

Dell Data Protection

Console ユーザーガイド

Advanced Threat Protection

暗号化ステータス

認証登録

Password Manager

v1.1



© 2016 Dell Inc.

Dell Data Protection | Encryption、Dell Data Protection | Endpoint Security Suite、Dell Data Protection | Endpoint Security Suite Enterprise、Dell Data Protection | Security Tools、および Dell Data Protection | Cloud Edition のマニュアル一式で使用される登録商標および商標：Dell™ および Dell ロゴ、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS®、および KACE™ は、Dell Inc. の商標です。Cylance® および Cylance ロゴは、米国およびその他の国における Cylance, Inc. の商標または登録商標です。McAfee® および McAfee ロゴは、米国およびその他の国における McAfee, Inc. の商標または登録商標です。Intel®、Pentium®、Intel Core Inside Duo®、Itanium®、および Xeon® は、米国およびその他の国における Intel Corporation の登録商標です。Adobe®、Acrobat®、および Flash® は、Adobe Systems Incorporated の登録商標です。Authen Tec® および Eikon® は、Authen Tec の登録商標です。AMD® は、Advanced Micro Devices, Inc. の登録商標です。Microsoft®、Windows®、および Windows Server®、Internet Explorer®、MS-DOS®、Windows Vista®、MSN®、ActiveX®、Active Directory®、Access®、ActiveSync®、BitLocker®、BitLocker To Go®、Excel®、Hyper-V®、Silverlight®、Outlook®、PowerPoint®、OneDrive®、SQL Server®、および Visual C++® は、米国および / またはその他の国における Microsoft Corporation の商標または登録商標のいずれかです。VMware® は、米国またはその他の国における VMware, Inc. の登録商標または商標です。Box® は、Box の登録商標です。DropboxSM は、Dropbox, Inc. のサービスマークです。Google™、Android™、Google™ Chrome™、Gmail™、YouTube®、および Google™ Play は、米国およびその他の国における Google Inc. の商標または登録商標のいずれかです。Apple®、Aperture®、App StoreSM、Apple Remote Desktop™、Apple TV®、Boot Camp™、FileVault™、 iCloudSM、iPad®、iPhone®、iPhoto®、iTunes Music Store®、Macintosh®、Safari®、および Siri® は、米国およびその他の国における Apple, Inc. のサービスマーク、商標、または登録商標のいずれかです。GO ID®、RSA®、および SecurID® は、EMC Corporation の登録商標です。EnCase™ および Guidance Software® は、Guidance Software の商標または登録商標のいずれかです。Travelstar® は、米国およびその他の国における Entrust®, Inc. の登録商標です。InstallShield® は、米国、中国、欧州共同体、香港、日本、台湾、および英国における Flexera Software の登録商標です。Micron® および RealSSD® は、米国およびその他の国における Micron Technology, Inc. の登録商標です。Mozilla® Firefox® は、米国および / またはその他の国における Mozilla Foundation の登録商標です。iOS® は、米国およびその他特定の国における Cisco Systems, Inc. の商標または登録商標であり、ライセンスに基づいて使用されています。Oracle® および Java® は、Oracle および / またはその関連会社の登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。SAMSUNG™ は、米国およびその他の国における SAMSUNG の商標です。Seagate® は、米国および / またはその他の国における Seagate Technology LLC の登録商標です。Travelstar® は、米国およびその他の国における HGST, Inc. の登録商標です。UNIX® は、The Open Group の登録商標です。VALIDITY™ は、米国およびその他の国における Validity Sensors, Inc. の商標です。VeriSign® およびその他の関連商標は、米国およびその他の国における VeriSign, Inc.、その関連会社、または子会社の商標または登録商標であり、Symantec Corporation にライセンス供与されています。KVM on IP® は、Video Products の登録商標です。Yahoo!® は、Yahoo! Inc. の登録商標です。

この製品は、7-Zip プログラムの一部を使用しています。ソースコードは、www.7-zip.org に掲載されています。ライセンス供与は、GNU LGPL ライセンス + unRAR 制限 (www.7-zip.org/license.txt) の対象です。

2016-07

以下を含む一件、または複数の米国特許によって保護されています：No. 7665125；No. 7437752；および No. 7665118。

本書に記載された情報は、通知なく変更される場合があります。

目次

1	はじめに	5
2	DDP Console	7
3	暗号化ステータス	9
4	Advanced Threat Protection	11
5	登録	13
	資格情報の初回登録	13
	登録の追加、変更、または表示	13
	パスワード	14
	リカバリ質問	14
	指紋	14
	モバイルデバイス	15
	Security Tools Mobile のセットアップ	15
	モバイルデバイスとコンピュータのペアリング	16
	別のモバイルデバイスの登録	16
	コンピュータとモバイルデバイスのペアリング解除	17
	ワンタイムパスワードによるログオン	18
	Security Tools Mobile の管理タスク	18
	Security Tools Mobile アプリ PIN のリセット	18
	Security Tools Mobile アプリのアンインストール	18
	スマートカード	19
6	Password Manager	21
	Password Manager の使用開始	21
	ログオンの管理	22
	カテゴリの追加	22

