Guida per l'utente della console Dell Data Protection

Threat Protection/Encryption Status/Authentication Enrollment/Password Manager v1.7

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 indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

Guida per l'utente della console Dell Data Protection

2017 - 04

Rev. A01

Sommario

1

Introduzione alla console DDP

Dell Data Protection | Endpoint Security Suite fornisce strumenti semplici ed intuitivi per aumentare la protezione del computer.

Le funzioni seguenti sono disponibili tramite la DDP Console nel sistema operativo di una workstation:

- Registrazione delle credenziali per l'uso con Endpoint Security Suite
- Utilizzo di credenziali a più fattori, comprese password, impronte e smart card
- Ripristino dell'accesso al computer in caso si sia dimenticata la password senza rivolgersi all'helpdesk o all'amministratore
- Backup e ripristino dei dati dei programmi
- Modifica facile della password di Windows
- Impostazione delle preferenze personali
- Visualizzazione dello stato di crittografia (sui computer con unità autocrittografanti)

  Visualizzazione dello stato di Threat Protection

DDP Console

La console DDP è l'interfaccia attraverso cui è possibile effettuare la registrazione, gestire le credenziali e configurare le domande di ripristino automatico.

È possibile accedere a queste applicazioni:

- La dashboard di Threat Protection consente di visualizzare lo stato di protezione del computer, sulla base dei criteri di Threat Protection.Lo strumento Encryption Status consente di visualizzare lo stato di crittografia relativo alle unità del computer.
- Lo strumento Registrazioni consente all'utente di impostare e gestire le credenziali, configurare le domande di ripristino automatico e visualizzare lo stato di registrazione delle credenziali. La possibilità dell'utente di registrare ogni tipo di credenziale è impostata dall'amministratore.
- Password Manager consente di compilare e inviare automaticamente i dati richiesti per accedere a siti Web, applicazioni Windows e risorse di rete. Inoltre, Password Manager consente di modificare le password di accesso tramite l'applicazione, garantendo la sincronizzazione delle password gestite da Password Manager con quelle della risorsa di destinazione.

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

Per assistenza telefonica sui prodotti Dell Data Protection, chiamare il numero +1-877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell Data Protection 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 servizio per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono esterni agli Stati Uniti, controllare Numeri di telefono internazionali di Dell ProSupport.

2

DDP Console

La console DDP consente di accedere alle applicazioni che garantiscono la sicurezza per tutti gli utenti del computer, visualizzare e gestire lo stato della crittografia relativa alle unità e alle partizioni del computer e, in base ai criteri impostati dall'amministratore, gestire i propri accessi a siti Web, programmi e risorse di rete; infine, consente di registrare facilmente le proprie credenziali di autenticazione.

Per aprire la console DDP, dal *desktop,* fare doppio clic sull'icona della **console DDP**.

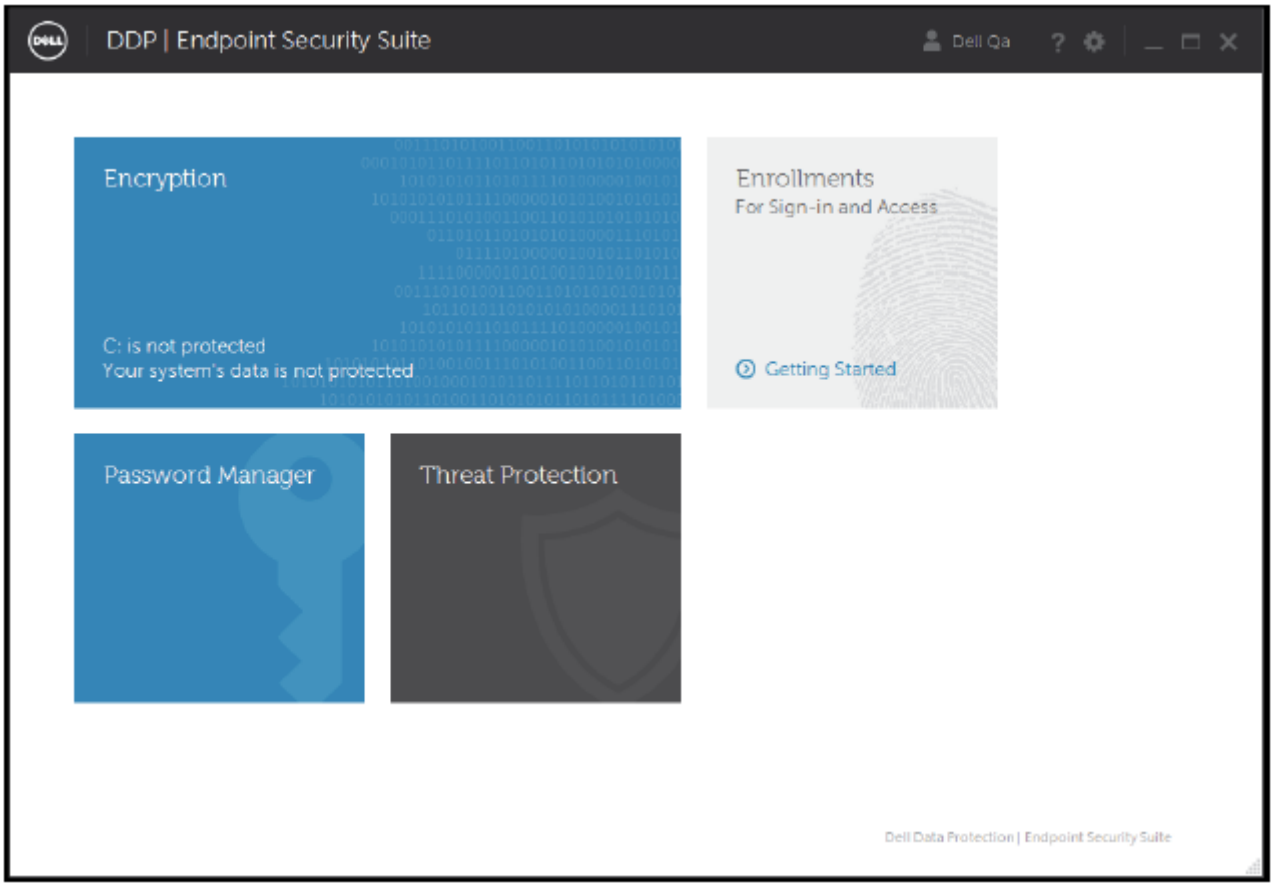
Una volta avviata la console DDP, sulla pagina vengono visualizzate le applicazioni Endpoint Security Suite:

- Threat Protection
- Stato crittografia
- Registrazioni
- Password Manager

  Per impostare le credenziali per la prima volta, selezionare il collegamento **Guida introduttiva** nel riquadro Registrazioni. Una procedura guidata mostra il breve processo di registrazione. Per ulteriori informazioni, vedere Prima registrazione delle credenziali.

