Dell Data Security Console

User Guide v3.9

January 2024
Rev. A01

DELL Technologies

メモ、注意、警告

メモ: 「メモ」は、製品をより上手に使用するための重要な情報であることを示します。

注意: **「注意」は、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: **「警告」は、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。**

Contents

1

はじめに

Data Security Console を使用すると、コンピュータのすべてのユーザーのセキュリティを確保するアプリケーションへのアクセス、コンピュータのドライブとパーティションの暗号化ステータスの表示および管理、PBA パスワードおよびリカバリの質問の容易な登録が可能です。

次の機能が利用可能です。

- PBA と使用するための認証情報の登録
- パスワード、スマートカードを含む多要素認証情報の利用
- パスワードを忘れた場合にヘルプデスクや管理者のサポートなしでのコンピュータへのアクセス回復
- Windows パスワードの容易な変更
- 個人的なプリファレンスの設定
- 暗号化ステータスの表示
- Firewall および Web Protection の表示（インストールされている場合）
- Advanced Threat Prevention ステータスの表示

サーバオペレーティングシステム上、Data Security Console から次の機能が使用できます。

- 暗号化ステータスの表示（自己暗号化ドライブ搭載のコンピュータ上）
- Advanced Threat Prevention の表示

Data Security Console

Data Security Console を開くには、デスクトップから Dell Data Security Console アイコン 

をダブルクリックします。

次のアプリケーションにアクセスすることができます。

- 暗号化ステータスには、コンピュータのドライブとパーティションの暗号化ステータスが表示されます。
- Advanced Threat Prevention ダッシュボードには、Advanced Threat Prevention ポリシーに基づいてコンピューターの保護ステータスが表示されます。
- Firewall および Web Protection ステータスのページには、コンピューターの Firewall および Web Protection による全体および個別の保護ステータスが表示されます。
- サインイン アクセス ツールでは、PBA パスワードのセットアップと管理、PBA セルフリカバリーの質問の設定、認証情報登録ステータスの表示を行うことができます。

本書では、これらのアプリケーションそれぞれの使用方法を説明します。

マニュアルのアップデートについて、定期的に dell.com/support をチェックしてください。

Dell ProSupport for Software へのお問い合わせ

Dell 製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 4310039）にご連絡ください。

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

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport for Software の各国の電話番号を記載したページを参照してください。

2

ナビゲーション

アプリケーションにアクセスするには、適切なタイルをクリックします。

タイトルバー

アプリケーション内からホームページに戻るには、アクティブなアプリケーションの名前の横にある、タイトルバーの左端の 戻る 矢印をクリックします。

別のアプリケーションに直接ナビゲートするには、アクティブなアプリケーションの名前の横にある下矢印をクリックし、アプリケーションを選択します。

Data Security Console を最小化、最大化、または閉じるには、タイトルバーの右端の該当するアイコンをクリックします。

最小化後に Data Security Console を復元するには、通知エリアアイコンをダブルクリックします。

ヘルプを開くには、タイトルバーで **?** をクリックします。

Data Security Console の詳細

Data Security Console、ポリシー、実行中のサービス、およびログに関する詳細を表示するには、タイトルバーの左側にあるギアアイコンをクリックします。この情報は、管理者がテクニカルサポートを提供する場合に必要になることがあります。

メニューから項目を選択します。

メニュー項目	目的
バージョン情報	バージョン情報です。
情報の表示	次の情報が含まれます。 ● 製品のバージョンと日付情報 ● Dell Encryption あるいは PBA の高度な認証が、企業またはローカル管理者によって管理されているかどうか ● オペレーティングシステム、BIOS、マザーボード、および Trusted Platform Module（TPM）のバージョン番号
MS 情報	Microsoft Windows システム情報ユーティリティを実行して、ハードウェア、コンポーネント、およびソフトウェア環境に関する詳細情報を表示します。
情報のコピー	管理者または Dell ProSupport に送信する電子メールに貼り付けられるよう、すべてのシステム情報をクリップボードにコピーします。
フィードバック	この製品に関するフィードバックを Dell に提供するためのフォームを表示します。（ドメイン以外のコンピュータでは、このオプションを常に使用できます。ドメインコンピュータでこのオプションを使用できるかどうかは、ポリシーによります。）
ポリシー	このコンピュータに適用されるポリシーの階層を表示します。
サービス	実行中のサービスに関する詳細を表示します。
サポート	Dell ProSupport の Web サイトに接続します。