ログオンの追加	22
資格情報のインポート	23
アイコンコンテキストメニュー	23
学習済みのログオン ページへのログオン	24
ウェブドメインのサポート	24
Windows 資格情報の入力	25
ウェブサイトの除外	25
ログオンフォームに学習させるためのプロンプトの無効化	26
Password Manager 資格情報のバックアップと復元	26
資格情報のバックアップ	26
資格情報の復元	26
 用語集	 27

はじめに

Dell Data Protection | Endpoint Security Suite Enterprise は、お使いのコンピュータのセキュリティを強化するための、使いやすく直感的なツールを提供します。

ワークステーションオペレーティングシステム上、**DDP Console** から次の機能が使用できます。

- **Endpoint Security Suite Enterprise** との使用のための資格情報の登録
- パスワード、指紋、スマートカードを含む多要素資格情報の利用
- 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
- プログラムデータのバックアップおよび復元
- **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（[自己暗号化ドライブ](#)搭載のコンピュータ上）
- **Advanced Threat Protection** ステータスの表示

サーバーオペレーティングシステム上、**DDP 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 Protection** ステータスの表示

DDP Console

DDP Console は、資格情報を登録および管理し、セルフリカバリ質問を設定することができるインタフェースです。

次のアプリケーションにアクセスすることができます。

- 暗号化ステータスツールでは、コンピュータのドライブの暗号化ステータスを表示することができます。
- 登録ツールでは、資格情報のセットアップと管理、セルフリカバリ質問の設定、および資格情報登録ステータスの表示を行うことができます。各資格情報のタイプに登録するためのユーザー機能は、管理者によって設定されます。
- **Password Manager** では、ウェブサイト、**Windows** アプリケーション、およびネットワークリソースにログオンするために必要なデータを自動的に入力し、送信することができます。また、**Password Manager** では、アプリケーションを使用してログオンパスワードを変更することも可能であり、**Password Manager** によって維持されているログオンパスワードがターゲットリソースのパスワードと同期化された状態であることを確実にします。

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。

アップデートされた文書について、dell.com/support を定期的にチェックするようにしてください。

ProSupport へのお問い合わせ

サポートのために **Dell ProSupport** にご連絡いただく前に、適切な技術専門スタッフが迅速に対応できるよう、**Dell ProSupport** へのお電話でのお問い合わせ時には[サービスタグ](#)をお手元にご用意ください。

ProSupport へのお問い合わせには、**Dell Data Protection** 製品向けの **24 時間 365 日**対応電話サポート（**877-459-7304**、内線 **4310039**）に電話をおかけください。

さらに、dell.com/support 製品のオンラインサポートを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。

DDP Console

DDP Console は、コンピュータのドライブおよびパーティションの暗号化ステータスの表示と管理、管理者によって設定されたポリシーに基づいたウェブサイト、プログラム、およびネットワークリソースへのログオンの管理、およびユーザーの認証資格情報の容易な登録のため、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を提供します。

DDP Console を開くには、デスクトップで **DDP Console** アイコンをダブルクリックします。

DDP Console が起動すると、ホームページに **Endpoint Security Suite Enterprise** アプリケーションが表示されます。

- [Advanced Threat Protection](#)
- [暗号化ステータス](#)
- [登録](#)
- [Password Manager](#)

初めて資格情報を設定するには、登録 タイルにある **はじめに** リンクを選択します。ウィザードが短い登録プロセスをガイドします。詳細については、「[資格情報の初回登録](#)」を参照してください。

ナビゲーション

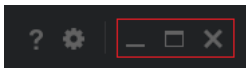
アプリケーションにアクセスするには、適切なタイルをクリックします。

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。

DDP 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にある適切なアイコンをクリックします。



最小化後に **DDP Console** を復元するには、そのシステムトレイアイコンをダブルクリックします。

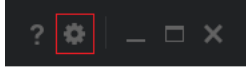


ヘルプを開くには、タイトルバーで **?** をクリックします。



DDP Console の詳細

DDP 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なことがあります。



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	バージョンおよび著作権情報が記載されています。
情報の表示	次の情報が含まれます。 <ul style="list-style-type: none">製品のバージョンと日付情報このコンピュータ上の DDP Console がエンタープライズまたはローカル管理者のどちらによって管理されている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デルに提供するためのフォームを表示します。
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	デルプロサポートのウェブサイトへ接続します。
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。

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**になります。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**保護済み**になります。

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。

Advanced Threat Protection

Advanced Threat Protection は、お使いのコンピュータまたはメモリ容量上で実行を試みているすべてのプロセスを監視し、異常または危険であるとみなされたものすべてにフラグを付けることによって、お使いのコンピュータをマルウェアから保護します。

Advanced Threat Protection は、Endpoint Security Suite Enterprise と共にデフォルトでインストールされます。

高度な監視と分析から出力されたお使いのコンピュータの統計を表示するには、Advanced Threat Protection タイルを選択してください。

Advanced Threat Protection ダッシュボード

Advanced Threat Protection ステータス ページには、コンピュータに関する次の情報が表示されます。

保護ステータス

Advanced Threat Protection が有効になっている時、および脅威が特定されていない、または識別された脅威が隔離、放棄、もしくはクリアされた時には、緑色のチェックマークが表示されます。

