

Dell Data Protection

# Konsolen-Benutzerhandbuch

Advanced Threat Protection

Verschlüsselungsstatus

Registrierung der Authentifizierung

Password Manager

v1.1



---

© 2016 Dell Inc.

Eingetragene Marken und in der Dokumentensammlung Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools, und Dell Data Protection | Cloud Edition verwendete Marken: Dell™ und das Dell-Logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® und KACE™ sind Marken von Dell Inc. Cylance® und das Cylance-Logo sind eingetragene Marken von Cylance, Inc. in den USA und anderen Ländern. McAfee® und das McAfee-Logo sind Marken oder eingetragene Marken von McAfee, Inc. in den USA und anderen Ländern. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® und Xeon® sind eingetragene Marken von Intel Corporation in den USA und anderen Ländern. Adobe®, Acrobat® und Flash® sind eingetragene Marken von Adobe Systems Incorporated. Authen Tec® und Eikon® sind eingetragene Marken von Authen Tec. AMD® ist eine eingetragene Marke von Advanced Micro Devices, Inc. Microsoft®, Windows® und 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® und Visual C++® sind entweder Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern. VMware® ist eine eingetragene Marke oder Marke von VMware, Inc. in den USA oder anderen Ländern. Box® ist eine eingetragene Marke von Box. DropboxSM ist eine Dienstmarke von Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® und Google™ Play sind entweder Marken oder eingetragene Marken von Google Inc. in den USA und anderen Ländern. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® und Siri® sind entweder Dienstmarken, Marken oder eingetragene Marken von Apple, Inc. in den USA und/oder anderen Ländern. GO ID®, RSA® und SecurID® sind eingetragene Marken von EMC Corporation. EnCase™ und Guidance Software® sind entweder Marken oder eingetragene Marken von Guidance Software. Entrust® ist eine eingetragene Marke von Entrust®, Inc. in den USA und anderen Ländern. InstallShield® ist eine eingetragene Marke von Flexera Software in den USA, China, der Europäischen Gemeinschaft, Hongkong, Japan, Taiwan und dem Vereinigten Königreich. Micron® und RealSSD® sind eingetragene Marken von Micron Technology, Inc. in den USA und anderen Ländern. Mozilla® Firefox® ist eine eingetragene Marke von Mozilla Foundation in den USA und/oder anderen Ländern. iOS® ist eine Marke oder eingetragene Marke von Cisco Systems, Inc. in den USA und gewissen anderen Ländern und wird unter Lizenz verwendet. Oracle® und Java® sind eingetragene Marken von Oracle und/oder ihrer Tochtergesellschaften. Andere Namen können Marken ihrer jeweiligen Inhaber sein. SAMSUNG™ ist eine Marke von SAMSUNG in den USA oder anderen Ländern. Seagate® ist eine eingetragene Marke von Seagate Technology LLC in den USA und/oder anderen Ländern. Travelstar® ist eine eingetragene Marke von HGST, Inc. in den USA und anderen Ländern. UNIX® ist eine eingetragene Marke von The Open Group. VALIDITY™ ist eine Marke von Validity Sensors, Inc. in den USA und anderen Ländern. VeriSign® und weitere zugehörige Marken sind die Marken oder eingetragenen Marken von VeriSign, Inc. oder seinen angegliederten Unternehmen oder Tochtergesellschaften in den USA und anderen Ländern und wird durch Symantec Corporation in Lizenz verwendet. KVM on IP® ist eine eingetragene Marke von Video Products. Yahoo!® ist eine eingetragene Marke von Yahoo! Inc.

Dieses Produkt verwendet Teile des Programms 7-Zip. Der Quellcode ist unter [www.7-zip.org](http://www.7-zip.org) verfügbar. Die Lizenzierung erfolgt gemäß der GNU LGPL-Lizenz und den unRAR-Beschränkungen ([www.7-zip.org/license.txt](http://www.7-zip.org/license.txt)).

2016-07

Geschützt durch ein oder mehrere US-Patente, darunter folgende: Nummer 7665125, Nummer 7437752 und Nummer 7665118.

Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden.