Advanced Threat Prevention	Advanced Threat Prevention ペインの標準 UI を有効にします。
ログ	トラブルシューティングのため、ログされたイベントの詳細リストを表示します。

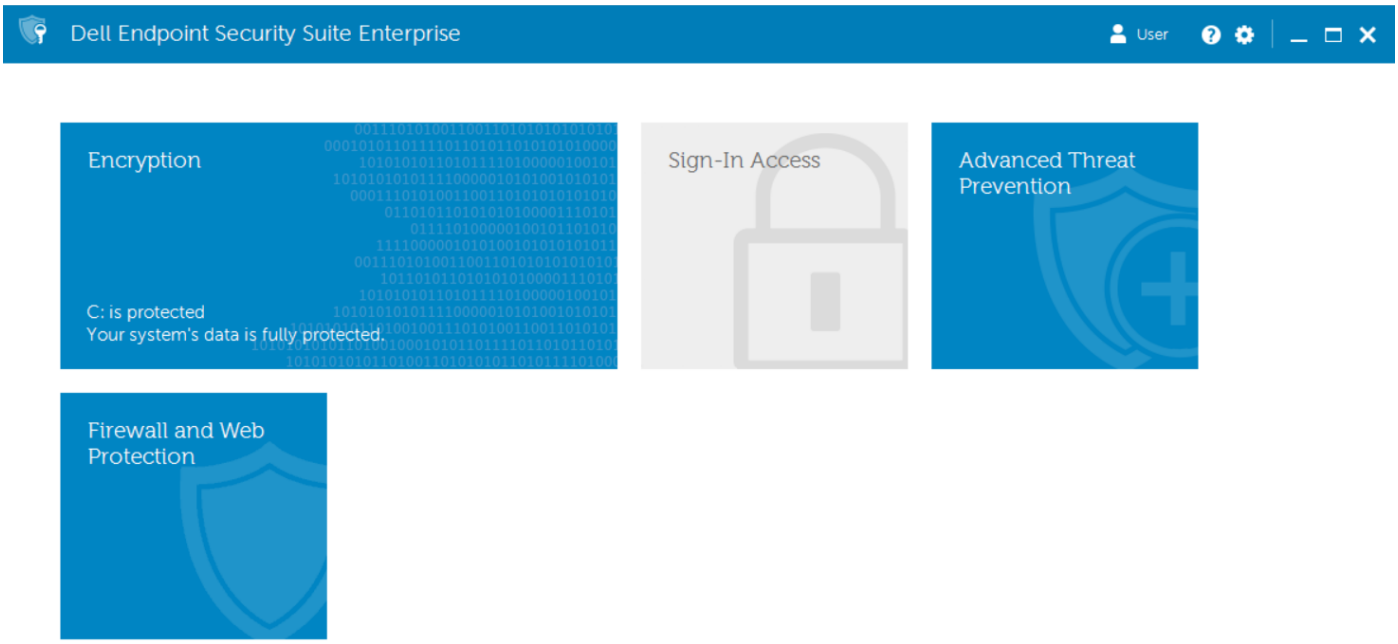
3

Advanced Threat Prevention

Advanced Threat Prevention 製品は、コンピュータ上またはメモリ領域で実行しようとするすべてのプロセスを監視し、異常または危険と思われるものにフラグ付けをしてマルウェアからコンピュータを保護します。

