Dell Data Protection Console - Benutzerhandbuch

Threat Protection/Verschlüsselungsstatus/
Authentifizierungsregistrierung/Password Manager v1.7

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Dell Data Protection Console - Benutzerhandbuch

2017 - 04

Rev. A01

Inhaltsverzeichnis

1

DDP Console – Einführung

Dell Data Protection | Endpoint Security Suite bietet einfach zu verwendende und intuitive Werkzeuge zur Erhöhung der Sicherheit auf Ihrem Computer.

Die folgenden Funktionen sind über die DDP Console auf dem Betriebssystem einer Workstation verfügbar:

- Registrieren von Anmeldeinformationen für die Verwendung mit Endpoint Security Suite
- Nutzen der Vorteile von mehrstufigen Anmeldeinformationen, einschließlich Passwörter, Fingerabdrücke und Smartcards
- Wiederherstellen des Zugangs zu Ihrem Computer ohne Helpdesk-Anrufe oder Administratorunterstützung, wenn Sie Ihr Passwort vergessen haben
- Sicherung und Wiederherstellung Ihrer Programmdaten
- Einfache und leichte Änderung Ihres Windows-Passworts
- Festlegen persönlicher Einstellungen
- Anzeigen des Verschlüsselungsstatus (auf Computern mit selbstverschlüsselnden Laufwerken)

  Anzeigen des Threat Protection-Status

DDP-Konsole

Die DDP Console ist die Oberfläche, über die Sie können sich registrieren, Ihre Anmeldeinformationen verwalten und Wiederherstellungsfragen konfigurieren können.

Sie haben Zugriff auf die folgenden Anwendungen:

- Auf dem Threat Protection-Dashboard wird der Schutzstatus des Computers basierend auf Threat Protection-Richtlinien angezeigt.Das Verschlüsselungsstatus-Tool ermöglicht Ihnen die Anzeige des Verschlüsselungsstatus der Laufwerke des Computers.
- Mit dem Eintragungstool können Sie Anmeldeinformationen einrichten und verwalten, Wiederherstellungsfragen konfigurieren und den Status Ihrer Anmeldeinformationseintragung anzeigen. Ob Sie die Möglichkeit zur Registrierung von allen Anmeldeinformationstypen haben, wird durch den Administrator festgelegt.
- Mit Password-Manager können Sie die Anmeldeinformationen für Websites, Windows-Anwendungen und Netzwerkressourcen automatisch ausfüllen und übermitteln lassen. Mit dem Password-Manager können Sie außerdem Ihre Anmeldekennwörter über die Anwendung ändern und damit sicherstellen, dass die durch Password Manager verwalteten Kennwörter mit denen der Zielressource synchron bleiben.

Diese Anleitung beschreibt, wie jede dieser Anwendungen verwendet wird.

Stellen Sie sicher, dass Sie in regelmäßigen Abständen dell.com/support nach aktualisierten Dokumenten überprüfen.

Kontaktaufnahme mit dem Dell ProSupport

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

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

Halten Sie bei Ihrem Anruf Ihren Service Code bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

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

2

DDP-Konsole

Die DDP Console bietet Zugriff auf Anwendungen, die die Sicherheit für alle Benutzer des Computers gewährleisten, um den Verschlüsselungsstatus der Laufwerke und Partitionen des Computers anzuzeigen und zu verwalten und, basierend auf vom Administrator festgelegten Richtlinien, ihre Anmeldungen bei Websites, Programmen und Netzwerkressourcen zu verwalten und ihre Anmeldeinformationen zur Authentifizierung auf einfache Weise zu registrieren.

Um die DDP Console vom *Desktop* zu öffnen, doppelklicken Sie auf das Symbol für die **DDP Console**.

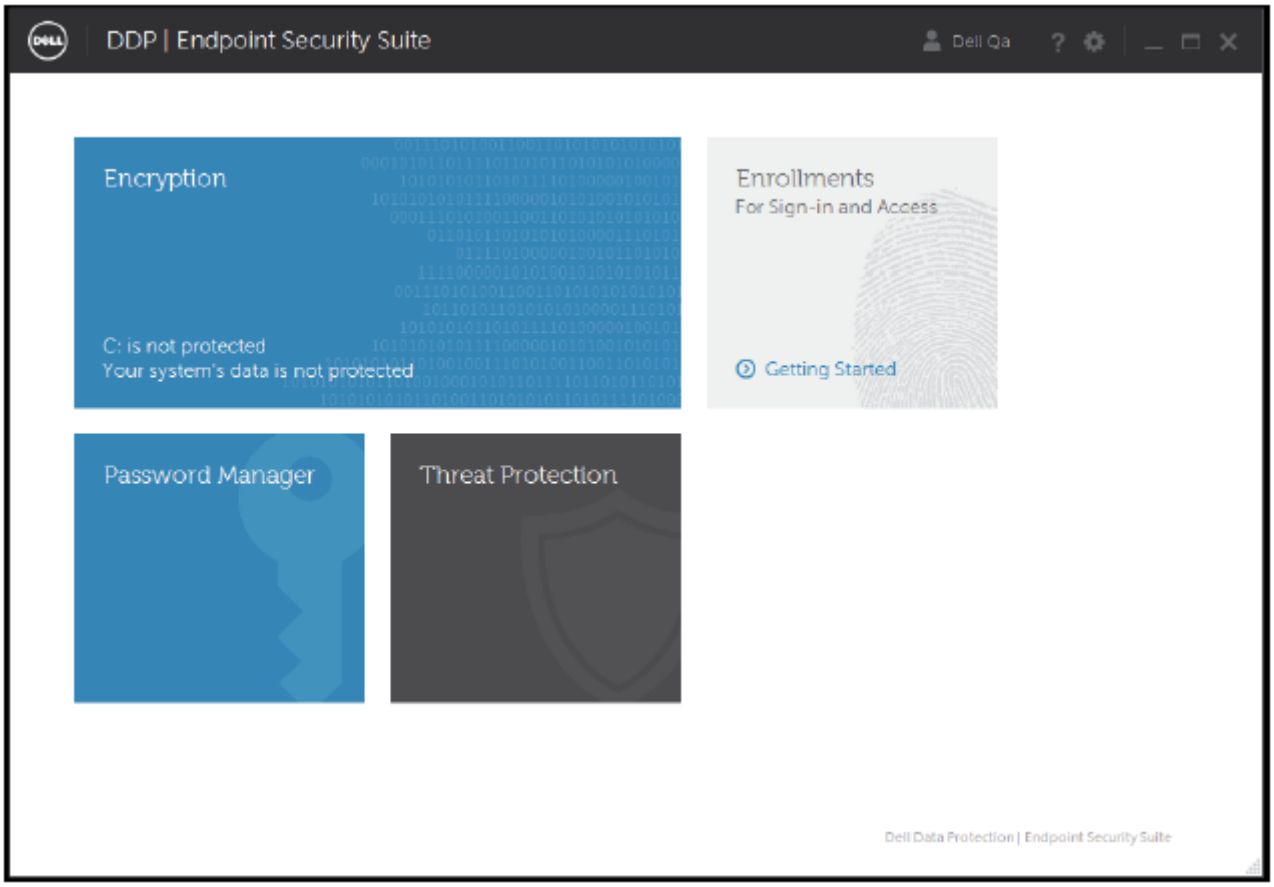
Wenn die DDP Console startet, werden auf der Startseite die Anwendungen Endpoint Security Suite angezeigt:

- Threat Protection
- Verschlüsselungsstatus
- Registrierungen
- Password Manager

  Um Anmeldeinformationen erstmalig einzurichten, wählen Sie den Link **Erste Schritte** auf der Kachel „Registrierungen“ aus. Ein Assistent leitet Sie durch den kurzen Registrierungsvorgang. Weitere Informationen finden Sie unter Erstmaliges Eintragen von Anmeldeinformationen.

Navigation

Klicken Sie zum Öffnen einer Anwendung auf die entsprechende Kachel.



Titelleiste

Um innerhalb einer Anwendung zur Startseite zurückzukehren, klicken Sie in der linken Ecke der Titelleiste auf den Rückwärtspfeil, der sich neben dem Namen der aktiven Anwendung befindet.

Um direkt zu einer anderen Anwendung zu navigieren, klicken Sie den Pfeil nach unten neben dem Namen der aktiven Anwendung, und wählen Sie eine andere Anwendung aus.

Um die DPP-Konsole zu minimieren, zu maximieren oder zu schließen, klicken Sie auf das entsprechende Symbol in der rechten Ecke der Titelleiste.

