザーが入力した電子メールアドレス宛に電子メールが送信されます。メールが表示されない場合、スパムをチェックしてください。
d Dell Server からのアカウント確認メールに含まれたハイパーリンクをクリックします。

> **メモ:**
> 電子メールが表示されない場合は、スパムをチェックしてください。

e Web ページに移動します。
f 確認 ページで、**ログインして続行する** をクリックします。
g ログインページで、**パスワードを忘れた** をクリックします。

> **メモ:**
> Dell Server はランダムなパスワードを割り当てています。このパスワードはリセットする必要があります。

h パスワードのリセット ページで、パスワードを入力して確定し、**登録** をクリックします。
登録の確認 ダイアログが表示され、内部ユーザーが入力した電子メールアドレス宛に電子メールが送信されます。
i アカウントの有効化メールを開いてリンクをクリックします。
この電子メールには、Data Guardian のインストールで使用する Dell Server 名も記載されています。
j ログイン ページで、登録に使用した電子メールアドレスとパスワードを入力します。
k **ログイン** をクリックします。
Data Guardian のダウンロードページが開きます。

Data Guardian for Windows のダウンロードおよびインストール

登録後、リンクをクリックして Windows クライアントをダウンロードできます。内部ユーザーの初期設定に応じて、次のリンクを使用できます。

- Security Management Server の場合、Windows クライアントで利用できるオプションを含むダウンロードページが開きます。
- Security Management Server Virtual で、Windows をクリックすると、dell.com/support サイトに移動します。
- 保護されたファイルを受信した場合は、カバーページに、クライアントをダウンロードするためのリンクが記載されています。
- クライアントをダウンロードするためのリンクが記載されたウェルカムメールを受信する場合があります。

次の手順は、Windows への Data Guardian のインストール方法を示します。

1 Windows で、コンピュータのオペレーティングシステムに応じて、**ダウンロード（32 ビット）**または **ダウンロード（64 ビット）**をクリックします。
2 お使いのコンピュータのディレクトリにセットアップファイルをダウンロードします。
3 セットアップファイルをダブルクリックして、インストーラを起動します。
4 言語を選択し、**OK** をクリックします。
5 Microsoft Visual C++ 2010 再頒布可能パッケージをインストールするよう求められた場合、**OK** をクリックします。
6 ようこそ 画面で **次へ** をクリックします。
7 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。
8 宛先フォルダ 画面で、**次へ** をクリックして、**C:\Program Files\Dell\Dell Data Guardian** のデフォルトの場所にインストールします。
9 構成タイプ 画面で、次のいずれかを選択します。

Hosted Dell Security Center	On-prem Dell Management Server
a Hosted Dell Security Center を選択します。 b 会社の環境がマルチテナントの場合、カバーページまたはウェルカムメールに記載されているインストール ID を入力します。 c **次へ** をクリックします。 d 手順 10 に進みます。	a On-prem Dell Management Server を選択します。 b *サーバ名：* フィールドで、このコンピュータが通信する Dell Server の名前を入力します。この名前は、受信したアクティブ化電子メール、またはダウンロードページの最上部に記載されています。 c **次へ** をクリックします。 d アクティベーションサーバの確認画面で、Dell Server URL アドレスが正しいことを確認します。インストーラが www または http（https）、およびポートを追加します。**次へ** をクリックします。 e 手順 10 に進みます。

10 管理タイプ ウィンドウでは、次のオプションを選択します。
- 外部ユーザー：企業ドメイン電子メールアドレス以外のアドレスを持つユーザー。

11 **インストール** をクリックしてインストールを開始します。
ステータスウィンドウにインストールの進捗状況が表示されます。
12 インストール完了 画面が表示されたら、**終了** をクリックします。
13 **はい** をクリックして再起動します。
Data Guardian のインストールが完了します。
14 「Data Guardian のアクティブ化」を参照してください。

メモ:
「Windows での Data Guardian の使用」のメモと例外を参照してください。たとえば、保護された .pdf ファイルはネットワークからは開けません。Word を使用すると、保護されている .pdf ファイルをネットワークから開くことができます。

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

Data Guardian のアクティブ化

Data Guardian をインストールし、コンピュータを再起動した後、次の手順に従ってアクティブ化を行います。

1 Windows にログインします。

通知エリアに、橙色の感嘆符の付いたクラウドアイコンが表示されます。

2 通知エリアにダイアログが表示されたら、**クリックしてアクティブ化** をクリックします。
ダイアログボックスが表示されない場合、通知エリアで **Data Guardian** アイコンをクリックして、**ユーザーのアクティブ化** を選択します。

> **メモ:**
> ホスティング環境では、外部ユーザーがアクティブ化できるテナントは 1 度に 1 つだけです。1 つのテナントをすでにアクティブ化している場合、Data Guardian をアンインストールして、別のインストール ID で再インストールする必要があります。必要に応じて、保護対象ドキュメントのアップロードと表示を Web ポータルで行うこともできます。

3 登録に使用した電子メールアドレスとパスワードを入力して、**アクティブ化** をクリックします。

> **メモ:**
> オンプレミス で登録前に Data Guardian をインストールした場合、アクティブ化する際に **登録** リンクをクリックします。

アクティブ化が完了すると、Data Guardian 通知エリア アイコンに緑色のチェックマーク  が表示されます。

4 ユーザーモードステータスを確認してください。指定したユーザーの 通知エリア アイコンをクリックし、**詳細** を選択します。
最上部で ユーザーモード が次の値になっています。

外部：ドメイン電子メールアドレス以外のアドレスを持つユーザー。

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

内部ユーザーからのアクセスの要求

Windows、Mac、Mobile で、外部ユーザーが Data Guardian をインストールしてアクティブ化した場合、そのユーザーは保護された Office ドキュメントまたは .pdf 形式のファイルへのアクセスを内部ユーザーから要求できます。外部ユーザーはファイルごとに個別に要求する必要があります。