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 DDP Console, fare clic sulla relativa icona nell'angolo a destra della barra del titolo.

Per ripristinare la DDP Console dopo averla ridotta a icona, fare doppio clic sull'icona nell'area di notifica.

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

Dettagli della DDP Console

Per visualizzare i dettagli sulla DDP 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.

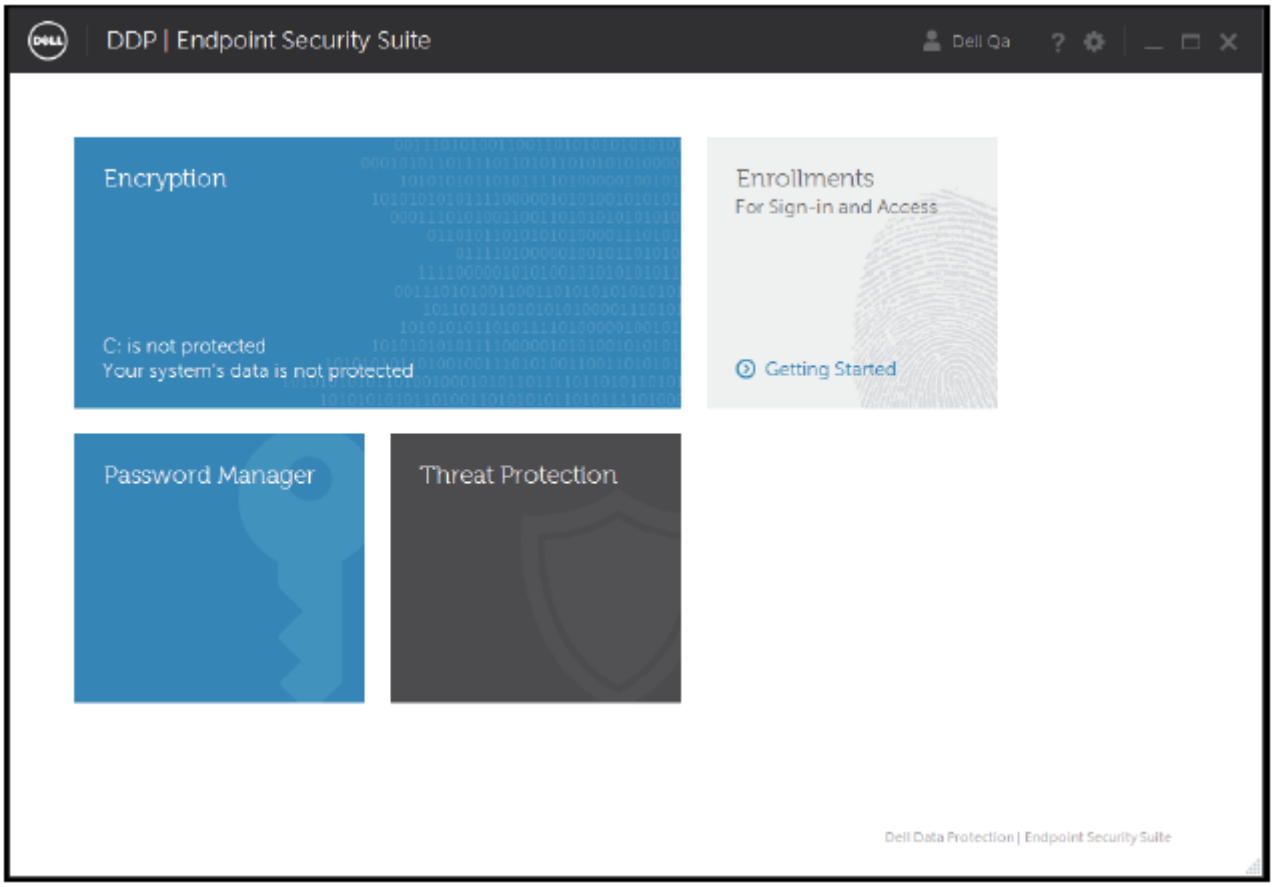
Voce di menu	Scopo
Informazioni su	Contiene informazioni sulla versione e sul copyright.
Mostra informazioni	Contiene: • informazioni sulla versione e sulla data del prodotto • se la DDP Console è gestita in questo computer dall'azienda o da un amministratore locale • numeri di versione del sistema operativo, 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 dai criteri aziendali.
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.
Registro	Visualizza un elenco dettagliato degli eventi registrati per la risoluzione dei problemi.
Avvia tracciamento	Consente di avviare e arrestare una registrazione delle attività di accesso per la risoluzione dei problemi.

