Dell Data Protection | Security Tools

Installation Guide v1.10.1

Legende

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

WARNUNG: Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schäden mit Todesfolge hin.

WICHTIG, HINWEIS, TIPP, MOBILE oder VIDEO: Ein Informationssymbol weist auf Begleitinformationen hin.

Security Tools Installation Guide
2016 - 09

Rev. A00

Inhaltsverzeichni

1

Einleitung

Dell Data Protection | Security Tools bietet Sicherheit und Schutz der Identität auf Dell-Computern für Administratoren und Benutzer. DDP | Security Tools ist auf allen Dell Latitude-, Optiplex- und Precision-Computern sowie auf ausgewählten Dell XPS Notebooks installiert. Falls Sie DDP | Security Tools *neu installieren* müssen, befolgen Sie bitte die Anweisungen in dieser Anleitung. Zusätzliche Unterstützung finden Sie unter www.dell.com/support > Endpoint Security Solutions.

Übersicht

DDP | Security Tools ist eine umfassende Sicherheitslösung, die die Advanced Authentication und die Preboot-Authentifizierung (PBA) unterstützt sowie die Verwaltung selbstverschlüsselnder Laufwerke ermöglicht.

DDP | Security Tools bietet mehrstufige Unterstützung für Windows-Authentifizierung mit Passwörtern, Fingerabdrucklesern und Smartcards – sowohl für „Kontaktkarten" als auch für „kontaktlose" Karten – sowie Selbsteintragung, einstufige Anmeldung (Single Sign-On [SSO]) und Einmalpasswörter (OTP).

Vor der Bereitstellung an Endbenutzer, können Administratoren die Security Tools-Funktionen mithilfe des DDP | Security Tools-Administratoreinstellungstools konfigurieren, beispielsweise, um die Preboot-Authentifizierung oder Authentifizierungsrichtlinien zuzulassen. Die Standardeinstellung sieht vor, dass Administratoren und Benutzer Security Tools sofort nach der Installation und Aktivierung nutzen können.

DDP Security Console

Die DDP Security Console ist die Security Tools-Benutzeroberfläche, über die Benutzer ihre Anmeldeinformationen eintragen und verwalten sowie (basierend auf den Administrator-Richtlinien) Wiederherstellungsfragen konfigurieren können. Benutzer haben auf folgende Security Tools-Anwendungen Zugriff:

- Das Verschlüsselungstool ermöglicht Benutzern, den Verschlüsselungsstatus der Computerlaufwerke anzuzeigen.
- Mit dem Eintragungstool können Benutzer Anmeldeinformationen einrichten und verwalten, Wiederherstellungsfragen konfigurieren und den Status ihrer Anmeldeinformationseintragung anzeigen. Diese Berechtigungen basieren auf den Richtlinien des Administrators.
- Mit Password-Manager können Benutzer die Anmeldeinformationen für Websites, Windows-Anwendungen und Netzwerkressourcen automatisch ausfüllen und übermitteln lassen. Benutzer können in Password-Manager auch ihre Anmeldeinformationen ändern. Dadurch wird gewährleistet, dass die mit Password-Manager verwalteten Passwörter mit denen der zugeordneten Ressourcen übereinstimmen.

Administratoreinstellungen

Das Administratoreinstellungstool wird zur Konfiguration von Security Tools für alle Benutzer des Computers verwendet, wodurch der Administrator Authentifizierungsrichtlinien festlegen, Benutzer verwalten sowie konfigurieren kann, welche Anmeldeinformationen zur Anmeldung erforderlich sind.

Mit dem Tool für die Administrator-Einstellungen können Administrator die Verschlüsselung und Preboot-Authentifizierung (PBA) aktivieren sowie PBA-Richtlinien konfigurieren und den Text auf dem PBA-Bildschirm anpassen.

Fahren Sie mit Anforderungen fort.

2

Anforderungen

- DDP | Security Tools ist auf allen Dell Latitude-, Optiplex- und Precision-Computern sowie auf ausgewählten Dell XPS Notebooks installiert und erfüllt die folgenden Mindestanforderungen. Wenn DDP | Security Tools erneut installiert werden muss, sollten Sie überprüfen, ob der Computer die Mindestanforderungen noch erfüllt. Weitere Informationen finden Sie unter www.dell.com/support > Endpoint Security Solutions .
- Windows 8.1 sollte bei selbstverschlüsselnden Laufwerken nicht auf Laufwerk 1 installiert werden. Diese Betriebssystemkonfiguration wird nicht unterstützt, weil Windows 8.1 eine Wiederherstellungspartition in Laufwerk 0 erstellt und somit die Authentifizierung vor dem Neustart unterbindet. Installieren Sie Windows 8.1 daher stattdessen entweder auf Laufwerk 0 oder stellen Sie Windows 8.1 als Image auf einem beliebigen Laufwerk wieder her.
- DDP | Security Tools unterstützt keine dynamischen Laufwerke.
- Computer mit selbstverschlüsselnden Laufwerken können nicht mit Hardware Crypto Accelerators verwendet werden. Sie sind nicht kompatibel, was die Bereitstellung der HCA verhindert. Beachten Sie bitte, dass Dell keine Computer mit selbstverschlüsselnden Laufwerken verkauft, die das HCA-Modul unterstützen. Eine solche Konfiguration wäre nur als After-Market-Konfiguration möglich.
- DDP | Security Tools unterstützt keine Multiboot-Konfiguration.
- Leeren Sie vor der Installation eines neuen Betriebssystems auf dem Client das Trusted Platform Module (TPM) im BIOS.
- Ein SED benötigt für die Bereitstellung von Advanced Authentication oder der Verschlüsselung kein TPM.

Drivers

- Supported Opal compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

ⓘ **WICHTIG:**
Due to the nature of RAID and SEDs, SED management does not support RAID. The issue with "RAID=On" with SEDs is that RAID requires access to the disk to read and write RAID-related data at a high sector not available on a locked SED from start and cannot wait to read this data until after the user is logged on. Change the SATA operation in the BIOS from "RAID=On" to "AHCI" to resolve the issue. If the operating system does not have the AHCI controller drivers pre-installed, the operating system will blue screen when switched from "RAID=On" to "AHCI."

Client Prerequisites

- The full version of Microsoft .Net Framework 4.5 (or later) is required for Security Tools. All computers shipped from the Dell factory are pre-installed with the full version of Microsoft .Net Framework 4.5. However, if you are not installing on Dell hardware or are upgrading Security Tools on older Dell hardware, you should verify which version of Microsoft .Net is installed and update the version, prior to installing Security Tools to prevent installation/upgrade failures. To install the full version of Microsoft .Net Framework 4.5, go to https://www.microsoft.com/en-us/download/details.aspx?id=30653

  To verify the version of .Net installed, follow these instructions on the computer targeted for installation: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx
- Drivers and firmware for your authentication hardware must be up-to-date on your computer. To obtain drivers and firmware for Dell computers, go to http://www.dell.com/support/home/us/en/19/Products/?app=drivers and select your computer model. Based on your authentication hardware, download the following:
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver

- O2Micro Smartcard Driver
- Dell ControlVault

  Other hardware vendors may require their own drivers.

The installer installs this component if not already installed on the computer:

Prerequisites

- Microsoft Visual C++ 2012 Update 4 or later Redistributable Package (x86/x64)

Software

Windows Operating Systems

The following table details supported software.

Windows Operating Systems (32- and 64-bit)

- Microsoft Windows 7 SP0-SP1

  - Enterprise

  - Professional

  ANMERKUNG: Legacy Boot mode is supported on Windows 7. UEFI is not supported on Windows 7.

- Microsoft Windows 8

  - Enterprise

  - Pro

  - Windows 8 (Consumer)

  ANMERKUNG: Windows 8 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

- Microsoft Windows 8.1 - 8.1 Update 1

  - Enterprise Edition

  - Pro Edition

  ANMERKUNG: Windows 8.1 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

- Microsoft Windows 10
  - Education Edition
  - Enterprise Edition
  - Pro Edition

ANMERKUNG: Windows 10 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

Mobile Device Operating Systems

The following mobile operating systems are supported with Security Tools One-time Password feature.