1 保護された Office ドキュメントを開いたときにアクセスを要求する必要があることが表示された場合、**はい** または **いいえ** をクリックします。
要求が正常に送信されたことを示すダイアログが表示されます。内部ユーザーはアクセスを承認または拒否することができます。外部ユーザーは結果について電子メールを受信します。内部ユーザーがアクセスを承認する前に、外部ユーザーが保護されたファイルを開いた場合、要求が保留中であることを示すメッセージが表示されます。

2 48 時間後、外部ユーザーはアクセスを再度要求することができます。
通知エリアで、外部ユーザーは Data Guardian アイコンを右クリックし、**詳細** ページを選択できます。**セキュリティ** タブをクリックします。要求の時間が なし に戻ると、外部ユーザーはアクセスを再度要求することができます。

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

外部ユーザーと Mac のタスク

Mac の内部ユーザータスク

以下のいずれかを行ってください。

- 保護されたドキュメント - 電子メール、ネットワーク共有、リムーバブルストレージのいずれかを使って外部ユーザーに送信します。
- Data Guardian のクラウド暗号化が有効になっている場合 - Dell Data Guardian インタフェースで、クラウドストレージプロバイダ列の横の列に保護対象ファイルをドラッグします。

Mac の外部ユーザータスク

Data Guardian の登録

内部ユーザーが初めてファイルを共有する場合、外部ユーザーは登録する必要があります。

Data Guardian を登録するには：

1 保護されたドキュメントを開いたとき、カバーページに警告が表示された場合は、リンクをクリックして有効な電子メールアドレスを登録します。

> **メモ:**
> カバーページには、オンプレミス の場合は Dell Server 名、Hosted Dell Security Center がマルチテナントの場合は特定のテナント用にインストール ID がリストされています。カバーページには、Data Guardian クライアントをダウンロードするためのリンクが含まれています。

2 会社の環境に応じて、次のいずれかを実行してください。

Hosted Dell Security Center

Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（ SaaS ）ソリューション。

a Dell Data Guardian Web ポータルが開いたら、電子メールアドレスを入力します。
b 下にスクロールして、**同意する** をクリックします。
c Dell Security Center ウィンドウで、下の アカウントが必要ですか? までスクロールして、**サインアップ** をクリックします。
d 新規アカウント ページに、電子メール、名、姓、パスワードを入力します。パスワードは 8 文字以上で、小文字、大文字、特殊文字、数字を含める必要があります。
e **サインアップ** をクリックします。
f 確認コードの登録と取得に使用した電子メールまで移動して、入力します。

> **メモ:**
> 電子メールが表示されない場合は、スパムをチェックしてください。

g **アカウントの確認** をクリックします。確認を完了すると、Web ポータルが開きます。
h 保護されたファイルをアップロードして、表示します。

Mac クライアントをダウンロードするためのリンクが含まれた電子メールを受信します。または、カバーページのリンクをクリックします。以下を参照してください。

On-prem Dell Management Server

Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。

a Dell Data Guardian ウィンドウが開いたら、メールアドレスを入力します。
b **登録** をクリックします。
c 登録ページでパスワードを入力して確定し、**サインイン** をクリックします。
登録の確認 ダイアログが表示され、内部ユーザーが入力した電子メールアドレス宛に電子メールが送信されます。メールが表示されない場合、スパムをチェックしてください。
d アカウントの確認メールを開いてリンクをクリックします。
この電子メールには、Data Guardian のインストールで使用する Dell Server 名も記載されています。
e 登録確認ページで、**ログインに戻る** をクリックします。

カバーページのリンクをクリックして、クライアントをダウンロードしてインストールします。以下を参照してください。

Data Guardian クライアントのダウンロードとインストール（ オプション ）

1 Dell Data Guardian ページで、登録に使用したメールアドレスとパスワードを入力します。
2 **ログイン** をクリックします。
Data Guardian ダウンロードページが開き、Windows、iOS、Android、Mac OS X のオプションが表示されます。
3 Mac OS X で **ダウンロード** をクリックします。
4 ドライバ & ダウンロード ページで、**Apple Mac OS** を選択し、**ダウンロード** をクリックします。
5 .Dmg ファイルをコンピュータのディレクトリにダウンロードして、.pkg ファイルを実行します。
6 ログイン / アクティブ化を行うには、次のいずれかを実行してください。

Hosted Dell Security Center

a 登録時に使用した電子メールアドレスを使用してください。
b ログイン情報は、.dmg にログインするために使用したものです。
c **ログイン** をクリックします。

On-prem Dell Management Server

a Data Guardian に内蔵されたオンラインヘルプを表示し、アカウント確認メールに記載されている Dell Server 名を入力します。
b 電子メールアドレスとパスワードも入力してください。ログイン情報は登録時に使用したものと同じです。
c **ログイン** をクリックします。

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

外部ユーザーと Mobile

内部ユーザーが保護されたファイルへのリンクをクラウドを介して共有している場合、ファイルには有効な電子メールアドレスを登録するためのリンクが含まれたカバーページが表示されます。

メモ:
カバーページには、オンプレミス の場合は Dell Server 名、Hosted Dell Security Center がマルチテナントの場合は特定のテナント用にインストール ID がリストされています。カバーページには、Data Guardian クライアントをダウンロードするためのリンクも含まれています。

Data Guardian ドキュメントを開いて表示するには、外部ユーザーは次を実行する必要があります。

- Data Guardian に登録する
- Data Guardian のダウンロードおよびインストール - 外部ユーザーはコンピュータの管理者権限を持っている必要があります。

