Dell Data Security Console

User Guide v3.9

January 2024
Rev. A01

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Contents

1

Einleitung

Die Data Security Console bietet Zugriff auf Anwendungen, die die Sicherheit für alle NutzerInnen des Computers gewährleisten, um den Verschlüsselungsstatus der Laufwerke und Partitionen des Computers anzuzeigen und zu managen und um ganz einfach PBA-Passwörter und Wiederherstellungsfragen einzutragen.

Die folgenden Funktionen sind verfügbar:

- Eintragen von Anmeldeinformationen für die Verwendung mit PBA
- Nutzen der Vorteile von mehrstufigen Anmeldeinformationen, einschließlich Passwörter und Smartcards
- Wiederherstellen des Zugangs zu Ihrem Computer ohne Helpdesk-Anrufe oder Administratorunterstützung, wenn Sie Ihr Passwort vergessen haben
- Einfache und leichte Änderung Ihres Windows-Passworts
- Festlegen persönlicher Einstellungen
- Anzeigen des Verschlüsselungsstatus
- Anzeigen des Firewall- und Web Protection-Status (falls installiert)
- Anzeigen des Advanced Threat Prevention-Status

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

- Anzeigen des Verschlüsselungsstatus (auf Computern mit selbstverschlüsselnden Laufwerken)
- Anzeigen von Advanced Threat Prevention

Data Security Console

Zum Öffnen der Data Security Console doppelklicken Sie vom Desktop aus auf das Dell Data Security Console-Symbol 

.

Sie haben Zugriff auf die folgenden Anwendungen:

- Verschlüsselungsstatus ermöglicht Ihnen, den Verschlüsselungsstatus der Computerlaufwerke und -partitionen anzuzeigen.
- Das Advanced Threat Prevention Dashboard zeigt basierend auf den Advanced Threat Protection-Richtlinien den Schutzstatus des Computers an.
- Auf der Seite „Firewall- und Web Protection-Status“ werden der allgemeine und der individuelle Schutzstatus von Firewall und Web Protection auf dem Computer angezeigt.
- Mit dem Tool „Sign-In Access“ können Sie PBA-Passwörter einrichten und managen, PBA-Wiederherstellungsfragen konfigurieren und den Status Ihrer Anmeldeinformationseintragung anzeigen.

Diese Anleitung beschreibt, wie jede dieser Anwendungen verwendet wird.

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

Dell ProSupport for Software kontaktieren

Telefonischen Support 24x7 für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

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

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

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

2

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 Data Security Console zu minimieren, zu maximieren oder zu schließen, klicken Sie auf das entsprechende Symbol in der rechten Ecke der Titelleiste.

Um die Data Security Console nach dem Minimieren wiederherzustellen, doppelklicken Sie auf das Infobereichsymbol.

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

Data Security Console – Details

Um Informationen zur Data Security Console, 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 Versionsinformationen.
Info anzeigen	Enthält die folgenden Informationen: • Produktversion und Datumsinformationen • ob Dell Encryption und/oder die erweiterte PBA-Authentifizierung vom Unternehmen oder einem lokalen Administrator verwaltet wird • Versionsnummern für Betriebssystem, BIOS, Hauptplatine und TPM (Trusted Platform Module).
MS Info	Führt das Dienstprogramm für Microsoft Windows-Systeminformationen aus, um detaillierte Informationen zur Hardware, zu den Komponenten und der Softwareumgebung anzuzeigen.
Info kopieren	Kopiert alle Systeminformationen in die Zwischenablage, um sie in eine E-Mail an Ihren Administrator oder den Dell ProSupport einzufügen.
Feedback	Zeigt ein Formular an, mit dem Sie Dell Feedback zu diesem Produkt geben können. (Auf Nicht-Domänencomputern ist diese Option jederzeit verfügbar. Auf Domänencomputern richtet sich diese Option nach der Richtlinie.)
Richtlinien	Zeigt eine Hierarchie der Richtlinien an, die auf diesem Computer gelten.