Um die DDP-Konsole nach dem Minimieren wiederherzustellen, doppelklicken Sie auf das Taskleistensymbol.

Um die Hilfe zu öffnen, klicken Sie auf das **?** in der Titelleiste.

DDP-Konsole – Details

Um Informationen zur DDP-Konsole, zu den Richtlinien, Ausführungsdiensten und Protokollen anzuzeigen, klicken Sie auf das Zahnradsymbol auf der linken Seite der Titelleiste. Diese Informationen können beispielsweise vom Administrator im Rahmen des technischen Supports benötigt werden.

Wählen Sie ein Element im Menü aus.

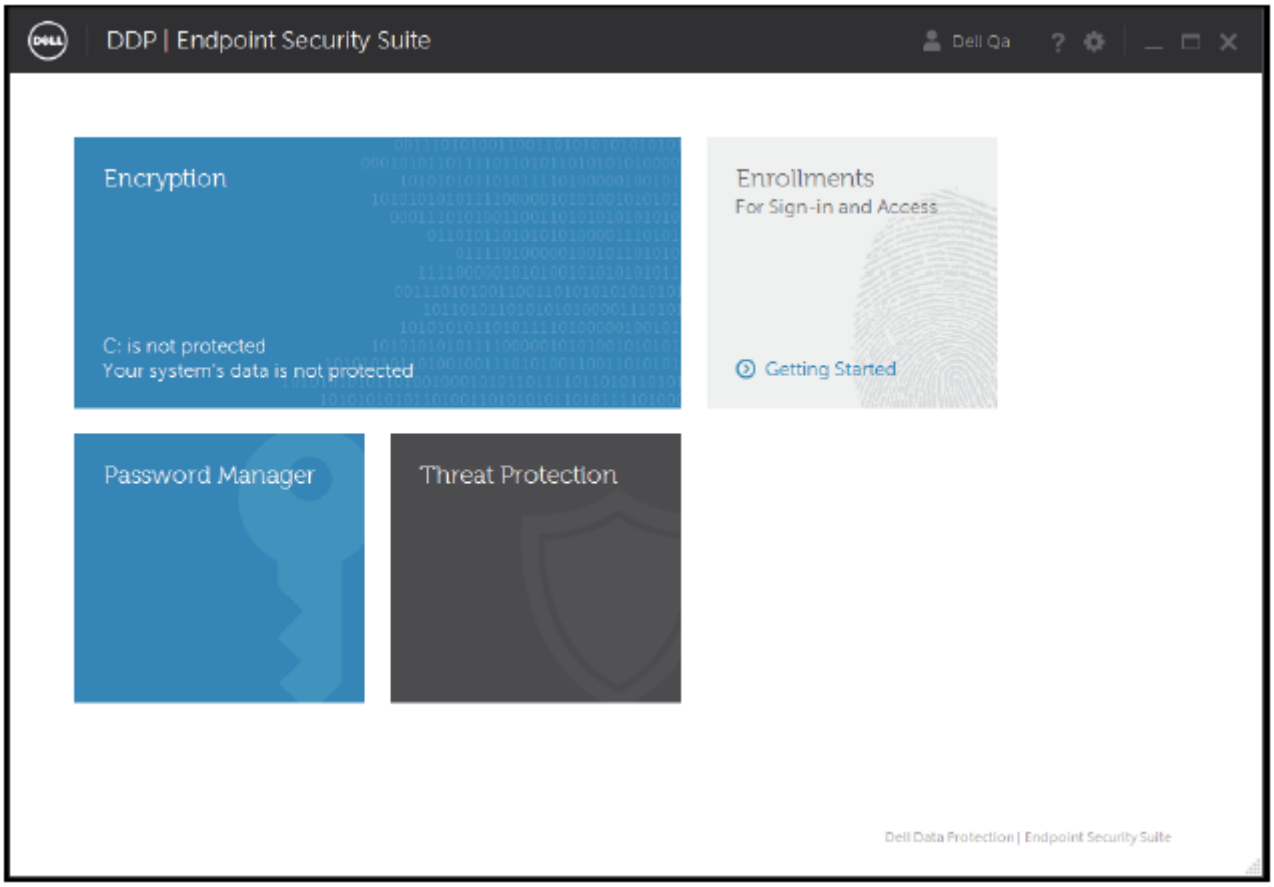
Menüelement	Zweck
Info	Enthält Versions- und Copyright-Informationen.
Info anzeigen	Enthält die folgenden Informationen: • Produktversion und Datumsinformationen • ob die DDP-Konsole auf diesem Computer durch einen Unternehmens- oder einen lokalen Administrator verwaltet wird • Versionsnummern für Betriebssystem, BIOS, Hauptplatine und TPM (Trusted Platform Module).
MS Info	Führt das Dienstprogramm für Microsoft Windows-Systeminformationen aus, um detaillierte Informationen zur Hardware, zu den Komponenten und der Softwareumgebung anzuzeigen.
Info kopieren	Kopiert alle Systeminformationen in die Zwischenablage, um sie in eine E-Mail an Ihren Administrator oder den Dell ProSupport einzufügen.
Feedback	Zeigt ein Formular an, mit dem Sie Dell Feedback zu diesem Produkt geben können. (Auf Nicht-Domänencomputern ist diese Option jederzeit verfügbar. Auf Domänencomputern richtet sich diese Option der Unternehmensrichtlinie.)
Richtlinien	Zeigt eine Hierarchie der Richtlinien an, die auf diesem Computer gelten.
Services	Zeigt Details zu den ausgeführten Diensten an.
Support	Stellt eine Verbindung zur Dell ProSupport-Website her.
Protokolle	Zeigt eine detaillierte Liste der protokollierten Ereignisse für Fehlerbehebungszwecke an.
Start Ablaufverfolgung	Hiermit können Sie sie Aufzeichnung der Anmeldeaktivitäten zur Fehlerbehebung starten und anhalten.

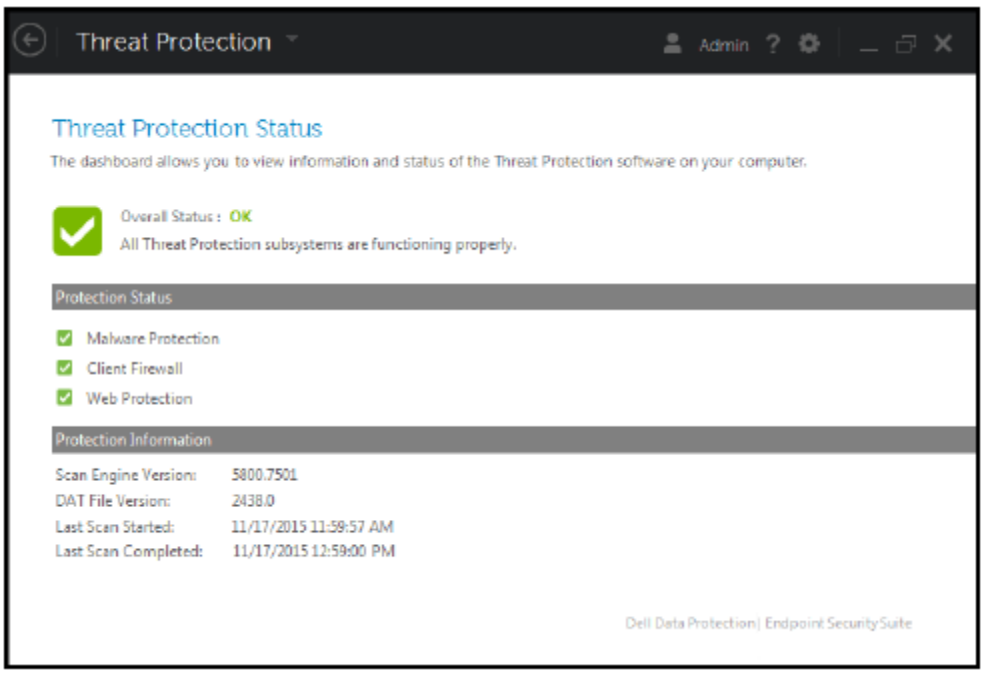
3

Threat Protection

Threat Protection-Dashboard

Benutzer greifen über die Threat Protection-Kachel in der DDP-Konsole auf das Threat Protection Status-Dashboard zu.