Data Guardian の登録

内部ユーザーが初めてファイルを共有する場合、外部ユーザーは登録する必要があります。

Data Guardian を登録するには：

1 カバーページの警告でリンクをクリックして、有効な電子メールアドレスを登録してください。
2 会社の環境に応じて、次の手順の中から選んでください。

Hosted Dell Security Center

Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（ SaaS ）ソリューション。

a Dell Data Guardian Web ポータルが開いたら、電子メールアドレスを入力します。
b 下にスクロールして、**同意する** をクリックします。
c Dell Security Center ウィンドウで、下の アカウントが必要ですか? までスクロールして、**サインアップ** をクリックします。
d 新規アカウント ページに、電子メール、名、姓、パスワードを入力します。パスワードは 8 文字以上で、小文字、大文字、特殊文字、数字を含める必要があります。
e **サインアップ** をクリックします。
f 確認コードの登録と取得に使用した電子メールまで移動して、入力します。

メモ:
電子メールが表示されない場合は、スパムをチェックしてください。

On-prem Dell Management Server

Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。

メモ:
オンプレミス には、登録前に Data Guardian をインストールできます。アクティブ化するには、**登録** リンクをクリックします。

a Dell Data Guardian ウィンドウが開いたら、メールアドレスを入力します。
b **登録** をクリックします。
c 登録ページでパスワードを入力して確定し、**サインイン** をクリックします。
登録の確認 ダイアログが表示され、内部ユーザーが入力した電子メールアドレス宛に電子メールが送信されます。メールが表示されない場合、スパムをチェックしてください。
d Dell Server からのアカウント確認メールに含まれたハイパーリンクをクリックします。

メモ:
電子メールが表示されない場合は、スパムをチェックしてください。

Hosted Dell Security Center

g **アカウントの確認** をクリックします。確認を完了すると、Web ポータルが開きます。

h 保護されたファイルを Web ポータルにドラッグして、**今すぐアップロード** をクリックします。

i 登録後に受信するウェルカムメールには、Windows クライアントをダウンロードするためのリンクが含まれています。

メモ:
Hosted Dell Security Center がマルチテナントの場合、必要になるインストール ID もリストされます。

On-prem Dell Management Server

e Web ページに移動します。

f 確認 ページで、**ログインして続行する** をクリックします。

g ログインページで、**パスワードを忘れた** をクリックします。

メモ:
Dell Server はランダムなパスワードを割り当てています。このパスワードはリセットする必要があります。

h パスワードのリセット ページで、パスワードを入力して確定し、**登録** をクリックします。
登録の確認 ダイアログが表示され、内部ユーザーが入力した電子メールアドレス宛に電子メールが送信されます。

i アカウントの有効化メールを開いてリンクをクリックします。
この電子メールには、Data Guardian のインストールで使用する Dell Server 名も記載されています。

j ログイン ページで、登録に使用した電子メールアドレスとパスワードを入力します。

k **ログイン** をクリックします。
Data Guardian のダウンロードページが開きます。

Data Guardian for Mobile のダウンロードおよびインストール

以下のいずれかを行ってください。

- Android デバイスでの Data Guardian のインストール / アンインストール
- iOS デバイスでの Data Guardian のインストール / アンインストール

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

外部ユーザーと Web ポータル

内部ユーザーのタスク

内部ユーザーは、次のいずれかを実行できます。

- 外部ユーザーに会社の URL を送信し、Deta Guardian Web ポータルにアクセスできるようにします。
- 保護されたファイルを外部ユーザーに送信します。ユーザーがファイルを開くと、表紙が表示されます。

外部ユーザーが実行できる操作は、保護された Office ドキュメントの .pdf ファイルおよび .xen ファイルの表示と、ポリシーに基づくファイルの編集のみです。ただし、外部ユーザーは Data Guardian クライアントをダウンロードする必要がありません。

Web ポータルでの外部ユーザーのタスク

Data Guardian Web ポータルに登録するには、次の手順に従います。

1 内部ユーザーから受信した、または保護対象ファイルのカバーページにある、Web ポータルの URL をクリックします。

2 ライセンス契約画面を下にスクロールして、**同意する** をクリックします。

3 会社の環境がホストか On-prem かによって、次のいずれかの方法を使用してください。

Hosted Dell Security Center	On-prem Dell Management Server
Dell Data Security ソフトウェアを管理するための、ホストされたサービスとしてのソフトウェア（SaaS）ソリューション。	Dell Data Security ソフトウェアを管理するための、エンタープライズネットワーク内にあるオンプレミスサーバ。
a 電子メールとパスワードを入力します。 b **サインイン** をクリックします。 c 電子メール、名、姓、およびパスワードを入力します。パスワードは 8 文字以上で、小文字、大文字、特殊文字、数字を含める必要があります。 d **サインアップ** をクリックします。 e 確認コードの登録と取得に使用した電子メールまで移動して、入力します。 f 確認コードを入力し、**アカウントの確認** をクリックします。 Web ポータルが開きます。	a b **アカウントをお持ちでない場合** をクリックします。 c 電子メールアドレスを入力して、**登録** をクリックします。 **メモ:** 外部として登録する内部ユーザーの場合、これは非ドメイン電子メールアドレスです。 d 登録 ページで、パスワードを入力して確認し、**登録** をクリックします。 確認 ページに、入力した電子メールアドレス宛てに確認の電子メールが送信されたことが表示されます。 e 「アカウントの確認」という件名の電子メールを開き、リンクをクリックしてアカウントのアクティブ化を完了します。 f 登録の確認 画面で、**ログインに戻る** をクリックします。 g 登録に使用した電子メールアドレスとパスワードを入力します。
内部ユーザーがキーを共有していない場合は、ウェブポータルにアクセスすることができますが、ファイルを開くことはできません。	