Mobile Device Operating Systems
Android Operating Systems • 4.0 - 4.0.4 Ice Cream Sandwich • 4.1 - 4.3.1 Jelly Bean • 4.4 - 4.4.4 KitKat • 5.0 - 5.1.1 Lollipop
iOS Operating Systems • iOS 7.x • iOS 8.x
Windows Phone Operating Systems • Windows Phone 8.1 • Windows 10 Mobile

Hardware

Authentication

The following table details supported authentication hardware.

Authentication
Fingerprint Readers • Validity VFS495 in Secure Mode • Broadcom Control Vault Swipe Reader • UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379 • Authentec Eikon and Eikon To Go USB Readers ⓘ ANMERKUNG: When using an external fingerprint reader, you must download and install the latest drivers required for your specific reader.
Contactless Cards • Contactless Cards using Contactless Card Readers built-in to specified Dell laptops
Smart Cards

Authentication

- PKCS #11 Smart cards using the ActivIdentity client

  ⓘ | ANMERKUNG: The ActivIdentity client is not pre-loaded and must be installed separately.

- Common Access Cards (CAC)

  ⓘ | ANMERKUNG: With multi-cert CACs, at logon, the user selects the correct certificate from a list.

- CSP Cards

- Class B/SIPR Net Cards

The following table details Dell computer models supported with SIPR Net cards.

Dell Computer Models - Class B/SIPR Net Card Support

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Dell Computer Models - UEFI Support

Authentication features are supported with UEFI mode on select Dell computers running Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 with qualified Opal Compliant SEDs. Other computers running Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 support Legacy Boot mode.

The following table details Dell computer models supported with UEFI.

Dell Computer Models - UEFI Support

- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7270
- Latitude E7275
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7470
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 14 Rugged Extreme
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M6800
- Precision M7510
- Precision M7710
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- Optiplex 3240 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Models 5175/5179)
- Venue Pro 11 (Model 7139)

Dell Computer Models - UEFI Support

- Latitude 14 Rugged

ANMERKUNG: Authentication features are supported with UEFI mode on these computers running Windows 8, Windows 8.1, and Windows 10 with qualified Opal Compliant SEDs. Other computers running Windows 7, Windows 8, Windows 8.1, and Windows 10 support Legacy Boot mode.

ANMERKUNG: On a supported UEFI computer, after selecting **Restart** from the main menu, the computer restarts and then displays one of two possible logon screens. The logon screen that appears is determined by differences in computer platform architecture. Some models display the PBA logon screen; other models display the Windows logon screen. Both logon screens are equally secure.

ANMERKUNG:
Ensure that the Enable Legacy Option ROMs setting is disabled in the BIOS.

To disable Legacy Option ROMs:

1 Restart the computer.
2 As it is restarting, press **F12** repeatedly to bring up the UEFI computer's boot settings.
3 Press the down arrow, highlight the **BIOS Settings** option, and press **Enter**.
4 Select **Settings** > **General** > **Advanced Boot Options**.
5 Clear the **Enable Legacy Option ROMs** checkbox and click **Apply**.

Opal Compliant SEDs

For the most up-to-date list of Opal compliant SEDs supported with the SED management, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296720.

International Keyboards

- The following table lists international keyboards supported with Preboot Authentication.

ANMERKUNG: These keyboards are supported ***with UEFI only***.

International Keyboard Support - UEFI

- DE-CH - Swiss German
- DE-FR - Swiss French

Language Support

DDP | Security Tools is Multilingual User Interface (MUI) compliant and supports the following languages.

ANMERKUNG:
PBA localization is not supported in Russian, Traditional Chinese, or Simplified Chinese on UEFI computers..

Language Support

- EN - English
- FR - French
- IT - Italian
- DE - German
- ES - Spanish
- JA - Japanese
- KO - Korean
- ZH-CN - Chinese, Simplified
- ZH-TW - Chinese, Traditional/Taiwan
- PT-BR - Portuguese, Brazilian
- PT-PT - Portuguese, Portugal (Iberian)
- RU - Russian

Authentication Options

The following authentication options require specific hardware: Fingerprints, Smart Cards, Contactless Cards, Class B/SIPR Net Cards, and **authentication on UEFI computers**.

The One-time Password feature requires that a TPM is present, enabled, and owned. For more information, see Clear Ownership and Activate the TPM. OTP is not supported with TPM 2.0.

The following tables show authentication options available with Security Tools, by operating system, when hardware and configuration requirements are met.

Non-UEFI

	PBA					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 7 SP0-SP1	X[1]					X	X	X	X	X
Windows 8	X[1]					X	X	X	X	X
Windows 8.1-Windows 8.1 Update 1	X[1]					X	X	X	X	X
Windows 10	X[1]					X	X	X	X	X

1. Available with a supported Opal SED.

UEFI

	PBA - on supported Dell computers					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 7										
Windows 8	X[2]					X	X	X	X	X

UEFI

	PBA - on supported Dell computers					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 8.1-Windows 8.1 Update 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X

2. Available with a supported OPAL SED on supported UEFI computers.

Interoperabilität

Dell Data Protection | Access deprovisionieren und deinstallieren

Falls DDP|A auf Ihrem Computer installiert ist oder war, müssen Sie **vor** der Installation von Security Tools die mit DDP|A verwaltete Hardware deprovisionieren und dann DDP|A deinstallieren. Wenn DDP|A nicht verwendet wurde, können Sie es einfach deinstallieren und dann den Installationsvorgang fortsetzen.

Mit DDP|A verwaltete Hardware, die deprovisioniert werden muss, umfasst Fingerabdruckleser, Smartcard-Lesegeräte, BIOS-Kennwörter, TPM und das selbstverschlüsselnde Laufwerk.

: Wenn Sie DDP|E-Verschlüsselungsprodukte ausführen, beenden Sie eine Verschlüsselungssuche oder lassen Sie sie pausieren. Wenn Sie Microsoft BitLocker ausführen, setzen Sie die Verschlüsselungsrichtlinie aus. Sobald DDP|A deinstalliert und das Aussetzen der Microsoft BitLocker-Richtlinie beendet wurde, initialisieren Sie das TPM, indem Sie die folgenden Anweisungen unter http://technet.microsoft.com/en-us/library/cc753140.aspx ausführen.

Mit DDP|A verwaltete Hardware deprovisionieren

Starten Sie DDP|A, und klicken Sie auf die Registerkarte **Erweitert**.

Wählen Sie **System zurücksetzen**. Sie müssen dazu die Anmeldeinformationen zur Bestätigung Ihrer Identität angeben. Nach der Bestätigung der Anmeldedaten führt DDP|A die folgenden Maßnahmen aus:

- Alle Anmeldedaten aus Dell ControlVault entfernen (wenn vorhanden)
- Dell ControlVault InhaberPasswort entfernen (wenn vorhanden)
- Alle Fingerabdrücke aus dem integrierten Fingerabdruckleser entfernen (wenn vorhanden)
- Alle BIOS-Kennwörter entfernen (BIOS System, BIOS Admin und HDD)
- Trusted Platform Module löschen
- DDP|A Credential Provider entfernen

Nach der Deprovisionierung des Computers führt DDP|A einen Neustart durch und stellt den standardmäßigen Bereitsteller der Anmeldeinformationen für Windows wieder her.

DDP|A deinstallieren

Nach der Deprovisionierung der Authentifizierungs-Hardware deinstallieren Sie DDP|A.

Starten Sie DDP|A, und setzen Sie das System zurück.

Auf diese Weise werden alle DDP|A-verwalteten Anmeldeinformationen und Kennwörter entfernt, und das Trusted Platform Module (TPM) wird gelöscht.

Klicken Sie zum Starten den Installationsprogramms auf **Deinstallieren**.

Sobald die Deinstallation abgeschlossen ist, klicken Sie auf **Ja**, um den Computer neu zu starten.

: Beim Entfernen von DDP|A wird auch das selbstverschlüsselnde Laufwerk entsperrt und die Authentifizierung vor dem Neustart entfernt.

TPM initialisieren

- Für diesen Vorgang müssen Sie Mitglied der lokalen Administratorgruppe oder dergleichen sein.
- Der Computer muss mit einem kompatiblen BIOS und TPM ausgestattet sein.

Diese Aufgabe ist bei der Verwendung von Einmalpasswort erforderlich.

- Folgen Sie den Anweisungen unter http://technet.microsoft.com/en-us/library/cc753140.aspx.