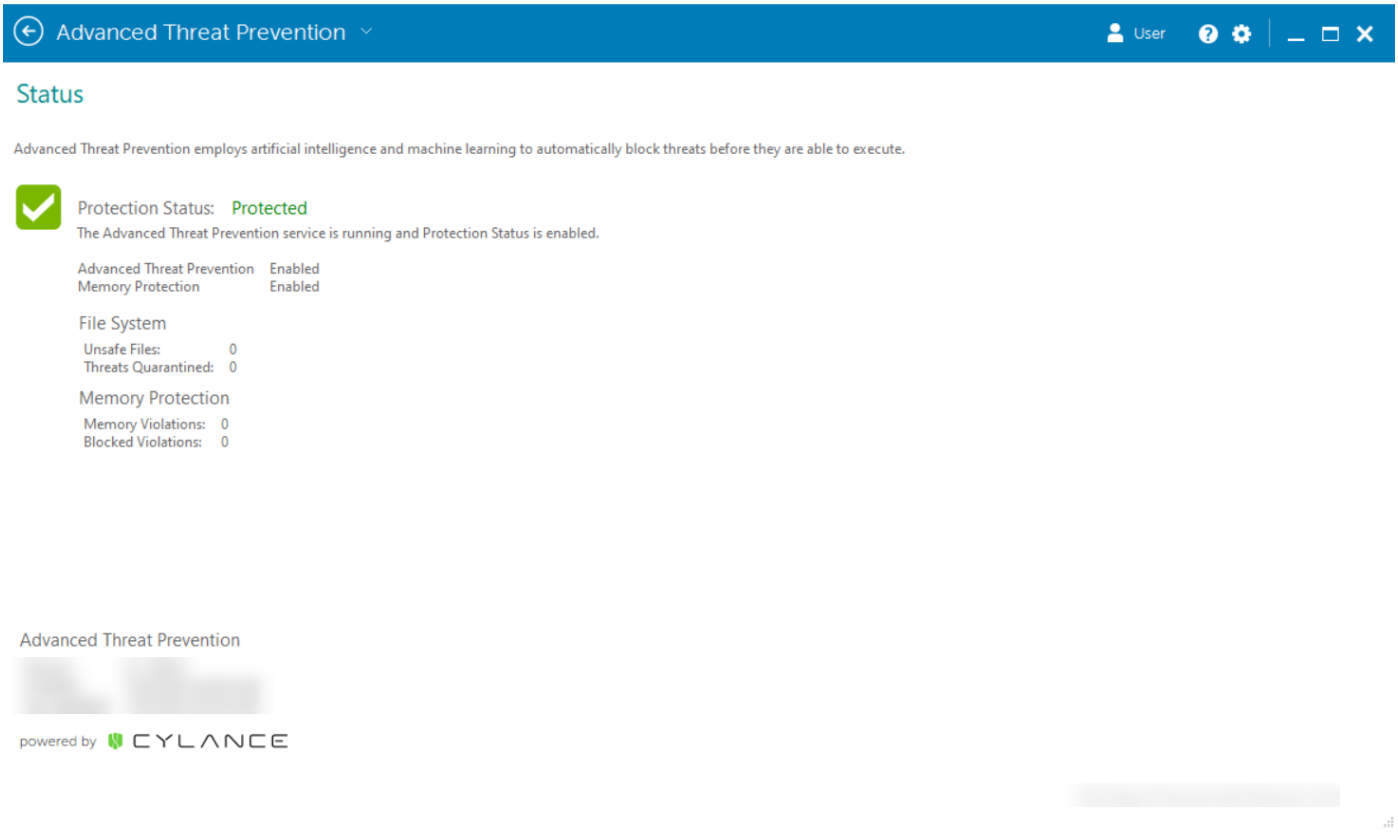
Advanced Threat Prevention はデフォルトで Endpoint Security Suite Enterprise と一緒にインストールされます。ファイアウォールおよび Web 保護が、Endpoint Security Suite Enterprise の一部としてオプションでインストールされています。

高度な監視と分析から得られたコンピュータの統計情報を表示するには、Advanced Threat Prevention タイルを選択します。



Advanced Threat Prevention のステータス

Advanced Threat Prevention のステータスページには、Data Security Console の **Advanced Threat Prevention** タイルからアクセスします。



保護ステータス

保護ステータスは、PC が保護された状態（緑色のチェック マーク）か、保護されていない状態（赤色の X 印）かを示します。このステータスは、Advanced Threat Prevention サービスが実行中かどうか、Dell Server で Advanced Threat Prevention がオンになっている（有効にされている）かどうかに基づきます。

- Advanced Threat Prevention - Dell Server で Advanced Threat Prevention がオンになっている（有効にされている）かどうかを示します。
- メモリー保護 - Dell Server でメモリー保護がオンになっている（有効にされている）かどうかを示します。

ファイルシステム

- 安全でないファイル - コンピュータ上に存在するマルウェアの可能性があるファイルの数
- 隔離された脅威 - コンピュータ上の元の場所から移され、実行できないようになっているファイルの数