4 Dell Data Guardian のアップロードページが開きます。

5 **参照** をクリックしてファイルを選択しアップロードするか、Web ポータルにファイルをドラッグ & ドロップします。

6 各ページのオンラインヘルプを表示するには、**?** をクリックします。

ファイルを編集するには、管理者がそのユーザーのポリシーを変更する必要があります。登録後に付与された場合、ウェブポータルからログアウトして、ログインし直す必要があります。

必要に応じて Data Guardian クライアントをダウンロードできます。カバーページには、Data Guardian クライアントをダウンロードするためのリンクが含まれています。カバーページには、オンプレミス の場合は Dell Server 名、Hosted Dell Security Center がマルチテナントの場合は特定のテナント用にインストール ID もリストされています。

内部ユーザーからのアクセスの要求

保護された Office ドキュメントまたは .pdf 形式のファイルをアップロードした際にアクセスできないことを示す アップロード失敗 ダイアログボックスが表示された場合、ファイルの作成者にアクセスを要求できます。

1 アップロード失敗 ダイアログで **はい** をクリックします。

2 内部ユーザーからアクセスの許可 / 拒否を示す電子メールが送信されるのを待ちます。

メモ:
内部ユーザーからの電子メールを受信しない場合、アクセスを再度要求する前に 48 時間待つ必要があります。内部ユーザーがアクセスを承認する前に保護されたファイルを開いた場合、要求が保留中であることを示すメッセージが表示されます。

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

保護された Office ドキュメントの表示

企業が Office ドキュメントを保護するポリシーを有効にし、内部ユーザーが保護されたファイルを外部ユーザーに送信した場合、外部ユーザーは、最初にドキュメントを開くときに Dell Server に接続する必要があります。この後、外部ユーザーは指定した期間（例：一週間）オフラインでドキュメントを開いて表示できます。外部ユーザーは、Dell Server に接続してから保護されたドキュメントを再度開く必要があります。

セキュリティ上の理由で、外部ユーザーは保護された Office ドキュメントで次の操作を実行できません。

- 印刷
- エクスポート
- 名前を付けて保存
- 共有

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

Hosted Dell Security Center および一時停止されたテナント

Hosted Dell Security Center では、指定された期間内に支払いを行わないテナントを一時停止にできます（Windows、Mac、Mobile、Web ポータル）。

Data Guardian の内部 / 外部ユーザーには、以下が発生する場合があります。

- すべてのプラットフォーム - Data Guardian をインストール、アクティブ化、または Data Guardian にログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。
- Mac - Data Guardian が開いているときにテナントが一時停止されている場合、エクスプローラとすべてのファイルを閉じた後に一時停止されているテナントのダイアログが表示され、保護されたファイルを開こうとします。
- Web ポータル：
  - すでにログインしていて暗号化されたファイルをアップロードした場合、アップロードに失敗したことを示すメッセージが表示されます。
  - 暗号化されたファイルまたは非暗号化ファイルがアップロードされてテナントが一時停止された場合、ダウンロードに失敗したことを示すメッセージが表示されます。
  - ログアウト後に再度ログインしようとすると、テナントが一時停止されていることを示すダイアログが表示されます。

管理者に連絡してください。

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

Data Guardian のアクセス グループ（オンプレミス）を利用してセキュリティを強化する

Data Guardian のアクセス グループは、暗号化されたデータを使用してコラボレーションを行うためのユーザー グループを作成することにより、セキュリティを強化します。ファイルの所有者がアクセス権を与えない限り、グループ外のユーザーは、データにアクセスしたり表示したりすることはできません。アクセス グループには、内部ユーザーと外部ユーザーを含めることができます。アクセス グループは、Windows、Mac、モバイル、Web ポータルで使用できます。

企業ごとに、次のいずれかのオプションを選択します。

- オプトイン モードで Data Guardian をインストールしている企業
- Force-Protected モードで Data Guardian をインストールしている企業
- Data Guardian をインストールしておらず、オプトイン モードの企業
- Data Guardian をインストールしておらず、Force-Protected モードの企業

また次の操作も実行できます。

- 暗号化されたファイルの所有者の変更
- キーへのアクセス権を取り消す

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

オプトイン モードで Data Guardian をインストールしている企業

企業がアクセス グループを使用して機密データのセキュリティを強化している場合、誰がアクセス グループのメンバーなのかを把握しておく必要があります。まず円滑な移行のために、既存の暗号化された共有ファイルを処理するための短い移行期間を設けます。移行期間の終了後、アクセス グループ内のユーザーは、所有者が作成した暗号化された共有ファイルを表示することができます。アクセス グループ外の人間にアクセス権を付与することができます。

アクセス グループ内のユーザーを特定する

管理者は、各ファイルへのアクセス権の必要性に応じて、アクセス グループに属するユーザーを所有者に通知します。これには、内部ユーザーと外部ユーザーを含めることができます。特定のユーザーと機密データを扱う場合は、そのコンテンツのためのアクセス グループを作成するように管理者に要求できます。

移行期間に暗号化された共有ファイルを処理する

Data Guardian をインストール済みで、既存ファイルが暗号化されている場合、企業にとってのベスト プラクティスは、共有する暗号化ファイルのために、短い移行期間を設けることです。円滑に移行するために、暗号化された共有ファイルについては、次の注意事項に留意してください。