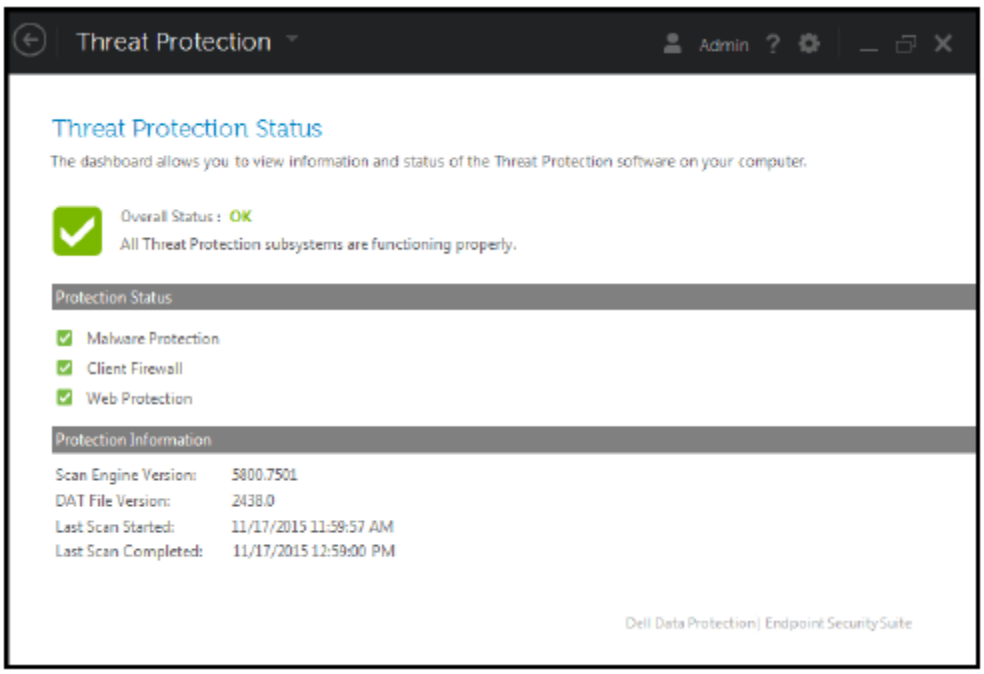
3

Threat Protection

Dashboard di Threat Protection

Gli utenti possono accedere alla dashboard dello Stato di Threat Protection attraverso il riquadro Threat Protection nella DDP Console.





- Protetto - Lo stato complessivo è protetto se i criteri *Protezione accesso*, *Protezione da exploit* e **Protezione all'accesso** sono impostati su Vero (abilitato).

  Oppure

  Il criterio *Protezione su richiesta - Scansione completa* o *Protezione su richiesta - Scansione rapida* è impostato su Vero (abilitato) e i criteri di pianificazione corrispondenti sono impostati.

- Vulnerabile - Lo stato complessivo è vulnerabile se uno dei seguenti criteri è impostato su Falso (disabilitato): *Protezione accesso*, *Protezione da exploit* e **Protezione all'accesso**.

  e

  I criteri *Protezione su richiesta - Scansione completa* o *Protezione su richiesta - Scansione rapida* sono impostati su Falso (disabilitato) o Vero (abilitato) senza aver impostato i criteri di pianificazione corrispondenti.

  Stato di 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 principali siano impostati o no sul valore Vero (abilitato):

- Protezione malware
- Firewall client
- Protezione Web

  Informazioni sulla protezione

  Il campo Informazioni sulla protezione fornisce le seguenti informazioni:

- Versione motore di analisi - La versione del motore di analisi usato. Il motore di analisi confronta i contenuti dei file scansionati con le minacce note.
- Versione file DAT - La versione del file DAT di Threat Protection che il motore usa per rilevare il malware durante una scansione.
- Ultima scansione avviata - Timestamp che indica quando è stata avviata l'ultima scansione riuscita.
- Ultima scansione completata - Timestamp che indica quando è stata completata l'ultima scansione.

  Menu Ingranaggio

  Il menu Ingranaggio fornisce l'accesso a:

- Informazioni su - Fornisce informazioni sulla versione di Endpoint Security Suite e sulla configurazione del computer client.
- Criteri: elenca molti criteri dell'agente. Attualmente, poiché troppo numerosi, non elenca i criteri di Threat Protection.
- Servizi - Visualizza lo stato di AntiMalware Management Plugin e la comunicazione con Dell Management Agent.
- Feedback - Fornisce un collegamento al sito Web del supporto Dell.
- Registri - Visualizza gli eventi relativi ai servizi, tra cui AntiMalware Management Plugin.
- Avvia tracciamento - Consente di avviare e arrestare una registrazione delle attività di sistema per la risoluzione dei problemi.

Notifiche popup

In base al criterio, le notifiche popup possono informare l'utente in merito a minacce che interessano:

- file e cartelle
- registro di sistema
- Processi di Endpoint Security Suite
- siti Web non verificati o dannosi
- pagine phishing

  L'utente **non** deve eseguire alcuna operazione. Tutte le correzioni saranno gestite da Endpoint Security Suite.

  Elimina notifiche popup

  Per eliminare i messaggi che avvisano l'utente di minacce, impostare la seguente chiave di Registro di sistema:

  [HKLM\Software\Dell\Dell Data Protection]

  "DDPTPHideToasters"=dword:1

  0=(Impostazione predefinita) Disabilitata, non nasconde le notifiche popup all'utente

  1=Abilitata, nasconde le notifiche popup all'utente

Filtrare le notifiche popup

Per visualizzare le notifiche di livello di gravità minimo, impostare questa chiave di registro:

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPEventSeverityFilter"=dword:3

0=Informazioni (visualizza tutti gli eventi), 1=Avviso, 2=Secondarie, 3=Principali (predefinita, mostra solo Principali e Critiche), 4=Critiche

Se "DDPTPHideToasters" è impostato su 1, le impostazioni di "DDPTPEventSeverityFilter" vengono ignorate.

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

Registrazioni

Lo strumento Registrazioni consente di registrare, modificare e controllare lo stato della registrazione in base ai criteri impostati dall'amministratore.

La prima volta che l'utente registra le proprie credenziali con la DDP Console, una procedura guidata mostra come registrare la modifica della password, le domande di ripristino, le impronte digitali, il dispositivo mobile e la smart card. A seconda del criterio, è possibile registrare o ignorare alcune credenziali. In seguito alla registrazione iniziale, è possibile fare clic sul riquadro Registrazione per aggiungere o modificare le credenziali.