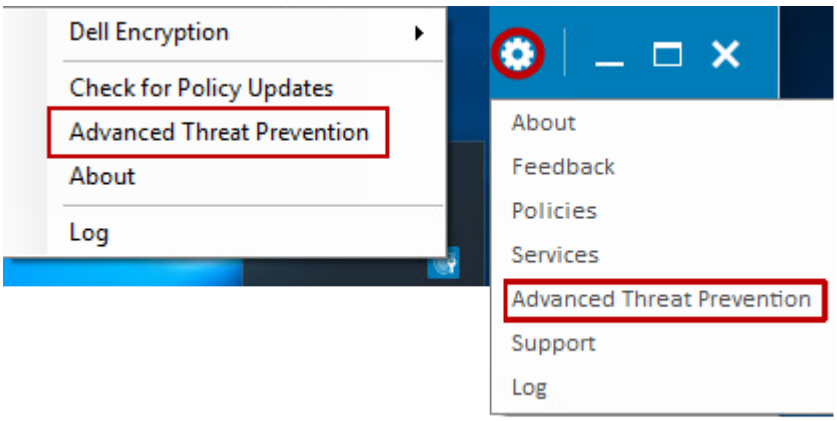
メモリ保護

- メモリ違反 - コンピュータメモリへの付加を試みたアプリケーションの試行回数。
- ブロックされた違反 - コンピュータメモリへの付加を試みたアプリケーションの試行がブロックされた回数。

標準 UI

標準 UI を使用すると、特定のエンドポイントでキャプチャされたイベントに関する詳細情報が表示される、Data Security Console のギアメニューまたはシステムトレイメニュー内の新しい機能を有効にすることができます。標準 UI ポリシーがリモート管理コンソールで有効になっている場合に**のみ**、標準 UI は有効になります。詳細については、リモート管理コンソールの右上隅の［**?**］を選択して、「管理者ヘルプ」を参照してください。

タイトルバーの左側にあるシステムトレイアイコンまたはギアアイコンをクリックして、Data Security Console で標準 UI を有効にすることができます。



