Dell Data Security Console

User Guide v3.9

January 2024
Rev. A01

DELL Technologies

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: un messaggio di ATTENZIONE evidenzia la possibilità che si verifichi un danno all'hardware o una perdita di dati ed indica come evitare il problema.

AVVERTENZA: un messaggio di AVVERTENZA evidenzia un potenziale rischio di danni alla proprietà, lesioni personali o morte.

Contents

1

Introduzione

Data Security Console fornisce accesso alle applicazioni che garantiscono protezione per tutti gli utenti del computer, per visualizzare e gestire lo stato di crittografia delle unità e partizioni del computer e per registrare facilmente le password PBA e domande di ripristino.

Sono disponibili le seguenti funzioni:

- Registrazione delle credenziali per l'uso con PBA
- Utilizzo di credenziali a più fattori, comprese password e smart card
- Ripristino dell'accesso al computer in caso si sia dimenticata la password senza rivolgersi all'helpdesk o all'amministratore
- Modifica facile della password di Windows
- Impostazione delle preferenze personali
- Visualizzazione dello stato di crittografia
- Visualizzazione dello stato di Firewall e Protezione Web (se installati)
- Visualizzazione dello stato di Advanced Threat Prevention.

Le funzioni seguenti sono disponibili tramite la Data Security Console nel sistema operativo di un server:

- Visualizzazione dello stato di crittografia (sui computer con unità autocrittografanti)
- Visualizzazione di Advanced Threat Prevention

Data Security Console

Per aprire Data Security Console, sul desktop, fare doppio clic sull'icona di Dell Data Security Console 

.

È possibile accedere a queste applicazioni:

- Stato crittografia permette di visualizzare lo stato di crittografia delle unità e delle partizioni del computer.
- La dashboard di Advanced Threat Protection visualizza lo stato di protezione del computer in base ai criteri di Advanced Threat Protection.
- La pagina di stato di Firewall e Protezione web visualizza lo stato generale e la protezione individuale di Firewall e Protezione Web dei computer.
- Lo strumento Sign-In Access consente all'utente di impostare e gestire la password PBA, configurare le domande di ripristino automatico PBA e visualizzare lo stato di registrazione delle credenziali.

La presente guida descrive la modalità di utilizzo di ogni applicazione.

Per la documentazione aggiornata, controllare periodicamente il sito Web dell.com/support .

Contattare Dell ProSupport for Software

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24x7.

Inoltre, il supporto online per i prodotti Dell è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Assicurarsi di avere a portata di mano il codice di matricola o il codice di servizio rapido per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono al di fuori degli Stati Uniti, vedere Numeri di telefono internazionali di Dell ProSupport for Software.

2

Esplorazione

Per accedere a un'applicazione, fare clic sul riquadro appropriato.

Barra del titolo

Per tornare alla pagina iniziale da un'applicazione, fare clic sulla freccia indietro nell'angolo a sinistra della barra del titolo, accanto al nome dell'applicazione attiva.

Per passare direttamente ad un'altra applicazione, fare clic sulla freccia verso il basso accanto al nome dell'applicazione attiva e selezionarne una.

Per ridurre a icona, ingrandire o chiudere la Data Security Console, fare clic sulla relativa icona nell'angolo a destra della barra del titolo.

Per ripristinare Data Security Console dopo aver ridotto la console a icona, fare doppio clic sulla relativa icona nell'area delle notifiche.

Per aprire la guida, fare clic su **?** sulla barra del titolo.

Dettagli sulla Data Security Console

Per visualizzare i dettagli sulla Data Security Console, sui criteri, sui servizi in esecuzione e sui registri, fare clic sull'icona a forma di ingranaggio nella parte sinistra della barra del titolo. Queste informazioni potrebbero essere necessarie ad un amministratore per fornire supporto tecnico.

Selezionare una voce dal menu.

Voce di menu	Scopo
Informazioni su	Contiene informazioni sulla versione.
Mostra informazioni	Contiene: • informazioni sulla versione e sulla data del prodotto • indicazione se Dell Encryption e/o l'autenticazione avanzata PBA sono gestiti a livello di azienda o da un amministratore locale • numeri di versione del sistema operativo, BIOS, scheda madre e TPM (Trusted Platform Module).
MS Info	Esegue l'utility Informazioni di sistema Microsoft Windows per visualizzare informazioni dettagliate sull'ambiente hardware, software e dei componenti.
Copia informazioni	Copia tutte le informazioni di sistema negli appunti per incollarle in un'e-mail all'amministratore di riferimento oppure a Dell ProSupport.
Feedback	Fornisce un modello da compilare per inviare a Dell un feedback sul prodotto. Sui computer non appartenenti al dominio, questa opzione è sempre disponibile. Sui computer del dominio, questa opzione è determinata dal criterio.