Prima registrazione delle credenziali

Per registrare le credenziali per la prima volta:

1 Nella pagina iniziale della console DDP, fare clic sul collegamento **Guida introduttiva** nel riquadro Registrazioni.
2 Nella pagina iniziale, fare clic su **Avanti**.
3 Nella finestra di dialogo Autenticazione richiesta, eseguire l'accesso utilizzando la password di Windows, quindi fare clic su **OK**.
4 Per modificare la password di Windows, nella pagina Password, inserire e confermare una nuova password, quindi fare clic su **Avanti**.
Se non si desidera modificare la password, fare clic su **Ignora**. La procedura guidata consente di ignorare una credenziale se non si desidera registrarla. Per tornare a una data pagina, fare clic su **Indietro**.
5 Seguire le istruzioni presenti in ogni pagina e fare clic sul pulsante appropriato: **Avanti**, **Ignora** o **Indietro**.
6 Nella pagina Riepilogo, confermare le credenziali registrate e, al termine della registrazione, fare clic su **Applica**.
Per tornare alla pagina di registrazione di una credenziale per apportare modifiche, fare clic su **Indietro** fino a raggiungere la pagina che si desidera modificare.

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 **Registrazioni**.

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 Stato 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 console DDP, piuttosto che in Windows. Se si modifica la password di Windows fuori dalla console DDP, 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 alcuna domanda di ripristino:

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 sul pulsante **Reimposta** per eliminare le selezioni della pagina e ricominciare.

Domande di ripristino già registrate

Se le domande di ripristino sono già state registrate, è possibile eliminarle o registrare nuove domande di ripristino.

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

Impronte

N.B.:
Per accedere a questa funzione, il computer deve essere dotato di un lettore di impronte digitali.

Per registrare le impronte digitali, attenersi alle seguenti istruzioni:

1 Fare clic sulla scheda **Impronte digitali**.
2 Nella pagina Impronte digitali, fare clic sul dito che si desidera registrare.
3 Per registrare le impronte, seguire le istruzioni visualizzate.

N.B.:
Per essere registrata, l'impronta del dito dovrà essere scansionata correttamente quattro volte. Il numero di scansioni necessarie per completare la registrazione delle impronte digitali dipende dalla qualità di ciascun rilevamento. L'amministratore ha definito il numero massimo e minimo di impronte digitali.

4 Fare clic su ogni dito in modo sequenziale per eseguire la scansione fino a raggiungere il numero minimo di impronte richiesto dal criterio.
Una finestra di dialogo informa se non è stato registrato il numero minimo di impronte. Fare clic su **OK** per continuare.
5 Completare la scansione del numero di impronte necessario e fare clic su **Salva**.
Per eliminare un'impronta sottoposta a scansione, nella pagina di registrazione delle impronte digitali, fare clic su un'impronta digitale evidenziata per annullarne la registrazione, fare clic su **Sì**, quindi fare clic su **Salva**.

Dispositivo mobile

La registrazione di un dispositivo mobile prevede l'uso della funzione Password monouso. L'OTP permette all'utente di accedere a Windows tramite una password generata dall'app Security Tools Mobile su un dispositivo mobile associato al computer. In alternativa, solo se consentito dai criteri, la funzione OTP può essere utilizzata per ripristinare l'accesso al computer in caso di password scaduta o dimenticata.

N.B.:
Se la scheda Dispositivo mobile non viene visualizzata nella console DDP, significa che la configurazione del computer non supporta questo metodo oppure un criterio impostato dall'amministratore non lo consente.

N.B.:
Le impostazioni dei criteri definiscono la modalità di utilizzo della funzione OTP, per l'accesso oppure per il ripristino dell'accesso al computer in caso di password scaduta o dimenticata. Non è possibile utilizzare la funzione OTP per entrambi gli scopi.

Per poter utilizzare la funzione OTP è necessario registrare o associare il proprio dispositivo mobile al computer. In caso di computer utilizzato da più utenti ciascuno di questi potrà registrare un dispositivo mobile con il computer. I dispositivi mobili possono essere registrati con più computer.

Se un dispositivo mobile è stato già registrato, la registrazione di un nuovo dispositivo annulla automaticamente l'associazione del dispositivo precedente.

Registrazione del dispositivo mobile

1 Nella pagina Registrazioni della console DDP, fare clic sulla scheda **Dispositivo mobile**.
2 In alto a destra, fare clic su **Registra**.
Si apre la pagina Registra password monouso.
3 Se questo è il primo computer da associare, selezionare **Sì**.

a Scaricare l'app Dell Data Protection | Security Tools Mobile dall'app store nel dispositivo mobile.
b Sul computer, fare clic su **Avanti**.

Impostare Security Tools Mobile

1 Aprire l'app Security Tools Mobile.

2 Creare ed inserire un PIN per accedere all'app Security Tools Mobile.

> **N.B.:**
> Il PIN può essere richiesto dal criterio quando il dispositivo mobile non è bloccato. Se per lo sblocco del dispositivo mobile non si utilizza un PIN, ne verrà richiesto uno per l'accesso all'app Security Tools Mobile.

3 Selezionare **Registra un computer**. (se necessario, toccare l'angolo superiore sinistro dello schermo del dispositivo mobile per accedere ai comandi).

Verrà visualizzato un codice nel dispositivo mobile. La lunghezza del codice e la combinazione alfanumerica sono stabilite in base al criterio impostato dall'amministratore.

Associare il dispositivo mobile al computer

1 Nel computer, nella pagina Codice mobile della DDP Console:

a Inserire nel campo il codice visualizzato nel dispositivo mobile.

b Fare clic su **Avanti**.

c Nella pagina Associa dispositivo selezionare una tra:

Codice QR - Viene visualizzato un codice QR.

Oppure

Inserimento manuale - Viene visualizzato un codice di associazione di 24 cifre.

2 Nel dispositivo mobile:

a Toccare **Associa dispositivi**.

b Selezionare la stessa opzione di associazione, **Scansione codice QR** o **Inserimento manuale**, che è stata selezionata sul computer.

c Selezionare un'opzione:

- Per il **codice QR**, posizionare il dispositivo mobile davanti allo schermo del computer in modo da consentire la scansione del codice QR.