Advanced Threat Protection 機能が無効化されている時、または脅威が識別され、対処が必要な場合は、赤丸で囲まれた X が表示されます。

Advanced Threat Protection - Advanced Threat Protection 機能が有効になっているかどうかを示します。

Memory Protection - Memory Protection エンジンが有効になっているかどうかを示します。

ファイルシステム

危険なファイル - マルウェアに似たファイルとして識別された脅威の数です。

隔離された脅威 - 隔離された危険なファイルの数です。

メモリ保護

メモリ違反 - 識別されたメモリ違反の数です。この数には、エクスプロイト、プロセスインジェクション、およびエスカレーションのメモリ違反が含まれます。

ブロックされた違反 - ブロックされたメモリ違反の数です。

Advanced Threat Protection エージェントバージョン、インストール日、最終アップデート日は、ページ下部に表示されます。

登録

登録ツールでは、ユーザーが管理者によって設定されたポリシーに基づいて、登録ステータスの登録、変更、およびチェックを行うことができます。

DDP Console に初めて資格情報を登録するときは、ウィザードがパスワード変更、リカバリ質問、指紋、モバイルデバイス、およびスマートカードの登録をガイドします。ポリシーに応じて、ユーザーは各資格情報を登録またはスキップすることができます。初期登録後は、登録 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。

資格情報の初回登録

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 DDP Console のホームページで、登録タイル上の **はじめに** リンクをクリックします。
- 2 ようこそ ページで **次へ** をクリックします。
- 3 認証が必要 ダイアログで、**Windows** パスワードを使ってログインし、**OK** をクリックします。
- 4 **Windows** パスワードを変更するには、パスワード ページで新規パスワードを入力して確認し、**次へ** をクリックします。パスワードの変更をスキップするには、**スキップ** をクリックします。ウィザードでは、資格情報を登録しない場合、その資格情報をスキップすることができます。前のページに戻るには、**戻る** をクリックします。
- 5 各ページの手順に従って、次の適切なボタンをクリックします。**次へ**、**スキップ**、または **戻る** をクリックします。
- 6 サマリ ページで登録した資格情報を確認し、登録が完了したら **適用** をクリックします。資格情報登録 ページに戻って変更を行うには、変更するページが表示されるまで **戻る** をクリックします。

資格情報の登録または変更の詳細については、「[登録の追加](#)、[変更](#)、または[表示](#)」を参照してください。

登録の追加、変更、または表示

登録を追加、変更、または表示するには、**登録** 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。

ステータス ページでは、サポートされている資格情報、それらのポリシー設定（必須または該当なし）、および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。

- 資格情報を初めて登録するには、資格情報の行で **登録** をクリックします。
- 既存の登録済み資格情報を削除するには、**削除** をクリックします。
- 資格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** 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。

資格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、資格情報登録ページに「資格情報の変更はポリシーによって許可されていません」というメッセージが表示されます。

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 ではなく DDP Console のみで変更するようにしてください。Windows パスワードが DDP Console 外で変更された場合、パスワードの不一致が生じ、リカバリ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。

以前に登録した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： このページでの選択をクリアし、もう一度やり直すには、**リセット** ボタンをクリックします。

リカバリ質問がすでに登録されている

リカバリ質問がすでに登録されている場合、リカバリ質問の削除または再登録のいずれかを実行できます。

- 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。
 - 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。
 - 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。

指紋

メモ： この機能を使用するには、コンピュータに指紋リーダーが必要です。

指紋を登録するには、次の手順を実行します。

- 1 **指紋** タブをクリックします。
- 2 指紋 ページで、登録する指をクリックします。
- 3 画面上の手順に従い、指紋を登録します。

メモ： 登録するには、指のスキャンが 4 回成功する必要があります。指紋登録を完了するために必要なスキャンの回数は、各スキャンの品質によって異なります。管理者が、指紋の最小および最大数を定義しました。

- 4 ポリシーによって必要とされる最少数の指紋を登録するまで、後続の各指をクリックします。
最少数の指紋を登録していないと、ダイアログがそれを通知します。**OK** をクリックして続行します。
- 5 必要な数の指紋のスキャンを終了したら、**保存** をクリックします。

スキャンした指紋を削除するには、指紋登録 ページでハイライト表示されている指紋をクリックして登録解除し、**はい** をクリックして削除を確認したあと、**保存** をクリックします。

モバイルデバイス

モバイルデバイス登録は、[ワンタイムパスワード \(OTP\)](#) 機能を提供します。OTP では、コンピュータとペアリングされているモバイルデバイスの **Security Tools Mobile** アプリによって生成されたパスワードを使用して **Windows** にログオンすることができます。また、ポリシーで許可されている場合は、パスワードの期限が切れた、またはパスワードを忘れたときのコンピュータへのアクセス回復のために **OTP** 機能を使用することもできます。

メモ: DDP Console に モバイルデバイス タブが表示されない場合は、コンピュータの構成上サポートされていない、または管理者が設定したポリシーで許可されていません。

メモ: OTP 機能の用途 (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お使いのコンピュータにログオンする、またはコンピュータへのアクセスを回復する) は、ポリシー設定によって決定されます。ログオンとリカバリの両方に使用することはできません。

OTP 機能を使用するには、お使いのモバイルデバイスを登録する、またはそれをコンピュータとペアリングする必要があります。複数のユーザーが存在するコンピュータでは、各ユーザーがそのコンピュータにそれぞれ 1 台のモバイルデバイスを登録することができます。モバイルデバイスは、複数のコンピュータに登録できます。