Criteri	Fornisce una gerarchia di criteri applicabili al computer.
Servizi	Visualizza i dettagli sui servizi in esecuzione.
Supporto	Fornisce un collegamento al sito Web di Dell ProSupport.
Advanced Threat Prevention	Abilita l'interfaccia utente standard per il riquadro Advanced Threat Prevention.
Registro	Visualizza un elenco dettagliato degli eventi registrati per la risoluzione dei problemi.

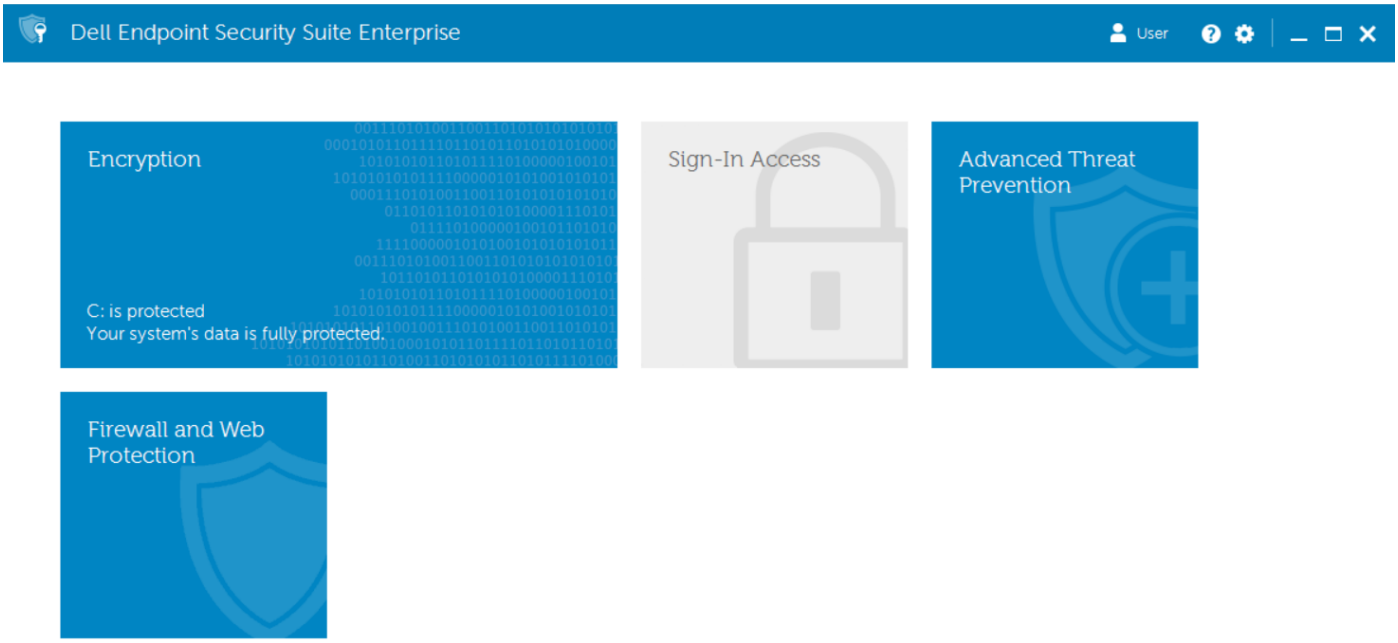
3

Advanced Threat Prevention

Advanced Threat Prevention protegge il computer dai malware monitorando tutti i processi che tentano l'esecuzione nel computer o nello spazio di memoria, e segnalando quelli ritenuti anormali o non sicuri.