次のオプションのいずれかを選択すると、Advanced Threat Prevention の詳細情報が表示されます。

- **脅威を表示**

  脅威を表示 オプションを選択すると、Advanced Threat Prevention により軽減された脅威と以下の詳細情報が表示されます。

  ファイルハッシュ ID - 脅威の SHA256 ハッシュ情報が表示されます。

  ファイル MD5 - MD5 ハッシュ。

  現在実行中? - 脅威が現在デバイスで実行されているかどうか。実行中、または 未実行 のいずれかが示されます。

  ファイルパス - 脅威が検出されたパス。ファイル名を含みます。

  スコア - 脅威のランク。

- **脆弱性を表示**

  脆弱性を表示 オプションを選択すると、Advanced Threat Prevention により軽減された脆弱性と以下の詳細情報が表示されます。

  イベント ID - 各脅威イベントに割り当てられた固有の番号。

  プロセス ID - メモリ保護によって識別されたアプリケーションのプロセス ID が表示されます。

  プロセスタグ - 起動サイクルごとにプロセスを分類する一意の識別子。

  イメージハッシュ - 脆弱性の SHA256 ハッシュ情報が表示されます。

  イメージパス - 脆弱性が発生したパス。ファイル名を含みます。

  ファイルバージョン - 脆弱なファイルのバージョン番号が表示されます。

- **スクリプトを表示**

  スクリプトを表示 オプションを選択すると、Advanced Threat Prevention により軽減されたスクリプトと以下の詳細情報が表示されます。

  スクリプトパス - スクリプトが発生したパス。ファイル名を含みます。

  イベント ID - 各スクリプトイベントに割り当てられた一意の番号。

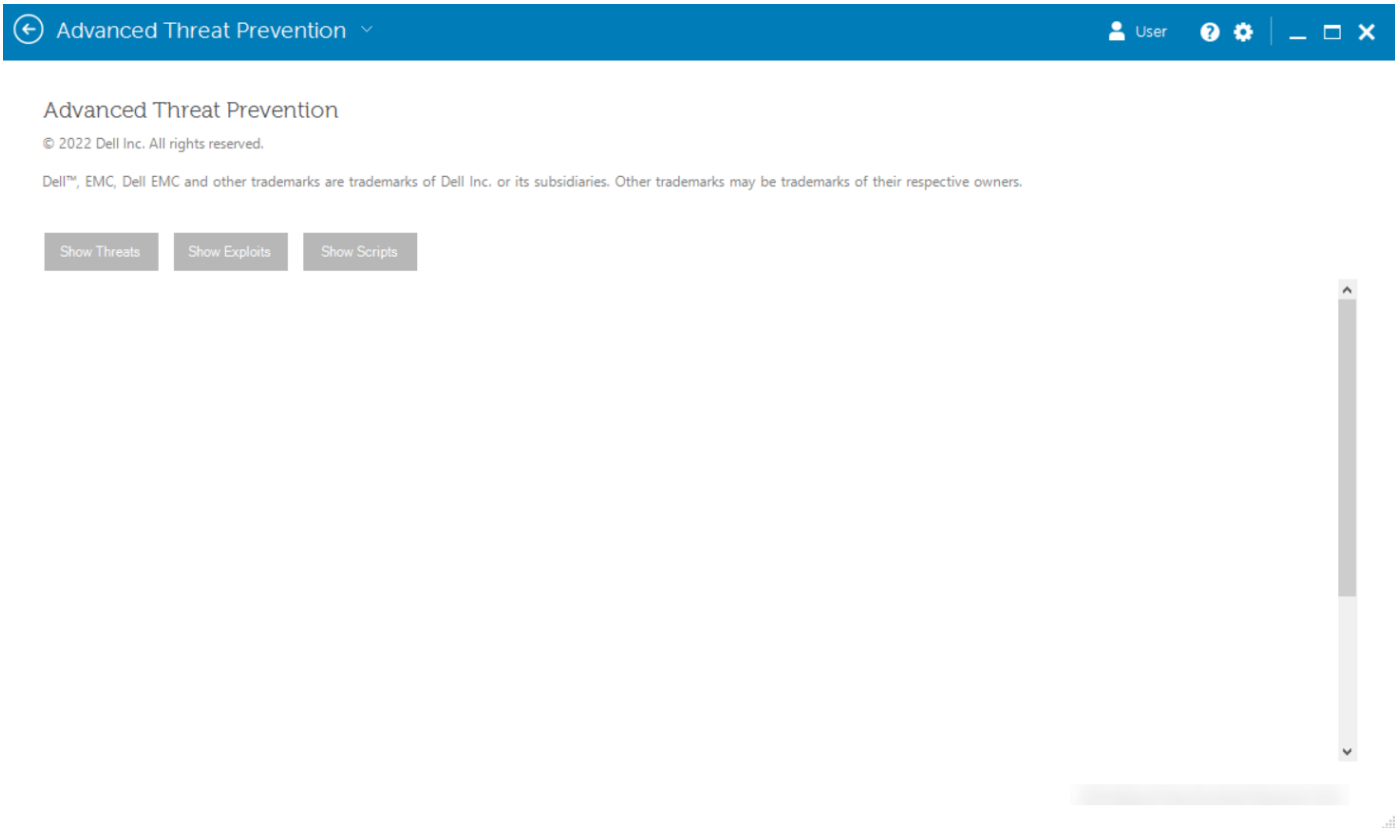
  ファイルのハッシュ ID - スクリプトの SHA256 ハッシュ情報が表示されます。