デバイスがすでに登録されている場合、新しいデバイスを登録することによって前のデバイスが自動的にペアリング解除されます。

DDP Console 上 :

- 1 DDP Console 登録 ページで、**モバイルデバイス** タブをクリックします。
- 2 右上の **登録** をクリックします。
ワンタイムパスワードの登録 ページが開きます。
- 3 これがペアリングする最初のコンピュータである場合は、**はい** を選択します。
 - a モバイルデバイスで、**App Store** から **Dell Data Protection | Security Tools Mobile** アプリをダウンロードします。
 - b コンピュータで、**次へ** をクリックします。

Security Tools Mobile のセットアップ

- 1 **Security Tools Mobile** アプリを開きます。
- 2 **Security Tools Mobile** アプリのアクセスに使う **PIN** を作成して入力します。

メモ: モバイルデバイスがロックされていないときは、ポリシーによって **PIN** が必要となる場合があります。モバイルデバイスのロック解除に **PIN** を使用していなければ、**Security Tools Mobile** アプリにアクセスするための **PIN** が必要になります。
- 3 **コンピュータの登録** を選択します。(必要な場合は、モバイル画面の左上隅をタップしてコマンドにアクセスしてください)。
モバイルデバイスにコードが表示されます。コードの長さや英数字の組み合わせは、管理者が設定したポリシーに基づきます。

モバイルデバイスとコンピュータのペアリング

- 1 コンピュータの DDP Console モバイルコード ページで、次の手順を実行します。
 - a モバイルデバイスからのコードをフィールドに入力します。
 - b 次へ をクリックします。
 - c デバイスのペアリング ページで、次のいずれかを選択します。
 - QR コード - QR コードが表示されます。
 - または
 - 手動入力 - 24 桁のペアリングコードが表示されます。
- 2 モバイルデバイス：
 - a デバイスのペアリング をタップします。
 - b コンピュータ上で選択したものと同一ペアリングオプション（QR コード または 手動入力）をクリックします。
 - c 次のいずれかを選択してください。
 - QR コード の場合は、コンピュータ画面の手前にモバイルデバイスを置き、QR コードをスキャンします。モバイルデバイスに表示されている数字の検証コードをメモしてから、次へ をタップします。

メモ： スキャンングに問題がありますか？ バーが表示される場合は再試行するか、手動入力 を選択します。

 - 手動入力 では、コンピュータからの 24 桁のペアリングコードを入力して、完了 をタップします。モバイルデバイスに表示されている数字の検証コードをメモしてから、次へ をタップします。
- 3 コンピュータの DDP Console で、次の手順を実行します。
 - a 次へ をクリックします。
 - b モバイルデバイスに表示されている検証コードを入力し、次へ をクリックします。
 - c オプションとして、モバイルデバイスの名前を変更します。
 - d 適用 をクリックします。
デバイスがペアリングされました。
- 4 モバイルデバイス：
 - a 続行 をタップします。
 - b オプションとして、コンピュータの名前を変更し、完了 をタップします。
 - c 終了 をタップします。

別のモバイルデバイスの登録

新しいデバイスを登録すると、前のデバイスが自動的にペアリング解除されます。ペアリング解除には、別途手順は必要ありません。

コンピュータとモバイルデバイスのペアリング解除


別のデバイスを登録することなくコンピュータとモバイルデバイスのペアリングを解除するには、次のいずれかを選択します。

- DDP Console 内：モバイルデバイス資格情報の横にある 登録ステータス ページで **削除** をクリックします。
- モバイルデバイス：
 - 1 **Security Tools Mobile** アプリを実行します。
 - 2 左上のメニューバーをタップし、ドロワーを開きます。
 - 3 **コンピュータの削除** をタップします。
 - 4 ペアリングを解除するコンピュータを選択します。
 - 5 **削除 (Android)** を選択するか、**完了 (iOS)** をタップします。
確認メッセージが表示されます。
 - 6 **すべて削除** を選択して、デバイスからすべての登録済みコンピュータを削除します。
すべて削除オプションは、複数のコンピュータを削除したとき、またはペアリングされているコンピュータのみを削除したときに表示されます。
- 登録済みコンピュータを削除し、PIN を削除するには、**デフォルト設定の復元** を選択します。デフォルトを復元すると、登録済みコンピュータ、および **Security Tools Mobile** アプリへのアクセスに使用する **PIN がすべて削除** されます。
- コンピュータを登録したままにするには、**キャンセル** を選択します。

ワンタイムパスワードによるログオン

メモ: OTP 認証は、Windows ログオンのみで使用できます。

OTP は、リカバリ（ロックアウトされたコンピュータへのアクセスを回復する）、または Windows ログオンのいずれかに使用することができます。両方に使用することはできません。