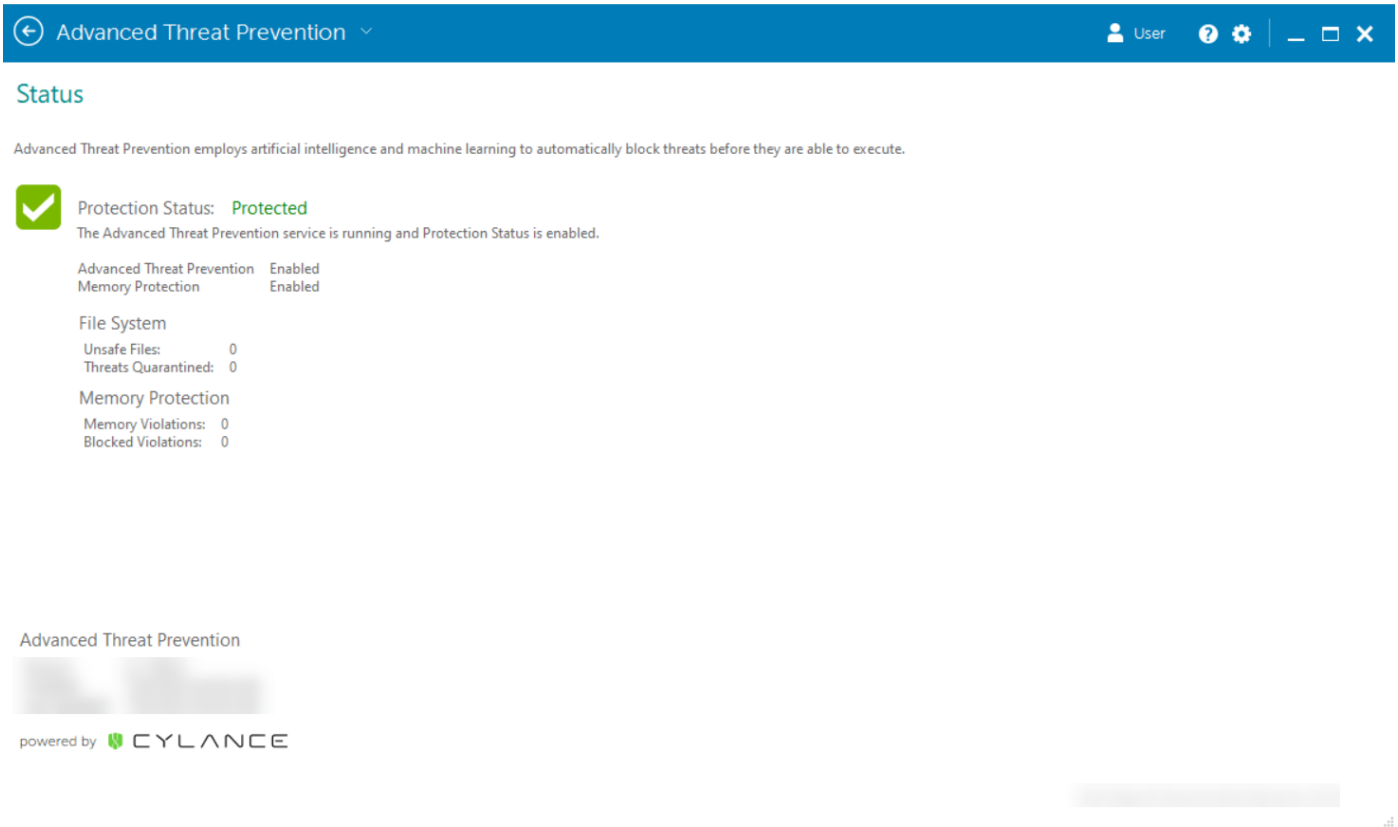
Advanced Threat Prevention è installato per impostazione predefinita con Endpoint Security Suite Enterprise. Le funzioni Firewall e Protezione Web vengono installate in via opzionale come parte di Endpoint Security Suite Enterprise.

Selezionare il riquadro di Advanced Threat Prevention per visualizzare le statistiche del computer risultanti dal monitoraggio e dall'analisi avanzati.



Stato di Advanced Threat Prevention

Accedere alla pagina Stato di Advanced Threat Prevention attraverso il riquadro **Advanced Threat Prevention** nella Data Security Console.



Stato protezione

Lo stato della protezione indica se il computer è protetto (indicato da un segno di spunta verde) o non protetto (indicato da una X rossa), a seconda che il servizio Advanced Threat Prevention sia in esecuzione o meno e il servizio Advanced Threat Prevention sia attivato (abilitato) nel Dell Server.

- Advanced Threat Prevention - Indica se Advanced Threat Prevention è attivato (abilitato) nel Dell Server.
- Protezione della memoria - Indica se la protezione della memoria è attivata (abilitata) nel Dell Server.

File system

- File non sicuri - Il numero dei file presenti nel computer che probabilmente sono dei malware.
- Minacce messe in quarantena - Numero dei file spostati dalla posizione originale sul computer e per cui non è consentita l'esecuzione.