Zuweisung löschen und TPM aktivieren

Weitere Informationen zum Löschen und Definieren der TMP-Zuweisung finden Sie unter https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Fahren Sie mit Installation und Aktivierung fort.

Installation und Aktivierung

In diesem Abschnitt wird die Installation von DDP | Security Tools auf einem lokalen Computer beschrieben. DDP | Security Tools kann nur von einem Benutzer mit Administratorrechten installiert und aktiviert werden.

ANMERKUNG:
Nehmen Sie während der Installation keine Änderungen am Computer vor, dazu gehört auch das Einsetzen oder Entfernen von externen (USB-)Laufwerken.

Installieren von DDP | Security Tools

Um Security Tools zu installieren:

1 Gehen Sie in den Installationsmedien von DDP | Security Tools zur Installationsdatei. Kopieren Sie sie auf den lokalen Computer.

ANMERKUNG: Sie finden die Installationsmedien unter www.dell.com/support > Endpoint Security Solutions.

2 Starten Sie das Installationsprogramm per Doppelklick.

3 Wählen Sie die gewünschte Sprache aus, und klicken Sie auf **OK**.

4 Klicken Sie auf **Weiter**, wenn der Begrüßungsbildschirm angezeigt wird.

5 Lesen Sie die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.

6 Klicken Sie auf **Weiter**, um Security Tools am standardmäßigen Speicherort von **C:\Program Files\Dell\Dell Data Protection.** zu installieren. **Wählen Sie**

7 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

8 Nach Abschluss der Installation ist ein Neustart erforderlich. Wählen Sie **Ja** zum Neustart und klicken Sie dann auf **Fertigstellen**.

Damit ist die Installation abgeschlossen.

Aktivierung von DDP | Security Tools

Wenn Sie die zum ersten Mal DDP Security Console ausführen und die Administratoreinstellungen auswählen, führt Sie der Aktivierungsassistent durch den Aktivierungsprozess.

Wenn die DDP Security Console noch nicht aktiviert ist, kann ein Endbenutzer sie dennoch ausführen. Wenn ein Endbenutzer die DDP Security Console als Erster verwendet, bevor ein Administrator DDP | Security Console aktiviert und die Einstellungen angepasst hat, werden die Standardeinstellung verwendet.

Um Security Tools zu aktivieren:

1 Als Administrator starten Sie Security Tools über die Desktop-Verknüpfung.

ANMERKUNG: Falls Sie als normaler Benutzer (mit einem standardmäßigen Windows-Konto) angemeldet sind, muss vor dem Start über das Administratoreinstellungstool eine Anpassung der Benutzerkontensteuerung (UAC) erfolgen. Der normale Benutzer meldet sich zunächst mit Administrator-Anmeldeinformationen bei dem Tool an und gibt nach Aufforderung das Administratorpasswort ein (das Passwort, das in den Administratoreinstellungen gespeichert wurde).

2 Klicken Sie auf die Kachel **Administratoreinstellungen**.

3 Auf der Willkommensseite klicken Sie auf **Weiter**.

4 Erstellen Sie das DDP | Security Console-Passwort und klicken Sie dann auf **Weiter**.

Das DDP | Security Console-Administratorpasswort muss vor der Konfiguration der Security Tools erstellt werden. Sie benötigen dieses Passwort jedes Mal, wenn Sie sich beim Administratoreinstellungstool anmelden. Das Passwort muss 8 bis 32 Zeichen lang sein und mindestens einen Buchstaben, eine Ziffer und ein Sonderzeichen enthalten.

5 Geben Sie unter **Speicherort der Sicherungsdatei** den Speicherort der Sicherungsdatei an, und klicken Sie auf **Weiter**. Der Speicherort der Sicherungsdatei muss ein Netzlaufwerk oder ein Wechseldatenträger sein. Die Sicherungsdatei enthält die Schlüssel, die zur Wiederherstellung von Daten auf diesem Computer erforderlich sind. Dell Support muss auf diese Datei zugreifen können, um Sie bei der Wiederherstellung zu unterstützen.

Wiederherstellungsdaten werden automatisch am angegebenen Speicherort gesichert. Falls der Speicherort nicht verfügbar ist (wenn beispielsweise das USB-Laufwerk nicht angeschlossen ist), fordert DDP|Security Tools zur Eingabe eines Speicherorts für die Sicherung der Daten auf. Damit die Verschlüsselung starten kann, ist der Zugriff auf die Wiederherstellungsdaten erforderlich.

6 Klicken Sie auf der Zusammenfassungsseite auf **Übernehmen**.

Die Security Tools-Aktivierung ist abgeschlossen.

Basierend auf den Standardeinstellungen können Administratoren und Benutzer die Funktion von Security Tools sofort nutzen.

Konfigurationsaufgaben für Administratoren

Die Security Tools Standardeinstellung sieht vor, dass Administratoren und Benutzer Security Tools sofort nach der Installation und Aktivierung ohne zusätzliche Konfiguration nutzen können. Benutzer werden automatisch als Security Tools-Benutzer hinzugefügt, wenn sie sich mit ihrem Windows-Passwort beim Computer anmelden. Standardmäßig ist die mehrstufige Windows-Authentifizierung jedoch deaktiviert. Ebenso sind Verschlüsselung und Preboot-Authentifizierung standardmäßig deaktiviert.

Um Security Tools-Funktionen zu konfigurieren, müssen Sie auf dem Computer Administratorrechte besitzen.

Administrator-Passwort und Sicherungsverzeichnis ändern

Nach der Security Tools-Aktivierung können das Administratorpasswort und der Speicherort der Sicherungsdatei bei Bedarf geändert werden.

1 Als Administrator starten Sie Security Tools über die Desktop-Verknüpfung.
2 Klicken Sie auf die Kachel **Administratoreinstellungen**.
3 Geben Sie im Dialogfeld „Authentifizierung" das Administrator-Passwort ein, das bei der Aktivierung eingerichtet wurde, und bestätigen Sie es mit **OK.**
4 Klicken Sie auf die Registerkarte **Administratoreinstellungen**.
5 Wenn Sie das Passwort ändern möchten, geben Sie auf der Administratorpasswort-Seite ein neues Passwort mit 8-32 Zeichen ein, darunter mindestens ein Buchstabe, eine Zahl und ein Sonderzeichen.
6 Geben Sie das Passwort zur Bestätigung ein zweites Mal ein und klicken Sie dann auf **Übernehmen**.
7 Um den Speicherort des Wiederherstellungsschlüssels zu ändern, wählen Sie im linken Fensterbereich **Speicherort der Sicherungsdatei ändern** aus.
8 Wählen Sie einen neuen Speicherort für die Sicherung aus, und klicken Sie dann auf **Übernehmen**.

   Der Speicherort der Sicherungsdatei muss ein Netzlaufwerk oder ein Wechseldatenträger sein. Die Sicherungsdatei enthält die Schlüssel, die zur Wiederherstellung von Daten auf diesem Computer erforderlich sind. Dell ProSupport muss auf diese Datei zugreifen können, um Sie bei der Wiederherstellung zu unterstützen.

   Wiederherstellungsdaten werden automatisch am angegebenen Speicherort gesichert. Falls der Speicherort nicht verfügbar ist (wenn beispielsweise das USB-Laufwerk nicht angeschlossen ist), fordert DDP|Security Tools zur Eingabe eines Speicherorts für die Sicherung der Daten auf. Damit die Verschlüsselung starten kann, ist der Zugriff auf die Wiederherstellungsdaten erforderlich.

Verschlüsselung und Preboot-Authentifizierung konfigurieren

Verschlüsselung- und Preboot-Authentifizierung (PBA) sind verfügbar, wenn Ihr Computer mit einem selbstverschlüsselndem Laufwerk (SED) ausgestattet ist. Beide Funktionen werden über die Registerkarte „Verschlüsselung" konfiguriert, die nur dann sichtbar ist, wenn Ihr Computer mit einem selbstverschlüsselnden Laufwerk (SED) ausgestattet ist. Wenn Sie die Verschlüsselung oder die PBA aktivieren, wird die jeweils andere Funktion ebenfalls aktiviert.

Bevor Sie die Verschlüsselung und PBA zum ersten Mal aktivieren, tragen Sie Wiederherstellungsfragen ein, damit Sie das Passwort wiederherstellen können, falls es verloren geht. Weitere Informationen finden Sie unter Konfigurieren der Anmeldeoptionen.