# Inhalt

1	Einleitung	5
2	DDP-Konsole	7
3	Verschlüsselungsstatus	9
4	Advanced Threat Protection	11
5	Eintragungen	13
	<b>Anmeldeinformationen erstmals eintragen</b>	13
	<b>Hinzufügen, Ändern oder Anzeigen von Registrierungen</b>	13
	<b>Passwort</b>	14
	<b>Wiederherstellungsfragen</b>	14
	<b>Fingerabdrücke</b>	15
	<b>Mobilgerät</b>	15
	Security Tools Mobile einrichten	16
	Mobilgerät und Computer koppeln	16
	Weiteres Mobilgerät eintragen	17
	Computer und Mobilgerät entkoppeln	17
	<b>Mit Einmalpasswort anmelden</b>	18
	<b>Schritte für die Security Tools   Mobile-Verwaltung</b>	18
	PIN für die Security Tools   Mobile-App zurücksetzen	18
	Security Tools   Mobile-App deinstallieren	18
	<b>Smart Cards</b>	19
6	Password-Manager	21
	<b>Erste Schritte mit Password-Manager</b>	21
	<b>Anmeldeinformationen verwalten</b>	22
	Hinzufügen einer Kategorie	22

Hinzufügen von Anmeldeinformationen. . . . .	22
<b>Anmeldeinformationen importieren . . . . .</b>	<b>23</b>
<b>Symbol-Kontextmenü. . . . .</b>	<b>23</b>
<b>Anmeldung bei Anmeldeseiten mit abgeschlossenem Training . . . . .</b>	<b>24</b>
<b>Unterstützung für Domänen . . . . .</b>	<b>25</b>
<b>Windows-Anmeldeinformationen eintragen . . . . .</b>	<b>25</b>
<b>Websites ausschließen . . . . .</b>	<b>25</b>
<b>Aufforderungen zum Trainieren von Anmeldeformularen deaktivieren. . . . .</b>	<b>26</b>
<b>Sichern und Wiederherstellen von Anmeldeinformationen für Kennwort-Manager. . . . .</b>	<b>26</b>
Anmeldeinformationen sichern . . . . .	26
Wiederherstellen von Anmeldeinformationen . . . . .	27
 Glossar . . . . .	 29

# Einleitung

Dell Data Protection | Endpoint Security Suite Enterprise bietet einfache und intuitive Tools zur Steigerung der Sicherheit Ihres Computers.

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

- Registrierung von Anmeldeinformationen mit Endpoint Security Suite Enterprise.
- Nutzen Sie die 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 Programmdateien
- Einfache und leichte Änderung Ihres Windows-Passworts
- Festlegen persönlicher Einstellungen
- Anzeigen des Verschlüsselungsstatus (auf Computern mit [selbstverschlüsselnden Laufwerken](#))
- Anzeigen des Status der Advanced Threat Protection

Die folgenden Funktionen sind über die DDP Console auf dem Betriebssystem eines Servers verfügbar:

- Anzeigen des Verschlüsselungsstatus (auf Computern mit selbstverschlüsselnden Laufwerken)
- Anzeigen des Status der Advanced Threat Protection

## DDP Console

Die DDP Console ist die Schnittstelle, durch die Sie Ihre Anmeldeinformationen registrieren und verwalten können, und die Selbst-Wiederherstellungsfragen konfigurieren können.

Sie haben Zugriff auf die folgenden Anwendungen:

- Das Verschlüsselungstool ermöglicht Ihnen, den Verschlüsselungsstatus der Computerlaufwerke anzuzeigen.
- 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 regelmäßig überprüfen, ob auf [dell.com/support](http://dell.com/support) aktualisierte Dokumentationen zur Verfügung stehen.

## Kontaktaufnahme mit dem Dell ProSupport

Bevor Sie den Dell ProSupport um Hilfe bitten, helfen Sie uns bitte dabei, den für Sie richtigen technischen Experten zu finden, indem Sie Ihre [Service-Tag-Nummer](#) zur Hand haben, wenn Sie anrufen.

Unsere ProSupport-Mitarbeiter für telefonischen Support rund um die Uhr für Ihr Dell Data Protection-Produkt erreichen Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

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

## DDP-Konsole

Die DDP Console bietet allen Benutzern des Computers Zugriff auf Sicherheitsanwendungen und ermöglicht das Anzeigen und Verwalten des Verschlüsselungsstatus der Laufwerke und Partitionen des Computers und – je nachdem, welche Richtlinie vom Administrator eingerichtet wurde – die Verwaltung ihrer Anmeldeinformationen für Websites, Programme und Netzwerkressourcen, sowie die einfache Registrierung von Anmeldeinformationen für die Authentifizierung.

Doppelklicken Sie zum Öffnen der DDP-Konsole auf dem *Desktop* auf das Symbol **DDP-Konsole**.