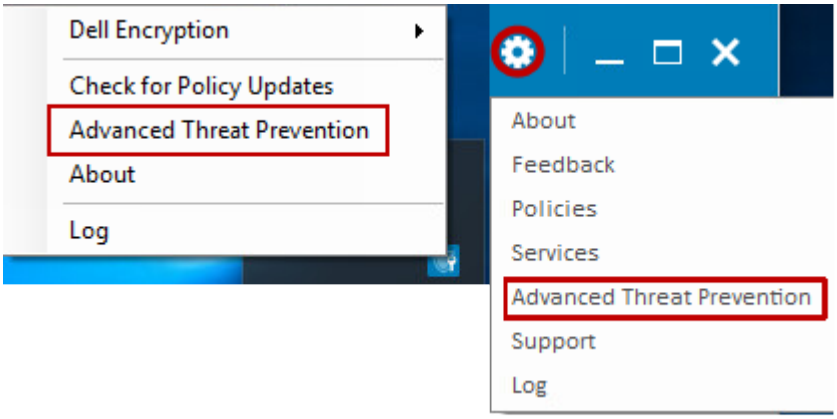
Protezione della memoria

- Violazioni memoria - Numero di tentativi da parte delle applicazioni di utilizzare la memoria del computer.
- Violazioni bloccate - Numero di tentativi bloccati di utilizzare la memoria del computer da parte delle applicazioni.

Interfaccia utente standard

L'interfaccia utente standard consente di utilizzare una nuova funzione all'interno del menu con l'ingranaggio o del menu nell'area di notifica nella Data Security Console, che consente di visualizzare informazioni dettagliate sugli eventi che sono stati acquisiti su un endpoint specifico. L'interfaccia utente standard può essere attivata **solo** se il criterio corrispondente è abilitato nella Remote Management Console. Per ulteriori informazioni, vedere *AdminHelp* selezionando **?** nell'angolo in alto a destra della Remote Management Console.

L'interfaccia utente standard può essere abilitata nella Data Security Console tramite l'icona nell'area di notifica o l'icona dell'ingranaggio sul lato sinistro della barra del titolo.



Selezionare una delle seguenti opzioni per visualizzare i dettagli completi su Advanced Threat Prevention:

- **Mostra minacce**

  L'opzione **Mostra minacce** visualizza le minacce che sono state ridotte da Advanced Threat Prevention e i seguenti dettagli:

  ID hash file - Visualizza le informazioni hash SHA256 della minaccia.

  MD5 file - L'hash MD5.

  In esecuzione? - La minaccia è in esecuzione sul dispositivo? In esecuzione o Non in esecuzione.

  Percorso file - Il percorso in cui la minaccia è stata trovata. Include il nome del file.

  Punteggio - Livello della minaccia.

- **Mostra exploit**

  L'opzione **Mostra exploit** visualizza gli exploit che sono stati ridotti da Advanced Threat Prevention e i seguenti dettagli:

  ID evento - numero univoco assegnato a ciascun evento di minaccia.

  ID processo - Visualizza l'ID del processo dell'applicazione identificati da Protezione della memoria.

  Tag processo - Identificatore univoco per la categorizzazione dei processi per ogni ciclo di avvio.

  Hash immagine - Visualizza le informazioni hash SHA256 dell'exploit.

  Percorso immagine - Il percorso di origine dell'exploit. Include il nome del file.

  Versione file - Visualizza il numero di versione del file di exploit.

- **Mostra script**

  L'opzione **Mostra script** visualizza gli script che sono stati ridotti da Advanced Threat Prevention e i seguenti dettagli:

  Percorso script - Il percorso di origine dello script. Include il nome del file.

  ID evento - Numero univoco assegnato a ciascun evento script.