  ファイル MD5 - MD5 ハッシュ。

  ドライブタイプ - 内蔵ドライブか外付けドライブかの詳細情報。

  インタプリタ名 - 悪意のあるスクリプトを識別したスクリプト制御機能の名前。

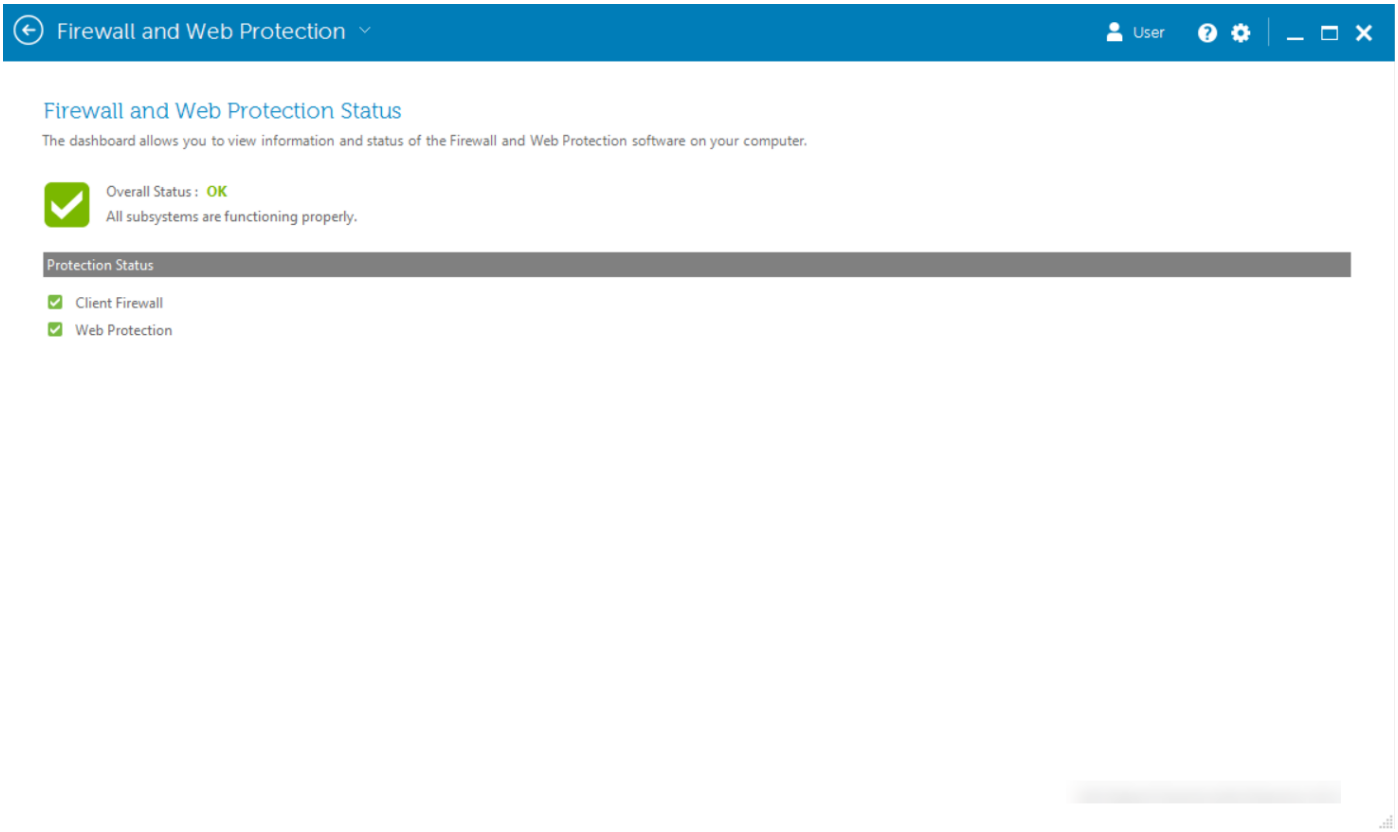
  インタプリタバージョン - スクリプト制御機能のバージョン番号。



表示されるイベントの一覧は、Data Security Console セッションの起動時に収集されたものです。新しいイベントを取得するには、Data Security Console を閉じてから再起動します。

Firewall および Web Protection のステータス

ファイアウォールおよび Web 保護のステータス ページには、Data Security Console の**ファイアウォールおよび Web 保護**タイルからアクセスします。



全体的な状態

全体的な状態は、PC が保護された状態にあるか脆弱な状態にあるかを示します。これは、Dell Server のファイアウォールおよび Web 保護ポリシー設定に基づきます。

- 保護対象 - *Web* 保護またはクライアント ファイアウォール ポリシーがオンになっている（有効にされている）場合、全体的な状態には［保護対象］と表示されます。
- 脆弱 - *Web* 保護およびクライアント ファイアウォール ポリシーがオフになっている（無効にされている）場合、全体的な状態には［脆弱］と表示されます。

保護ステータス

保護ステータス フィールドには、保護状態（緑色のチェックマーク）か、脆弱（赤色の X 印）かが個別に表示されます。このステータスは、Dell Server で次のポリシーがオンになっている（有効にされている）かどうかに基づきます。