- ファイルの所有者または作成者は、内部か外部かにかかわらず、引き続きファイルにアクセスできます。
- アクセス グループ内の内部または外部ユーザーは、ほとんどの共有ファイルにアクセスできます。一部のファイルに関連付けられているキーの種類によっては、一部のファイルにアクセスできない場合があります。
- アクセス グループ外の内部ユーザー：ユーザーはキーへのアクセス権を取得するために、移行期間中に共有ファイルを開く必要があります。移行期間中に暗号化された共有ファイルを開かないと、ファイルへのアクセス権を失います。
- アクセス グループ外の外部ユーザー：すでに暗号化されたファイルへのアクセス権がある場合、外部ユーザーは移行期間中でも移行期間後でも、引き続きアクセスすることができます。

移行期間後に、ファイル アクセスができなくなった場合、所有者にアクセス権を要求できます。

移行期間後に、暗号化された共有ファイルへのアクセスを回復する

オプトイン モードの Windows および Mac では、次の操作によりアクセス権を回復できます。

- 保護された Office ドキュメント - アクセス権を要求するよう内部および外部ユーザーに求めるダイアログが表示され、ファイルの所有者がアクセス権を付与するかどうかを決定します。
- 基本ファイル保護で暗号化されたその他のファイル タイプ - 共有後のプロンプトはありません。ユーザーはファイルの所有者を知っている必要があり、さらに、暗号化されたファイルを右クリックして、[Data Guardian] タブでキー ID を確認する必要があります。ユーザーはこの情報を所有者に送信してアクセス権を要求できます。

移行期間後に新たに暗号化されたファイルでのコラボレーション

移行期間後に作成して暗号化する新しいファイル：

- アクセス グループ内の内部または外部ユーザー：すべての暗号化された共有ファイルにアクセスできます。
  - アクセス グループから削除されたユーザーは、アクセス権を失います。
  - ファイルの所有者がグループから削除されても、他のユーザーは引き続きアクセスできます。
- アクセス グループ外の内部または外部ユーザー：暗号化されたファイルを表示できません。
  - アクセス グループ内の内部ユーザーはアクセス権を付与できます。
  - 外部ユーザーが暗号化されたファイルの所有者である場合は、別のユーザーにアクセス権を付与できます。
  - グループ外の内部または外部ユーザーが保護された Office ドキュメントを受け取り開こうとすると、アクセス権を要求することを求めるダイアログが表示されます。
  - グループ外の内部または外部ユーザーが基本ファイル保護のファイル タイプを受け取り開こうとしている場合は、暗号化ファイルを右クリックして [Data Guardian] タブでキー ID を見つけ、その情報を所有者に送信することができます。

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

Force-Protected モードで Data Guardian をインストールしている企業

企業がアクセス グループを使用して機密データのセキュリティを強化している場合、誰がアクセス グループのメンバーなのかを把握しておく必要があります。まず円滑な移行のために、既存の暗号化された共有ファイルを処理するための短い移行期間を設けます。移行期間の終了後、アクセス グループ

内のユーザーは、所有者が作成した暗号化された共有ファイルを表示することができます。アクセス グループ外の人間にアクセス権を付与することができます。

アクセス グループ内のユーザーを特定する

管理者は、各ファイルへのアクセス権の必要性に応じて、アクセス グループに属するユーザーを所有者に通知します。これには、内部ユーザーと外部ユーザーを含めることができます。特定のユーザーと機密データを扱う場合は、そのコンテンツのためのアクセス グループを作成するように管理者に要求できます。

移行期間に暗号化された共有ファイルを処理する

Data Guardian をインストール済みで、既存ファイルが暗号化されている場合、企業にとってのベスト プラクティスは、共有する暗号化ファイルのために、短い移行期間を設けることです。円滑に移行するために、暗号化された共有ファイルについては、次の注意事項に留意してください。

- ファイルの所有者または作成者は、内部か外部かにかかわらず、引き続きファイルにアクセスできます。
- アクセス グループ内の内部または外部ユーザーは、ほとんどの共有ファイルにアクセスできます。一部のファイルに関連付けられているキーの種類によっては、一部のファイルにアクセスできない場合があります。
- アクセス グループ外の内部ユーザー：ユーザーはキーへのアクセス権を取得するために、移行期間中に共有ファイルを開く必要があります。移行期間中に暗号化された共有ファイルを開かないと、ファイルへのアクセス権を失います。
- アクセス グループ外の外部ユーザー：すでに暗号化されたファイルへのアクセス権がある場合、外部ユーザーは移行期間後も引き続きアクセスすることができます。

移行期間後に、ファイル アクセスができなくなった場合、所有者にアクセス権を要求できます。

移行期間後に、暗号化された共有ファイルへのアクセスを回復する

Force-Protected モードの Windows および Mac では、次の操作によりアクセス権を回復できます。

- 保護された Office ドキュメント - アクセス権を要求するよう内部および外部ユーザーに求めるダイアログが表示され、ファイルの所有者がアクセス権を付与するかどうかを決定します。
- 基本ファイル保護で暗号化されたその他のファイル タイプ - 共有後のプロンプトはありません。ユーザーはファイルの所有者を知っている必要があり、さらに、暗号化されたファイルを右クリックして、[Data Guardian] タブでキー ID を確認する必要があります。ユーザーはこの情報を所有者に送信してアクセス権を要求できます。

移行期間後に新たに作成されたファイルでのコラボレーション

移行期間後に作成して暗号化する新しいファイル：

- アクセス グループ内の内部または外部ユーザー：すべての暗号化された共有ファイルにアクセスできます。
  - アクセス グループから削除されたユーザーは、アクセス権を失います。
  - ファイルの所有者がグループから削除されても、他のユーザーは引き続きアクセスできます。
- アクセス グループ外の内部または外部ユーザー：暗号化されたファイルを表示できません。
  - アクセス グループ内の内部ユーザーはアクセス権を付与できます。
  - 外部ユーザーが暗号化されたファイルの所有者である場合は、別のユーザーにアクセス権を付与できます。
  - グループ外の内部または外部ユーザーが暗号化されたファイルを受け取り開こうとすると、アクセス権を要求することを求めるダイアログが表示されます。