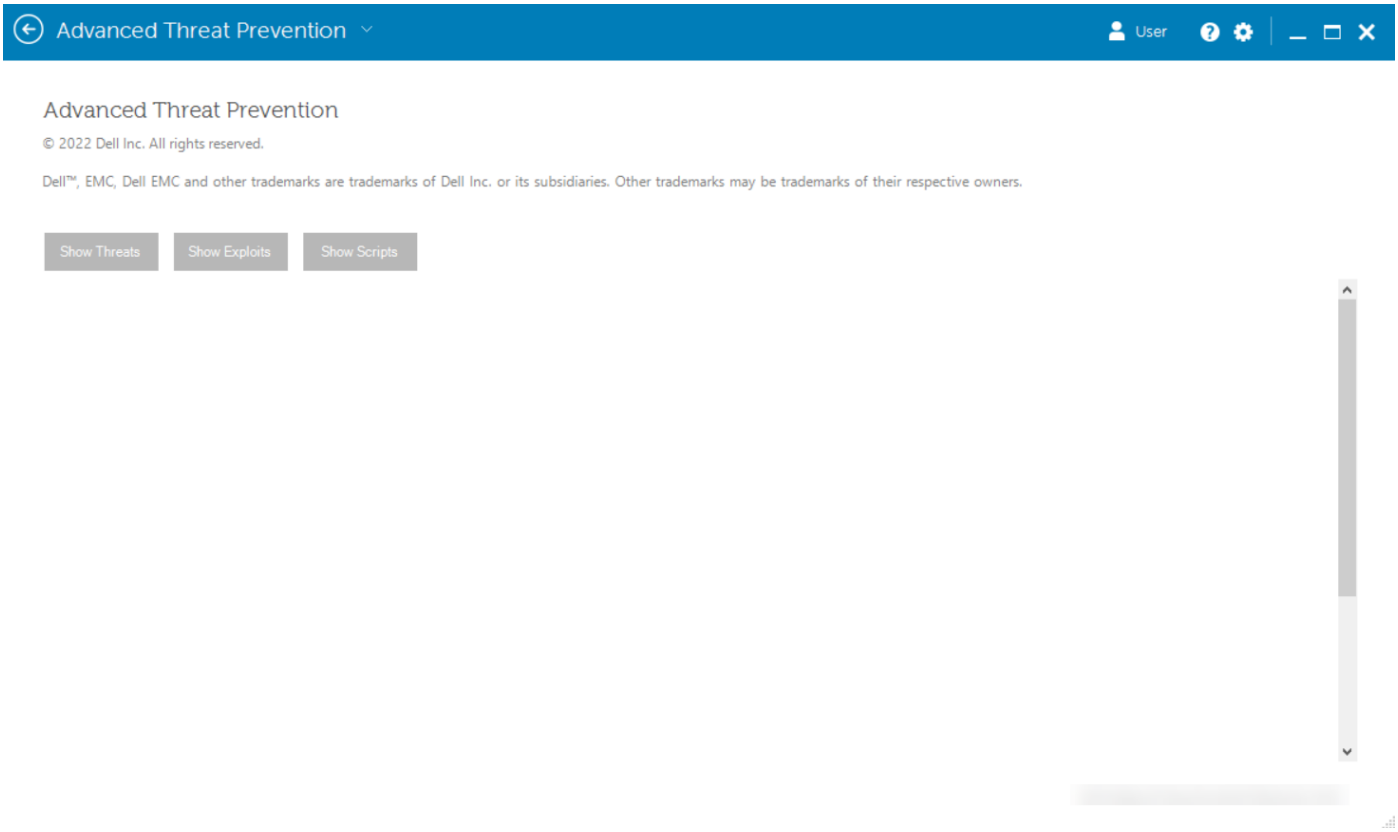
  ID hash file - Visualizza le informazioni hash SHA256 dello script.

  MD5 file - L'hash MD5.

  Tipo di unità - Specifica se l'unità è interna o esterna.

  Nome interprete - Il nome della funzione di controllo script che ha identificato lo script dannoso.