  Annotare il codice numerico di verifica visualizzato sul dispositivo mobile e toccare **Avanti**.

  > **N.B.:**
  > Se viene visualizzata la barra *Problemi di scansione?*, riprovare oppure selezionare l'opzione **Inserimento manuale**.

- Per l'**inserimento manuale**, inserire il codice di associazione di 24 cifre dal computer e toccare **Operazione completata**.

  Annotare il codice numerico di verifica visualizzato sul dispositivo mobile e toccare **Avanti**.

3 Nel computer, nella DDP Console:

a Fare clic su **Avanti**.

b Immettere il codice di verifica visualizzato nel dispositivo mobile e fare clic su **Avanti**.

c Modificare il nome del dispositivo mobile (facoltativo).

d Fare clic su **Applica**.

I dispositivi sono associati.

4 Nel dispositivo mobile:

a Toccare **Continua**.

b Modificare il nome del computer (facoltativo) e toccare **Operazione completata**.

c Toccare **Fine**.

Registrare un altro dispositivo mobile

La registrazione di un nuovo dispositivo annulla automaticamente l'associazione del dispositivo precedente. Non è richiesta una procedura separata per annullare l'associazione.

Annullare l'associazione tra computer e dispositivo mobile

Per annullare l'associazione di un computer e un dispositivo mobile senza registrare un altro dispositivo, selezionare una delle seguenti opzioni:

- Nella console DDP, nella pagina Stato registrazioni, accanto alla credenziale del dispositivo mobile, fare clic su **Elimina**.
- Sul dispositivo mobile, consultare la procedura descritta di seguito.

1 Sul dispositivo mobile, completare i passaggi seguenti:
   a Avviare l'app Security Tools Mobile.
   b In alto a sinistra, toccare la barra del menu per aprire il drawer.
   c Toccare **Rimuovi computer**.
   d Selezionare il computer per cui annullare l'associazione.
   e Selezionare **Rimuovi** (Android) o toccare **Operazione completata** (iOS).
   Appare un messaggio di avvenuta dissociazione.
   f Selezionare **Rimuovi tutti** per rimuovere tutti i computer registrati dal dispositivo.
   L'opzione Rimuovi tutti compare quando si rimuovono più computer e quando si rimuove l'unico computer associato.

   - Selezionare **Ripristina impostazioni predefinite** per rimuovere il computer registrato e il PIN. Se si ripristinano le impostazioni predefinite, verranno rimossi tutti i computer registrati e il PIN utilizzato per accedere all'applicazione Security Tools Mobile.
   - Selezionare **Annulla** per lasciare il computer registrato.

Accesso con password monouso

N.B.:
L'autenticazione tramite OTP può essere utilizzata solo per accessi Windows.

La funzione OTP può essere utilizzata per il ripristino, cioè per ottenere nuovamente l'accesso a un computer dal quale si è stati bloccati, o per l'accesso Windows. Tuttavia, la funzione non può essere utilizzata per entrambi gli scopi.

Se consentito da un criterio, e se il simbolo OTP  viene visualizzato sulla schermata di accesso, è possibile accedere a Windows con l'OTP.

Per accedere, selezionare una delle seguenti operazioni:

1 Dal computer, nella schermata di accesso di Windows, selezionare l'icona OTP  .
2 Nel dispositivo mobile, aprire l'app Security Tools Mobile e inserire il PIN.
3 Selezionare il computer a cui si desidera accedere.
   Se il nome del computer non viene visualizzato nel dispositivo mobile, potrebbe sussistere una di queste condizioni:

   - Il dispositivo mobile non è registrato o associato al computer al quale si tenta di accedere.
   - Se l'utente possiede più di un account utente di Windows, Endpoint Security Suite non è installato nel computer al quale si sta cercando di accedere o si sta tentando di accedere a un account utente differente da quello utilizzato per associare il computer al dispositivo mobile.

4 Toccare **Password monouso.**
Viene visualizzata una password nella schermata del dispositivo mobile.

N.B.:

Se necessario, fare clic sul simbolo Aggiorna  per ottenere un nuovo codice. Dopo i primi due aggiornamenti dell'OTP, dovranno trascorrere trenta secondi prima di poter generare un'altra OTP.

Il computer e il dispositivo mobile devono essere sincronizzati in modo da poter riconoscere la stessa password nello stesso momento. Se si tenta di generare rapidamente una password dopo l'altra, il computer e il dispositivo mobile non riusciranno a sincronizzarsi e di conseguenza non sarà possibile utilizzare la funzione OTP. In tal caso, attendere per trenta secondi in modo che i due dispositivi possano nuovamente sincronizzarsi, quindi riprovare.

5 Dal computer, nella schermata di accesso di Windows, digitare la password visualizzata nel dispositivo mobile e premere **Invio**.
Se la funzione OTP è stata utilizzata per il ripristino, dopo aver ottenuto l'accesso al computer, seguire le istruzioni visualizzate per reimpostare la password.

Attività di gestione di Security Tools Mobile

Queste attività vengono eseguite utilizzando l'app Security Tools Mobile nel dispositivo mobile.

Reimpostare il PIN dell'app Security Tools Mobile

Per reimpostare il PIN dell'app Security Tools Mobile:

1 Toccare le opzioni del menu in alto a destra.
2 Selezionare **Reimposta PIN**.
3 Immettere e confermare il nuovo PIN.

Disinstallare l'app Security Tools Mobile

Nel dispositivo mobile:

1 Annullare l'associazione fra il dispositivo e il computer.
2 Eliminare o disinstallare l'app Security Tools Mobile nel modo in cui si eliminerebbe normalmente un'app dal dispositivo mobile.

Smart card

N.B.:
Per poter accedere a questa funzione, è necessario che il computer sia dotato di un lettore di smart card.

Per registrare le smart card, attenersi alle seguenti istruzioni:

1 Fare clic sulla scheda **Smart card** .
2 Registrare la smart card, in base al tipo di scheda:
- Inserire la smart card nel lettore di schede.
- In caso di scheda senza contatto, collocare e mantenere la scheda sopra o accanto al lettore.