Services	Zeigt Details zu den ausgeführten Diensten an.
Support	Stellt eine Verbindung zur Dell ProSupport-Website her.
Advanced Threat Prevention	Aktiviert die standardmäßige Benutzeroberfläche für den Advance Threat Prevention-Bereich.
Protokolle	Zeigt eine detaillierte Liste der protokollierten Ereignisse für Troubleshooting an.

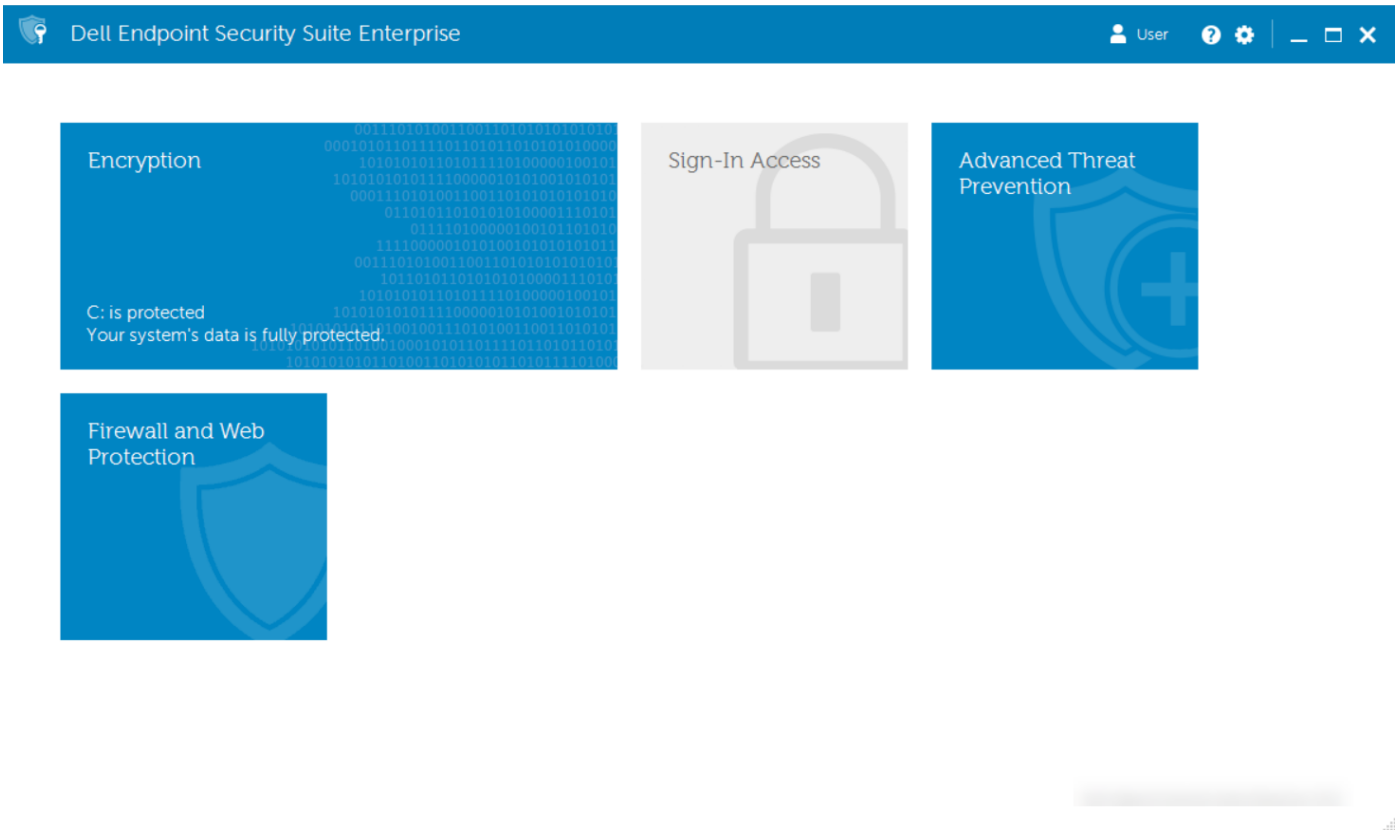
3

Advanced Threat Prevention

Advanced Threat Prevention 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.