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

Data Guardian をインストールしておらず、オプトイン モードの企業

企業が機密データのセキュリティ強化を目的に Data Guardian のアクセス グループの利用を計画している場合、ベスト プラクティスは、内部または外部ユーザーと共有するファイルをすべて特定し、管理者が所有者のために作成するアクセス グループのメンバーを決定することです。まず円滑な移行のために、既存の共有ファイルを処理するための短い移行期間を設けます。移行期間が完了すると、アクセス グループ内のユーザーは、所有者が作成した暗号化された共有ファイルを表示できます。アクセス グループ外の人間とコラボレーションしながら、セキュリティも強化するために、アクセス権を付与することができます。

アクセス グループ内のユーザーを特定する

管理者は、各ファイルへのアクセス権の必要性に応じて、アクセス グループに属するユーザーを所有者に通知します。これには、内部ユーザーと外部ユーザーを含めることができます。特定のユーザーと機密データを扱う場合は、そのコンテンツのためのアクセス グループを作成するように管理者に要求できます。

移行期間に共有ファイルを処理する

Data Guardian がインストールされている場合、管理者がポリシーを有効にしていれば、Windows または Mac でスイープが実行され、次のファイルが暗号化されます。

- 基本ファイル保護のために設定された.txt や.png などの追加ファイル タイプ
- データ分類ファイル（ Windows ）
- TITUS 分類ファイル（ Windows ）

すでにファイルを使用してコラボレーションしている場合、またはファイルを内部または外部のユーザーと共有している場合、ユーザーはアクセス グループに属している場合とそうでない場合があります。円滑な移行のためのベスト プラクティスは、他のユーザーと共有する暗号化されたファイルを処理するための短い移行期間を設けることです。この移行期間中は、コンピューターにログインしている必要があります。

そうしたファイルの共有またはコラボレーションを継続する場合は、次の点に注意してください。

- 上記にリストされている共有ファイルの場合、最初にログインしてコンピューターをスイープした人間が所有者になります。
- 別のユーザーがファイルの所有者になってしまい、元の作成者がアクセス グループに属していない場合、元の所有者は新しい所有者にアクセス権を要求する必要があります。元の所有者が管理者に所有権の変更を要求することもできます。
- 外部ユーザーのコンピューターはスイープされないため、保護されていない共有ファイルのコピーはスイープされず、暗号化されません。
- Data Guardian のクラウド暗号化が有効になっていて、ユーザーがフォルダーまたはファイルをクラウド ストレージ プロバイダーで共有している場合、そのファイルもスイープされます。

移行期間後に新たに作成されたファイルでのコラボレーション

移行期間後に作成して暗号化する新しいファイル：

- アクセス グループ内の内部または外部ユーザー：すべての暗号化された共有ファイルにアクセスできます。
  - アクセス グループから削除されたユーザーは、アクセス権を失います。
  - ファイルの所有者がグループから削除されても、他のユーザーは引き続きアクセスできます。
- アクセス グループ外の内部または外部ユーザー：暗号化されたファイルを表示できません。

- アクセス グループ内の内部ユーザーはアクセス権を付与できます。
- 外部ユーザーが暗号化されたファイルの所有者である場合は、別のユーザーにアクセス権を付与できます。
- グループ外の内部または外部ユーザーが暗号化されたファイルを受け取り開こうとすると、アクセス権を要求することを求めるダイアログが表示されます。

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

Data Guardian をインストールしておらず、Force-Protected モードの企業

企業が機密データのセキュリティ強化を目的に Data Guardian のアクセス グループの利用を計画している場合、ベスト プラクティスは、内部または外部ユーザーと共有するファイルをすべて特定し、管理者が所有者のために作成するアクセス グループのメンバーを決定することです。まず円滑な移行のために、既存の共有ファイルを処理するための短い移行期間を設けます。移行期間が完了すると、アクセス グループ内のユーザーは、所有者が作成した暗号化された共有ファイルを表示できます。アクセス グループ外の人間とコラボレーションしながら、セキュリティも強化するために、アクセス権を付与することができます。

アクセス グループ内のユーザーを特定する

管理者は、各ファイルへのアクセス権の必要性に応じて、アクセス グループに属するユーザーを所有者に通知します。これには、内部ユーザーと外部ユーザーを含めることができます。特定のユーザーと機密データを扱う場合は、そのコンテンツのためのアクセス グループを作成するように管理者に要求できます。

移行期間に共有ファイルを処理する

Data Guardian がインストールされている場合、管理者がポリシーを有効にしていれば、Windows または Mac でスイープが実行され、次のファイルが暗号化されます。

- Office 文書
- PDF
- 基本ファイル保護のために設定された.txt や.png などの追加ファイル タイプ

円滑な移行のためのベスト プラクティスは、他のユーザーと共有する暗号化されたファイルを処理するための短い移行期間を設けることです。この移行期間中は、コンピューターにログインしている必要があります。

そうしたファイルの共有またはコラボレーションを継続する場合は、次の点に注意してください。

- 上記にリストされている共有ファイルの場合、最初にログインしてコンピューターをスイープした人間が所有者になります。
- 別のユーザーがファイルの所有者になってしまい、元の作成者がアクセス グループに属していない場合、元の所有者は新しい所有者にアクセス権を要求する必要があります。元の所有者が管理者に所有権の変更を要求することもできます。
- 外部ユーザーのコンピューターはスイープされないため、保護されていない共有ファイルのコピーはスイープされず、暗号化されません。
- Data Guardian のクラウド暗号化が有効になっていて、ユーザーがフォルダーまたはファイルをクラウド ストレージ プロバイダーで共有している場合、そのファイルもスイープされます。