3 Quando la scheda viene rilevata, vengono visualizzati una casella di controllo verde e il messaggio *Registra la smart card*. Selezionare **Registrare la smart card**.
4 Nella finestra di dialogo Registrazione completata, fare clic su **OK**.

Per annullare la registrazione di tutte le smart card associate a un utente, nella pagina di registrazione della smart card, selezionare **Rimuovi smart card registrate dall'account**.

6

Password Manager

Password Manager consente di accedere automaticamente a siti Web, programmi Windows e risorse di rete, e consente di gestire le credenziali di accesso con un unico strumento. Inoltre, Password Manager consente agli utenti di modificare le password di accesso tramite l'applicazione, garantendo la sincronizzazione delle password gestite da Password Manager con quelle delle risorse di destinazione.

Password Manager è supportato da Internet Explorer e da Mozilla Firefox. Password Manager non è supportato dagli account Microsoft (precedentemente Windows Live ID).

N.B.:
Se si esegue Password Manager in Firefox, è necessario installare e registrare l'estensione di Password Manager. Per istruzioni sull'installazione delle estensioni in Mozilla Firefox, consultare https://support.mozilla.org/.

N.B.:
L'uso delle icone di Password Manager (icone di pre-addestramento e addestramento) in Mozilla Firefox è diverso dall'uso in Microsoft Internet Explorer:

- La funzione di doppio clic sulle icone di Password Manager non è disponibile.
- L'azione predefinita non è mostrata in grassetto nel menu di scelta rapida a discesa.
- Se una pagina contiene più moduli di accesso, è possibile visualizzare più di un'icona di Password Manager.

N.B.:
A causa della struttura in continua evoluzione delle pagine di accesso Web, Password Manager potrebbe non supportare tutti i siti Web.

Guida introduttiva a Password Manager

Password Manager raccoglie e archivia le credenziali di accesso man mano che si lavora. È possibile iniziare a utilizzare Password Manager immediatamente dopo aver installato Endpoint Security Suite. Quando si immettono le credenziali in una pagina di accesso, Password Manager rileva il

modulo di accesso e consente di scegliere se si desidera consentire a Password Manager di salvare le credenziali.

Sono disponibili tre opzioni:

- Fare clic su **Salva Accesso** per memorizzare le credenziali di accesso in Password Manager.
- Se ***non*** si desidera salvare le credenziali di accesso, ogni volta che si accede al sito Web o al programma, verrà richiesto se si desidera salvare le credenziali di accesso. Se si preferisce non visualizzare più questa richiesta, selezionare **Mai per questo sito**. Nell'elenco delle Esclusioni siti Web sarà creato un record. Vedere Escludere di siti Web per ulteriori dettagli.
- Se non si desidera salvare le credenziali, fare clic su **Non salvare accesso**.

Questa finestra di dialogo viene visualizzata anche se l'utente ha precedentemente salvato le credenziali per un sito Web o un programma, ma inserisce un diverso nome utente e password. Con un nuovo nome utente, se si seleziona **Salva accesso**, viene memorizzato un nuovo set di credenziali. Con il nome utente e la nuova password precedentemente salvati, se si seleziona **Salva accesso**, le credenziali originali vengono aggiornate con la nuova password.

Gestione degli accessi

Logon Manager semplifica e centralizza la gestione di tutti gli accessi ai siti Web, ai programmi Windows e alle risorse di rete.

Per aprire Logon Manager:

1 Nella pagina iniziale della console DDP, fare clic sul riquadro **Password Manager**.
2 Fare clic sulla scheda **Logon Manager**.

È possibile aggiungere accessi e categorie, nonché ordinarli e filtrarli:

Aggiungi accesso - Consente di aggiungere un nuovo set di credenziali di accesso. In base al criterio, per poter aggiungere una credenziale di accesso, potrebbe essere richiesto di immettere le credenziali memorizzate in .

Aggiungi categoria - Consente di aggiungere una nuova categoria (come e-mail, storage, notizie, risorse aziendali, social media) a scopo di ordinamento e filtraggio.

Ordina: consente di ordinare gli accessi per account, nome utente o categoria. Fare clic su un'intestazione di colonna per ordinare in base alla colonna.

Filtra: consente di selezionare una categoria dall'elenco *Visualizza* per visualizzare tutte le credenziali di accesso, ad eccezione di quelle presenti nella categoria selezionata. Per rimuovere il filtro, selezionare *Tutto*.

È possibile gestire gli accessi:

Avvia - Apre il sito Web o il programma e trasmette le credenziali di accesso in base alle impostazioni stabilite dall'utente.

Modifica - Consente all'utente di modificare i dati di accesso archiviati di un sito Web o di un programma.

Elimina - Consente all'utente di rimuovere da Password Manager i dati di accesso archiviati.

Aggiungi - Consente all'utente di aggiungere una nuova credenziale di accesso, una nuova categoria o nuovi dati di accesso.

Aggiunta della categoria

Prima di aggiungere gli accessi, creare le categorie (quali E-mail, Archiviazione, News, Risorse aziendali e Social Media) in modo da classificare gli accessi man mano che vengono creati. In tal modo sarà possibile ordinare e filtrare gli accessi per categoria.

Per aggiungere una categoria, nella pagina Logon Manager, fare clic su **Aggiungi categoria**, digitare un nome della categoria, quindi fare clic su **Salva**.

Aggiunta degli accessi

1 Nella pagina Logon Manager, fare clic su **Aggiungi accesso**.
In base al criterio impostato, per poter aggiungere un accesso è possibile che all'utente venga richiesto di eseguire l'autenticazione.
2 Aprire il sito Web o il programma a cui accedere.
3 Nella finestra di dialogo Aggiungi accesso, fare clic su **Continua**.
4 Nella finestra di dialogo successiva, inserire:
- **Categoria** - È possibile scegliere una categoria per l'accesso al sito Web o al programma che si sta memorizzando. Se non sono state aggiunte categorie questo elenco risulterà vuoto.
- **Nome account** - Lasciare così com'è per accettare il nome pre-compilato o digitare il nome del sito Web o del programma.
- **Titolo non rilevato** - Questi campi vengono rilevati da Password Manager come campi della pagina di accesso in cui è possibile inserire le informazioni di accesso. Questi campi generalmente comprendono Nome utente o E-mail, e Password.