Verschlüsselung und Preboot-Authentifizierung werden wie folgt aktiviert:

1 Klicken Sie in der DDP Security Console auf die **Administrator-Einstellungen** Kachel.

2 Stellen Sie sicher, dass der Speicherort der Sicherungsdatei auf Ihrem Computer zugänglich ist.

> ANMERKUNG: Ist die Verschlüsselung aktiviert und es erscheint die Meldung „Speicherort nicht gefunden" (wobei sich der Speicherort auf einem USB-Laufwerke befindet), ist entweder Ihr USB-Laufwerk nicht angeschlossen oder mit einem anderen als dem Steckplatz verbunden, den Sie beim Sichern verwendet haben. Wird die Meldung angezeigt, obwohl sich der Speicherort auf einem Netzwerklaufwerk befindet, ist das Netzwerklaufwerk von dem Computer aus nicht zugänglich. Der Speicherort der Sicherungsdatei muss über die Registerkarte **Administratoreinstellungen** geändert werden, indem Sie auf **Speicherort der Sicherungsdatei ändern** klicken und als Speicherort den aktuellen Steckplatz oder ein zugängliches Laufwerk auswählen. Wenige Sekunden nach der Neuzuweisung des Speicherorts kann die Verschlüsselung fortgesetzt werden.

3 Klicken Sie auf die Registerkarte **Verschlüsselung** und dann auf **Verschlüsseln**.

4 Auf der Willkommensseite klicken Sie auf **Weiter**.

5 Ändern oder Bestätigen Sie auf der Seite Vorstart-Richtlinien die folgenden Werte und klicken Sie dann auf **Weiter**.

Versuche mit nicht gespeicherter Benutzeranmeldung	Höchstzahl der Anmeldeversuche durch einen unbekannten Benutzer (damit ist ein Benutzer gemeint, der sich bisher noch nicht beim Computer angemeldet hat [für den noch keine Anmeldedaten gespeichert sind]).
Versuche mit gespeicherter Benutzeranmeldung	Höchstzahl der Anmeldeversuche durch einen bekannten Benutzer.
Versuche beim Beantworten von Wiederherstellungsfragen	Anzahl der Versuche, die ein Benutzer für die Eingabe der richtigen Antwort hat.
Crypto Erase-Passwort aktivieren	Markieren Sie die Option, um sie zu aktivieren.
Crypto Erase-Passwort eingeben	Ein Wort oder Code mit bis zu 100 Zeichen als ausfallsichere Sicherheitsmaßnahme. Durch die Eingabe dieses Wortes oder Codes in das Feld „Benutzername" oder „Kennwort" während der PBA-Authentifizierung werden die Authentifizierungstoken aller Benutzer gelöscht und das SED gesperrt. Danach kann nur ein Administrator eine Entsperrung des Gerätes erzwingen. Lassen Sie dieses Feld leer, wenn Sie für den Notfall kein Crypto Erase-Passwort verfügbar haben wollen.

6 Geben Sie auf der Seite „Vorstart-Anpassungen" den benutzerdefinierten Text ein, der auf dem Preboot-Authentifizierungsbildschirm (PBA) angezeigt werden soll, und klicken Sie dann auf **Weiter**.

PBA-Titel-Text	Dieser Text erscheint oben auf dem PBA-Bildschirm. Wenn Sie dieses Feld leer lassen, wird kein Titel angezeigt. Der Text wird nicht umgebrochen und kann daher bei Eingabe von mehr als 17 Zeichen abgeschnitten werden.
Text für Support-Informationen	Dieser Text wird auf dem Bildschirm mit den Informationen zum PBA-Support angezeigt. Dell empfiehlt, in dieser Meldung anzugeben, wie der Benutzer sich an einen Helpdesk oder den Sicherheitsadministrator wenden kann. Wenn in diesem Feld kein Text eingegeben wird, stehen dem Benutzer keine Kontaktangaben für den Support zur Verfügung. Textumbruch erfolgt auf Wortebene, nicht auf Zeichenebene. Wenn z. B. ein einzelnes Wort mit etwa 50 Zeichen vorliegt, wird es nicht umgebrochen, und es wird keine Bildlaufleiste angezeigt. Der Text wird also abgeschnitten.
Text des Rechtshinweises	Dieser Text wird angezeigt, bevor sich der Benutzer bei dem Gerät anmelden darf. Beispiel: „Durch Klicken auf OK verpflichten Sie sich, die Richtlinie für eine angemessene Nutzung des Computers einzuhalten." Wenn in diesem Feld kein Text eingegeben wird, werden kein

Text und keine OK/Abbrechen-Schaltfläche angezeigt. Textumbruch erfolgt auf Wortebene, nicht auf Zeichenebene. Wenn z. B. ein einzelnes Wort mit etwa 50 Zeichen vorliegt, wird es nicht umgebrochen, und es wird keine Bildlaufleiste angezeigt. Der Text wird also abgeschnitten.

7 Klicken Sie auf der Zusammenfassungsseite auf **Übernehmen**.

8 Klicken Sie auf **Herunterfahren**, wenn Sie dazu aufgefordert werden.

Um mit der Verschlüsselung zu beginnen, muss der Computer vollständig heruntergefahren werden.

9 Starten Sie den Computer dann erneut.

Die Authentifizierung wird jetzt von Security Tools durchgeführt. Benutzer müssen sich auf dem Bildschirm Preboot-Authentifizierung mit ihrem Windows-Passwort anmelden.

Verschlüsselungs- und Preboot-Authentifizierungseinstellungen ändern

Nachdem Sie die Verschlüsselung zum ersten Mal aktiviert und die Preboot-Richtlinie und -Anpassung konfiguriert haben, stehen Ihnen auf der Registerkarte „Verschlüsselung“ folgende Optionen zur Verfügung:

Preboot-Richtlinie oder -Anpassung ändern - Klicken Sie auf die Registerkarte **Verschlüsselung** und dann auf **Ändern**.

Das SED entschlüsseln, beispielsweise zur Deinstallation: Klicken Sie auf **Entschlüsseln**.

Nachdem Sie die Verschlüsselung zum ersten Mal aktiviert und die Preboot-Richtlinie und -Anpassung konfiguriert haben, stehen Ihnen auf der Registerkarte „Preboot-Einstellungen“ folgende Optionen zur Verfügung:

Preboot-Richtlinie oder -Anpassung ändern - Klicken Sie auf die Registerkarte **Preboot-Einstellungen** und wählen Sie **Vorstart-Anpassungen** oder **Vorstart-Anmeldungsrichtlinien** aus.

Anweisungen zur Deinstallation finden Sie unter Deinstallationsvorgänge.

Authentifizierungsoptionen konfigurieren

Mithilfe der Steuerungen der Registerkarte „Authentifizierung“ in den Administratoreinstellungen können Sie Anmeldeoptionen für Benutzer festlegen und die einzelnen Einstellungen anpassen.

ⓘ ANMERKUNG: Die Einmalpasswort-Funktion wird unter den Wiederherstellungsoptionen nicht angezeigt, wenn TPM nicht vorhanden ist bzw. nicht zugewiesen oder aktiviert wurde.

Anmeldeoptionen konfigurieren

Auf der Seite „Anmeldeoptionen“ können Sie Anmeldungsrichtlinien konfigurieren. Standardmäßig sind alle unterstützten Anmeldeinformationen unter „Verfügbare Optionen“ aufgelistet.

Um die Anmeldeoptionen zu konfigurieren:

Wählen Sie im linken Bildschirmbereich unter Authentifizierung **Anmeldeoptionen** aus.

Um eine Rolle auszuwählen, die Sie einrichten möchten, wählen Sie die Rolle in der Liste **Anmeldeoptionen anwenden auf** aus: **Benutzer** oder **Administratoren**. Alle Änderungen, die Sie auf dieser Seite vornehmen, beziehen sich nur auf die von Ihnen ausgewählte Rolle.

Legen Sie die verfügbaren Optionen für die Authentifizierung fest.

Standardmäßig ist jede Authentifizierungsmethode so konfiguriert, dass sie individuell, also nicht in Kombination mit anderen Authentifizierungsmethoden, verwendet wird. Sie können die Standardeinstellungen folgendermaßen ändern:

Um eine Kombination von Authentifizierungsoptionen einzurichten, klicken Sie unter „Verfügbare Optionen“ auf , um die erste Authentifizierungsmethode auszuwählen. Wählen Sie im Dialogfeld „Verfügbare Optionen“ die zweite Authentifizierungsmethode aus, und klicken Sie anschließend auf **OK**.