移行期間後に新たに作成されたファイルでのコラボレーション

移行期間後に作成して暗号化する新しいファイル：

- アクセス グループ内の内部または外部ユーザー：すべての暗号化された共有ファイルにアクセスできます。

- アクセス グループから削除されたユーザーは、アクセス権を失います。
- ファイルの所有者がグループから削除されても、他のユーザーは引き続きアクセスできます。

- アクセス グループ外の内部または外部ユーザー：暗号化されたファイルを表示できません。
  - アクセス グループ内の内部ユーザーはアクセス権を付与できます。
  - 外部ユーザーが暗号化されたファイルの所有者である場合は、別のユーザーにアクセス権を付与できます。
  - グループ外の内部または外部ユーザーが暗号化されたファイルを受け取り開こうとすると、アクセス権を要求することを求めるダイアログが表示されます。

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

暗号化されたファイルの所有者の変更

アクセス グループの移行期間中に、自分が作成した暗号化された共有ドキュメントの所有者に別のユーザーが指定された場合は、管理者に自分を所有者として指定するように要求することができます。

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

キーへのアクセス権を取り消す

暗号化ファイルのアクセス権を外部ユーザーに与えた場合、そのユーザーはそのファイルを開くためのキーを所有しています。
外部ユーザーに与えられたファイルのアクセス権を無効にする場合は、必要に応じて、管理者にキーの取り消しをリクエストできます。この操作は外部ユーザーにのみ適用されます。

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

Windows での保護ファイルの事前共有

Data Guardian をインストールし、1 つ以上のアクセス グループに割り当てる必要があります。
内部ユーザーまたは外部ユーザーがアクセス グループに属していない場合は、保護されたファイルを事前に共有できます。

1 保護対象ファイルを右クリックして、[**保護されたファイル アクセス**] を選択します。
[保護されたファイル アクセス共有] の [選択ファイル] に、ドキュメント名が表示されます。

2 [共有する *E* メール] で [**追加**] をクリックして、アクセス グループに属していない外部ユーザーまたは内部ユーザーの有効な E メール アドレスを入力します。
一度に最大 10 個の個別アドレスを追加できます。

3 E メール アドレスを変更するには、[**変更**] をクリックします。

4 E メール アドレスを削除するには、エントリを選択して [**削除**] をクリックします。

> **メモ:**
> ファイル所有者の名前が表示されますが、この名前は選択も削除もできません。

5 [使用できるグループ] に、自分の所属するアクセス グループが表示されます。1 つ以上のグループを選択し、矢印を使用して [共有グループ] に追加します。

6 **OK** をクリックします。成功メッセージが表示されます。

> **メモ:**
> 外部ユーザーは、保護されたドキュメントを別の外部ユーザーと共有することはできません。

外部ユーザーが Data Guardian で保護されたファイルを初めて受信する場合、このユーザーは Data Guardian をインストールするか、Web ポータルを使用して保護されたファイルを表示する必要があります。

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

Mac での保護ファイルの事前共有

Data Guardian をインストールし、1 つ以上のアクセス グループに割り当てる必要があります。
内部ユーザーまたは外部ユーザーがアクセス グループに属していない場合は、保護されたファイルを事前に共有できます。

1 保護対象ファイルを右クリックして、[**保護されたファイル アクセス**] を選択します。
[保護されたファイル アクセス共有] の [選択ファイル] に、ドキュメント名が表示されます。

2 [共有する *E* メール] で [**追加**] をクリックして、アクセス グループに属していない外部ユーザーまたは内部ユーザーの有効な E メール アドレスを入力します。
一度に最大 10 個の個別アドレスを追加できます。

3 E メール アドレスを削除するには、エントリを選択して [**削除**] をクリックします。

> **メモ:**
> ファイル所有者の名前が表示されますが、この名前は選択も削除もできません。

4 [使用できるグループ] に、自分の所属するアクセス グループが表示されます。1 つ以上のグループを選択し、矢印を使用して [共有グループ] に追加します。

5 **OK** をクリックします。成功メッセージが表示されます。

> **メモ:**
> 外部ユーザーは、保護されたドキュメントを別の外部ユーザーと共有することはできません。

外部ユーザーが Data Guardian で保護されたファイルを初めて受信する場合、このユーザーは Data Guardian をインストールするか、Web ポータルを使用して保護されたファイルを表示する必要があります。

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

iOS または Android での保護ファイルの事前共有

内部ユーザーまたは外部ユーザーがアクセス グループに属していない場合は、保護されたファイルを事前に共有できます。

1 保護されたファイルをタップします。

2

> **メモ:**
> [ユーザー] タブには、ファイル所有者の名前が表示されますが、この名前は選択も削除もできません。すでに内部ユーザーまたは外部ユーザーとファイルを共有している場合は、これらのユーザーの名前が表示されます。

3 [ユーザー] タブで、アクセス グループに属していない外部ユーザーまたは内部ユーザーの E メール アドレスを追加するには、右下にあるプラス アイコン (+) をクリックします。

4 メール アドレスを削除するには、スワイプして [**削除**] をタップします。

5 アクセス グループを表示するには、[**グループ**] タブをタップします。

6 保護されたファイルを共有するグループをタップします。

> **メモ:**
> チェックマークは、保護されたファイルを共有するために選択したグループを示します。

7 右上にある [**共有**] をタップします。
成功メッセージが表示されます。外部ユーザーは、保護されたドキュメントを別の外部ユーザーと共有することはできません。

外部ユーザーが Data Guardian で保護されたファイルを初めて受信する場合、このユーザーは Data Guardian をインストールするか、Web ポータルを使用して保護されたファイルを表示する必要があります。