- Geschützt - Der Gesamtstatus ist geschützt, wenn die Richtlinien für *Zugriffsschutz*, *Exploit-Schutz* und **zugriffsbasierten Schutz** auf „Wahr“ (aktiviert) eingestellt sind.

  oder

  Die Richtlinie für*On-Demand-Schutz- Vollständiger Scan* oder *On-Demand-Schutz - Schneller Scan* sind auf True (Wahr) gesetzt (aktiviert) und die zugehörigen Zeitplanungsrichtlinien sind festgelegt.

- Anfällig - Der Gesamtstatus ist anfällig, wenn eine der folgenden Richtlinien auf „Falsch“ (deaktiviert) eingestellt ist: *Zugriffsschutz*, *Exploit-Schutz* und **zugriffsbasierter Schutz**.

  und

  Sowohl die Richtlinie für *On-Demand -Schutz - Vollständiger Scan* als auch die Richtlinie für *On-Demand-Schutz - Schneller Scan* werden auf „Falsch“ (deaktiviert) gesetzt oder „Wahr“ (aktiviert) gesetzt, ohne dass entsprechende Zeitplanungsrichtlinien festgelegt wurden.

  Schutzstatus

  Das Feld „Schutzstatus“ zeigt den individuellen Status als „Geschützt“ (gekennzeichnet durch ein grünes Häkchen) oder „Ungeschützt“ (gekennzeichnet durch ein rotes X) an, je nachdem, ob die folgenden Master-Richtlinien auf „Wahr“ (Aktiviert) gesetzt sind:

- Malware-Schutz
- Client-Firewall
- Web-Schutz

  Schutzinformationen

  Das Feld „Schutzinformationen“ enthält die folgenden Informationen:

- Scan-Engine-Version - Die Version der verwendeten Scan-Engine. Die Suchmaschine vergleicht die Inhalte der gescannten Dateien gegen bekannte Bedrohungen.
- DAT-Dateiversion - Die Version der „Threat Protection“-DAT-Datei, welche die Engine verwendet, um während eines Scans Malware zu erkennen.
- Letzter gestarteter Scan – Zeitstempel, wann der letzte erfolgreiche Scan gestartet wurde.
- Letzter Scan beendet – Zeitstempel, als der letzte erfolgreiche Scan beendet wurde.

  Menü „Extras“

  Das Menü „Extras“ enthält die folgenden Optionen:

- Über – Enthält Informationen zur Endpoint Security Suite-Version und der Konfiguration des Client-Computers.
- Richtlinien – Auflistung vieler Agent-Richtlinien. Derzeit werden hier aufgrund der großen Anzahl keine Threat Protection-Richtlinien angezeigt.
- Services – Zeigt den Zustand des AntiMalware Management-Plugins und die Kommunikation mit dem Dell Management Agent an.
- Feedback – Stellt einen Link zur Dell Support-Website bereit.
- Feedback – Zeigt Ereignisse in Zusammenhang mit Services, einschließlich des Anti-Malware Management Plugins, an.
- Start Ablaufverfolgung – Hiermit können Sie sie Aufzeichnung der Systemaktivitäten zur Fehlerbehebung starten und anhalten.

Popup-Benachrichtigungen

Basierend auf den Richtlinien kann der Benutzer mit Popup-Benachrichtigungen über Bedrohungen für die folgenden Objekte informiert werden:

- Dateien und Ordner
- Registrierungsdatei
- Endpoint Security Suite – Prozesse
- Nicht verifizierte und bösartige Websites
- Phishing-Seiten

  Der Benutzer muss **keine** Maßnahmen ergreifen. Alle Abhilfemaßnahmen werden von der Endpoint Security Suite abgewickelt.

  Popup-Benachrichtigungen unterdrücken

  Um die Nachrichten zu unterdrücken, mit denen Benutzer über Bedrohungen informiert werden, setzen Sie den folgenden Registrierungsschlüssel:

  [HKLM\Software\Dell\Dell Data Protection]

"DDPTPHideToasters"=dword:1

0=(Standardeinstellung) Deaktiviert, die Popup-Benachrichtigungen nicht verbergen

1=Aktiviert, Popup-Benachrichtigungen verbergen

Popup-Benachrichtigungen filtern

Um Benachrichtigungen für die niedrigste Sicherheitsstufe anzuzeigen, legen Sie den folgenden Registrierungsschlüssel fest:

[HKLM\Software\Dell\Dell Data Protection]

„DDPTPEventSeverityFilter“=dword:3

0=Information (es werden alle Ereignisse angezeigt), 1=Warnung, 2=Niedrig, 3=Hoch (standardmäßig werden nur die folgenden Kategorien angezeigt: Hoch und Kritisch), 4=Kritisch

Wenn „DDPTPHideToasters“ auf 1 gesetzt ist, werden die Einstellungen für „DDPTPEventSeverityFilter“ ignoriert.

4

Verschlüsselungsstatus

Auf der Seite „Verschlüsselung“ wird der Verschlüsselungsstatus des Computers angezeigt. Ist eine Festplatte, ein Laufwerk oder eine Partition nicht verschlüsselt, wird der Status als *Schutz aufgehoben* angezeigt. Ein Laufwerk oder eine Partition, das bzw. die verschlüsselt ist, wird mit dem Status als *Geschützt* angezeigt.

Um den Verschlüsselungsstatus zu aktualisieren, klicken Sie mit der rechten Maustaste auf die jeweilige Festplatte, das Laufwerk oder die Partition und dann auf **Aktualisieren**.

5

Registrierungen

Mit dem Registrierungstool können Sie basierend auf den vom Administrator festgelegten Richtlinien Registrierungen und Änderungen vornehmen sowie den Registrierungsstatus überprüfen.

Wenn Sie Ihre Anmeldeinformationen zum ersten Mal über die DDP Console eintragen, führt Sie ein Assistent durch den Eintragungsprozess für Passwortänderung, Wiederherstellungsfragen, Fingerabdrücke, Mobilgeräte und Smart Card. Je nach Richtlinie können Sie die einzelnen Anmeldeinformationen registrieren oder übergehen. Nach der erstmaligen Registrierung können Sie auf die Kachel „Registrierungen“ klicken, um Anmeldeinformationen hinzuzufügen oder zu ändern.

Erstmaliges Eintragen von Anmeldeinformationen

Gehen Sie wie folgt vor, um Anmeldeinformationen erstmals einzutragen:

1 Klicken Sie auf der Startseite Security Tools auf den Link **Erste Schritte** auf der Registrierungsschaltfläche.

2 Klicken Sie auf dem Begrüßungsbildschirm auf **Weiter**.

3 Melden Sie sich auf dem Dialogfeld „Authentifizierung erforderlich“ mit Ihrem Windows-Kennwort an und klicken Sie auf **OK**.

4 Um Ihr Windows-Kennwort zu ändern, geben Sie auf der Seite „Kennwort“ ein neues Passwort ein, bestätigen es und klicken dann auf **Weiter**.

   Um den Schritt der Kennwort-Änderung zu überspringen, klicken Sie auf **Überspringen**. Der Assistent bietet Ihnen die Möglichkeit, eine Anmeldeinformation zu überspringen, falls Sie diese nicht eintragen möchten. Um zu einer vorherigen Seite zurückzukehren, klicken Sie auf **Zurück**.

5 Folgen Sie den jeweiligen Bildschirmanweisungen, und klicken Sie nach Bedarf auf die folgenden Schaltflächen: **Weiter**, **Überspringen** und **Zurück**.

6 Bestätigen Sie auf der Zusammenfassungsseite die eingetragenen Anmeldeinformationen, und klicken Sie anschließend auf **Übernehmen**.

   Um zu einer Seite für die Eintragung von Anmeldeinformationen zurückzukehren und dort Änderungen durchzuführen, klicken Sie solange auf **Zurück**, bis Sie auf der Seite angekommen sind, die Sie ändern möchten.

Detailliertere Informationen über die Registrierung von Anmeldeinformationen oder die Änderung von Anmeldeinformationen finden Sie unter Hinzufügen, Ändern oder Anzeigen von Registrierungen.

Hinzufügen, Ändern oder Anzeigen von Registrierungen

Klicken Sie zum Hinzufügen, Ändern oder Anzeigen von Registrierungen auf die Kachel **Registrierungen**.

Register im linken Fenster zeigen verfügbare Eintragungen an. Sie variieren je nach Plattform und Hardware.

Die Seite „Status“ zeigt die unterstützten Anmeldeinformationen, die zugehörigen Richtlinieneinstellungen („Erforderlich“ oder „–“) sowie den Eintragungsstatus an. Über diese Seite können Benutzer ihre Registrierungen auf Basis der durch den Administrator definierten Richtlinie verwalten.