ポリシーで許可されている場合は、OTP シンボル  がログオン画面に表示され、OTP を使用して Windows にログオンできます。

OTP を使用してログオンするには、次の手順を実行します。

- 1 コンピュータの Windows ログオン画面で、OTP アイコン  を選択します。
- 2 モバイルデバイスで Security Tools Mobile アプリを開き、PIN を入力します。
- 3 アクセスするコンピュータを選択します。
モバイルデバイスにコンピュータ名が表示されない場合は、次のいずれかの状態が存在する可能性があります。
 - モバイルデバイスがアクセスしたいコンピュータに登録またはペアリングされていない。
 - 複数の Windows ユーザーアカウントを持っている場合は、アクセスしようとしているコンピュータ上に DDP | Endpoint Security Suite Enterprise がインストールされていない、またはコンピュータとモバイルデバイスのペアリングに使用したアカウントとは異なるユーザーアカウントにログオンしようとしている。
- 4 ワンタイムパスワードをタップします。
モバイルデバイス画面にパスワードが表示されます。

メモ: 必要であれば、更新シンボル  をクリックして新しいコードを取得します。最初 2 回の OTP 更新後、別の OTP を生成できるようになるまでに 30 秒の遅延が発生します。
コンピュータとモバイルデバイスは、両方が同時に同じパスワードを認識できるように同期化されている必要があります。パスワードを急速に連続して作成しようとすると、コンピュータとモバイルデバイスが非同期状態となり、OTP 機能が失敗する原因となります。この問題が発生した場合は、2 つのデバイスが再度同期化されるまで 30 秒程待ってから、再試行してください。
- 5 コンピュータの Windows ログオン画面で、モバイルデバイスに表示されているパスワードを入力し、**Enter** を押します。
リカバリに OTP を使用した場合は、コンピュータへのアクセスを回復した後、画面に表示される手順に従ってパスワードをリセットします。

Security Tools Mobile の管理タスク

これらのタスクは、モバイルデバイス上の Security Tools Mobile アプリを使用して実行します。

Security Tools Mobile アプリ PIN のリセット

Security Tools Mobile アプリ PIN をリセットするには、次の手順を実行します。

- 1 右上のメニューオプションをタップします。
- 2 PIN のリセット を選択します。
- 3 新しい PIN を入力して確認します。

Security Tools Mobile アプリのアンインストール

モバイルデバイス上で、次の手順を実行します。

- 1 デバイスとコンピュータのペアリングを解除します。
- 2 お使いのモバイルデバイスからアプリを削除する通常の方法で、Security Tools Mobile アプリを削除またはアンインストールします。

スマートカード

メモ: この機能を使用するには、コンピュータにスマートカードリーダーが必要です。

スマートカードを登録するには、次の手順を実行します。

- 1 スマートカード タブをクリックします。
- 2 カードのタイプに基づいて、スマートカードを登録します。
 - カードリーダーにスマートカードを挿入します。
 - 非接触型カードの場合は、リーダーの上またはその近くにカードを配置して固定します。
- 3 カードが検知されると、緑色のチェックボックスとカードの登録が表示されます。**カードの登録** を選択します。
- 4 登録の成功 ダイアログで **OK** をクリックします。

ユーザーに関連付けられている全てのスマートカードの登録を解除するには、スマートカード登録 ページで **アカウントから登録済みカードを削除する** を選択します。

Password Manager

Password Manager では、ウェブサイト、**Windows** プログラム、およびネットワークリソースへの自動ログオンと、ログオン資格情報の管理を単一のツールで行うことができます。また、**Password Manager** では、ユーザーはアプリケーションを使用してログオンパスワードを変更することが可能になり、**Password Manager** によって維持されているログオンパスワードが対象リソースのパスワードと同期化された状態であることを確実にします。

Password Manager は、**Internet Explorer** および **Mozilla Firefox** でサポートされています。**Password Manager** は、**Microsoft アカウント**（旧 **Windows Live ID**）ではサポートされていません。

メモ：Firefox 上で **Password Manager** を実行している場合は、**Password Manager** 拡張機能をインストールおよび登録する必要があります。Mozilla Firefox での拡張機能のインストール手順については、<https://support.mozilla.org/> を参照してください。

メモ：Mozilla Firefox での **Password Manager** アイコン（学習前および学習済みアイコンの両方）の使用は、Microsoft Internet Explorer での使用とは異なります。

- **Password Manager** アイコンでのダブルクリック機能が使用できない。
- ドロップダウンコンテキストメニューでデフォルトアクションが太字で表示されない。
- ページに複数のログオンフォームがある場合、複数の **Password Manager** アイコンが表示されることがある。

メモ：ウェブログオンページの構造は常に変化し続けているため、**Password Manager** はすべてのウェブサイトを常時サポートできない場合があります。

Password Manager の使用開始

Password Manager は、ユーザーの作業に伴ってログオン資格情報を収集し、保管します。**Endpoint Security Suite Enterprise** をインストールしてからすぐに **Password Manager** の使用を開始することができます。資格情報をログオンページに入力すると、**Password Manager** がログオンフォームを検知し、**Password Manager** で資格情報を保存するかどうかを選択できます。

これには、次の 3 つのオプションがあります。

- **ログオンを保存する** をクリックして、**Password Manager** に資格情報を保存します。
- ログオンを**保存しない**場合は、ウェブサイトやプログラムにログオンするたびに、ログオン資格情報を保存するためのプロンプトが再度表示されます。プロンプトが表示されないようにするには、**このサイトに対しては保存しない** を選択します。ウェブサイト除外 リストに記録が作成されます。詳細については、「**ウェブサイトの除外**」を参照してください。
- 資格情報を保存しない場合は、**ログオンを保存しない** をクリックします。