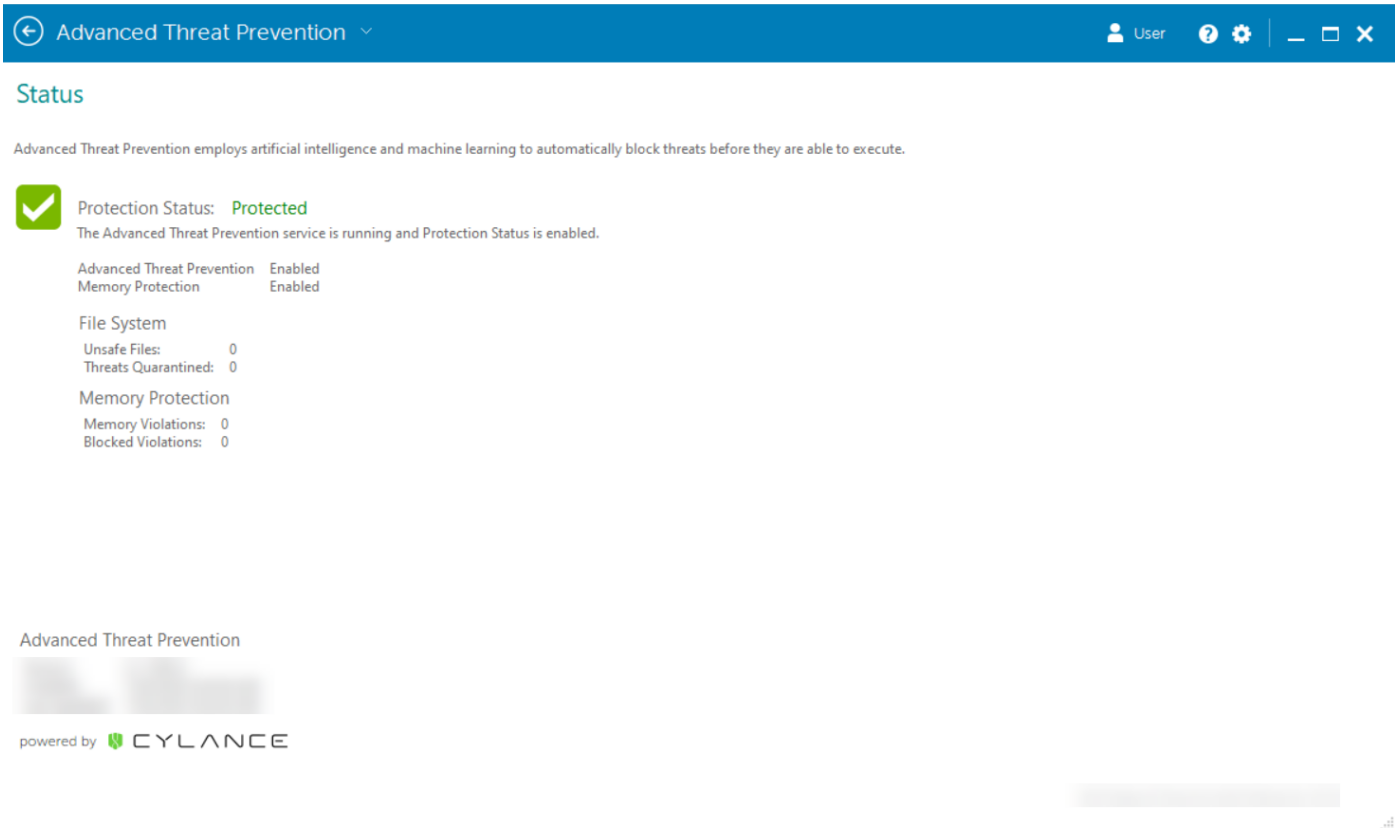
Advanced Threat Prevention wird standardmäßig zusammen mit Endpoint Security Suite Enterprise installiert. Firewall und Webschutz werden optional als Bestandteil von Endpoint Security Suite Enterprise installiert.

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



Advanced Threat Prevention – Status

Greifen Sie über die **Advanced Threat Prevention**-Kachel in der Data Security Console auf die Advanced Threat Prevention-Statusseite zu.