- Um eine Anmeldeinformation zum ersten Mal einzutragen, klicken Sie in der Zeile der Anmeldeinformation auf **Registrieren**.
- Um eine bereits eingetragene Anmeldeinformation zu löschen, klicken Sie auf **Löschen**.
- Wenn die Richtlinie nicht zulässt, dass Benutzer ihre eigenen Anmeldeinformationen registrieren oder ändern, sind die Links **Registrieren** und **Löschen** auf der Statusseite deaktiviert.

- Um eine vorhandene Registrierung zu ändern, klicken Sie auf die entsprechende Registerkarte im linken Bereich.

  Wenn Richtlinie keine Registrierung oder Änderung von Anmeldeinformationen zulässt, wird die Meldung „Änderung der Anmeldeinformationen laut Richtlinie unzulässig“ auf der Seite für die Eintragung von Anmeldeinformationen angezeigt.

Passwort

So ändern Sie Ihr Windows-Passwort:

1 Klicken Sie auf die Registerkarte **Kennwort**.
2 Geben Sie Ihr derzeitiges Windows-Passwort ein.
3 Geben Sie das neue Passwort ein, wiederholen Sie es zur Bestätigung und klicken Sie anschließend auf **Ändern**.
Kennwortänderungen sind sofort gültig.

4 Klicken Sie im Eintragungsdialog auf **OK**.

> **ANMERKUNG:**
> Sie sollten Ihr Windows-Passwort nur in der DDP Console und nicht in Windows ändern. Falls das Windows-Passwort außerhalb der DDP Console geändert wird, stimmen die Passwörter nicht mehr überein. In diesem Fall muss eine Wiederherstellung durchgeführt werden.

Wiederherstellungsfragen

Auf der Seite „Wiederherstellungsfragen“ können Sie Ihre Wiederherstellungsfragen und -antworten erstellen, löschen oder ändern. Wiederherstellungsfragen ermöglichen es Ihnen, über ein Frage-Antwort-Verfahren auf Ihr Windows-Konto zuzugreifen, wenn Sie beispielsweise Ihr Passwort vergessen haben oder dieses abgelaufen ist.

> **ANMERKUNG:**
> Wiederherstellungsfragen werden nur dazu verwendet, den Zugriff auf einen Computer wiederherstellen. Die Fragen und Antworten können nicht für die Anmeldung verwendet werden.

Gehen Sie folgendermaßen vor, falls Sie noch keine Wiederherstellungsfragen eingetragen haben:

1 Klicken Sie auf die Registerkarte **Wiederherstellungsfragen**.
2 Wählen Sie in einer Liste vordefinierter Fragen aus, geben Sie dann Ihre Antworten ein, und bestätigen Sie diese.
3 Klicken Sie auf **Registrieren**.

> **ANMERKUNG:**
> Klicken Sie auf die Schaltfläche **Wiederherstellen**, um die Auswahl auf dieser Seite zu löschen und erneut zu beginnen.

Wiederherstellungsfragen bereits eingetragen

Wenn bereits Wiederherstellungsfragen eingetragen wurden, können Sie diese entweder löschen oder erneut eintragen.

1 Klicken Sie auf die Registerkarte **Wiederherstellungsfragen**.
2 Klicken Sie auf die entsprechende Schaltfläche:
   - Um die Wiederherstellungsfragen vollständig zu löschen, klicken Sie auf **Löschen**.
   - Um die Wiederherstellungsfragen und die zugehörigen Antworten neu zu definieren, klicken Sie auf **Erneut registrieren**.

Fingerabdrücke

ANMERKUNG:
Um diese Funktion nutzen zu können, muss Ihr Computer über einen Fingerabdruckleser verfügen.

Gehen Sie folgendermaßen vor, um Fingerabdrücke einzutragen:

1 Klicken Sie auf die Registerkarte **Fingerabdrücke**.
2 Klicken Sie auf der Seite „Fingerabdrücke“ auf den Finger, den Sie eintragen möchten.
3 Folgen Sie den Anweisungen im Bildschirm, um Ihren Fingerabdruck einzutragen.

ANMERKUNG:
Der jeweilige Finger muss vier Mal erfolgreich gescannt werden, um als eingetragen zu gelten. Die Anzahl der zur Fingerabdruckeintragung erforderlichen Scans richtet sich nach der Qualität der einzelnen Fingerabdruckscans. Mindest- und Maximalanzahl der Fingerabdrücke wurden vom Administrator festgelegt.

4 Klicken Sie auf den jeweils nächsten zu scannenden Finger, bis Sie die gemäß Richtlinie erforderliche Mindestanzahl von Fingerabdrücken eingetragen haben.
Falls Sie nicht die Mindestanzahl an Fingerabdrücken eingetragen haben, werden Sie anhand eines Dialogfelds darüber informiert. Klicken Sie zum Fortfahren auf **OK**.
5 Schließen Sie den Scanvorgang für die erforderliche Anzahl an Fingerabdrücken ab und klicken Sie dann auf **Speichern**.
Um einen gescannten Fingerabdruck zu löschen, klicken Sie auf der Seite für die Fingerabdruckeintragung auf einen markierten Fingerabdruck, um die Eintragung für diesen Abdruck aufzuheben. Klicken Sie dann zum Bestätigen des Löschvorgangs auf **Ja** und anschließend auf **Speichern**.

Mobilgerät

Die Eintragung eines Mobilgeräts umfasst die Einmalkennwort-Funktion (OTP). Mit OTP kann sich der Benutzer auf einem Mobilgerät, das mit einem Computer gekoppelt ist, über ein Passwort bei Windows anmelden, das durch die Security Tools | Mobile-App generiert wurde. Wenn Ihr Administrator dies gemäß Richtlinie zulässt, kann die OTP-Funktion auch verwendet werden, um den Computerzugang wiederherzustellen, wenn das Passwort vergessen wurde.

ANMERKUNG:
Wenn die Registerkarte „Mobilgerät“ in Ihrer DDP Console nicht angezeigt wird, wird diese Funktion in Ihrer Computerkonfiguration nicht unterstützt, oder die von Ihrem Administrator definierte Richtlinie schließt diese Funktion aus.

ANMERKUNG:
Die Richtlinieneinstellungen legen fest, wie die OTP-Funktion genutzt werden kann – entweder zur Anmeldung oder zur Wiederherstellung des Computerzugangs, wenn Sie Ihr Passwort vergessen haben oder es abgelaufen ist. Die Funktion kann nicht für die Anmeldung und die Wiederherstellung verwendet werden.

Zur Verwendung der OTP-Funktion müssen Sie Ihr Mobilgerät auf dem Computer eintragen, bzw. es mit dem Computer koppeln. Auf einem Computer mit mehreren Benutzer kann jeder Benutzer ein Mobilgerät auf dem Computer eintragen. Mobilgeräte können auf mehreren Computern eingetragen werden.

Wenn bereits ein Gerät eingetragen ist, wird durch die Eintragung eines neuen Geräts die Eintragung des vorhandenen Geräts automatisch aufgehoben.

Das Mobilgerät eintragen

1 Klicken Sie auf der Eintragungsseite der DDP Console auf die Registerkarte **Mobilgerät**.

2 Klicken Sie oben rechts auf **Registrieren**.
Die Seite „Einmalpasswort eintragen“ wird angezeigt.

3 Wenn dies der erste Computer ist, der gekoppelt werden soll, wählen Sie **Ja** aus.

a Laden Sie auf dem Mobilgerät die Dell Data Protection | Security Tools | Mobile-App von Ihrem App-Store herunter.

b Klicken Sie auf dem Computer auf **Weiter**.

Security Tools Mobile einrichten

1 Öffnen Sie die Security Tools | Mobile-App.

2 Erstellen Sie eine PIN-Nummer für den Zugriff auf die Security Tools | Mobile-App, und geben Sie sie ein.

ANMERKUNG:
Die PIN wird möglicherweise gemäß Richtlinie angefordert, wenn das mobile Gerät nicht gesperrt ist. Wenn Sie keine PIN verwenden, um das Gerät zu entsperren, benötigen Sie eine solche, um auf die Security Tools | Mobile-App zuzugreifen.

3 Wählen Sie **Einen Computer registrieren** aus. (Tippen Sie ggf. in die obere linke Ecke auf dem Bildschirm Ihres Mobilgeräts, um auf die Befehle zuzugreifen.)
Auf dem Mobilgerät wird ein Code angezeigt. Die Länge des Codes und die alphanumerische Kombination basieren auf den Richtlinieneinstellungen des Administrators.