Sie können beispielsweise als Anmeldeinformationen sowohl einen Fingerabdruck, als auch ein Passwort verlangen. Wählen Sie im Dialogfeld die zweite Authentifizierungsmethode aus, die zusammen mit der Authentifizierung durch Fingerabdruck verwendet werden soll.

Um jede Authentifizierungsmethode einzeln verwenden zu können, lassen Sie im Dialogfeld „Verfügbare Optionen“ die Einstellung für die zweite Authentifizierungsmethode auf **Ohne** eingestellt und klicken Sie dann auf **OK**.

Um eine Anmeldeoption zu entfernen, klicken Sie unter „Verfügbare Optionen“ auf der Seite „Anmeldeoption“ auf das **X**, um das Verfahren zu entfernen.

Um eine neue Kombination an Authentifizierungsmethoden hinzuzufügen, klicken Sie auf **Eine Option hinzufügen**.

Legen Sie Wiederherstellungsoptionen für Benutzer fest, die ihre Zugangsdaten nach der Abmeldung wiederherstellen möchten.

Um Benutzern die Festlegung von Wiederherstellungsfragen zur Wiederherstellung Ihrer Anmeldedaten zu ermöglichen, wählen Sie **Wiederherstellungsfragen** aus.

Entfernen Sie die Markierung, wenn Sie das Einrichten von Wiederherstellungsfragen verhindern möchten.

Um Benutzern die Wiederherstellung ihrer Anmeldedaten über ein mobiles Gerät zu ermöglichen, wählen Sie **Einmalpasswort** aus. Wenn die Option „Einmalpasswort“ (OTP) als das Wiederherstellungsverfahren ausgewählt ist, ist sie als Anmeldeoption auf dem Anmeldebildschirm von Windows nicht verfügbar.

Um die OTP-Funktion zur Anmeldung zu verwenden, deaktivieren Sie diese Methode unter Wiederherstellungsoptionen. Wenn OTP als Wiederherstellungsoption deaktiviert wird, erscheint die OTP-Option auf der Windows-Anmeldeseite, sofern sich mindestens ein Benutzer für OTP eingetragen hat.

: Als Administrator kontrollieren Sie, wie das Einmalpasswort verwendet werden kann – entweder zur Authentifizierung oder zur Wiederherstellung. Die OTP-Funktion kann zur Authentifizierung oder zur Wiederherstellung verwendet werden, aber nicht für beides. Die Konfiguration betrifft entweder alle Benutzer des Computers oder alle Administratoren, basierend auf der Auswahl im Anmeldeoptionen-Feld **Anmeldeoptionen übernehmen für**.

Wird die Einmalpasswort-Option in den Wiederherstellungsoptionen nicht angezeigt wird, wird diese Option auf der Konfiguration Ihres Computers nicht unterstützt. Weitere Informationen finden Sie unter Anforderungen.

Wenn Sie möchten, dass der Benutzer bei Verlust oder Vergessen der Anmeldeinformationen Kontakt mit dem Help Desk aufnimmt, deaktivieren Sie die Kontrollkästchen unter „Wiederherstellungsoptionen“: Wiederherstellungsfragen und Einmalpasswort.

Wählen Sie **Toleranzzeitraum** aus, um einen Zeitraum festzulegen, in dem Benutzer ihre Anmeldeinformationen für die Authentifizierung eintragen können.

Sie können mit der Funktion „Toleranzzeitraum“ ein Datum angeben, ab dem eine konfigurierte Anmeldeoption durchgesetzt wird. Sie können also eine Anmeldeoption vor dem Datum ihrer Durchsetzung konfigurieren und eine Zeitspanne festlegen, in der Benutzer ihre Daten eintragen können. Standardmäßig wird die Richtlinie sofort durchgesetzt.

Um den Zeitpunkt für die Durchsetzung der Anmeldeoption im Dialogfeld „Toleranzzeitraum“ von *Sofort* in ein anderes Datum zu ändern, wählen Sie im Dropdown-Menü die Option **Bestimmtes Datum** aus. Klicken Sie rechts neben dem Datumsfeld auf den Pfeil nach unten, um einen Kalender aufzurufen, in dem Sie das Datum auswählen können. Die Durchsetzung der Richtlinie beginnt in der Regel um 00:01 Uhr am ausgewählten Datum.

Benutzer können bei ihrer nächsten Windows-Anmeldung an die Eintragung der erforderlichen Anmeldeinformationen erinnert werden (Standardeinstellung), oder aber Sie richten regelmäßige Erinnerungen ein. Wählen Sie das Erinnerungsintervall in der Dropdown-Liste *Benutzer erinnern* aus.

:

Wie die Erinnerung dem Benutzer dann angezeigt wird, richtet sich danach, ob der Benutzer beim Auslösen der Erinnerungsmeldung den Windows-Anmeldebildschirm geöffnet hat oder bereits in einer Windows-Sitzung arbeitet. Erinnerungen werden nicht auf Anmeldebildschirmen für die Preboot-Authentifizierung angezeigt.

Funktionsumfang während des Toleranzzeitraums

Während des angegebenen Toleranzzeitraums erhalten Benutzer bei jeder Anmeldung die Benachrichtigung „Zusätzliche Anmeldeinformationen", wenn sie die für die neue Anmeldeoption erforderlichen Anmeldeinformationen noch nicht eingetragen haben. Die Benachrichtigung lautet: *Zusätzliche Anmeldeinformationen für die Registrierung verfügbar.*

Wenn zusätzliche Anmeldeinformationen verfügbar, aber nicht erforderlich sind, wird die Benachrichtigung nach der Änderung der Richtlinie nur ein Mal angezeigt.

Je nach Kontext geschieht Folgendes, wenn ein Benutzer auf die Benachrichtigung klickt:

Falls noch keine Anmeldeinformationen eingetragen sind, wird der Einrichtungsassistent geöffnet. Damit können administrative Benutzer computerspezifische Einstellungen ändern, und Benutzer können die üblichen Anmeldeinformationen eintragen.

Nach der ersten Registrierung von Anmeldeinformationen wird per Klick auf die Benachrichtigung der Einrichtungsassistent der DPP Security Console geöffnet.

Funktionsumfang nach Ablauf des Toleranzzeitraums

Nach Ablauf des Toleranzzeitraums können Benutzer sich nur anmelden, wenn sie die gemäß Anmeldeoption erforderlichen Anmeldeinformationen eingetragen haben. Bei Anmeldeversuchen mit einer Anmeldeinformation oder einer Kombination aus Anmeldeinformationen, die nicht der Anmeldeoption entsprechen, wird oben im Windows-Anmeldebildschirm der Einrichtungsassistent angezeigt.

Wenn der Benutzer die erforderlichen Anmeldeinformationen registriert, wird die Anmeldung bei Windows durchgeführt.

Wenn der Benutzer die erforderlichen Anmeldeinformationen nicht registriert oder den Assistenten abbricht, gelangt er automatisch zurück zum Windows-Anmeldebildschirm.

Klicken Sie zum Speichern der Einstellungen für die ausgewählte Rolle auf **Übernehmen**.

Password-Manager-Authentifizierung konfigurieren

Auf der Seite „Password-Manager" können Sie konfigurieren, wie sich Benutzer bei Password-Manager authentifizieren.

So konfigurieren Sie die Password-Manager-Authentifizierung:

Wählen Sie im linken Fensterbereich, unter Authentifizierung, **Password-Manager** aus.

Um eine Rolle auszuwählen, die Sie einrichten möchten, wählen Sie die Rolle in der Liste **Anmeldeoptionen anwenden auf** aus: **Benutzer** oder **Administratoren**. Alle Änderungen, die Sie auf dieser Seite vornehmen, beziehen sich nur auf die von Ihnen ausgewählte Rolle.

Aktivieren Sie optional das Kontrollkästchen **Keine Authentifizierung erforderlich**, um zuzulassen, dass die ausgewählte Benutzerrolle automatisch bei allen Softwareanwendungen und Internetseiten mit den Password Manager gespeicherten Anmeldeinformationen angemeldet wird.