Schutzstatus

Der Schutzstatus gibt an, ob der Computer geschützt (ein grünes Häkchen) oder nicht geschützt (ein rotes X) ist. Dies ist abhängig davon, ob Advanced Threat Prevention ausgeführt wird und Advanced Threat Prevention auf dem Dell Server aktiviert ("ein") ist.

- Advanced Threat Prevention – Zeigt an, ob Advanced Threat Prevention für den Dell Server aktiviert ("ein") ist.
- Memory Protection – Zeigt an, ob Memory Protection auf dem Dell Server aktiviert ("ein") ist.

Dateisystem

- Unsichere Dateien – Anzahl der Dateien auf dem Computer, bei denen es sich möglicherweise um Malware handeln könnte.
- Bedrohungen in Quarantäne – Dateien, die von Ihrem ursprünglichen Speicherort auf dem Computer entfernt und am Ausführen gehindert wurden.

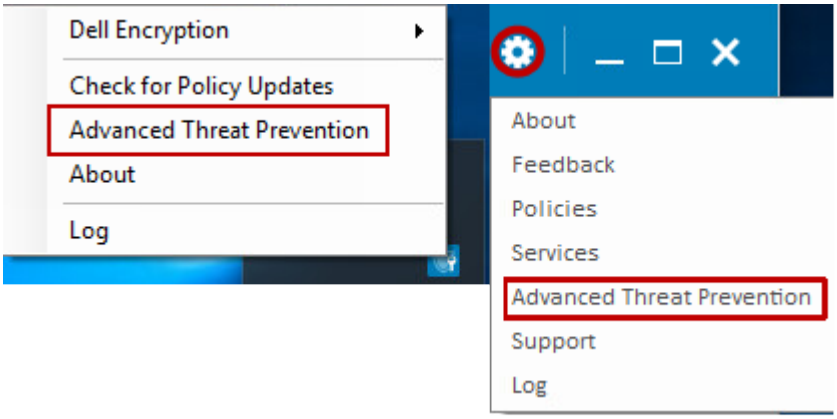
Speicherschutz

- Speicherangriffe – Anzahl der Anwendungen, die versucht haben in den Computerspeicher einzudringen.
- Blockierte Angriffe – Anzahl der blockierten Versuche von Anwendungen, in den Computerspeicher einzudringen.

Standard-UI

Standard UI ermöglicht eine neue Funktion innerhalb des Extra-Menüs oder Systray Menüs in der Data Security Console, wo detaillierte Informationen darüber zu finden sind, welche Ereignisse für einen bestimmten Endpunkt aufgezeichnet wurden. Standard UI kann **nur** aktiviert werden, wenn die Standard UI Richtlinie in der Remote-Managementkonsole aktiviert ist. Weitere Informationen finden Sie unter *AdminHelp* durch Auswahl von **?** in der oberen rechten Ecke der Remote-Managementkonsole.

Standard UI kann für Data Security Console über das Symbol für Sistray bzw. Extras-Menü links in der Titelleiste aktiviert werden.



Wählen Sie eine der folgenden Optionen aus, um ausführliche Informationen zu Advanced Threat Prevention anzuzeigen.

- **Bedrohungen anzeigen**

  Die Option **Bedrohungen anzeigen** zeigt Bedrohungen, die durch Advanced Threat Prevention entschärft wurden. sowie die folgenden Details:

  Datei-Hash-ID – Zeigt SHA256-Hash-Informationen für die Bedrohung.

  Datei-MD5 – Das MD5-Hash.

  Derzeit aktuell? - Ist die Bedrohung derzeit auf diesem Gerät aktuell? Aktuell oder nicht aktuell.

  Dateipfad – Der Pfad, an dem die Bedrohung gefunden wurde. Beinhaltet den Dateinamen.

  Bewertung – Bewertung der Bedrohung.

- **Exploits anzeigen**

  Die Option **Exploits anzeigen** zeigt Exploits an, die durch Advanced Threat Prevention entschärft wurden, sowie die folgenden Details:

  Ereignis-ID – Eindeutige Nummer, die jedem Bedrohungsereignis zugewiesen ist.