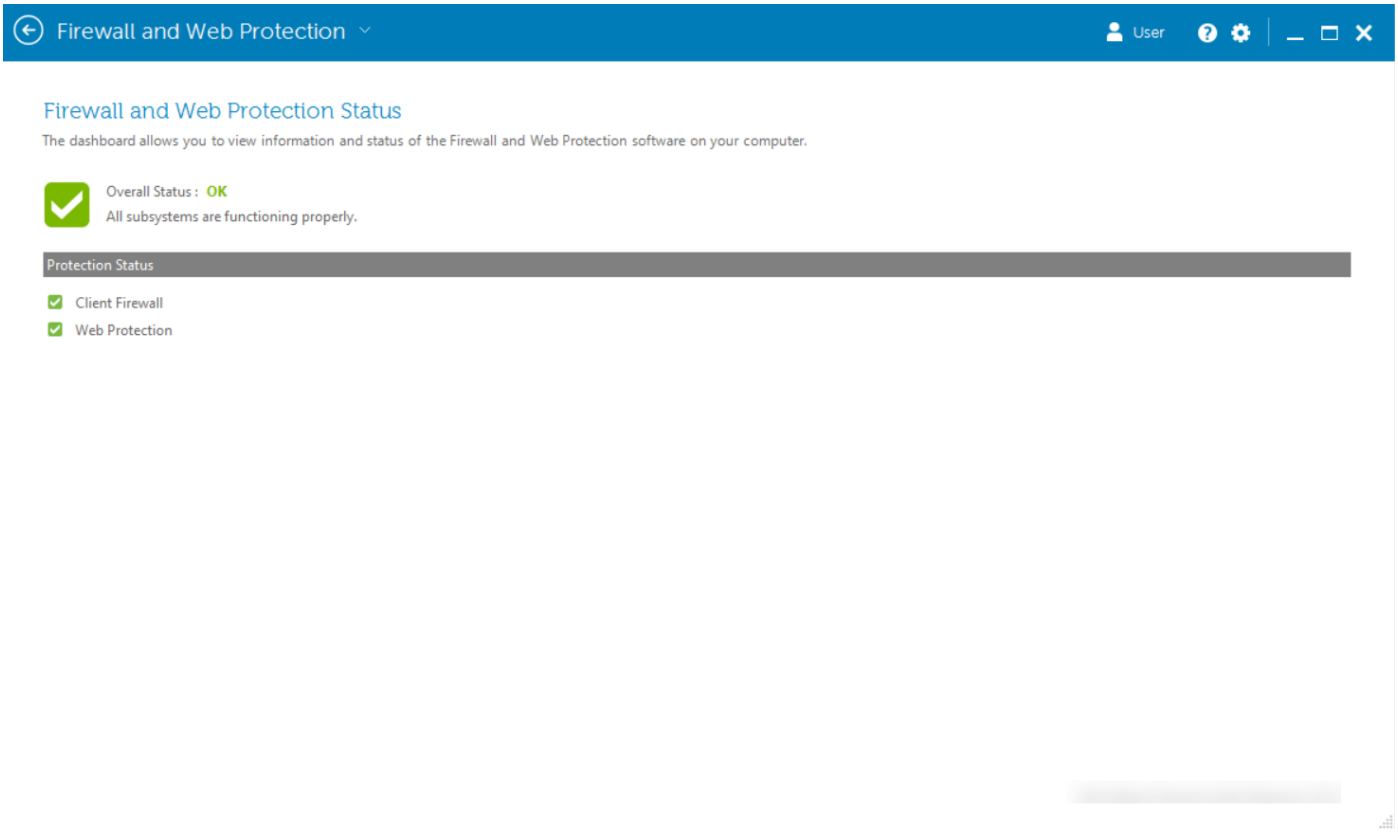
  Versione interprete - Il numero di versione della funzione di controllo script.



L'elenco di eventi visualizzato viene raccolto quando viene avviata la sessione della Data Security Console. Per recuperare nuovi eventi, chiudere la Data Security Console, quindi riavviarla.

Stato di Firewall e Protezione Web

Accedere alla pagina Stato di Firewall e Protezione Web attraverso il riquadro **Firewall e Protezione Web** nella Data Security Console.



Stato complessivo

Lo stato complessivo indica se il computer è protetto o vulnerabile, in base alle impostazioni dei criteri Firewall e Protezione Web nel Dell Server.

- Protetto - Lo stato complessivo è protetto se i criteri *Protezione Web* o *Firewall client* sono abilitati.
- Vulnerabile - Lo stato complessivo è Vulnerabile se i criteri *Protezione Web* e *Firewall client* sono disabilitati.

Stato protezione

Il campo Stato di protezione visualizza i singoli stati Protetto (indicato da un segno di spunta verde) o Vulnerabile (indicato da una X rossa) a seconda che i seguenti criteri siano attivati (abilitati) o meno nel Dell Server:

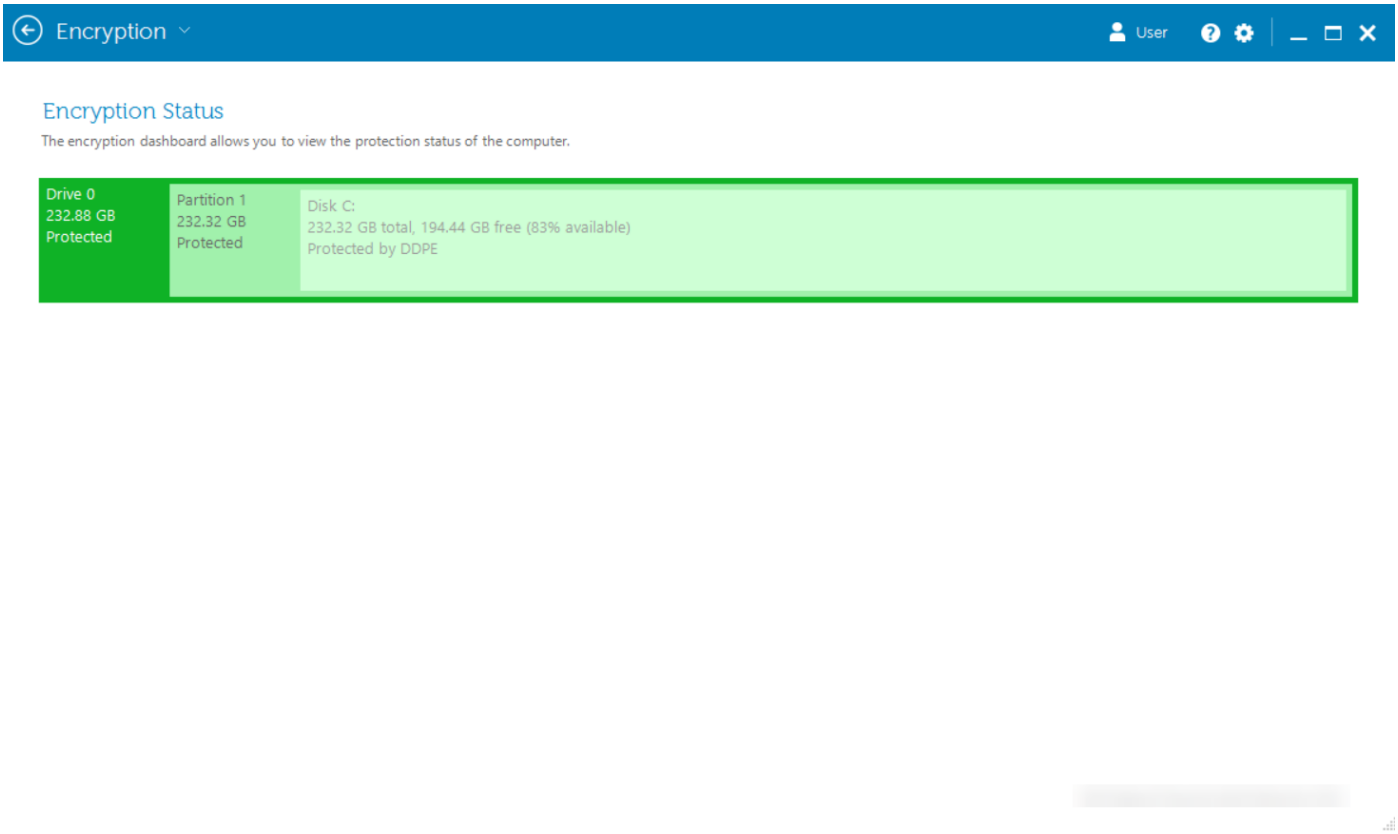
- Firewall Client - Lo stato complessivo è Protetto se il criterio *Firewall client* è abilitato.
- Protezione Web - Lo stato complessivo è Protetto se il criterio *Protezione Web* è abilitato.

4

Stato crittografia

La pagina Crittografia mostra lo stato di crittografia del computer. Se un disco, un'unità o una partizione non è crittografato il suo stato risulterà *Non protetto*. Un'unità o partizione crittografata mostra lo stato *Protetto*.

Per aggiornare lo stato di crittografia, fare clic con il pulsante destro del mouse sul disco, sull'unità o sulla partizione appropriati, quindi su **Aggiorna**.



5

Sign-in Access

Lo strumento Sign-in Access consente di registrare, modificare e controllare lo stato della registrazione in base al criterio impostato dall'amministratore.

In seguito alla registrazione iniziale, è possibile fare clic sul riquadro Sign-in Access per aggiungere o modificare le credenziali.

N.B.: Il riquadro Sign-in Access viene visualizzato solo se la PBA è attiva.

Prima registrazione delle credenziali

Per registrare le credenziali per la prima volta:

1. Dalla pagina iniziare Data Security Console, fare clic sul riquadro **Sign-In Access**.
2. Per modificare la password di Windows, nella pagina Password inserire la password corrente, inserire e confermare una nuova password e fare clic su **Modifica**.
3. Nella pagina Domande di ripristino, selezionare e fornire le risposte per almeno tre domande di ripristino, quindi fare clic su **Registra**.

Per informazioni più dettagliate sulla registrazione o sulla modifica di una credenziale, consultare la sezione Aggiunta, modifica o visualizzazione delle registrazioni.

Aggiunta, modifica o visualizzazione delle registrazioni

Per aggiungere, modificare o visualizzare le registrazioni, fare clic sul riquadro **Sign-In Access**.

Le schede nel riquadro a sinistra forniscono un elenco delle registrazioni disponibili. Queste variano in base alla piattaforma o al tipo di hardware.