このダイアログは、ウェブサイトまたはプログラムに対して以前保存した資格情報があるときに、それとは異なるユーザー名またはパスワードを入力した場合にも表示されます。新規ユーザー名の場合、**ログオンを保存** を選択すると、新しい資格情報セットが保管されます。以前保存されたユーザー名と新しいパスワードの場合、**ログオンを保存** を選択すると、元の資格情報が新しいパスワードでアップデートされます。

ログオンの管理

Logon Manager は、ウェブサイト、Windows プログラム、およびネットワークリソースへのすべてのログオンの管理を簡素化し、一元化します。

Logon Manager を開くには、次の手順を実行します。

- 1 DDP Console ホームページで、**Password Manager** タイルをクリックします。
- 2 **Logon Manager** タブをクリックします。

ログオンおよびカテゴリを追加して、それらを並べ替えたりフィルタリングすることができます。

- ➕ **ログオンの追加** - 新しいログオン資格情報セットを追加することができます。ポリシーに応じて、ログオンを追加するには **Endpoint Security Suite Enterprise** に格納されている資格情報の入力が必要になる場合があります。
- ➕ **カテゴリの追加** - 並べ替えおよびフィルタリング用に、新規カテゴリ（電子メール、ストレージ、ニュース、コーポレートリソース、ソーシャルメディアなど）を追加することができます。

並べ替え：アカウント、ユーザー名、またはカテゴリでログオンを並べ替えます。列見出しをクリックし、列順にソートします。

フィルタ：ビューリストからカテゴリを選択し、選択したカテゴリ以外のすべてのログオンを非表示にします。フィルタを取り除くには、**すべて**を選択します。

ログオンは次のように管理することができます。

- 🔧 **起動** - ウェブサイトまたはプログラムを開き、ユーザー設定に基づいてログオン資格情報を送信します。
- ✎ **編集** - ウェブサイトまたはプログラムの保管済みログオンデータを変更することができます。
- ✖ **削除** - **Password Manager** から保管済みのログオンデータを削除することができます。
- ➕ **追加** - 新規ログオン、カテゴリ、または新規ログオンデータを追加できます。

カテゴリの追加

ログオンを追加する前に、ログオンを作成するたびにそれらをカテゴリ化できるように、カテゴリ（電子メール、ストレージ、ニュース、コーポレートリソース、ソーシャルメディアなど）を作成します。この後、ログオンをカテゴリ別に並べ替えおよびフィルタリングすることができます。

カテゴリを追加するには、**Logon Manager** ページで **カテゴリの追加** をクリックし、カテゴリ名を入力して **保存** をクリックします。

ログオンの追加

- 1 **Logon Manager** ページで **ログオンの追加** をクリックします。
ポリシーに基づいて、ログオンを追加するための認証が必要になる場合があります。
- 2 ログオン先のウェブサイトまたはプログラムを開きます。
- 3 ログオンの追加 ダイアログで、**続行** をクリックします。
- 4 次のダイアログで、以下を入力します。
 - **カテゴリ** - 保管するウェブサイトまたはプログラムログオンのカテゴリを選択します。カテゴリを追加していない場合、このリストは空になります。
 - **アカウント名** - 事前入力された名前を受け入れるにはそのままにしておきます。あるいは、ウェブサイトまたはプログラムの名前を入力します。
 - **未検知のタイトル** - これらのフィールドは、ログオン情報を入力するログオンページ上のフィールドとして、**Password Manager** によって検知されます。これらのフィールドには、通常、ユーザー名または電子メール、およびパスワードが含まれます。
- 5 フィールド名が未検知のタイトルになっている、またはログオンフィールドとして誤ったフィールドが含まれている場合は、**その他のフィールド** ボタンをクリックしてフィールド名を編集するか、フィールドを削除します。

- 6 その他のフィールド ダイアログで **未検知のタイトル** をクリックし、各フィールドに正しいフィールド名を入力します。
その他のフィールド ダイアログが表示されるときは、フィールドの名前変更に役立つように、ログオンの追加 ダイアログでアクティブであったフィールドがハイライト表示されます。
フィールドがログオンに不要な場合は、チェックボックスを選択解除してログオン情報から除外します。
 - 7 変更を保存するには、**OK** をクリックします。
 - 8 ログオンの追加 ダイアログで、ログオンに必要なフィールドを完了します。
- メモ:** 既存のログオンを保管しているため、パスワードは、ウェブサイトまたはプログラムのパスワードの変更 機能にアクセスしなければ変更できません。
- 9 **Password Manager** でログオン情報を自動で入力および送信する場合は、**ログインデータを自動送信する** を選択します。
 - 10 **保存** をクリックします。
Logon Manager ページにウェブサイトまたはプログラムログオンが表示されます。

資格情報のインポート

ウェブブラウザに保管されている資格情報を **Password Manager** にインポートすることができます。

- 1 **Password Manager** ツールで **資格情報のインポート** を選択します。
 - 2 インポートするブラウザを選択し、**スキャン** をクリックします。
 - 3 プロンプトが表示されたら、選択したブラウザのパスワードを入力します。
- メモ:** インポートしてもパスワードがインポートされない場合は、ブラウザがインポートするデータを保存しているかどうかを確認します。
Firefox を使用している場合は、Sync にログオンします。資格情報のインポートを再試行してください。