Beim Start der DDP Console zeigt die Startseite die Endpoint Security Suite Enterprise -Anwendungen an:

- [Advanced Threat Protection](#)
- [Verschlüsselungsstatus](#)
- [Eintragungen](#)
- [Password-Manager](#)

Wählen Sie für die Ersteinrichtung der Anmeldeinformationen den Link **Erste Schritte** auf der Kachel Registrierungen aus. Ein Assistent leitet Sie durch den kurzen Registrierungsvorgang. Weitere Informationen finden Sie unter [Anmeldeinformationen erstmals eintragen](#).

## 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.



Klicken Sie zum Öffnen der Hilfe 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: <ul style="list-style-type: none"><li>• Produktversion und Datumsinformationen</li><li>• ob die DDP-Konsole auf diesem Computer durch einen Unternehmens- oder einen lokalen Administrator verwaltet wird</li><li>• Versionsnummern für Betriebssystem, BIOS, Hauptplatine und <a href="#">Trusted Platform Module (TPM)</a>.</li></ul>
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.
Richtlinien	Zeigt eine Hierarchie der Richtlinien an, die auf diesem Computer gelten.
Services	Zeigt Details zu den ausgeführten Diensten an.
Unterstützung	Stellt eine Verbindung zur Dell ProSupport-Website her.
Protokolle	Zeigt eine detaillierte Liste der protokollierten Ereignisse für Fehlerbehebungszwecke an.

## 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 *Ungeschützt* angezeigt. Ein Laufwerk oder eine Partition, das bzw. die verschlüsselt ist, wird mit dem Status *Geschützt* angezeigt.

Um den Verschlüsselungsstatus zu aktualisieren, klicken Sie mit der rechten Maustaste auf den Datenträger, das Laufwerk oder die Partition, und wählen Sie **Aktualisieren** aus.



## Advanced Threat Protection

Advanced Threat Protection schützt Ihren Computer gegen Malware, indem alle Prozesse, die versuchen, auf Ihrem Computer oder innerhalb von Speicherplatz ausgeführt zu werden, überwacht werden und solche, die als anormal oder unsicher angesehen werden, gekennzeichnet werden.

Advanced Threat Protection wird standardmäßig zusammen mit Endpoint Security Suite Enterprise installiert.

Wählen Sie zur Anzeige der aus der erweiterten Überwachung und Analyse hervorgehenden Statistiken Ihres Computers die Kachel „Advanced Threat Protection“ aus.

### Advanced Threat Protection-Dashboard

Die Advanced Threat Protection Status-Seite zeigt die folgenden Informationen über den Computer an.

#### Schutzstatus

Eine grüne Markierung erscheint, wenn „Advanced Threat Protection“ aktiviert ist und keine Bedrohungen identifiziert wurden oder die identifizierten Bedrohungen unter Quarantäne gestellt, ausgeschlossen oder gelöscht wurden.

Wenn die „Advanced Threat Protection“-Funktion deaktiviert ist, oder Bedrohungen identifiziert wurden und angegangen werden müssen, wird ein X in einem roten Kreis angezeigt.

**Advanced Threat Protection** – gibt an, ob die „Advanced Threat Protection“-Funktion aktiviert ist.

**Speicherschutz** – gibt an, ob das „Speicherschutz“-Modul aktiviert ist.

#### Dateisystem

**Unsichere Dateien** – Die Anzahl der Bedrohungen, die als Malware ähnelnde Dateien identifiziert wurden.

**Unter Quarantäne gestellte Bedrohungen** – Gibt die Anzahl von unsicheren Dateien an, die unter Quarantäne gestellt wurden.

#### Speicherschutz

**Speicherverletzungen** – Gibt die Anzahl identifizierter Speicherverletzungen an. Diese Zahl schließt Speicherverletzungen in Form von Exploitation, Process Injection und Escalation ein.

**Blockierte Speicherverletzungen** – Gibt die Anzahl von Speicherverletzungen an, die blockiert wurden.

Die Version des „Advanced Threat Protection“-Agenten, das Installationsdatum und das Datum der letzten Aktualisierung erscheinen unten auf der Seite.



## Eintragungen

Über das Eintragungswerkzeug und auf Basis der durch den Administrator definierten Richtlinie können Sie sich eintragen, die Eintragung ändern oder den Status der Eintragung 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.