Legen Sie die verfügbaren Optionen für die Authentifizierung fest.

Standardmäßig ist jede Authentifizierungsmethode so konfiguriert, dass sie individuell, also nicht in Kombination mit anderen Authentifizierungsmethoden, verwendet wird. Sie können die Standardeinstellungen folgendermaßen ändern:

Um eine Kombination von Authentifizierungsoptionen einzurichten, klicken Sie unter „Verfügbare Optionen" auf , um die erste Authentifizierungsmethode auszuwählen. Wählen Sie im Dialogfeld „Verfügbare Optionen" die zweite Authentifizierungsmethode aus, und klicken Sie anschließend auf **OK**.

Sie können beispielsweise als Anmeldeinformationen sowohl einen Fingerabdruck, als auch ein Passwort verlangen. Wählen Sie im Dialogfeld die zweite Authentifizierungsmethode aus, die zusammen mit der Authentifizierung durch Fingerabdruck verwendet werden soll.

Um jede Authentifizierungsmethode einzeln verwenden zu können, lassen Sie im Dialogfeld „Verfügbare Optionen" die Einstellung für die zweite Authentifizierungsmethode auf **Ohne** eingestellt und klicken Sie dann auf **OK**.

Um eine Anmeldeoption zu entfernen, klicken Sie unter „Verfügbare Optionen" auf der Seite „Anmeldeoption" auf das **X**, um das Verfahren zu entfernen.

Um eine neue Kombination an Authentifizierungsmethoden hinzuzufügen, klicken Sie auf **Eine Option hinzufügen**.

Um die Einstellungen für die ausgewählte Rolle zu speichern, klicken Sie auf **Übernehmen.**

 : Klicken Sie auf die Standardeinstellungen-Schaltfläche, um die Standardeinstellungen wiederherzustellen.

Wiederherstellungsfragen konfigurieren

Auf der Seite „Wiederherstellungsfragen" können Sie die Fragen auswählen, die den Benutzern präsentiert werden, wenn diese persönliche Wiederherstellungsfragen festlegen. Wiederherstellungsfragen ermöglichen es den Benutzern, Zugriff auf Ihren Computer zu erhalten, wenn sie ihr Passwort vergessen haben oder das Passwort abgelaufen ist.

Um Wiederherstellungsfragen zu konfigurieren:

Wählen Sie im linken Fensterbereich, unter Authentifizierung, **Wiederherstellungsfragen** aus.

Wählen Sie auf der Seite „Wiederherstellungsfragen" mindestens drei vordefinierte Wiederherstellungsfragen aus.

Optional können Sie bis zu drei eigene Fragen zur Auswahlliste hinzufügen.

Klicken Sie zum Speichern der Wiederherstellungsfragen auf **Anwenden**.

Authentifizierung über Fingerabdrücke konfigurieren

So konfigurieren Sie die Authentifizierung über Fingerabdrücke:

Wählen Sie im linken Fensterbereich unter „Authentifizierung" den Eintrag **Fingerabdrücke** aus.

Legen Sie bei „Eintragungen" die minimale und die maximale Anzahl der Finger fest, die ein Benutzer eintragen kann.

Stellen Sie die Empfindlichkeit des Scanvorgangs für die Fingerabdrücke ein.

Durch eine geringere Empfindlichkeit wird die Abweichungstoleranz und damit die Akzeptanz eines falschen Fingerabdrucks erhöht. Bei der höchsten Einstellung besteht die Gefahr, dass legitime Fingerabdrücke abgelehnt werden. Mit der Empfindlichkeitseinstellung „Mehr" können Sie die Quote einer fälschlichen Akzeptanz auf 1 pro 10.000 Scanvorgänge reduzieren.

Klicken Sie zum Entfernen aller Fingerabdruckscans und Registrierungen von Anmeldeinformation aus dem Speicher des Fingerabdrucklesers auf **Fingerabdruckleser löschen**. Dadurch werden nur die Daten entfernt, die Sie gerade hinzufügen. Zuvor gespeicherte Scans und Eintragungen werden nicht gelöscht.

Um die Einstellungen zu speichern, klicken Sie auf **Übernehmen**.

Einmalpasswort-Authentifizierung konfigurieren

Um die Einmalpasswort-Funktion zu nutzen, generiert der Benutzer ein Einmalpasswort mittels der Dell Data Protection | Security Tools Mobile-App auf seinem Mobilgerät und gibt dieses Passwort dann auf dem Computer ein. Das Passwort kann nur einmal verwendet werden und läuft nach einer bestimmten Gültigkeitsdauer ab.

Um die Sicherheit zusätzlich zu erhöhen, kann der Administrator die Mobilanwendung sichern, indem er die Eingabe eines Passworts konfiguriert.

Auf der Seite „Mobilgeräte“ können Sie Einstellungen zur weiteren Erhöhung der Sicherheit des Mobilgeräts und des Einmalpassworts konfigurieren.

Um die Einmalpasswort-Authentifizierung zu konfigurieren:

Wählen Sie im linken Fensterbereich unter Authentifizierung **Mobilgerät** aus.

Um beim Zugriff auf die Security Tools Mobile-App auf dem Mobilgerät ein Passwort abzufragen, wählen Sie **Password erforderlich** aus.

: Das Aktivieren der Richtlinie *Passwort erforderlich* nach der Anmeldung von mobilen Geräten auf einem Computer führt dazu, dass alle mobilen Geräten abgemeldet werden. Benutzer müssen ihre mobilen Geräte erneut eintragen, nachdem diese Richtlinie aktiviert wurde.

Wenn das Kontrollkästchen **Kennwort erforderlich** aktiviert ist, müssen Benutzer ihre mobilen Geräte für den Zugriff auf die Security Tools Mobile-App entsperren. Ist auf dem mobilen Gerät keine Gerätesperre vorhanden ist, ist die Eingabe eines Passworts erforderlich.

Um die Länge des Einmalpassworts (OTP) auszuwählen, wählen Sie für **Länge des Einmalpassworts** die Anzahl der erforderlichen Passwortzeichen aus.

Um die Anzahl der Versuche auszuwählen, die einem Benutzer zur Verfügung stehen, um das Einmalpasswort korrekt einzugeben, wählen Sie für **Anzahl der Anmeldeversuche** eine Zahl zwischen **5** und **30** aus.

Ist die Maximalzahl erreicht, wird die OTP-Funktion deaktiviert bis der Benutzer sein Mobilgerät erneut registriert hat.

: Dell empfiehlt, zusätzlich zum Einmalpasswort mindestens eine weitere Authentifizierungsmethode zu verwenden.

Smart Card-Eintragung konfigurieren

DDP|Security Tools unterstützt zwei Arten von Smart Cards: Kontakt-Karten und kontaktlose Karten.

Kontaktkarten erfordern einen Smart Card-Leser, in den die Karte eingeschoben wird. Kontaktkarten sind nur mit Domänen-Computern kompatibel. CAC- und SIPRNet-Karten sind Kontaktkarten. Aufgrund der erweiterten Funktionalität dieser Karten muss der Benutzer nach dem Einschieben der Karte ein Zertifikat auswählen.

Kontaktlose Karten werden von Nicht-Domänen-Computern und von Computern mit Domänen-Spezifikationen unterstützt.

Benutzer können als Smart Card pro Benutzerkonto eine Kontaktkarte oder mehrere kontaktlose Karten eintragen.

Smart Cards werden von der Preboot-Authentifizierung nicht unterstützt.

: Wird eine Smart Card von einem Konto entfernt, bei dem mehrere Karten eingetragen wurden, werden alle Karten gleichzeitig ausgetragen.

Um die Smart Card-Eintragung zu konfigurieren:

Wählen Sie auf der Registerkarte „Authentifizierung“ des Tools für die Administratoreinstellungen die Option **Smartcard** aus.

Erweiterte Berechtigungen konfigurieren

Zum Anpassen erweiterter Endbenutzeroptionen klicken Sie auf **Erweitert**. Unter *Erweitert* können Sie Benutzern optional die Möglichkeit geben, Anmeldeinformationen selbst einzutragen. Optional können Sie Benutzern auch die Möglichkeit geben, ihre eingetragenen Anmeldeinformationen zu ändern und die Anmeldung in einen Schritt zu aktivieren.

Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:

Eintragung von Anmeldeinformationen durch Benutzer zulassen – Dieses Kontrollkästchen ist standardmäßig aktiviert. Benutzer können ihre Anmeldeinformationen ohne Eingriff durch einen Administrator eintragen. Wenn Sie die Aktivierung des Kontrollkästchens aufheben, müssen die Anmeldeinformationen durch einen Administrator eingetragen werden.

Änderung eingetragener Anmeldeinformationen durch Benutzer zulassen – Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn diese Option markiert ist, können Benutzer ihre eingetragenen Anmeldeinformationen ohne Eingriff durch einen Administrator ändern oder löschen. Wenn Sie die Markierung des Kontrollkästchens aufheben, müssen die Anmeldeinformationen durch einen Administrator geändert oder gelöscht werden.

: Gehen Sie für das Eintragen von Anmeldeinformationen auf die Seite *Benutzer* des Tools „Administratoreinstellungen", wählen Sie einen Benutzer aus und klicken Sie auf **Eintragen**.

Einstufige Anmeldung zulassen – Die einstufige Anmeldung entspricht dem Single Sign-on (SSO). Das Kontrollkästchen ist standardmäßig aktiviert. Wenn diese Funktion aktiviert ist, müssen Benutzer ihre Anmeldeinformationen nur auf dem Preboot-Authentifizierungs-Bildschirm eingeben. Die Benutzer werden automatisch bei Windows angemeldet. Wenn Sie diese Markierung entfernen, müssen sich Benutzer möglicherweise wiederholt anmelden.

: Diese Option ist nur verfügbar, wenn auch die Einstellung **Benutzern die Eintragung ihrer Anmeldeinformationen erlauben** ausgewählt wurde.

Klicken Sie nach Abschluss auf **Übernehmen**.

Smart Card und biometrische Dienste (optional)

Wenn Sie nicht möchten, dass Security Tools die mit Smartcards und biometrischen Geräten verbundenen Dienste für den Autostart einrichtet, kann die Autostart-Funktion für diese Dienste deaktiviert werden.

Ist diese Funktion deaktiviert, unternimmt Security Tools für folgende drei Dienste keinen Startversuch:

SCardSvr – Verwaltet den Zugang zu den von einem Computer gelesenen Smartcards. Wird dieser Dienst gestoppt, kann der Computer keine Smartcards lesen. Wird dieser Dienst deaktiviert, können alle direkt davon abhängigen Dienste nicht gestartet werden.

SCPolicySvc – Ermöglicht es, das System so zu konfigurieren, dass der Benutzer-Desktop bei Entfernen der Smartcard gesperrt wird.

WbioSrvc – Der Biometrie-Dienst von Windows ermöglicht es Client-Anwendungen, biometrische Daten ohne direkten Zugriff auf Biometrie-Hardware oder -Proben zu erfassen, zu vergleichen, zu ändern und zu speichern. Der Dienst wird in einem bevorzugten SVCHOST-Prozess gehostet.

Das Deaktivieren der Funktion bewirkt auch, dass keine Warnmeldungen in Verbindung zu den nicht ausgeführten Diensten angezeigt werden.

Automatischen Start von Diensten deaktivieren

Falls der Registrierungsschlüssel nicht existiert oder auf 0 gesetzt ist, ist diese Funktion standardmäßig aktiviert.

Führen Sie **Regedit** aus.

Machen Sie den folgenden Registrierungsschlüssel ausfindig:

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Legen Sie den Wert 0 fest, um die Funktion zu aktivieren. Legen Sie den Wert 1 fest, um die Funktion zu deaktivieren.

Benutzerauthentifizierung verwalten

Mithilfe der Steuerungen der Registerkarte „Authentifizierung“ in den Administratoreinstellungen können Sie Anmeldeoptionen für Benutzer festlegen und die jeweiligen Einstellungen anpassen.

Um die Benutzerauthentifizierung zu verwalten:

1 Klicken Sie als Administrator auf die Schaltfläche **Administratoreinstellungen**.

2 Klicken Sie auf **Benutzer**, um Benutzer zu verwalten und deren Eintragungsstatus anzuzeigen. Über diese Registerkarte können Sie außerdem Folgendes tun:

- Neue Benutzer eintragen
- Anmeldeinformationen hinzufügen oder ändern
- Anmeldeinformationen eines Benutzers entfernen

ANMERKUNG:
Unter **Anmeldung** und **Sitzung** werden der Eintragungsstatus eines Benutzers angezeigt.

Lautet der Status bei **Anmeldung** auf **OK**, wurden alle Eintragungen vorgenommen, die der Benutzer zum Durchführen von Anmeldungen benötigt. Lautet der Status bei **Sitzung** auf **OK**, wurden alle Eintragungen vorgenommen, die der Benutzer zum Verwenden von Password-Manager benötigt.

Lauten beide **Stati** auf **Nein**, muss der Benutzer zusätzliche Eintragungen durchführen. Um herauszufinden, welche Eintragungen noch ausstehen, wählen Sie das Tool **Administratoreinstellungen** aus, und öffnen Sie die Registerkarte **Benutzer**. Grau hinterlegte Kontrollkästchen stellen unvollständige Eintragungen dar. Kicken Sie alternativ auf die Kachel **Eintragungen**, und überprüfen Sie in der Registerkarte **Status** die Spalte **Richtlinie**, in der die erforderlichen Eintragungen aufgeführt sind.

Neue Benutzer hinzufügen


: Neue Windows-Benutzer werden automatisch hinzugefügt, wenn sie sich bei Windows anmelden oder Anmeldeinformationen registrieren.

Klicken Sie auf **Benutzer hinzufügen**, um den Eintragungsprozess für einen bereits bestehenden Windows-Benutzer zu starten.

Wählen Sie im Dialogfeld *Benutzer auswählen* die Option **Objekttypen** aus.

Geben Sie in das Textfeld den Objektnamen eines Benutzers ein, und klicken Sie auf **Namen überprüfen**.

Klicken Sie anschließend auf **OK**.

Der Eintragungsassistent wird gestartet.

Fahren Sie mit Anmelden oder Ändern der Benutzeranmeldeinformationen für weitere Anweisungen fort.

Anmelden oder Ändern der Benutzeranmeldeinformationen

Der Administrator kann zwar die Anmeldeinformationen für den Benutzer eintragen oder ändern, einige Eintragungsaktivitäten erfordern jedoch die Anwesenheit des Benutzers, z. B. die Beantwortung der Wiederherstellungsfragen oder das Scannen der Fingerabdrücke des Benutzers.

So können Sie Anmeldeinformationen von Benutzern eintragen oder ändern:

Klicken Sie in den Administratoreinstellungen auf die Registerkarte **Benutzer**.

Klicken Sie auf der Benutzer-Seite auf **Eintragen**.

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

Melden Sie sich im Dialogfeld „Authentifizierung erforderlich“ mit dem Windows-Passwort des Benutzers an, und klicken Sie auf **OK**.

Um das Windows-Passwort des Benutzers zu ändern, geben Sie auf der Seite „Passwort“ ein neues Passwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.

Um den Schritt der Passwort-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**.

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

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.

Weitere Informationen über das Registrieren von Anmeldeinformation, oder das Ändern von Anmeldeinformationen finden Sie im *Dell Data Protection / Console User Guide* (Dell Data Protection / Konsolen-Benutzerhandbuch).

Eingetragene Anmeldeinformation entfernen

Klicken Sie auf die Kachel **Administratoreinstellungen**.

Klicken Sie auf die Registerkarte **Benutzer**, und machen Sie den Benutzer ausfindig, dessen Anmeldeinformation Sie entfernen möchten.

Fahren Sie mit der Maus über das grüne Häkchen der Anmeldeinformation, die Sie entfernen möchten. Das Symbol ändert sich in ⊗.

Klicken Sie auf das ⊗-Symbol, und klicken Sie anschließend auf **Ja**, um den Löschvorgang zu bestätigen.

: Eine Anmeldeinformation kann nicht auf diese Weise entfernt werden, wenn es sich um die einzige eingetragene Anmeldeinformation des Benutzers handelt. Auch das Passwort kann nicht mit dieser Methode entfernt werden. Verwenden Sie den Entfernen-Befehl, um den Computerzugang eines Benutzers vollständig zu entfernen.