Mobilgerät und Computer koppeln

1 Führen Sie auf dem Computer die folgenden Schritte auf der Seite „DDP-Konsole – Code für Mobilgerät“ aus:

a Geben Sie den Code Ihres Mobilgeräts in das Feld ein.

b Klicken Sie auf **Weiter**.

c Wählen Sie auf der Seite „Gerät koppeln“ eine der folgenden Optionen aus:
QR-Code – Ein QR-Code wird angezeigt.

oder

Manuelle Eingabe – Es wird ein 24-stelliger Kopplungscode angezeigt.

2 Gehen Sie auf dem Mobilgerät folgendermaßen vor:

a Tippen Sie auf **Geräte koppeln**.

b Wählen Sie den gleichen Kopplungsoption (**QR-Code scannen** oder **Manuelle Eingabe**), die Sie zuvor auf dem Computer ausgewählt haben.

c Wählen Sie eine der folgenden Optionen aus:

- Bei Verwendung eines **QR-Codes** positionieren Sie das Mobilgerät vor dem Computerbildschirm, um den QR-Code zu scannen.
  Notieren Sie den numerischen Verifizierungscode, der auf dem Mobilgerät angezeigt wird. Tippen Sie anschließend auf **Weiter**.

  ANMERKUNG:
  Wenn der Balken *Schwierigkeiten beim Scannen?* angezeigt wird, versuchen Sie es noch einmal, oder wählen Sie alternativ die Option **Manuelle Eingabe**.

- Bei **Manueller Eingabe** geben Sie den 24-stelligen Kopplungscode des Computers ein und tippen Sie auf **Fertig**.
  Notieren Sie den numerischen Verifizierungscode, der auf dem Mobilgerät angezeigt wird. Tippen Sie anschließend auf **Weiter**.

3 Führen Sie auf dem Computer auf der Seite „DDP-Konsole“ die folgenden Schritte aus:

a Klicken Sie auf **Weiter**.

b Geben Sie den auf dem Mobilgerät angezeigten Verifizierungscode ein und klicken Sie auf **Weiter**.

c Ändern Sie optional den Namen des Mobilgeräts.

d Klicken Sie auf **Anwenden**.

Die Geräte werden gekoppelt.

4 Gehen Sie auf dem Mobilgerät folgendermaßen vor:

a Tippen Sie auf **Fortfahren**.

b Ändern Sie optional den Namen des Computers, und tippen Sie dann auf **Fertig**.

c Tippen Sie auf **Fertigstellen**.

Weiteres Mobilgerät eintragen

Durch Eintragen eines neuen Geräts wird das vorherige Geräts automatisch entkoppelt. Zum Entkoppeln sind keine separaten Schritte erforderlich.

Computer und Mobilgerät entkoppeln

Um einen Computer und ein Mobilgerät zu entkoppeln, ohne ein anderes Gerät einzutragen, wählen Sie eine der folgenden Optionen aus:

- In der DDP Console: Klicken Sie auf der Seite „Eintragungsstatus“ neben den Anmeldeinformationen für das Mobilgerät auf **Löschen**.
- Auf dem mobilen Gerät: siehe die nachfolgenden Schritte.

1 Auf dem mobilen Gerät führen Sie die folgenden Schritte aus:

a Öffnen Sie die Security Tools | Mobile-App.

b Tippen Sie oben links auf die Menüleiste, um die Schublade zu öffnen.

c Tippen Sie auf **Computer entfernen**.

d Wählen Sie den zu entkoppelnden Computer aus.

e Wählen Sie **Entfernen** (Android) oder tippen Sie auf **Fertig** (iOS).

Daraufhin wird eine Bestätigungsmeldung angezeigt.

f Wählen Sie **Alle entfernen** aus, um alle registrierten Computer von Ihrem Gerät zu entfernen.

Die Option „Alle entfernen“ wird angezeigt, wenn Sie mehrere Computer entfernen und Sie dabei den einzigen gekoppelten Computer entfernen.

- Wählen Sie **Standardeinstellungen wiederherstellen** zum Entfernen der registrierten Computer und Entfernen der PIN. Wenn Sie die Standardeinstellungen wiederherstellen, werden alle eingetragenen Computer und die PIN, die Sie für den Zugriff auf die Security Tools Mobile-App verwenden, entfernt.
- Wählen Sie **Abbrechen** aus, um den Computer angemeldet zu belassen.

Anmeldung mit einmaligem Passwort

ANMERKUNG:
Die OTP-Authentifizierung kann nur für Windows-Anmeldungen verwendet werden.

OTP kann entweder für die Wiederherstellung, also für den Zugriff auf den Computer, wenn Sie gesperrt wurden, oder für die Windows-Anmeldung verwendet werden. OTP kann jedoch nicht für beides verwendet werden.

Wenn dies gemäß Richtlinie zulässig ist und das OTP-Symbol  auf Ihrem Anmeldebildschirm erscheint, können Sie sich mit OTP bei Windows anmelden.

So melden Sie sich mit OTP an:

1 Wählen Sie auf dem Computer im Windows-Anmeldebildschirm das OTP-Symbol  aus.

2 Öffnen Sie auf dem Mobilgerät die Security Tools | Mobile-App, und geben Sie die PIN ein.

3 Wählen Sie den Computer aus, auf den Sie zugreifen möchten.

Falls der Computername nicht auf dem Mobilgerät angezeigt wird, liegt möglicherweise eine der folgenden Bedingungen vor:

- Das Mobilgerät wurde nicht eingetragen bzw. nicht mit dem Computer gekoppelt, auf den Sie zugreifen möchten.
- Falls Sie über mehrere Windows-Benutzerkonten verfügen, ist entweder Endpoint Security Suite nicht auf dem Computer installiert, auf den Sie zugreifen möchten, oder Sie versuchen, sich bei einem Benutzerkonto anzumelden, das nicht mit dem Konto übereinstimmt, das zum Koppeln zwischen Computer und Mobilgerät verwendet wurde.

4 Tippen Sie auf **Einmalpasswort**.

Auf dem Mobilgerät wird ein Passwort angezeigt.

ANMERKUNG:

Klicken Sie ggf. auf das Symbol zum Aktualisieren  , um einen neuen Code zu erhalten. Nach zwei OTP-Aktualisierungen kann ein weiteres OTP erst nach einer zeitlichen Verzögerung von 30 Sekunden generiert werden.

Der Computer und das Mobilgerät müssen synchron sein, damit beide dasselbe Passwort gleichzeitig erkennen können. Wenn Sie versuchen, in kurzen Abständen Passwörter nacheinander zu generieren, sind Computer und Mobilgerät nicht mehr synchron und die OTP-Funktion schlägt fehl. Falls dieses Problem auftritt, warten Sie 30 Sekunden, bis die beiden Geräte wieder synchron sind, und versuchen Sie es dann erneut.

5 Geben Sie auf dem Computer im Windows-Anmeldebildschirm das auf dem Mobilgerät angezeigte Passwort ein, und drücken Sie die **Eingabetaste**.

Falls Sie OTP für die Wiederherstellung verwendet haben und Sie wieder Zugriff auf Ihren Computer haben, folgen Sie den Anweisungen im Bildschirm, um das Passwort zurückzusetzen.

Schritte für die Security Tools | Mobile-Verwaltung

Diese Schritte werden über die Security Tools | Mobile-App auf dem Mobilgerät ausgeführt.

PIN für die Security Tools | Mobile-App zurücksetzen

Gehen Sie wie folgt vor, um die PIN für die Security Tools | Mobile-App zurückzusetzen:

1 Tippen Sie oben rechts auf die Menüoptionen.

2 Wählen Sie **PIN zurücksetzen** aus.

3 Geben Sie die neue PIN ein, und bestätigen Sie sie.

Security Tools | Mobile-App deinstallieren

Gehen Sie auf dem Mobilgerät folgendermaßen vor:

1 Entkoppeln Sie Mobilgerät und Computer.

2 Löschen oder deinstallieren Sie die Security Tools Mobile-App auf die gleiche Weise, wie Sie normalerweise Apps auf Ihrem Mobilgerät löschen.

Smart Cards

ANMERKUNG:
Um diese Funktion nutzen zu können, muss Ihr Computer über einen Smart-Card-Leser verfügen.