### Anmeldeinformationen erstmals eintragen

Gehen Sie wie folgt vor, um Anmeldeinformationen erstmals einzutragen:

- 1 Klicken Sie auf der Kachel **Erste Schritte** der DDP-Konsolen-Startseite auf den Link „Eintragungen“.
- 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-Passwort zu ändern, geben Sie auf der Seite „Passwort“ ein neues Passwort ein, bestätigen es und klicken dann auf **Weiter**.

Wenn Sie die Passwortänderung überspringen möchten, 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** oder **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 zum Eintragen oder Ändern 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 **Eintragen**.

- Um eine bereits eingetragene Anmeldeinformation zu löschen, klicken Sie auf **Löschen**.
- Wenn die Richtlinie nicht zulässt, dass Sie ihre eigenen Anmeldeinformationen registrieren oder ändern, sind die Links **Registrieren** und **Löschen** auf der Seite „Status“ deaktiviert.
- Um eine vorhandene Registrierung zu ändern, klicken Sie auf die entsprechende Registerkarte im linken Bereich.  
Wenn eine Richtlinie die Eintragung oder Änderung von [Anmeldeinformationen](#) nicht zulässt, wird auf der Eintragungsseite der Anmeldeinformationen die Meldung „Die Richtlinie lässt das Ändern der Anmeldeinformationen nicht zu.“ angezeigt.

## Passwort

So ändern Sie Ihr Windows-Passwort:

- 1 Klicken Sie auf die Registerkarte **Passwort**.
- 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 Eintragsdialog auf **OK**.

**ANMERKUNG:** Sie sollten Ihr Windows-Passwort nur in der DDP Console und nicht in Windows ändern. Wird das Windows-Kennwort außerhalb von DDP Console geändert, tritt eine Kennwort-Nichtübereinstimmung auf, die eine Wiederherstellung erforderlich macht.

## 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 **Eintragen**.

**ANMERKUNG:** Klicken Sie auf **Zurücksetzen**, um die Auswahl auf dieser Seite zurückzusetzen und von vorne 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 **Neu eintragen**.

# 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 schließlich auf **Speichern**.

# Mobilgerät

Über die Mobilgeräteregistrierung wird die [One-time Password \(OTP\)](#)-Funktion bereitgestellt. 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.

**Auf der DDP-Konsole:**

- 1 Klicken Sie auf der Eintragungssseite der DDP-Konsole auf die Registerkarte **Mobilgerät**.
- 2 Klicken Sie oben rechts auf **Eintragen**.  
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 die Option **Einen Computer eintragen** 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** – Es wird ein QR-Code angezeigt.

oder

**Manuelle Eingabe** – Es wird ein 24-stelliger Koppelungscode angezeigt.
- 2 Gehen Sie auf dem Mobilgerät folgendermaßen vor:
  - a Tippen Sie auf **Geräte koppeln**.
  - b Wählen Sie die gleiche Kopplungsoption aus (**QR-Code scannen** oder **Manuelle Eingabe**), die Sie auf dem Computer ausgewählt haben.
  - c Wählen Sie eine der folgenden Optionen aus:
    - Um die Option **QR-Code** zu wählen, platzieren Sie das Mobilgerät so vor dem Computerbildschirm, dass es den QR-Code scannen kann.

Notieren Sie den numerischen Verifizierungscode, der auf dem Mobilgerät angezeigt wird. Tippen Sie anschließend auf **Weiter**.

**ANMERKUNG:** Wenn die Leiste *Probleme beim Scannen?* angezeigt wird, versuchen Sie es noch einmal, oder wählen Sie alternativ die Option **Manuelle Eingabe** aus.

  - Um die Option **Manuelle Eingabe** zu wählen, geben Sie den 24-stelligen Kopplungscode des Computers ein, und tippen Sie dann auf **Abgeschlossen**.

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 **Übernehmen**.  
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 **Abgeschlossen**.
  - c** Tippen Sie auf **Fertig stellen**.

### Weiteres Mobilgerät eintragen

Durch Eintragen eines neuen Geräts wird das vorherige Gerät 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:

- Öffnen Sie die DDP Console. Klicken Sie auf der Seite „Eintragungstatus“ neben den Anmeldeinformationen für das Mobilgerät auf **Löschen**.
- Gehen Sie auf dem Mobilgerät folgendermaßen vor:
  - 1** Öffnen Sie die Security Tools | Mobile-App.
  - 2** Tippen Sie oben links auf die Mentileiste, um die Schublade zu öffnen.
  - 3** Tippen Sie auf **Computer entfernen**.
  - 4** Wählen Sie den zu entkoppelnden Computer aus.
  - 5** Wählen Sie **Entfernen** (Android) aus, oder tippen Sie auf **Fertig** (iOS).  
Daraufhin wird eine Bestätigungsmeldung angezeigt.
  - 6** Wählen Sie **Alle entfernen** aus, um alle eingetragenen 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** aus, um den eingetragenen Computer und die PIN zu entfernen. 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 die Eintragung des Computers aufrecht zu erhalten.