アイコンコンテキストメニュー

ウェブサイトまたはプログラムにアクセスするときは、**Password Manager** アイコンが表示されます。

- +** は、学習させることが可能なログオンフォームを示します。
 - +** が表示されていない場合、ログオンフォームはすでに学習済みです。アイコンをダブルクリックして、プログラムまたはウェブサイトにもログオンします。
- アイコンをクリックすると、ログオンフォームが学習済みか否かに応じて、コンテキストメニューに異なるオプションが表示されます。

現在のログオンフィールドが学習済みではない場合は、コンテキストメニューに次のオプションが表示されます。

<u>Password Manager に追加</u>	ログオンの追加 ダイアログが開きます。
<u>アイコン設定</u>	トレーニング可能なログオンページにおける Password Manager アイコン表示のユーザーによる設定を可能にします。
<u>Password Manager を開く</u>	Password Manager の管理 ツールが起動し、 Logon Manager ページが開きます。
<u>ヘルプ</u>	オンラインヘルプが開きます。

現在のログオンフィールドが学習済みの場合は、コンテキストメニューに次のオプションが表示されます。

<u>ログオンデータの入力</u>	ログオンフォームの学習時における選択内容に応じて、自動的にログオン、またはユーザー名およびパスワードフィールドに自動入力し、ログオンデータを送信できるようにします。
<u>ログオンの編集</u>	ログオンの編集 ダイアログが開きます。
<u>ログオンの追加</u>	ログオンの追加 ダイアログが開きます。
<u>Password Manager を開く</u>	Logon Manager ページが開きます。
<u>ヘルプ</u>	オンラインヘルプが開きます。

Password Manager アイコンがログオンフォームと共に表示されない場合は、ブラウザのパスワード保存機能をオフにします。

- **Mozilla Firefox** の場合：メニュー アイコン > オプション > セキュリティと進み、**サイトのパスワードを保存する** チェックボックスの選択を解除します。
- **Internet Explorer** の場合：ギア アイコン > インターネットオプション > コンテンツ タブ > オートコンプリート設定と進み、**フォームのユーザー名およびパスワード** チェックボックスの選択を解除します。

学習済みのログオン ページへのログオン

ウェブサイトまたはプログラムログオンを開くとき、**Password Manager** はそのページが学習済みであるかどうかを検知します。学習済みであれば、**Password Manager** アイコンがログオンエリアに表示されます。学習済みでなければ、学習済みでないフォームに対するプロンプトが無効化されている場合を除き、**Password Manager** アイコンが表示されます。

ログオンするには、次の操作のいずれかを選択します。

- 登録されている資格情報をスキャンします。指紋またはスマートカードを登録している場合は、登録されている指で指紋リーダーにタッチするか、登録されているカードをカードリーダーに提示します。
- **Password Manager** アイコンをクリックし、コンテキスト メニューから **ログオンデータの入力** を選択します。
- **Password Manager** ホットキーの組み合わせ、**Ctrl+Win+H** を押します。**Password Manager** のポップアップに学習したサイトが提示され、サイトを迅速に起動できます。

メモ：ホットキーの組み合わせは、DDP Console > Password Manager > 設定 から変更できます。

サイトまたはプログラムに対して複数のログオンが保管されている場合は、使用するアカウントを選択するプロンプトが表示されます。

ウェブドメインのサポート

特定のウェブドメインのためにログオンページを学習させたが、異なるログオンページからそのウェブドメインのアカウントにアクセスしたい場合は、新しいログオンページに移動します。既存のログオンを使用するか、**Password Manager** に新しいログオンを追加するかを確認するためのプロンプトが表示されます。

- **ログオンの使用** をクリックすると、以前作成されたアカウントへログオンされます。次に新しいログオンページからそのアカウントにアクセスする時は、以前に作成されたアカウントに自動的にログオンされます。
- **ログオンの追加** をクリックすると、**ログオンの追加** ダイアログが表示されます。

Windows 資格情報の入力

一部のプログラムでは、ログオン用に **Windows** 資格情報の使用が許可されています。

ユーザー名とパスワードを入力する代わりに、[ログオンの追加](#) および [ログオンの編集](#) ダイアログにあるドロップダウンメニューから **Windows** 資格情報を選択します。

ユーザー名については、次のタイプから選択してください。

- **Windows** ユーザー名
- **Windows** ユーザープリンシパル名
- **Windows** ドメイン\ユーザー名
- **Windows** ドメイン

パスワードについては、**Windows** パスワードを使用します。

これらのオプションは変更できません。

古いパスワードの使用

Password Manager でパスワードを変更したにも関わらず、新規パスワードがプログラムに拒否される場合があります。この場合、そのプログラムでは、最新のパスワードの代わりに以前のパスワード（このログオンページで以前に入力したパスワード）を使用することができます。

パスワード履歴 を選択します。認証後、パスワード履歴 リストから古いパスワードを選択するためのプロンプトが表示されます。リストには、**7** つのパスワードが含まれます。