Führen Sie für das Eintragen von Smart Cards die folgenden Schritte aus:

1 Klicken Sie auf die Registerkarte **Smart Card**.
2 Tragen Sie die Smart Card je nach Kartentyp ein:
   - Legen Sie die Smart Card in den Kartenleser ein.
   - Bei einer kontaktlosen Karte genügt es, diese auf dem Lesegerät zu platzieren oder sie in dessen Nähe zu halten.
3 Wird die Karte erkannt, wird ein grünes Kontrollkästchen und die Aufforderung *Die Karte anmelden* angezeigt. Wählen Sie **Karte registrieren** aus.
4 Klicken Sie im Eintragungsdialog auf **OK**.

Um die Eintragung aller mit dem Benutzer verknüpften Smart Cards aufzuheben, wählen Sie auf der Seite für die Smart Card-Eintragung **Registrierte Karten von Ihrem Konto entfernen** aus.

6

Password Manager

Mit dem Kennwort-Manager können Sie sich automatisch auf Websites, bei Windows-Programmen und Netzwerkressourcen anmelden und Anmeldeinformationen in einem Tool verwalten. Mit dem Kennwort-Manager können Benutzer außerdem ihre Anmeldekennwörter über die Anwendung ändern und damit sicherstellen, dass die durch den Kennwort-Manager verwalteten Kennwörter mit denen der Zielressource synchron bleiben.

Der Kennwort-Manager wird von Internet Explorer und Mozilla Firefox unterstützt. Der Kennwort-Manager wird von Microsoft-Konten (früher Windows Live ID) nicht unterstützt.

ANMERKUNG:
Falls Sie Password-Manager auf Firefox verwenden, müssen Sie die Passwort-Manager-Erweiterung installieren und registrieren. Weitere Anweisungen zum Installieren von Erweiterungen in Mozilla Firefox finden Sie unter https://support.mozilla.org/.

ANMERKUNG:
Die Verwendung von Password-Manager-Symbolen (bei „trainierten“ wie „nicht trainierten“ Symbolen) in Mozilla Firefox unterscheidet sich von ihrer Verwendung im Microsoft Internet Explorer:

- Passwort-Manager-Symbole können nicht doppelt angeklickt werden.
- Die Standardmaßnahme wird im Dropdown-Kontextmenü nicht in Fettschrift angezeigt.
- Falls eine Seite mehrere Anmeldeformulare hat, sehen Sie u. U. mehr als ein Passwort-Manager-Symbol.

ANMERKUNG:
Da sich die Struktur von Anmeldebildschirmen auf Websites häufig ändert, kann der Password-Manager möglicherweise nicht immer alle Websites unterstützen.

Erste Schritte mit Password-Manager

Password-Manager erfasst und speichert Ihre Anmeldeinformationen während Sie arbeiten. Sie können Password Manager unmittelbar nach der Installation von Endpoint Security Suite verwenden. Wenn Sie Anmeldeinformationen auf einer Anmeldeseite eingeben, erkennt Password Manager das

Anmeldeformular. Außerdem können Sie auswählen, ob Password Manager Ihre Anmeldeinformationen speichern soll.

Sie haben drei Optionen:

- Klicken Sie auf **Anmeldung speichern**, um Ihre Anmeldeinformationen im Password Manager zu speichern.
- Wenn Sie Ihre Anmeldeinformationen ***nicht*** speichern möchten, werden Sie bei jeder Anmeldung auf der Website oder beim Programm erneut gefragt, ob Sie die Anmeldeinformationen speichern möchten. Wenn Sie nicht mehr gefragt werden möchten, wählen Sie **Niemals für diese Website** aus. In der Liste der ausgeschlossenen Websites wird ein Eintrag erstellt. Unter Websites ausschließen erhalten Sie weitere Informationen.
- Wenn Sie nicht möchten, dass die Anmeldeinformationen gespeichert werden, klicken Sie auf **Anmeldeinformationen nicht speichern**.

Dieses Dialogfeld wird auch angezeigt, wenn Sie über zuvor gespeicherte Anmeldeinformationen für eine Website oder ein Programm verfügen, sie jedoch einen anderen Benutzernamen oder ein abweichendes Kennwort eingeben. Mit einem neuen Benutzernamen wird, wenn Sie **Anmeldeinformationen speichern** auswählen, ein neuer Satz mit Anmeldeinformationen gespeichert. Mit dem zuvor

gespeicherten Benutzernamen und neuen Kennwort werden, wenn Sie **Anmeldeinformationen speichern** auswählen, Ihre ursprünglichen Anmeldeinformationen mit dem neuen Kennwort aktualisiert.

Anmeldedaten verwalten

Der Logon-Manager vereinfacht und zentralisiert die Verwaltung aller Ihrer Anmeldeinformationen auf Websites, in Windows-Programmen und bei Netzwerkressourcen

So öffnen Sie den Logon-Manager:

1 Klicken Sie auf der DDP Console-Startseite auf die Kachel **Password Manager**.
2 Klicken Sie auf die Registerkarte **Logon Manager**.

Sie können Anmeldeinformationen und Kategorien hinzufügen und diese sortieren und filtern:

Anmeldung hinzufügen - Ermöglicht das Hinzufügen eines neuen Satzes von Anmeldeinformationen. Je nach Richtlinie werden Sie möglicherweise aufgefordert, Anmeldeinformationen einzugeben, die in gespeichert sind, um eine Anmeldung hinzufügen.

Kategorie Hinzufügen - Ermöglicht Ihnen das Hinzufügen einer neuen Kategorie (wie E-Mail, Speicher, Nachrichten, Unternehmensressourcen, soziale Medien) zum Sortieren und Filtern.

Sortieren: Sortieren der Anmeldeinformationen nach Konto, Benutzername oder Kategorie. Klicken Sie auf eine Spaltenüberschrift, um diese nach der zugehörigen Spalte zu sortieren.

Filtern: Wählen Sie eine Kategorie aus der Liste *Anzeigen* zum Ausblenden aller Anmeldungen mit Ausnahme von denjenigen in der ausgewählten Kategorie. Um den Filter zu entfernen, wählen Sie *Alle* aus.

Sie können Anmeldeinformationen wie folgt verwalten:

Starten – Öffnet die Website oder das Programm und übermittelt die Anmeldeinformationen auf Basis der Benutzereinstellungen.

Bearbeiten –- Mit dieser Option können Sie die gespeicherten Anmeldedaten für eine Website oder ein Programm ändern.

Löschen – Mit dieser Option können Sie die gespeicherten Anmeldedaten aus dem Kennwort-Manager löschen.

Hinzufügen – Mit dieser Option können Sie eine neue Anmeldung, eine Kategorie oder neue Anmeldedaten hinzufügen.

Kategorie hinzufügen

Bevor Sie Anmeldeinformationen hinzufügen können, müssen Sie Kategorien (z. B. E-Mail, Speicher, News, Unternehmensressourcen und Social Media) erstellen, so dass Sie Ihre Anmeldeinformationen während der Erstellung kategorisieren können. Anschließend können Sie Ihre Anmeldeinformationen nach Kategorie sortieren und filtern.

Um eine Kategorie hinzuzufügen, klicken Sie auf der Seite „Logon Manager“ auf **Kategorie hinzufügen**, geben Sie einen Kategorienamen ein und klicken Sie auf **Speichern**.

Anmeldung hinzufügen

1 Klicken Sie auf der Seite „Logon Manager“ auf **Anmeldung hinzufügen**.
Je nach Richtlinie werden Sie möglicherweise aufgefordert, sich zu authentifizieren, um eine Anmeldeinformation hinzuzufügen.
2 Öffnen Sie die Website oder das Programm, an der/dem Sie sich anmelden möchten.

3 Klicken Sie im Dialogfeld „Anmeldeinformationen hinzufügen“ auf **Fortfahren**.

4 Geben Sie im nächsten Dialogfeld Folgendes ein:

- **Kategorie** – Wählen Sie eine Kategorie für die Website- oder Programmanmeldung aus, die Sie speichern möchten. Wenn Sie noch keine Kategorien hinzugefügt haben, ist diese Liste leer.
- **Kontoname** – Belassen Sie den vorausgefüllten Namen oder geben Sie den Namen der Website oder des Programms ein.
- **Nicht erkannter Titel** - Diese Felder werden durch Kennwort Manager als Felder auf der Anmeldungsseite erkannt, in die Sie Ihre Anmeldeinformationen eingeben. Diese Felder umfassen in der Regel den Benutzernamen oder die E-Mail-Adresse und das Passwort.

5 Wenn ein Feld als „Nicht erkannter Titel“ angezeigt wird oder wenn die falschen Felder als Anmeldefelder berücksichtigt wurden, klicken Sie auf die Schaltfläche **Weitere Felder**, um Feldnamen zu bearbeiten oder Felder zu entfernen.