## Mit Einmalpasswort anmelden

**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.

Soweit von der Richtlinie unterstützt und falls das OTP-Symbol  auf Ihrem Anmeldebildschirm angezeigt wird, können Sie sich über 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 Enterprise 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 *Karte registrieren* angezeigt. Wählen Sie die Option **Karte registrieren** aus.
- 4 Klicken Sie im Eintragsdialog auf **OK**.

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



## 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 Password-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:

- Password-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 Password-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 den Password-Manager unmittelbar nach der Installation von Endpoint Security Suite Enterprise verwenden. Wenn Sie Anmeldeinformationen auf einer Anmeldeseite eingeben, erkennt der Kennwort-Manager das Anmeldeformular und gibt Ihnen die Möglichkeit, Ihre Anmeldeinformationen zu speichern.

Sie haben drei Optionen:

- Klicken Sie auf **Anmeldeinformationen speichern**, um Ihre Anmeldedaten bei Password-Manager zu speichern.
- Wenn Sie *nicht* möchten, dass Ihre Anmeldeinformationen gespeichert werden, werden Sie bei jeder Anmeldung bei der Website oder dem Programm erneut gefragt, ob Sie die Anmeldeinformationen speichern möchten. Wenn Sie nicht erneut gefragt werden möchten, wählen Sie **Niemals für diese Website**. In der Liste der ausgeschlossenen Websites wird ein Eintrag erstellt. Weitere Informationen finden Sie unter [Websites ausschließen](#).
- 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. Wenn Sie mit einem neuen Benutzernamen die Option **Anmeldeinformationen speichern** auswählen, wird ein neuer Satz mit Anmeldeinformationen gespeichert. Wenn Sie mit dem zuvor gespeicherten Benutzernamen und dem neuen Kennwort die Option **Anmeldeinformationen speichern** auswählen, werden die ursprünglichen Anmeldeinformationen durch das neue Kennwort aktualisiert.

## Anmeldeinformationen 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-Konsolen-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:

- + **Hinzufügen von Anmeldeinformationen** – Mit dieser Option können Sie einen neuen Satz mit Anmeldeinformationen hinzufügen. Je nach Richtlinie werden Sie möglicherweise aufgefordert, Anmeldeinformationen einzugeben, die in Endpoint Security Suite Enterprise gespeichert sind, um eine Anmeldung hinzuzufügen.
- + **Hinzufügen einer Kategorie** – Mit dieser Option können Sie eine neue Kategorie (z. B. E-Mail, Speicher, News, Unternehmensressourcen, Soziale Medien) hinzufügen und diese zum Sortieren und Filtern verwenden.

**Sortieren:** Sortieren Sie die 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 *Ansicht* aus, um alle Anmeldungen auszublenden, die nicht der ausgewählten Kategorie entsprechen. 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.

### Hinzufügen einer Kategorie

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.

Klicken Sie zum Hinzufügen einer Kategorie auf der Seite „Logon-Manager“ auf **Kategorie hinzufügen**, geben Sie einen Kategorienamen ein, und klicken Sie dann auf **Speichern**.

### Hinzufügen von Anmeldeinformationen

- 1 Klicken Sie auf der Seite „Logon-Manager“ auf **Anmeldeinformationen 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 Anmeldung an der Website oder in dem Programm aus, die Sie speichern möchten. Wenn Sie noch keine Kategorien hinzugefügt haben, ist diese Liste leer.

- **Kontoname** – Lassen Sie dieses Feld unverändert, um den vorausgefüllten Namen zu übernehmen, oder geben Sie den Namen der Website oder des Programms ein.
  - **Nicht erkannter Titel** – Diese Felder werden vom Kennwort-Manager als die Felder auf der Anmeldeseite 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 die Feldnamen zu bearbeiten oder Felder zu entfernen.
  - 6 Klicken Sie im Dialogfeld „Weitere Felder“ auf **Nicht erkannter Titel**, und geben Sie den korrekten 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** aus.
- 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** aus.
- 2 Wählen Sie den Browser aus, von dem der Import erfolgen soll, und klicken Sie auf **Suchen**.
- 3 Geben Sie bei Aufforderung das Passwort für den ausgewählten Browser ein.