  Prozess-ID – Zeigt die Prozess-ID der Anwendung, die durch Memory Protection erkannt wurde.

  Prozess-Tag – Eine eindeutige Kennung für Prozesse im Startzyklus.

  Image-Hash - Zeigt die SHA256-Hash-Informationen für das Exploit.

  Image-Pfad – Der Pfad, an dem das Exploit seinen Ursprung hat. Beinhaltet den Dateinamen.

  Dateiversion – Zeigt die Versionsnummer der Exploit-Datei.

- **Skripte anzeigen**

  Die Option **Skripte anzeigen** zeigt Skripte, die durch Advanced Threat Prevention entschärft wurden, sowie folgende Details:

  Skriptpfad – Der Pfad, von dem das Skript stammt. Beinhaltet den Dateinamen.

  Ereignis-ID – Eindeutige Nummer, die jedem Skriptereignis zugewiesen ist.

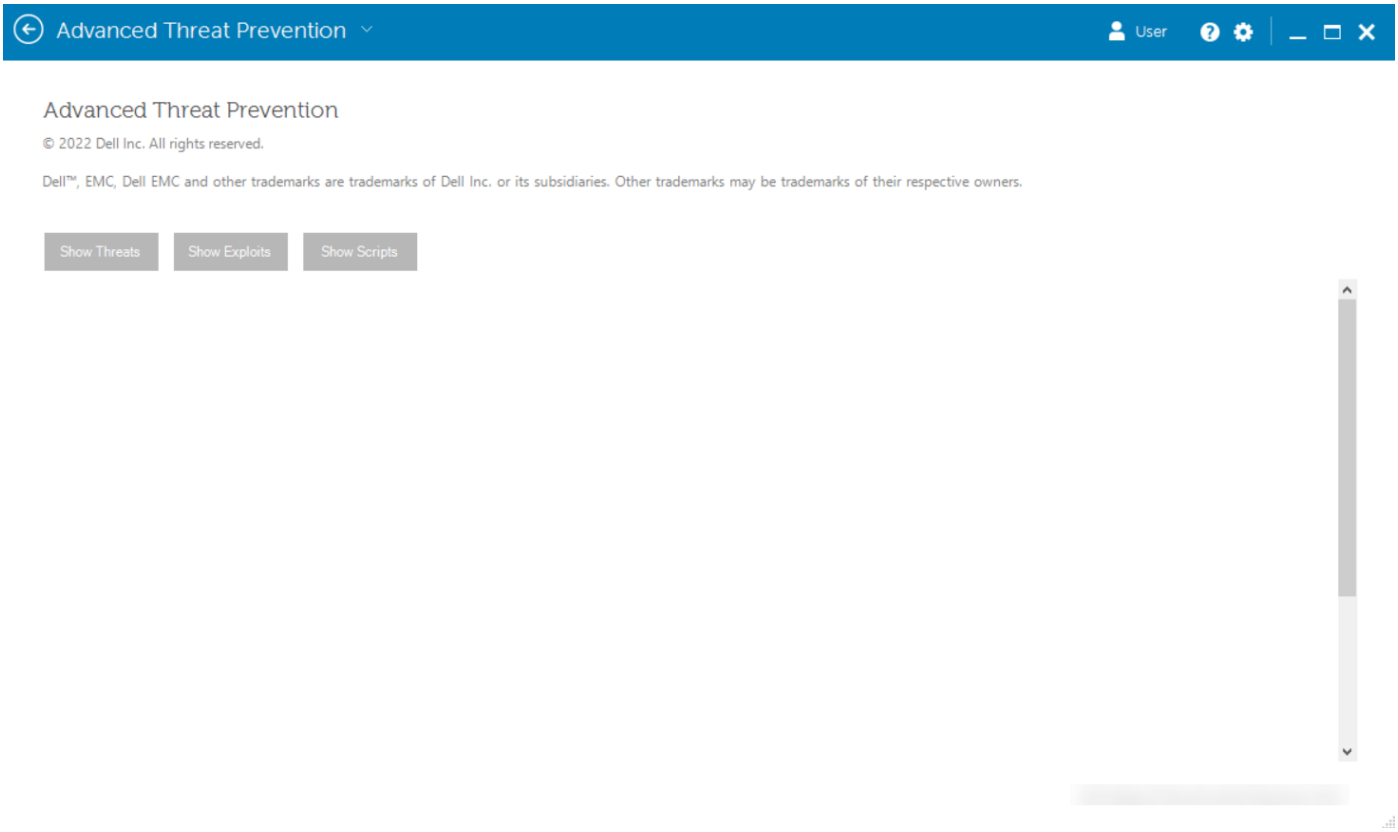
  Datei-Hash-ID – Zeigt den SHA256-Hash-Informationen für das Skript an.