6 Klicken Sie im Dialogfeld „Weitere Felder“ auf **Nicht erkannter Titel** und geben Sie den richtigen Feldnamen für jedes Feld ein.

Wenn das Dialogfeld „Weitere Felder“ angezeigt wird, wird das Feld, das auf dem Dialogfeld „Anmeldeinformationen hinzufügen“ aktiv war, markiert, um Sie bei der Umbenennung der Felder zu unterstützen.

Wenn ein Feld für die Anmeldung nicht erforderlich ist, deaktivieren Sie das zugehörige Kontrollkästchen, um es aus den erforderlichen Anmeldeinformationen auszuschließen.

7 Klicken Sie zum Speichern der Änderungen auf **OK**.

8 Füllen Sie auf dem Dialogfeld „Anmeldeinformationen hinzufügen“ die Felder aus, die für die Anmeldung erforderlich sind.

> **ANMERKUNG:**
> Da Sie eine bereits vorhandene Anmeldung speichern, können Sie lediglich das Passwort ändern, indem Sie zur Funktion „Passwort ändern“ der Website oder des Programms wechseln.

9 Wenn Sie möchten, dass Password-Manager die Anmeldeinformationen automatisch einträgt und übermittelt, wählen Sie **Anmeldedaten automatisch übermitteln**.

10 Klicken Sie auf **Speichern**.

Daraufhin werden die Website- oder Programmanmeldeinformationen auf der Seite „Logon-Manager“ angezeigt.

Anmeldeinformationen importieren

Sie können die in Webbrowsern gespeicherten Anmeldeinformationen in Password-Manager importieren.

1 Wählen Sie im Kennwort-Manager die Option **Anmeldeinformationen importieren**.

2 Wählen Sie den Browser aus, von dem der Import erfolgen soll, und klicken Sie auf **Scannen**.

3 Geben Sie bei Aufforderung das Passwort für den ausgewählten Browser ein.

> **ANMERKUNG:**
> Wenn beim Import keine Kennwörter importiert werden, überprüfen Sie, ob der Browser Daten zum Import gespeichert hat. Falls Sie Firefox verwenden, melden Sie sich bei Sync an. Versuchen Sie erneut, Ihre Anmeldeinformationen zu importieren.

Symbol-Kontextmenü

Wenn Sie eine Website besuchen oder ein Programm aufrufen, wird das Symbol für den Password-Manager angezeigt.

Das  zeigt an, dass das Anmeldeformular „trainiert“ werden kann.

Wird das  nicht angezeigt, wurde das Anmeldeformular bereits „trainiert“. Doppelklicken Sie auf das Symbol, um sich bei dem Programm oder der Website anzumelden.

Wenn Sie auf das Symbol klicken, wird ein Kontextmenü mit weiteren Optionen angezeigt, und zwar basierend darauf, ob das Anmeldeformular trainiert wurde oder nicht.

Wenn die aktuellen Anmeldefelder noch nicht trainiert wurden, zeigt das Kontextmenü die folgenden Optionen an:

Zu Password-Manager hinzufügen – Damit wird das Dialogfeld Anmeldeinformationen hinzufügen geöffnet.

Symboleinstellungen - Der Benutzer kann die Anzeige des Password-Manager-Symbols auf den lernfähigen Anmeldeseiten konfigurieren.

Password Manager öffnen - Startet das Tool *Password Manager Administration* und öffnet die Seite „Logon Manager".

Hilfe – Öffnet die Online-Hilfe.

Wenn die aktuellen Anmeldefelder trainiert sind, zeigt das Kontextmenü die folgenden Optionen an:

Eintragen von Anmeldedaten – Je nachdem, was Sie ausgewählt haben, als Sie sich das Anmeldeformular angeschaut haben, erfolgt die Anmeldung entweder automatisch oder die Felder „Benutzername" und „Kennwort" werden ausgefüllt, sodass Sie die Anmeldedaten nur noch absenden müssen.

Anmeldung bearbeiten - Damit wird das Dialogfeld „Anmeldung bearbeiten" geöffnet.

Anmeldeinformationen hinzufügen – hiermit wird das Dialogfeld „Anmeldeinformationen hinzufügen" geöffnet.

Password Manager öffnen – Startet die Seite des Password Manager.

Hilfe – Öffnet die Online-Hilfe.

Wenn die Symbole für den Kennwort-Manager in den Anmeldeformularen nicht angezeigt werden, schalten Sie die Funktion zum Speichern von Kennwörtern in Ihren Browsern aus:

- In Mozilla Firefox: Menüsymbol > Optionen > Sicherheit > deaktivieren des Kontrollkästchens **Kennwörter für Websites merken**
- In Internet Explorer: Zahnradsymbol > Internetoptionen > Registerkarte Inhalt > Einstellungen automatisch vervollständigen > deaktivieren des Kontrollkästchens **Benutzername und Kennwörter in Formularen**

Anmeldung bei Anmeldeseiten mit abgeschlossenem Training

Wenn Sie eine Anmeldung bei einer Website oder in einem Programm öffnen, erkennt der Kennwort-Manager, ob die Seite trainiert ist. Ist die Seite trainiert, wird das Symbol für den Kennwort-Manager im Anmeldebereich angezeigt. Ist die Seite nicht trainiert, wird das Symbol für den Kennwort-Manager angezeigt, es sei denn, die Aufforderungen für untrainierte Formulare wurde deaktiviert

Wählen Sie zur Anmeldung eine der folgenden Optionen aus:

- Registrierte Anmeldeinformationen einlesen Wenn Sie einen Fingerabdruck oder eine Smart Card eingetragen haben, können Sie den Fingerabdruckleser mit dem entsprechenden Finger berühren bzw. die eingetragene Smart Card auf oder vor das Kartenlesegerät halten.
- Klicken Sie auf das Symbol für Password Manager und wählen Sie **Anmeldedaten ausfüllen** aus dem Kontextmenü aus.
- Drücken Sie die Tastenkombination für den Kennwort-Manager: **Strg+Win+H** Password-Manager zeigt daraufhin die trainierten Seiten in einem Popup-Fenster an, so dass Sie die gewünschte Seite schnell starten können.

ANMERKUNG:
Sie können die Tastenkombination unter „DDP-Konsole > Password-Manager

Wenn für die jeweilige Seite mehr als eine Anmeldeinformation gespeichert wurde, werden Sie aufgefordert, das zu verwendende Konto auszuwählen.

Unterstützung für Domänen

Wenn Sie eine Anmeldeseite für eine bestimmte Webdomäne trainiert haben, aber über eine andere Anmeldeseite auf das Konto dieser Domäne zugreifen möchten, navigieren Sie zur neuen Anmeldeseite. Sie werden dort aufgefordert, bestehende Anmeldeinformationen zu verwenden oder neue Anmeldeinformationen zu Password-Manager hinzuzufügen.

- Wenn Sie auf *Anmeldung verwenden* klicken, werden Sie bei Ihrem bestehenden Konto angemeldet. Wenn Sie das nächste Mal über die neue Anmeldeseite auf dieses Konto zugreifen, werden Sie automatisch bei dem zuvor erstellten Konto angemeldet.
- Wenn Sie auf *Anmeldung hinzufügen* klicken, wird das Dialogfeld Anmeldung hinzufügen angezeigt.

Windows-Anmeldeinformationen eintragen

Einige Programm unterstützen die Verwendung der Windows-Anmeldeinformationen für die Anmeldung.

Anstatt Ihren Benutzernamen und das zugehörige Kennwort einzugeben, wählen Sie die Windows-Anmeldeinformationen aus den Drop-Down-Menüs aus, die in den Dialogfeldern *Anmeldeinformationen hinzufügen* und *Anmeldeinformationen bearbeiten* verfügbar sind.

Wählen Sie für den Benutzernamen aus den folgenden Typen aus:

- Windows-Benutzername
- Windows-UPN
- Windows-Domäne\Benutzername
- Windows-Domäne

Wählen Sie als Passwort Ihr Windows-Passwort aus.

Diese Optionen können nicht geändert werden.

Altes Passwort verwenden

Es kann vorkommen, dass ein Passwort in Password-Manager geändert wurde und das Programm das neue Passwort anschließend ablehnt. In diesem Fall besteht im Programm die Möglichkeit, ein vorheriges (also ein zuvor auf dieser Anmeldeseite eingegebenes) Kennwort zu verwenden.