5 Se il nome di un campo viene visualizzato come Titolo non rilevato o se sono stati inclusi i campi sbagliati come campi di accesso, fare clic sul pulsante **Altri campi** per modificare i nomi dei campi o per rimuoverli.

6 Nella finestra Altri campi, fare clic su **Titolo non rilevato** e immettere il nome corretto per ciascun campo.

Quando appare la finestra di dialogo Più campi, il campo che risultava attivo nella finestra di dialogo Aggiungi accesso viene evidenziato, al fine di aiutare l'utente a rinominare i campi.

Se un campo è inutile ai fini dell'accesso, per escluderlo dalle informazioni di accesso deselezionare la relativa casella di controllo.

7 Per salvare le modifiche, fare clic su **OK**.

8 Nella finestra di dialogo Aggiungi accesso, compilare i campi necessari per l'accesso.

> **N.B.:**
> Dato che si sta memorizzando un accesso esistente, la password può essere modificata solo attraverso la funzione Modifica password del sito Web o del programma.

9 Se si desidera che Password Manager compili e trasmetta automaticamente le informazioni di accesso, selezionare **Invia automaticamente i dati di accesso**.

10 Fare clic su **Salva**.

Nella pagina Logon Manager viene visualizzato l'accesso al sito Web o al programma.

Importare credenziali

È possibile importare in Password Manager le credenziali archiviate nei browser Web.

1 Nello strumento Password Manager, selezionare **Importa credenziali**.

2 Selezionare il browser da importare e fare clic su **Scansiona**.

3 Quando richiesto, immettere la password per il browser selezionato.

> **N.B.:**
> se l'importazione non riesce, verificare che il browser abbia dati memorizzati da importare. Se si utilizza Firefox, accedere a Sync. Eseguire un nuovo tentativo di importazione delle credenziali.

Menu di scelta rapida dell'icona

Quando si visita un sito Web o un programma, viene visualizzata l'icona di Password Manager.

Il simbolo  indica che il modulo di accesso può essere addestrato.

Se il simbolo  non è presente, significa che il modulo di accesso è già stato addestrato. Fare doppio clic sull'icona per accedere al programma o al sito Web.

Quando si fa clic sull'icona un menu di scelta rapida mostra diverse opzioni, a seconda che il modulo sia addestrato o no.

Se i campi di accesso correnti non sono ancora addestrati, il menu di scelta rapida mostra le seguenti opzioni:

Aggiungi a Password Manager - Consente di aprire la finestra di dialogo Aggiungi accesso.

Impostazioni icona- Permette all'utente di configurare la visualizzazione dell'icona di Password Manager nelle pagine di accesso addestrabili.

Apri Password Manager - Avvia lo strumento *Password Manager Administration* e apre la pagina Logon Manager.

Guida - Consente di aprire la guida online.

Se i campi di accesso correnti sono addestrati, il menu di scelta rapida mostra le seguenti opzioni:

Inserisci dati di accesso - A seconda delle selezioni effettuate durante l'addestramento del modulo di accesso, consente di accedere o inserire automaticamente nome utente e password per inviare i dati di accesso.

Modifica accesso - Consente di aprire la finestra di dialogo corrispondente.

Aggiungi accesso - Consente di aprire la finestra di dialogo corrispondente.

Apri Password Manager - Consente di aprire la pagina Logon Manager.

Guida - Consente di aprire la guida online.

Se le icone di Password Manager non vengono visualizzate con i moduli di accesso, disattivare la funzione di salvataggio password del browser:

- In Mozilla Firefox: icona menu > Opzioni > Sicurezza > deselezionare la casella di controllo **Ricorda le password dei siti**
- In Internet Explorer: icona ingranaggio > Opzioni Internet > scheda Contenuto > Impostazioni di Completamento automatico > deselezionare la casella di controllo **Nome utente e password sui moduli**

Accedere alle pagine di accesso addestrate

Quando l'utente apre l'accesso a un sito Web o a un programma, Password Manager rileva se la pagina è addestrata. In tal caso, nell'area di accesso appare l'icona di Password Manager. Se la pagina non è addestrata, viene visualizzata l'icona di Password Manager, a meno che non siano stati disabilitati i prompt per i moduli non addestrati.

Per accedere, selezionare una delle seguenti operazioni:

- Eseguire la scansione delle credenziali registrate. Un utente con una smart card o impronte digitali registrate può toccare il lettore di impronte con un'impronta registrata o presentare una scheda registrata al lettore di schede.
- Fare clic sull'icona di Password Manager e selezionare **Inserisci dati di accesso** dal menu di scelta rapida.
- Premere la combinazione di tasti di scelta rapida di Password Manager: **Ctrl+Win+H**. Il pop-up di Password Manager presenta i siti addestrati in un pop-up, consentendone l'avvio rapido.

N.B.:
La combinazione di tasti di scelta rapida può essere modificata in DDP Console > Password Manager > Impostazioni.

Se è stato salvato più di un accesso al sito o al programma, verrà richiesto di scegliere l'account da utilizzare.

Supporto dei domini Web

Se è stata addestrata una pagina di accesso per uno specifico dominio web, ma si desidera accedere all'account in quel dominio Web da un'altra pagina di accesso, passare alla nuova pagina di accesso. Un messaggio richiederà all'utente se desidera usare un accesso esistente o preferisce aggiungerne uno nuovo a Password Manager.

- Se si fa clic su *Usa accesso*, viene effettuato l'accesso all'account creato in precedenza. La volta successiva che l'utente accederà allo stesso account dalla nuova pagina, l'accesso avverrà automaticamente all'account creato in precedenza.
- Se si fa clic su *Aggiungi accesso*, viene visualizzata la finestra di dialogo Aggiungi accesso.