  Datei-MD5 – Das MD5-Hash.

  Laufwerkstyp – Gibt an, ob das Laufwerk intern oder extern ist.

  Interpreter-Name – Der Name der Skript-Kontrollfunktionen, die das bösartige Skript identifiziert hat.

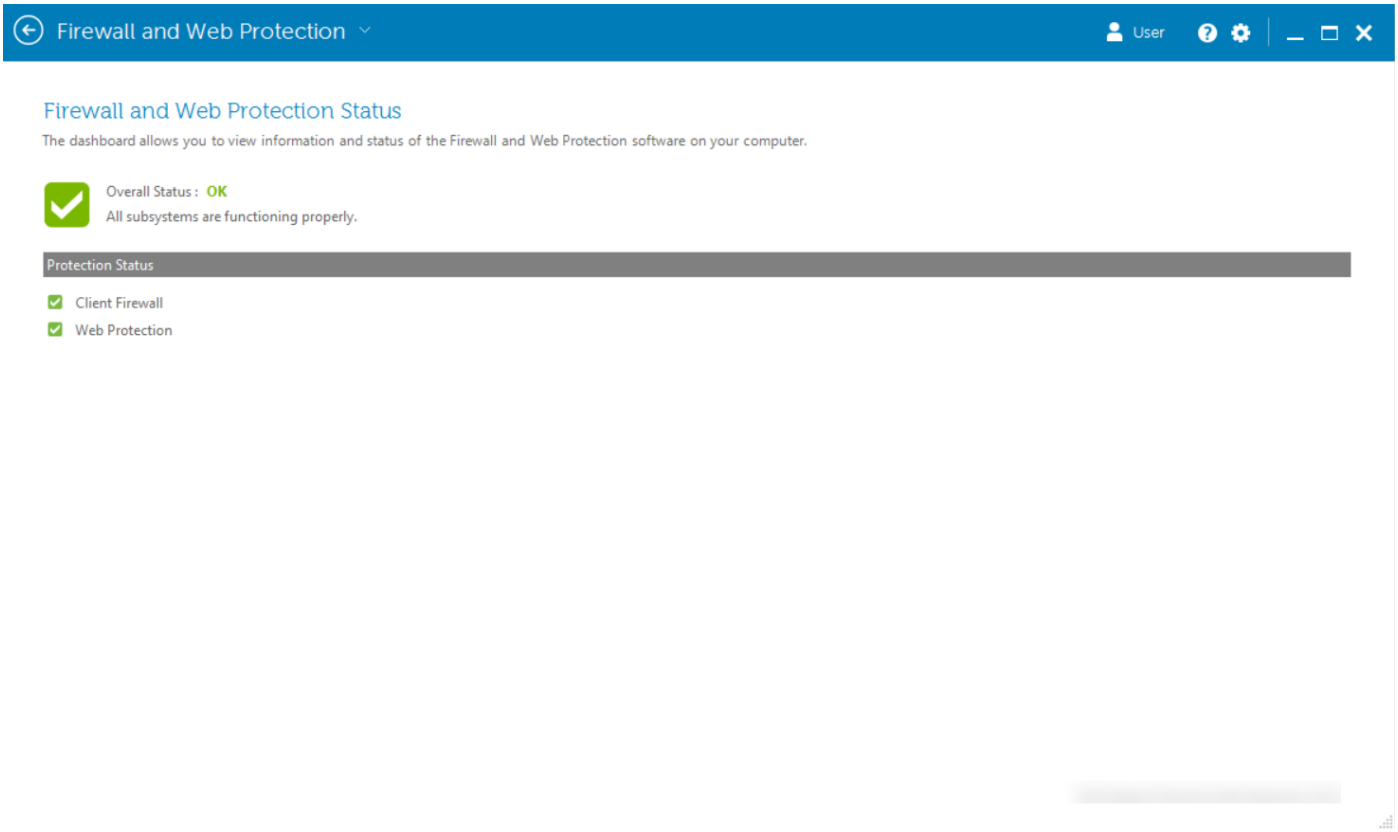
  Interpreter-Version – Die Versionsnummer der Skript-Kontrollfunktion.