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

Web ポータルでの保護ファイルの事前共有

内部ユーザーまたは外部ユーザーがアクセス グループに属していない場合は、保護されたファイルを事前に共有できます。

1 Web ポータルに、保護されたドキュメントをアップロードします。
1 つ以上のアクセス グループが割り当てられていると、[保護されたファイル アクセス] アイコンが、[ダウンロード] アイコンの横に表示されます。
2 [**保護されたファイル アクセス**] アイコンをクリックします。
[保護されたファイル アクセス共有] の [選択ファイル] に、ドキュメント名が表示されます。
3 [共有する *E* メール] で、[**新規追加**] をクリックします。
4 アクセス グループに属していない外部または内部ユーザーの有効な E メール アドレスを入力し、チェックマークをクリックして保存します。一度に最大 10 個の個別アドレスを追加できます。

> **メモ:**
> E メール アドレスを削除するには、[**X**] をクリックします。ドキュメントを共有しているユーザーの名前はハイライトされ、選択も削除もできません。

5 [使用できるグループ] に、自分の所属するアクセス グループが表示されます。[**すべて選択**] をクリックするか、オプションの横にある矢印アイコンをクリックして、[共有グループ] に追加します。あるいは削除します。
6 **OK** をクリックします。

> **メモ:**
> 外部ユーザーは、保護されたドキュメントを別の外部ユーザーと共有することはできません。

外部ユーザーが Data Guardian で保護されたファイルを初めて受信する場合、このユーザーは Web ポータルをインストールする必要があります。

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

外部ユーザーとして保護ファイルを事前共有

Data Guardian をインストールし、1 つ以上のアクセス グループに割り当てる必要があります。
ユーザーが保護されたファイルの作成者または所有者である場合、そのファイルを内部ユーザーと事前共有できます。保護されたドキュメントを別の外部ユーザーと共有することはできません。ファイルを所有していない場合は、共有できません。

- [共有する *E* メール] には、保護されたドキュメントを共有している他のユーザーの名前は表示されません。
- [使用できるグループ] には、グループが表示されません。個人の場合に限り、共有できます。

1 保護対象ファイルを右クリックして、[**保護されたファイル アクセス**] を選択します。
[保護されたファイル アクセス共有] の [選択ファイル] に、ドキュメント名が表示されます。
2 [共有する *E* メール] で [**追加**] をクリックして、アクセス グループに属していない外部ユーザーまたは内部ユーザーの有効な E メール アドレスを入力します。
一度に最大 10 個の個別アドレスを追加できます。
3 E メール アドレスを変更するには、[**変更**] をクリックします。

4 E メール アドレスを削除するには、エントリを選択して [**削除**] をクリックします。

> **メモ:**
> ファイルの所有者であるユーザーは、名前の選択も削除もできません。

5 **OK** をクリックします。成功メッセージが表示されます。

ユーザーが Data Guardian で保護されたファイルを初めて受信する場合、このユーザーは Data Guardian をインストールするか、Web ポータルを使用して保護されたファイルを表示する必要があります。

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

保護対象 E メールのアクセス権を与えられたユーザーを変更する

管理者が設定したポリシーによっては、保護対象 E メールを右クリックして、アクセス グループのユーザーに送信することができます。E メールのアクセス権が与えられるユーザーを変更できます。

1 Outlook で [保護] ラベルが付いている E メールを右クリックします。
2 画面の下の方にある [**保護対象 E メールへのアクセス**] を選択します。
共有アクセス権を持つユーザーの一覧が表示されます。
3 ユーザーに与えられた保護対象 E メールのアクセス権を無効にする場合は、そのユーザーを個別に削除します。

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

よくあるご質問（FAQ）

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

その他のよくあるご質問（FAQ）

質問

質問

コンピュータ名を変更したところ、ポリシーアップデートを取得できなくなり、クラウドへの暗号化も実行されていません。

回答

現在、Dell Server は最初にアクティブ化されたエンドポイントしか認識しません。エンドポイント名を変更すると、Dell Server がポリシーの送信先を認識しなくなり、Data Guardian も正常に機能しなくなります。

解決策

Data Guardian をアンインストールして再インストールします。アンインストールするには管理者権限が必要です。

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

Office ドキュメントおよび保護モードの FAQ

質問

Office ドキュメント（.docx、.pptx、.xlsx、.docm、.pptm、.xlsm）を開こうとしましたが、カバーページが表示されます。

回答

管理者が Office ドキュメントを保護するポリシーを設定した場合、管理者またはユーザーのいずれかは、Data Guardian をインストールする必要があります。通知エリアの Data Guardian アイコンにアクティブ化されていることを示す緑色のチェックマークが表示されていることを確認してください。

解決策

Data Guardian をインストールまたはアクティブ化する必要があるか判断します。「Data Guardian のインストール」または「アクティブ化で起こりうる問題」を参照してください。

質問

保護された Office ドキュメント（ Word、PowerPoint、または Excel ）を開くことができません。

回答

次を確認してください。

- ファイル制限機能の設定 - 管理者が Office ドキュメントを保護するポリシーを設定している場合、**ファイル > オプション** でこの設定を使用しないでください。

解決策

ファイル制限機能の設定 を確認するには：

1 Office ドキュメントで、**ファイル > オプション** を選択します。
2 リストから **セキュリティ センター** を選択します。
3 右側にある、**セキュリティ センターの設定** をクリックします。
4 リストから **ファイル制限機能の設定** を選択します。
5 *Word/Excel/PowerPoint 2007* 以降のドキュメントやテンプレートの場合、開く チェックボックスが選択されていないことを確認します。
6 **OK** をクリックします。