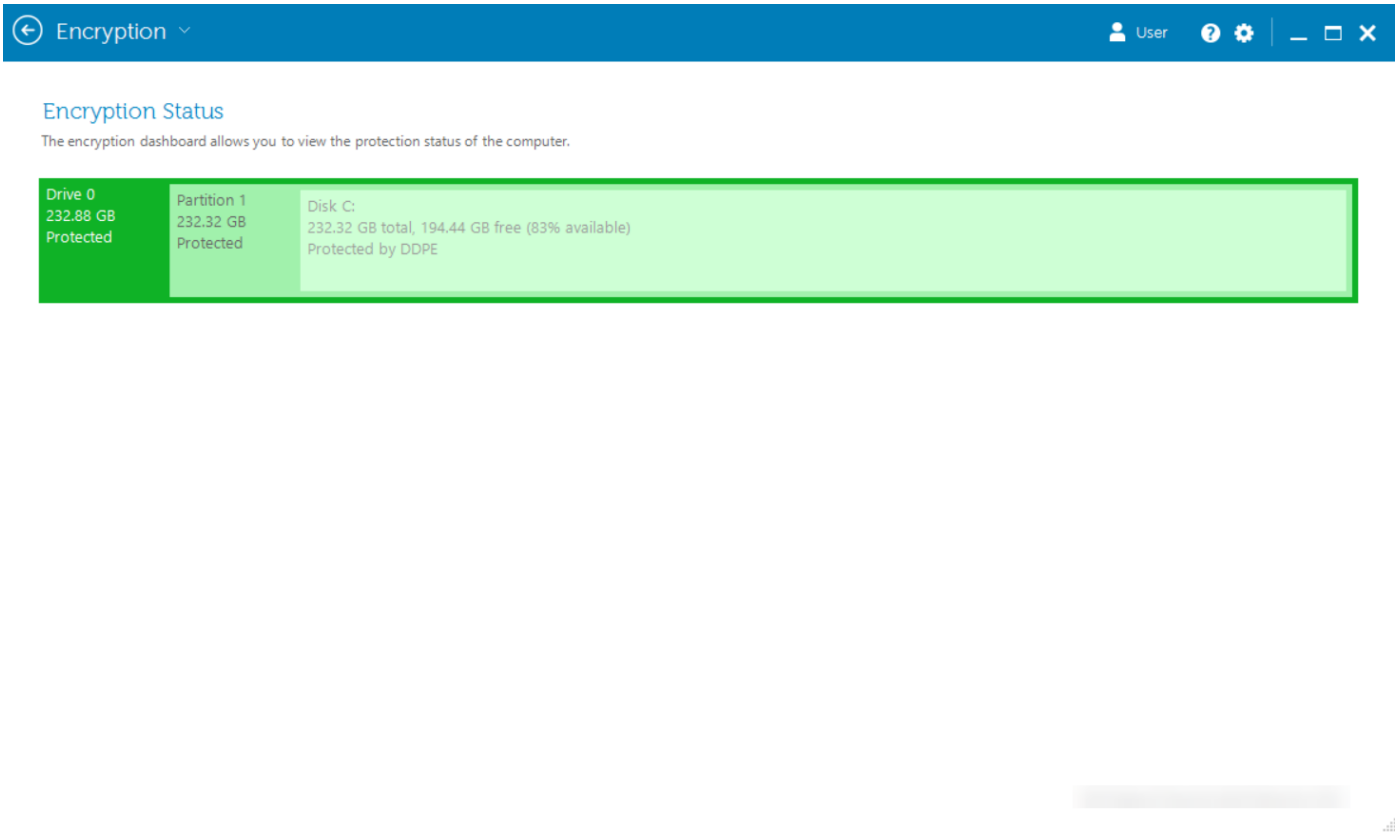
- クライアントファイアウォール - クライアントファイアウォール ポリシーがオンになっている（有効にされている）場合、全体的な状態には 保護対象 と表示されます。
- Web 保護 - *Web* 保護ポリシーがオンになっている（有効にされている）場合、全体的な状態には［保護対象］と表示されます。

4

暗号化ステータス

暗号化 ページはコンピュータの暗号化ステータスを表示します。ディスク、ドライブ、またはパーティションが暗号化されていない場合は、ステータスが 未保護 となります。ドライブまたはパーティションが暗号化されている場合は、ステータスが 保護 と表示されます。

暗号化ステータスをアップデートするには、該当するディスク、ドライブ、またはパーティションを右クリックして、**更新** を選択します。



5

サインインアクセス

サインインアクセスでは、管理者が設定したポリシーに基づいて、登録ステータスを登録、変更、チェックすることができます。

初回登録後に、サインインアクセス タイルをクリックして資格情報を追加または変更することができます。

メモ: サインインアクセス タイルは、PBA がアクティブになっている場合にのみ表示されます。

資格情報を初めて登録する

初めて資格情報を登録するには、次の手順を実行します。

1. Data Security Console ホームページで、**サインインアクセス** タイルをクリックします。
2. Windows パスワードを変更するには、パスワード ページで現在のパスワードを入力し、次に新規パスワードを入力して確認し、**変更** をクリックします。
3. リカバリ質問 ページで、3 つのリカバリ質問を選択してそれに対する回答を入力し、**登録** をクリックします。