La pagina Sign-In Access mostra le credenziali supportate, le impostazioni dei criteri (Richiesto o ND) e il loro stato di registrazione. Da questa pagina gli utenti possono gestire le proprie registrazioni, in base al criterio stabilito dall'amministratore:

- Per registrare una credenziale per la prima volta, sulla riga della credenziale, fare clic su **Registra**.
- Per eliminare una credenziale registrata esistente, fare clic su **Elimina**.
- Se il criterio non consente agli utenti di registrare o modificare le proprie credenziali, i collegamenti **Registra** e **Elimina** sulla pagina dello stato risultano inattivi.
- Per modificare una registrazione esistente, fare clic sulla scheda appropriata nel riquadro a sinistra.

  Se il criterio non consente la registrazione o la modifica di una credenziale, nella pagina di registrazione delle credenziali viene visualizzato un messaggio per informare che la modifica delle credenziali non è consentita dal criterio.

Password

Per modificare la password di Windows:

1. Fare clic sulla scheda **Password**.
2. Inserire la password di Windows in uso.
3. Immettere la nuova password e riscriverla per confermarla, quindi fare clic su **Cambia**.

   Le modifiche della password sono immediatamente valide.

4. Nella finestra di dialogo Registrazione completata, fare clic su **OK**.

N.B.:

Le password di Windows si dovrebbero modificare solo nella Data Security Console, piuttosto che in Windows. Se si modifica la password di Windows fuori dalla Data Security Console, potrebbe verificarsi un problema di password non corrispondente, che richiede un'operazione di ripristino.

Domande di ripristino

La pagina Domande di ripristino consente di creare, eliminare o modificare le domande e le risposte di ripristino. Le domande di ripristino forniscono un metodo basato su domanda e risposta degli utenti per accedere ai rispettivi account di Windows se, ad esempio, la password è scaduta o è stata dimenticata.

N.B.:

Si utilizzano le domande di ripristino solo per recuperare l'accesso ad un computer. Le domande e le risposte non possono essere usate per l'accesso.

Se non è stata registrata nessuna domanda di ripristino PBA precedente:

1. Fare clic sulla scheda **Domande di ripristino**.
2. Selezionare una domanda da un elenco di domande predefinite, quindi inserire e confermare la risposta.
3. Fare clic su **Registra**.

N.B.:

Fare clic su **Reimposta** per eliminare le selezioni della pagina e ricominciare.

Domande di ripristino già registrate

Se le domande di ripristino PBA sono già state registrate, è possibile eliminarle o registrarle nuovamente.

1. Fare clic sulla scheda **Domande di ripristino**.
2. Fare clic sul pulsante appropriato:
   - Per rimuovere completamente le domande di ripristino PBA, fare clic su **Elimina**.
   - Per ridefinire le domande di ripristino PBA e le rispettive risposte, fare clic su **Ripeti registrazione**.

6

Glossario

Credenziale: una credenziale è un elemento che prova l'identità di una persona, come ad esempio la relativa password Windows.

Autenticazione di preavvio (PBA, Preboot Authentication) – L'Autenticazione di preavvio funge da estensione del BIOS o del firmware di avvio e garantisce un ambiente sicuro e a prova di manomissione, esterno al sistema operativo come livello di autenticazione affidabile. La PBA impedisce la lettura di qualsiasi informazione dal disco rigido, come il sistema operativo, finché l'utente non dimostra di possedere le credenziali corrette.

Protetto - Per un'unità autocrittografante (SED), un computer è protetto se è stata attivata l'unità SED e se è stata implementata l'autenticazione di pre-avvio (PBA).

Unità autocrittografanti (SED, Self-Encrypting Drive) - Disco rigido che dispone di un meccanismo di crittografia incorporato che crittografa tutti i dati archiviati nei supporti e decrittografa automaticamente tutti i dati in uscita dai supporti. Questo tipo di crittografia è completamente noto all'utente.

Single Sign-On (SSO) - Il SSO semplifica la procedura di accesso quando è abilitata l'autenticazione a più fattori sia a livello di preavvio che di accesso a Windows. Se abilitato, l'autenticazione verrà richiesta al solo preavvio e gli utenti accederanno automaticamente a Windows. Se è disabilitato, l'autenticazione potrebbe essere richiesta più volte.

Trusted Platform Module (TPM) - Il TPM è un chip di protezione che svolge tre funzioni principali: archiviazione protetta, misurazioni e attestazione. Il client di crittografia utilizza il TPM per la sua funzione di archiviazione protetta. Il TPM è inoltre in grado di fornire contenitori crittografati per l'insieme di credenziali del software.