Wählen Sie **Passwortverlaufsliste** aus. Nach der Authentifizierung werden Sie aufgefordert, ein altes Passwort aus der Passwortverlaufsliste auszuwählen. Die Liste enthält sieben Passwörter.

Websites ausschließen

Um zu verhindern, dass Websites von Password-Manager verwaltet werden, klicken Sie auf die Registerkarte **Website-Ausschlüsse**.

Ausgeschlossene Websites weisen die folgenden Eigenschaften auf:

- Kein Kennwort-Manager-Symbol anfordern.
- Benutzer nicht automatisch anmelden.
- Kennworterinnerungen nicht anzeigen.

So fügen Sie eine neue Website zur Ausschlussliste hinzu:

1 Klicken Sie auf die Registerkarte **Website-Ausschlüsse**.
2 Klicken Sie auf **Website hinzufügen**.

3 Geben Sie die URL der auszuschließenden Website ein.
4 Klicken Sie auf **Speichern**.

Nachdem Sie eine Website ausgeschlossen haben, wird diese nicht mehr über den Password-Manager verwaltet. Löschen Sie einfach die Website aus der Liste „Website-Ausschlüsse“, um den Ausschluss zurückzunehmen. Um eine Website aus der Ausschlussliste zu entfernen, klicken Sie auf „X“.

Nachdem Sie mehrere Websites hinzugefügt haben, können Sie:

- die Liste in auf- oder absteigender Reihenfolge nach Website sortieren. Klicken Sie dazu auf die Spaltenüberschrift der Website.
- die Liste durchsuchen. Geben Sie dazu einen Teil der Internetadresse in das Suchfeld ein. Die Liste wird während Sie tippen gefiltert.

Aufforderungen zum Trainieren von Anmeldeformularen deaktivieren

Sie können die vorhandenen trainierten Anmeldeinformationen beibehalten und gleichzeitig die Aufforderungen zum Trainieren neuer Anmeldeformulare deaktivieren.

So deaktivieren Sie Eingabeaufforderungen für neue Anmeldungen:

1 Öffnen Sie die DDP Console.
2 Klicken Sie auf die Schaltfläche **Password Manager**.
3 Klicken Sie auf die Registerkarte **Einstellungen**.
4 Deaktivieren Sie das Kontrollkästchen **Aufforderung zum Hinzufügen einer Anmeldung bei Anzeige des Anmeldebildschirms**.

Sichern und Wiederherstellen von Anmeldeinformationen für Kennwort-Manager

Mit dem Kennwort-Manager können Sie die Anmeldedaten, die vom Kennwort-Manager verwaltet werden, auf sichere Art sichern. Diese Daten können dann auf jedem mit Password-Manager geschützten Computer wiederhergestellt werden.

ANMERKUNG:
Die gesicherten Password-Manager-Daten enthalten keine Anmeldeinformationen für das Betriebssystem oder die PBA (Preboot Authenticication) und keine anmeldungsspezifischen Informationen wie Fingerabdrücke.

Sichern von Anmeldeinformationen

Zur Sicherung der Anmeldeinformationen gehen Sie wie folgt vor:

1 Klicken Sie auf die Registerkarte **Sichern von Anmeldeinformationen**, um den Sicherungsvorgang einzurichten.
2 Klicken Sie auf **Durchsuchen**, um zum gewünschten Sicherungsverzeichnis zu navigieren.
Wenn Sie versuchen, die Daten auf ein lokales Laufwerk zu sichern, wird eine Empfehlung angezeigt, die Daten auf eine tragbares Speichermedium oder ein Netzwerklaufwerk zu sichern.
3 Geben Sie das Passwort ein und bestätigen Sie es. Dieses Passwort muss verwendet werden, falls diese gesicherten Anmeldeinformationen später wiederhergestellt werden müssen.
4 Klicken Sie auf **Sichern**.
5 Geben Sie Ihr Windows-Passwort ein.
6 Klicken Sie im Dialogfeld „Erfolgreich“ auf **OK**.

ANMERKUNG:

Um ein Protokoll des ausgeführten Sicherungsvorgangs in Form einer Textdatei anzuzeigen, klicken Sie auf das ⚙ und wählen Sie **Protokolle** aus.

Wiederherstellen von Anmeldeinformationen

Für die Wiederherstellung der Anmeldeinformationen muss das Sicherungsverzeichnis zugänglich sein.

Um Ihre Anmeldeinformationen wiederherzustellen, gehen Sie wie folgt vor:

1 Klicken Sie auf die Registerkarte **Wiederherstellen von Anmeldeinformationen**
2 Klicken Sie auf **Durchsuchen**, um zur Sicherungsdatei zu navigieren und geben Sie das Kennwort für die Datei ein.
3 Klicken Sie auf **Wiederherstellen**.

WARNUNG:

Durch das Wiederherstellen von Password-Manager-Daten werden vorhandene Daten überschrieben. Anmeldeinformationen und andere Daten, die nach der Datensicherung hinzugefügt wurden, gehen verloren.

4 Klicken Sie auf **Weiter**.

ANMERKUNG:

Zur Anzeige eines Textprotokolls zur Wiederherstellungsoperation, die auf diesem Computer ausgeführt wurde, klicken Sie auf das Symbol ⚙ in der Titelleiste und wählen Sie **Protokoll** aus.

Glossar

Anmeldeinformationen – Über Anmeldeinformationen, wie beispielsweise einen Fingerabdruck oder das Windows-Passwort wird die Identität einer Person nachgewiesen.

Einmalpasswort (OTP) – Ein Einmalpasswort ist ein Passwort mit begrenzter Gültigkeit, das nur einmal verwendet werden kann. Für die OTP-Funktion muss ein TPM vorhanden, aktiviert und zugewiesen sein. Für die Aktivierung der OTP-Funktion muss ein Mobilgerät mit dem Computer über die Security Console und die Security Tools Mobile-App gekoppelt werden. Die Security Tools Mobile-App generiert das Passwort auf dem Mobilgerät, mit dem die Anmeldung auf dem Computer über den Windows-Anmeldebildschirm erfolgt. Je nach Richtlinie kann die OTP-Funktion verwendet werden, um den Zugriff auf den Computer wiederherzustellen, falls das Passwort abgelaufen ist oder vergessen wurde, vorausgesetzt, das OTP wurde nicht bereits für die Anmeldung am Computer verwendet. Die OTP-Funktion kann zur Authentifizierung oder zur Wiederherstellung verwendet werden, aber nicht für beides. OTP ist sicherer als einige andere Authentifizierungsmethoden, weil das generierte Passwort nur einmal verwendet werden kann und nach kurzer Zeit abläuft.

Preboot-Authentifizierung (PBA) – Die Preboot-Authentifizierung dient als Erweiterung des BIOS oder der Systemstart-Firmware und schafft eine sichere, manipulationsgeschützte Umgebung außerhalb des Betriebssystems als vertrauenswürdige Authentifizierungsebene. Die PBA unterbindet den Zugriff auf die Festplatte und somit auch auf das Betriebssystem, bis der Benutzer die richtigen Anmeldeinformationen eingibt.

Geschützt – Bei selbstverschlüsselnden SED-Laufwerken ist der Computer geschützt, wenn das SED aktiviert wurde und die PBA (Pre-Boot-Authentifizierung) eingesetzt wird.

Selbstverschlüsselnde Laufwerke (SEDs) - Eine Festplatte mit einem eingebauten Verschlüsselungsmechanismus, der automatisch alle Daten verschlüsselt, die auf dem Medium gespeichert werden und alle Daten entschlüsselt, die das Medium verlassen. Dieser Typ der Verschlüsselung ist für den Benutzer völlig transparent.

Single Sign-on (SSO): Die einstufige Anmeldung vereinfacht den Anmeldevorgang, wenn die mehrstufige Authentifizierung sowohl vor dem Neustart als auch bei der Windows-Anmeldung aktiviert ist. Wenn aktiviert, ist eine Authentifizierung nur vor dem Neustart erforderlich, und Benutzer werden automatisch bei Windows angemeldet. Wenn nicht aktiviert, ist die Authentifizierung möglicherweise mehrfach erforderlich.

Trusted Platform Module (TPM) – Das TPM ist ein Sicherheits-Chip mit drei Hauptfunktionen: sicherer Speicher, Messung und Bestätigung. Beim Encryption-Client wird das TPM für den sicheren Speicher genutzt. Das TPM kann auch verschlüsselte Container für das Software-Vault bereitstellen. Das TPM ist auch für die Verwendung der Einmalpasswort-Funktion erforderlich.