Alle eingetragenen Eintragungen eines Benutzers entfernen

Klicken Sie auf die Kachel **Administratoreinstellungen**.

Klicken Sie auf die Registerkarte **Benutzer**, und machen Sie den Benutzer ausfindig, den Sie entfernen möchten.

Klicken Sie auf **Entfernen**. (Der Befehl „Entfernen“ wird im unteren Bereich der Benutzereinstellungen in Rot angezeigt.)

Nach dem er entfernt wurde, kann sich der Benutzer erst wieder am Computer anmelden, wenn er erneut Anmeldedaten eingetragen hat.

5

Deinstallationsaufgaben

DDP | Security Tools kann nur von einem Benutzer mit mindestens **lokalen Administratorrechten** deinstalliert werden.

Deinstallierung von DDP | Security Tools

Die Anwendungen müssen in dieser Reihenfolge deinstalliert werden:

1. DDP | Client Security Framework

2. DDP | Security Tools Authentication

3. DDP | Security Tools

Falls Sie einen Computer mit einem selbstverschlüsselnden Laufwerk haben, befolgen Sie folgende Anweisungen zur Deinstallation:

1 Deprovisionierung des SED:
   a Klicken Sie in den Administratoreinstellungen auf die Registerkarte **Verschlüsselung.**
   b Klicken Sie zum Deaktivieren auf **Entschlüsseln.**
   c Starten Sie den Computer nach der Entschlüsselung des selbstverschlüsselnden Laufwerks neu.
2 Wählen Sie in der Windows-Systemsteuerung **Programm deinstallieren** aus.

   ANMERKUNG: Start > Systemsteuerung > Programme und Funktionen > Programm deinstallieren.
3 Deinstallieren Sie **Client Security Framework** und starten Sie den Computer dann neu.
4 Deinstallieren Sie **Security Tools Authentication** über die Windows-Systemsteuerung.
   Sie werden in einer Meldung gefragt, ob Sie die Benutzerdaten speichern möchten.

   Klicken Sie auf **Ja,** wenn Sie Security Tools später neu installieren möchten. Andernfalls klicken Sie auf **Nein**.

   Starten Sie den Computer nach der Deinstallation erneut.
5 Deinstallieren Sie **Security Tools** über die Windows-Systemsteuerung.
   Sie werden in einer Meldung gefragt, ob Sie die Anwendung und ihre Komponenten vollständig entfernen möchten.

   Klicken Sie auf **Ja**.

   Daraufhin wird das Dialogfeld *Deinstallation abgeschlossen* angezeigt.
6 Wählen Sie **Ja, ich möchte meinen Computer jetzt neu starten** und klicken Sie dann auf **Fertigstellen**.
7 Zum Abschluss der Deinstallation wird der Computer neu gestartet.

6

Wiederherstellung

Für den Fall, dass ein Benutzer seine Anmeldeinformationen verliert oder diese ablaufen, stehen Wiederherstellungsoptionen zur Verfügung:

- **Einmalpasswort (OTP):** Der Benutzer generiert ein OTP mithilfe der Security Tools | Mobile-App auf einen registrierten Mobilgerät und gibt das OTP auf dem Windows-Anmeldebildschirm ein, um wieder Zugriff auf den Computer zu erlangen. Diese Option ist nur verfügbar, wenn der Benutzer ein Mobilgerät mit Security Tools auf dem Computer eingetragen hat. Um die OTP-Funktion für die Wiederherstellung zu verwenden, darf der Benutzer nicht OTP für die Anmeldung auf dem Computer verwendet haben.

  ⓘ ANMERKUNG: Für die Funktion für das Einmalpasswort (OTP) muss das TPM vorhanden, aktiviert und zugewiesen sein. Folgen Sie den Anweisungen unter Löschen der Besitzrechte und aktivieren Sie das TPM. Ein OTP kann zur Authentifizierung oder Wiederherstellung verwendet werden, jedoch nicht für beides. Weitere Details finden Sie unter Konfigurieren Anmeldeoptionen.

- **Wiederherstellungsfragen:** Der Benutzer beantwortet eine Reihe von persönlichen Fragen korrekt, um wieder auf den Computer zugreifen zu können. Diese Option ist nur verfügbar, wenn der Administrator die Wiederherstellungsfragen konfiguriert und aktiviert und der Benutzer Wiederherstellungsfragen eingegeben hat. Diese Option kann verwendet werden, um wieder Zugriff auf den Computer über den Preboot-Authentifizierungsbildschirm und den Windows-Anmeldebildschirm zu erhalten.

Beide Wiederherstellungsmethoden erfordern Vorbereitung, entweder durch Eintragung von Wiederherstellungsfragen oder durch Eintragung eines Mobilgeräts über Security Tools auf dem Computer.

Selbstwiederherstellung, Wiederherstellungsfragen zur Windows-Anmeldung

Um Wiederherstellungsfragen zu beantworten, die über den Windows-Anmeldebildschirm erneuten Computerzugang ermöglichen:

1 Um die Wiederherstellungsfragen zu nutzen, klicken Sie auf **Sie können auf Ihr Konto nicht zugreifen?**

Daraufhin werden die Wiederherstellungsfragen angezeigt, die Sie während der Eintragung ausgewählt hatten.

2 Geben Sie die Antworten ein, und klicken Sie auf **OK**.

Nach der erfolgreichen Eingabe der Antworten auf die Fragen gelangen Sie in den Modus „Zugriffswiederherstellung“. Die nächste Aktion richtet sich nach den fehlgeschlagenen Anmeldeinformationen.

- Wenn Sie nicht in der Lage sind, das richtige Windows-Kennwort einzugeben, wird der Bildschirm „Kennwort ändern“ angezeigt.
- Wenn ein Fingerabdruck nicht erkannt werden konnte, wird die Seite für die Fingerabdruckregistrierung angezeigt, so dass Sie den Fingerabdruck erneut registrieren können.

Selbstwiederherstellung, PBA-Wiederherstellungsfragen

Gehen Sie wie folgt vor, um Wiederherstellungsfragen für die Wiedererlangung des Zugriffs auf dem Preboot-Authentifizierungs-Bildschirm zu beantworten:

1 Geben Sie auf dem PBA-Bildschirm Ihren Benutzernamen ein.
2 Wählen Sie im linken unteren Bereich des Bildschirms **Optionen** aus.
3 Wählen Sie im Menü „Optionen" **Passwort vergessen** aus.
4 Beantworten Sie die Wiederherstellungsfragen und klicken Sie auf **Anmelden.**

Selbstwiederherstellung, Einmalpasswort

Hier wird beschrieben, wie Sie die Einmalpasswort-Funktion (OTP) nutzen können, um den Computerzugang wiederherzustellen, wenn Sie beispielsweise Ihr Windows-Passwort vergessen haben, dieses abgelaufen ist oder die maximal zulässige Anzahl an Anmeldeversuchen überschritten wurde. Die Einmalpasswort-Option (OTP) ist nur dann verfügbar, wenn der Benutzer ein Mobilgerät eingetragen hat und das OTP nicht zur Anmeldung bei Windows verwendet wurde.

ANMERKUNG: Für die Funktion für das Einmalpasswort muss ein TPM vorhanden, aktiviert und zugewiesen sein. OTP kann entweder für die Windows-Authentifizierung oder für die Wiederherstellung verwendet werden, jedoch nicht für beides. Der Administrator kann die Richtlinie so festlegen, dass OTP entweder für die Wiederherstellung oder für die Authentifizierung verwendet wird, oder er kann diese Funktion deaktivieren.

So verwenden Sie OTP für die Wiederherstellung des Zugriffs auf den Computer:

1 Klicken Sie auf dem Windows-Anmeldebildschirm auf das OTP-Symbol  .
2 Öffnen Sie auf dem Mobilgerät die Security Tools Mobile-App, und geben Sie das Passwort 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 DDP | Security Tools 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**.
6 Wählen Sie auf dem Computer auf dem Bildschirm mit dem Wiederherstellungsmodus die Option **Ich habe mein Windows-Passwort vergessen** aus, und folgen Sie den Anweisungen auf dem Bildschirm, um das Passwort zurückzusetzen.

Glossar

Deprovisionierung: Beim Deprovisionieren wird die PBA-Datenbank entfernt und die PBA deaktiviert. Die Deprovisionierung tritt erst nach dem Herunterfahren in Kraft.

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.

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.