ウェブサイトの除外

Password Manager がウェブサイトを管理しないようにするには、**ウェブサイト除外** タブをクリックします。

ウェブサイト除外には、以下の特徴があります。

- **Password Manager** アイコンを呼び出さない。
- ユーザーを自動的にログインしない。
- パスワードリマインダーを表示しない。

除外リストに新しいウェブサイトを追加するには、次の手順を実行します。

- 1 **ウェブサイト除外** タブをクリックします。
- 2 **ウェブサイトの追加** をクリックします。
- 3 除外するウェブサイトの **URL** を入力します。
- 4 **保存** をクリックします。

ウェブサイトが除外されると、そのウェブサイトは **Password Manager** によって管理されなくなります。除外を無効にするには、ウェブサイト除外 リストからウェブサイトを単に削除します。除外リストからウェブサイトを削除するには、**X** をクリックします。

複数のウェブサイトを追加した後は、次の操作を実行できます。

- ウェブサイトを昇順または降順で並べ替えるには、ウェブサイト列見出しをクリックします。
- リスト内で検索するには、**URL** の一部を検索フィールドに入力します。入力するに従って、リストもフィルタリングされます。

ログオンフォームに学習させるためのプロンプトの無効化

既存の学習済みログオンを維持しながら、新しいログオンフォームを学習させるためのプロンプトを無効にすることができます。新規ログオンに対するプロンプトを無効にするには、次の手順を実行します。

- 1 DDP Console を開きます。
- 2 **Password Manager** タイルをクリックします。
- 3 **設定** タブをクリックします。
- 4 ログオン画面でログオンを追加するプロンプトを表示する チェックボックスを選択解除します。

Password Manager 資格情報のバックアップと復元


Password Manager では、Password Manager によって管理されているログオンデータをセキュアにバックアップすることができます。このデータは、Password Manager によって保護されている任意のコンピュータ上で復元できます。

メモ：バックアップされている Password Manager データには、オペレーティングシステムや [Preboot Authentication \(PBA\)](#) ログオン資格情報、または指紋などの資格情報固有の情報は含まれません。

資格情報のバックアップ

資格情報をバックアップするには、次の手順を実行します。

- 1 **資格情報のバックアップ** タブをクリックし、バックアッププロセスを設定します。
- 2 **参照** をクリックし、希望するバックアップ場所に移動します。
データをローカルドライブにバックアップしようとする、データをポータブルストレージまたはネットワークドライブにバックアップするための推奨が表示されます。
- 3 パスワードを入力し、確認します。バックアップしたこれらの資格情報を後ほど復元する必要がある場合は、このパスワードを使用する必要があります。
- 4 **バックアップ** をクリックします。
- 5 **Windows** パスワードを入力します。
- 6 成功 ダイアログで **OK** をクリックします。

メモ：実行したバックアップ操作のテキストログを表示するには、 をクリックし、**ログ** を選択します。

資格情報の復元


資格情報を復元するには、バックアップの場所が使用可能である必要があります。

資格情報を復元するには、次の手順を実行します。

- 1 **資格情報の復元** タブをクリックします。
- 2 **参照** をクリックしてバックアップファイルにナビゲートし、次にそのファイルのパスワードを入力します。
- 3 **復元** をクリックします。

警告： Password Manager データの復元により、すべての既存データが上書きされます。バックアップの作成後に追加されたログオンおよびその他のデータは失われます。

- 4 **次へ** をクリックします。

メモ：復元操作のテキストログを表示するには、タイトルバーの  アイコンをクリックし、**ログ** を選択します。

用語集

Trusted Platform Module (TPM) – TPM は、セキュアストレージ、計測、および認証という 3 つの主要機能を備えたセキュリティチップです。DDPJE は、セキュアストレージ機能のために TPM を使用します。TPM はまた、DDPJE ソフトウェア資格情報コンテナに対して暗号化されたコンテナを提供し、DDPJE HCA 暗号化キーを保護することもできます。デルは、TPM のプロビジョニングを推奨します。TPM は、DDPJE HCA、BitLocker Manager、およびワンタイムパスワード機能の使用に必須です。

ワンタイムパスワード (OTP) - ワンタイムパスワードは一度しか使用できないパスワードで、有効時間が限定されています。OTP には、TPM が存在し、有効化され、所有されている必要があります。OTP を有効にするには、DDP Console および Security Tools Mobile アプリを使用して、モバイルデバイスをコンピュータとペアリングします。Security Tools Mobile アプリは、Windows ログオン画面でのコンピュータへのログオンに使用されるパスワードをモバイルデバイス上に生成します。コンピュータへのログオンに OTP を使用しなかった場合は、ポリシーに基づき、パスワードの期限が切れたときに、またはパスワードを忘れたときに、OTP 機能を使用してコンピュータへのアクセスを回復することができます。OTP 機能は、認証またはリカバリのいずれかに使用できますが、両方には使用できません。生成されたパスワードが一度しか使用できず、短時間で失効するため、OTP セキュリティは他の認証手法よりも優れています。

起動前認証 (PBA) – 起動前認証は、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の外部から改ざんを防止できるセキュアな環境を保証します。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。

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

自己暗号化ドライブ (SED) - メディアに保存されているすべてのデータを自動的に暗号化し、メディアから取り出すすべてのデータを自動的に復号化する、ビルトイン暗号化メカニズムを持つ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。

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。



0XXXXXA0X