資格情報の登録方法、または資格情報の変更方法の詳細については、「登録の追加、変更、表示」を参照してください。

登録の追加、変更、表示

登録を追加、変更、または表示するには、**サインインアクセス** タイルをクリックします。

左ペインのタブには、利用可能な登録がリストされています。これは、お使いのプラットフォームまたはハードウェアのタイプに応じて異なります。

サインイン アクセス ページでは、サポートされている認証情報、それらのポリシー設定（必須または該当なし）、登録ステータスが表示されます。ユーザーは、管理者によって設定されたポリシーに基づいて、このページから登録を管理できます。

- 認証情報を初めて登録する場合は、認証情報の行で**登録**をクリックします。
- 既存の登録済み認証情報を削除するには、**削除**をクリックします。
- 認証情報の登録または変更がポリシーによって許可されていない場合は、ステータス ページの**登録**リンクおよび**削除**リンクが非アクティブになっています。
- 既存の登録を変更するには、左ペインで該当するタブをクリックします。

  認証情報の登録または変更がポリシーによって許可されていない場合は、「認証情報を変更することはポリシーで許可されていません」というメッセージが認証情報の登録ページに表示されます。

パスワード

Windows パスワードを変更するには、次の手順を実行します。

1. **パスワード** タブをクリックします。
2. 現在の Windows パスワードを入力します。
3. 新しいパスワードを入力し、確認用にもう一度入力して、**変更** をクリックします。

   パスワードの変更はただちに有効になります。

4. 登録の成功 ダイアログで **OK** をクリックします。

   メモ:

   Windows パスワードは、Windows 上ではなく Data Security Console でのみ変更する必要があります。Windows パスワードが Data Security Console 以外で変更された場合、パスワードの不一致が発生し、復元操作が必要になります。

リカバリ質問

リカバリ質問 ページでは、リカバリ質問と回答を作成、削除、または変更することができます。リカバリ質問は、たとえば、パスワードの期限が切れた、またはパスワードを忘れた場合に、ユーザーが Windows アカウントにアクセスするための質問および回答に基づく方法を提供します。

メモ:

リカバリ質問は、コンピュータへのアクセスの回復のみに使用されます。質問と回答は、ログオンには使用できません。

登録済みの PBA リカバリ質問がない場合は、次の手順を実行します。

1. **リカバリ質問** タブをクリックします。
2. 事前定義された質問のリストから選択し、次に回答を入力して確定します。
3. **登録** をクリックします。

メモ:

リセット ボタンをクリックして、このページでの選択箇所を消去し、再起動します。

リカバリ質問がすでに登録されている

PBA リカバリ質問がすでに登録されている場合、削除することも再登録することもできます。

1. **リカバリ質問** タブをクリックします。
2. 次の該当するボタンをクリックします。
   - PBA リカバリ質問を完全に削除するには、**削除** をクリックします。
   - PBA リカバリ質問と回答を再定義する場合は、**再登録** をクリックします。

6

用語集

資格情報 - 資格情報とは、Windows パスワードなど、ある人物の身元を証明するものです。

起動前認証（PBA）- 起動前認証（PBA）は、BIOS または起動ファームウェアの拡張機能としての役割を果たし、信頼された認証レイヤとして、オペレーティングシステム外部のセキュアな耐タンパ環境を保証します。PBA は、ユーザーが正しい資格情報を持っていることを立証するまで、オペレーティングシステムなどをハードディスクから読み取ることができないようにします。

保護済み - 自己暗号化ドライブ（SED）の場合、コンピュータは、SED がアクティブ化され、起動前認証（PBA）が導入されると保護されます。

自己暗号化ドライブ（SED） - メディアに保存されるすべてのデータの暗号化とメディアから出力されるすべてのデータの復号化を自動的に実行する暗号化メカニズムが内蔵されたハードドライブです。このタイプの暗号化は、ユーザーに対して完全に透過的です。

シングルサインオン（SSO） - SSO は、起動前と Windows ログオンの両方で多因子認証が有効になっているとき、ログオン処理を簡素化します。有効になっている場合、認証は起動前のみで必要となり、ユーザーは Windows に自動的にログオンされます。有効ではない場合は、数回にわたる認証が必要となることがあります。

Trusted Platform Module（TPM） – TPM は、セキュアストレージ、測定、および構成証明という 3 つの主要機能を備えたセキュリティチップです。Encryption クライアントは、セキュアなストレージ機能のために TPM を使用します。TPM はまた、ソフトウェア資格情報コンテナ用に暗号化されたコンテナも提供できます。