Die angezeigte Ereignisliste wird erfasst, wenn die Data Security Console Sitzung gestartet wird. Wenn Sie neue Ereignisse starten möchten, schließen Sie Data Security Console und starten Sie diese erneut.

Firewall- und Webschutzstatus

Greifen Sie über die Kachel **Firewall- und Webschutz** in der Data Security Console auf die Statusseite für Firewall- und Webschutz zu.



Gesamtstatus

Der Gesamtstatus zeigt an, welcher Computer geschützt oder anfällig ist. Dies basiert auf den Einstellungen zu Firewall- und Webschutz für den Dell Server.

- Geschützt – Der Gesamtstatus ist „Geschützt“, wenn *Webschutz* oder *Client-Firewall* aktiviert ist („ein“).
- Anfällig – Der Gesamtstatus ist "Anfällig", wenn *Web -Schutz* und *Client -Firewall* deaktiviert sind ("aus").

Schutzstatus

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

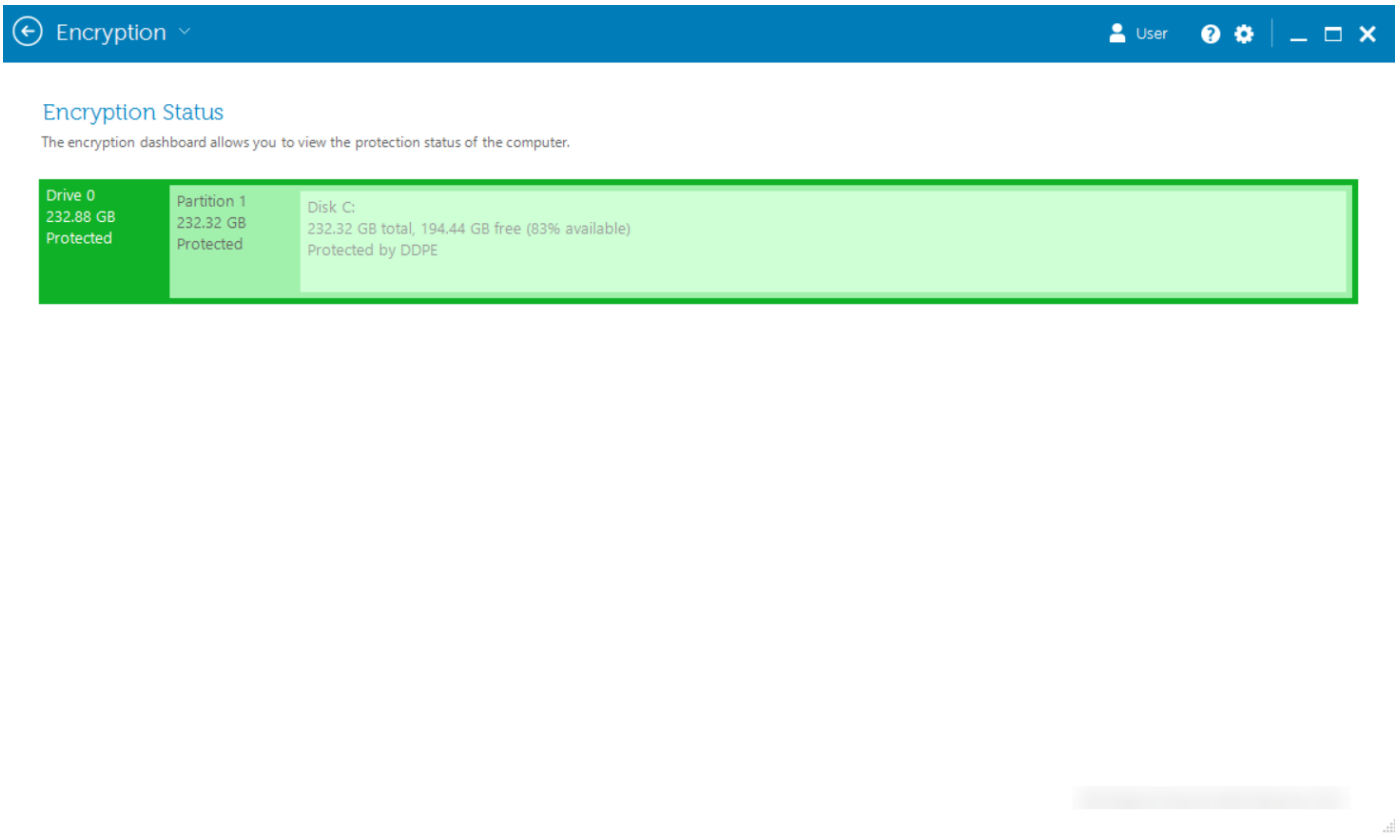
- Client-Firewall – Der Gesamtstatus ist "Geschützt", wenn *Client Firewall* aktiviert ist ("ein").
- Web-Schutz – Der Gesamtstatus ist "Geschützt", wenn *Web Protection* aktiviert ist ("ein").