**ANMERKUNG:** Falls durch den Importvorgang keine Passwörter importiert werden, überprüfen Sie, ob im Browser importierfähige Daten gespeichert sind. 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.

Wenn das  nicht vorhanden ist, 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:

<i>Zu Password-Manager hinzufügen: Symboleinstellungen</i>	Damit wird das Dialogfeld „Anmeldeinformationen hinzufügen“ geöffnet. Der Endbenutzer kann die Anzeige des Password-Manager-Symbols auf den lernfähigen Anmeldeseiten konfigurieren.
<i>Password-Manager öffnen:</i>	Damit wird das Tool <i>Password-Manager-Verwaltung</i> mit der Seite „Logon-Manager“ aufgerufen.
<i>Hilfe:</i>	Ruft die Online-Hilfe auf.

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

<i>Anmeldeinformationen ausfüllen:</i>	Je nachdem, welche Auswahl Sie beim Trainieren des Anmeldeformulars getroffen haben, erfolgt die Anmeldung entweder automatisch oder die Felder für Benutzername und Passwort werden ausgefüllt, damit Sie die Anmeldeinformationen übermitteln können.
<i>Anmeldeinformationen bearbeiten:</i>	Öffnet das Dialogfeld „Anmeldeinformationen bearbeiten“.
<i>Anmeldeinformationen hinzufügen:</i>	Öffnet das Dialogfeld „Anmeldeinformationen hinzufügen“.
<i>Password-Manager öffnen:</i>	Öffnet die Seite „Logon-Manager“.
<i>Hilfe:</i>	Ruft die Online-Hilfe auf.

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:

- Mozilla Firefox: Menüsymbol > Einstellungen > Sicherheit > Kontrollkästchen **Kennwörter für Seiten speichern** deaktivieren
- Internet Explorer: Zahnradsymbol > Internetoptionen > Registerkarte Inhalt > Einstellungen automatisch vervollständigen > Kontrollkästchen bei **Benutzernamen und Passwörter in Formularen** deaktivieren

## 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 den Password-Manager, und wählen Sie die Option **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 > Einstellungen“ ändern.

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 dem zuvor erstellten 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 *Anmeldeinformationen hinzufügen* klicken, wird das Dialogfeld [Hinzufügen von Anmeldeinformationen](#) 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 **Passwortverlauf** 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.
- Kennwörterinnerungen 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 **Auffordern, Anmeldeinformationen auf dem Anmeldebildschirm hinzuzufügen**.

## 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 [Preboot Authentication \(PBA\)](#) und keine anmeldungsspezifischen Informationen wie Fingerabdrücke.

### Anmeldeinformationen sichern

Zur Sicherung der Anmeldeinformationen gehen Sie wie folgt vor:

- 1 Klicken Sie auf die Registerkarte **Anmeldeinformationen sichern**, um den Sicherungsprozess einzurichten.
- 2 Klicken Sie auf **Durchsuchen**, und navigieren Sie zum gewünschten Sicherungsspeicherort.  
Wenn Sie versuchen, die Daten auf ein lokales Laufwerk zu sichern, wird eine Empfehlung angezeigt, die Daten auf ein 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 **Protokoll anzeigen** 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 **Anmeldeinformationen wiederherstellen**.
- 2 Klicken Sie auf **Durchsuchen**, um zur Sicherungsdatei zu navigieren, und geben Sie dann das Passwort 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:** Um ein Protokoll des Wiederherstellungsvorgangs in Form einer Textdatei anzuzeigen, klicken Sie auf das Symbol  in der Titelleiste, und wählen Sie **Protokoll anzeigen** 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. Zur Aktivierung von OTP muss ein Mobilgerät mit dem Computer über die DDP-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.

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

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.

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.

Trusted Platform Module (TPM) – Das TPM ist ein Sicherheits-Chip mit drei Hauptfunktionen: sicherer Speicher, Messung und Bestätigung. Bei DDP|E wird das TPM für den sicheren Speicher genutzt. Das TPM kann darüber hinaus verschlüsselte Container für den DDP|E Software Vault und zum Schutz des DDP|E HCA-Verschlüsselungsschlüssels bereitstellen. Dell empfiehlt, das TPM bereitzustellen. Zur Nutzung von DDP|E HCA, BitLocker Manager und der Einmalpasswort-Funktion ist das TPM ebenfalls erforderlich.







0XXXXXA0X