Inserire le credenziali di Windows

Alcuni programmi consentono l'uso delle credenziali Windows per l'accesso.

Anziché digitare il nome utente e la password, è possibile selezionare le credenziali di Windows dai menu a discesa disponibili nelle finestre di dialogo *Aggiungi accesso* e *Modifica accesso*.

È possibile scegliere fra i seguenti tipi di nome utente:

- Nome utente di Windows
- Nome principale utente di Windows
- Dominio\Nome utente di Windows
- Dominio di Windows

Utilizzare la propria password Windows.

Queste opzioni non possono essere modificate.

Usare una password precedente

È possibile che la password di Password Manager sia stata modificata e quindi il programma non accetta la nuova password. In tal caso, il programma permette di usare una password precedente (una password immessa in precedenza nella pagina di accesso) al posto di quella più recente.

Selezionare **Cronologia password**. Al termine dell'autenticazione, viene richiesto di scegliere una vecchia password dall'elenco Cronologia password. L'elenco comprende sette password.

Escludere i siti Web

Per impedire che i siti Web siano gestiti da Password Manager, fare clic sulla scheda **Esclusioni siti Web**.

I siti Web esclusi presentano le seguenti caratteristiche:

- non richiamano un'icona di Password Manager;
- non eseguono l'accesso automatico degli utenti;
- non mostrano i promemoria delle password.

Per aggiungere un nuovo sito Web all'elenco delle esclusioni:

1 Fare clic sulla scheda **Esclusioni siti Web**.
2 Fare clic su **Aggiungi sito Web**.
3 Immettere l'URL del sito Web da escludere.
4 Fare clic su **Salva**.

Una volta escluso un sito Web, questo non verrà gestito da Password Manager. Per invertire l'operazione di esclusione basta semplicemente eliminare il sito Web dall'elenco di Esclusioni siti Web. Per rimuovere un sito Web dall'elenco delle esclusioni, fare clic sulla X.

Dopo aver aggiunto diversi siti Web, l'utente può:

- fare clic sull'intestazione di colonna Siti Web per ordinare l'elenco per sito Web, in ordine crescente o decrescente;
- immettere parte dell'URL nel campo di ricerca per effettuare una ricerca all'interno dell'elenco; l'elenco viene filtrato man mano che l'utente digita l'URL.

Disabilitare i prompt per addestrare i moduli di accesso

L'utente può mantenere accessi addestrati già esistenti ma disabilitare messaggi di richiesta per addestrare nuovi moduli di accesso.

Per disabilitare i messaggi di richiesta per nuovi accessi:

1 Aprire la DDP Console.
2 Fare clic sul riquadro **Password Manager**.
3 Fare clic sulla scheda **Impostazioni**.
4 Deselezionare la casella di controllo **Richiedi di aggiungere un accesso quando sei in una schermata di accesso**.

Eseguire backup e ripristino delle credenziali di Password Manager

Password Manager consente di eseguire in modo protetto il backup dei dati di accesso gestiti da Password Manager. Tali dati possono essere ripristinati in qualsiasi computer protetto tramite Password Manager.

N.B.:
I dati di Password Manager di cui è stato eseguito il backup non includono le credenziali del sistema operativo o di accesso (PBA, Preboot Authentication) o le informazioni specifiche delle credenziali, come le impronte digitali.

Backup delle credenziali

Per eseguire il backup delle credenziali:

1 Fare clic sulla scheda **Esegui backup delle credenziali** per impostare il processo di backup.
2 Fare clic su **Sfoglia** e passare alla posizione di backup desiderata.
Se si tenta di eseguire il backup dei dati in un'unità locale, viene visualizzato un avviso che consiglia di eseguire il backup dei dati in un dispositivo di archiviazione portatile o in un'unità di rete.
3 Immettere e confermare la password. Utilizzare questa password se le credenziali di cui è stato eseguito il backup dovranno essere successivamente ripristinate.
4 Fare clic su **Backup**.
5 Immettere la password di Windows.
6 Nella finestra di dialogo Operazione completata, fare clic su **OK**.

N.B.:
Per visualizzare un registro di testo dell'operazione di backup effettuata, fare clic su e selezionare **Registro**.

Ripristinare le credenziali

Per poter ripristinare le credenziali deve essere disponibile il percorso del backup.

Per ripristinare le credenziali:

1 Fare clic sulla scheda **Ripristina credenziali**.
2 Fare clic su **Sfoglia** per accedere al file di backup, quindi inserire la password per il file.
3 Fare clic su **Ripristina**.

AVVERTENZA:

Il ripristino dei dati di Password Manager sovrascriverà tutti i dati esistenti. Gli accessi e gli altri dati aggiunti dopo la creazione del backup andranno persi.

4 Fare clic su **Avanti**.

N.B.:

Per visualizzare un registro di testo dell'operazione di ripristino, fare clic sull'icona nella barra del titolo e selezionare **Registro**.

7

Glossario

Credenziale - Serve per dimostrare l'identità di una persona, come ad esempio le relative impronte digitali o la password di Windows.

Password monouso (OTP) - La Password monouso è una password utilizzabile solo una volta e valida per una durata limitata. L'OTP richiede che il TPM sia presente, abilitato e di proprietà. Per abilitare la OTP, deve essere associato un dispositivo mobile al computer tramite la Security Console e l'app Security Tools Mobile. L'app Security Tools Mobile genera la password nel dispositivo mobile utilizzato per accedere alla schermata di accesso di Windows nel computer. In base ai criteri, la funzione OTP può essere utilizzata per ripristinare l'accesso al computer qualora la password sia stata dimenticata o sia scaduta, solo se l'OTP non è stata utilizzata per accedere al computer. La funzione OTP può essere utilizzata per l'autenticazione o per il ripristino, ma non per entrambi gli scopi. La sicurezza garantita dall'OTP è di gran lunga superiore a quella di altri metodi di autenticazione dal momento che la password generata può essere utilizzata solo una volta e scade entro un periodo di tempo breve.

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. La presenza del TPM è necessaria anche per l'utilizzo della funzione Password monouso (OTP).