4

Verschlüsselungsstatus

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

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



5

Sign-in Access

Mit Sign-in Access können Sie basierend auf den vom Administrator festgelegten Richtlinien Registrierungen und Änderungen vornehmen sowie den Registrierungsstatus überprüfen.

Nach der erstmaligen Registrierung können Sie auf die Kachel „Sign-in Access“ klicken, um Anmeldeinformationen hinzuzufügen oder zu ändern.

ANMERKUNG: Die Kachel „Sign-in Access“ wird nur angezeigt, wenn die PBA aktiv ist.

Erstmaliges Eintragen von Anmeldeinformationen

Gehen Sie wie folgt vor, um Anmeldeinformationen erstmals einzutragen:

1. Klicken Sie auf der Startseite von Data Security Console auf die Kachel **Sign-In Access**.
2. Um Ihr Windows-Passwort zu ändern, geben Sie auf der Seite „Passwort“ ein neues Passwort ein, bestätigen es und klicken dann auf **Ändern**.
3. Wählen Sie auf der Seite „Wiederherstellungsfrage“ drei Wiederherstellungsfragen aus und geben Sie die entsprechenden Antworten ein. Klicken Sie anschließend auf **Registrieren**.

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

Hinzufügen, Ändern oder Anzeigen von Registrierungen

Klicken Sie zum Hinzufügen, Ändern oder Anzeigen von Registrierungen auf die Kachel **Sign-In Access**.

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

Die Seite „Sign-In Access“ zeigt die unterstützten Anmeldeinformationen, die zugehörigen Richtlinieneinstellungen („Erforderlich“ oder „–“) sowie den Registrierungsstatus an. Über diese Seite können Nutzer ihre Registrierungen auf Basis der durch den Administrator definierten Richtlinie verwalten.

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

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

Passwort

So ändern Sie Ihr Windows-Passwort:

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

   Kennwortänderungen sind sofort gültig.

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

ANMERKUNG:

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

Wiederherstellungsfragen

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

ANMERKUNG:

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

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

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

ANMERKUNG:

Klicken Sie auf die Schaltfläche **Zurücksetzen**, um die Auswahl auf dieser Seite zu löschen und erneut zu beginnen.

Wiederherstellungsfragen bereits eingetragen

Wenn bereits PBA-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 PBA-Wiederherstellungsfragen vollständig zu löschen, klicken Sie auf **Löschen**.
   - Um die PBA-Wiederherstellungsfragen und die zugehörigen Antworten neu zu definieren, klicken Sie auf **Erneut registrieren**.

6

Glossar

Anmeldeinformationen – Über Anmeldeinformationen, wie beispielsweise ein Windows-Passwort, wird die Identität einer Person nachgewiesen.

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

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

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

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

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