Dell Data Protection | Security Tools

Guida all'installazione

v 1.9

2016-01

Sommario

1

Introduzione

Dell Data Protection | Security Tools (DDP | ST) fornisce sicurezza e protezione dell'identità agli amministratori e agli utenti dei computer Dell. DDP|ST è preinstallato in tutti i computer Dell Latitude, Optiplex e Precision, e in alcuni notebook Dell XPS. Se si desidera procedere alla *reinstallazione* di DDP|ST, seguire le istruzioni riportate in questa guida. Per ulteriore assistenza, consultare www.dell.com/support > Soluzioni per la sicurezza degli endpoint.

Panoramica

DDP|ST è una soluzione di sicurezza end-to-end progettata per fornire supporto per l'autenticazione avanzata, per l'Autenticazione di preavvio (PBA) e per la gestione delle unità autocrittografanti.

DDP|ST offre supporto a più fattori per l'autenticazione Windows con password, lettori di impronte e smart card, "senza contatti" e "con contatti", così come per l'autoregistrazione, l'accesso singolo (Single Sign-On [SSO]) e la Password monouso (OTP).

Prima di rendere Security Tools disponibile agli utenti finali, gli amministratori possono voler configurare le funzioni di Security Tools utilizzando lo strumento Impostazioni amministratore di DDP Security Console, per esempio, per abilitare l'autenticazione di preavvio e i criteri di autenticazione. Tuttavia, le impostazioni predefinite consentono agli amministratori e agli utenti di iniziare ad utilizzare Security Tools subito dopo l'installazione e l'attivazione.

DDP Security Console

DDP Security Console è l'interfaccia di Security Tools attraverso la quale gli utenti possono registrare e gestire le proprie credenziali e configurare le domande di ripristino automatico, in base ai criteri impostati dall'amministratore. Gli utenti possono accedere a queste applicazioni di Security Tools:

- Lo strumento Crittografia permette agli utenti di visualizzare lo stato di crittografia delle unità del computer.
- Lo strumento Registrazioni permette agli utenti di configurare e gestire le credenziali, configurare le domande di ripristino automatico e visualizzare lo stato di registrazione delle credenziali. Questi privilegi sono basati sui criteri impostati dall'amministratore.
- Password Manager permette agli utenti di compilare e inviare automaticamente i dati richiesti per accedere a siti Web, applicazioni Windows e risorse di rete. Password Manager offre anche la possibilità all'utente di modificare, tramite l'applicazione, le proprie password di accesso gestite da Password Manager in modo che siano sincronizzate con le password della risorsa assegnata.

Impostazioni amministratore

Lo strumento Impostazioni amministratore consente di configurare Security Tools per tutti gli utenti del computer, permettendo all'amministratore di impostare criteri di autenticazione, gestire gli utenti e configurare le credenziali da utilizzare per l'accesso a Windows.

Tramite lo strumento Impostazioni amministratore, l'amministratore può abilitare la crittografia e l'Autenticazione di preavvio (PBA), configurare i criteri di PBA e personalizzare il testo di PBA visualizzato.

Continuare con Requisiti.

2

Requisiti

- DDP|ST è preinstallato in tutti i computer Dell Latitude, Optiplex e Precision, e in alcuni notebook Dell XPS che soddisfano i requisiti minimi seguenti. Qualora fosse necessario reinstallare DDP|ST, verificare che il computer soddisfi ancora tali requisiti minimi. Per maggiori informazioni, consultare www.dell.com/support > Soluzioni per la sicurezza degli endpoint.
- Windows 8.1 non deve essere installato nell'unità 1 delle unità autocrittografanti. La configurazione di questo sistema operativo non è supportata in quanto Windows 8.1 crea un'unità di partizione di ripristino 0 che, a sua volta, interrompe l'autenticazione di preavvio. Al contrario, è possibile installare Windows 8.1 nell'unità configurata come unità 0 oppure ripristinare Windows 8.1 come immagine in qualsiasi unità.
- DDP|ST non supporta dischi dinamici.
- I computer dotati di unità autocrittografanti non possono essere utilizzati con Hardware Crypto Accelerator. Sono presenti incompatibilità che impediscono il provisioning dell'HCA. Si noti che Dell non vende computer con unità autocrittografanti che supportano il modulo HCA. Questa configurazione non supportata potrebbe essere una configurazione post vendita.
- DDP|ST non supporta la configurazione del disco ad avvio multiplo.
- Prima di installare un nuovo sistema operativo nel client, deselezionare il Trusted Platform Module (TPM) nel BIOS.
- Per un'unità autocrittografante non è necessario che il TPM fornisca l'Autenticazione avanzata o la crittografia.
- **Il RAID Intel, integrato nei computer portatili,** è supportato con la PBA quando si utilizza il DDP|Hardware Crypto Accelerator. Il RAID non è supportato in sistemi con unità autocrittografanti. Per maggiori informazioni, consultare Driver.

Driver

- Le unità autocrittografanti compatibili con Opal richiedono driver Intel Rapid Storage Technology aggiornati, che si trovano all'indirizzo http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA.

IMPORTANTE: Per via della natura dei RAID e delle unità autocrittografanti, SED Management non supporta il RAID. Il problema di "RAID=On" con le unità autocrittografanti consiste nel fatto che un'unità RAID richiede l'accesso al disco per leggere e scrivere dati ad essa correlati in un settore elevato, che non è disponibile in un'unità autocrittografante bloccata fin dall'avvio, e non può attendere che l'utente abbia eseguito l'accesso per leggere tali dati. Per risolvere il problema, modificare l'operazione SATA nel BIOS da "RAID=On" ad "AHCI". Se nel sistema operativo non sono preinstallati i driver del controller AHCI, dopo il passaggio da "RAID=On" ad "AHCI" verrà restituita una schermata blu.

Prerequisiti del client

- Per utilizzare Security Tools è necessaria la versione completa di Microsoft .Net Framework 4.0 (o superiore). In tutti i computer spediti dalla fabbrica Dell è preinstallata la versione completa di Microsoft .Net Framework 4.0. Tuttavia, se non si sta installando Security Tools in hardware Dell o si sta aggiornando Security Tools nei vecchi hardware Dell, è necessario verificare la versione di Microsoft .Net installata e aggiornare la versione, prima di installare Security Tools, al fine di prevenire errori di installazione/aggiornamento. Per installare la versione completa di Microsoft .Net Framework 4.0, visitare il sito http://www.microsoft.com/en-us/download/details.aspx?id=17851.

  Per verificare la versione di .Net installata, seguire queste istruzioni nel computer destinato all'installazione: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx.
- I driver e il firmware dell'hardware di autenticazione del computer devono essere aggiornati. Per ottenere i driver e il firmware dei computer Dell, visitare http://www.dell.com/support/home/us/en/19/Products/?app=drivers e selezionare il proprio modello di computer. In base all'hardware di autenticazione di cui si dispone, scaricare i seguenti:
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smartcard Driver
  - Dell ControlVault

  Altri fornitori di hardware potrebbero richiedere l'utilizzo dei propri driver.

Il programma di installazione installa questo componente se non è già installato nel computer:

Prerequisiti
• Microsoft Visual C++ 2012 Update 4 o versione successiva del Redistributable Package (x86/x64)

Software

Sistemi operativi Windows

La tabella seguente descrive in dettaglio il software supportato.

Sistemi operativi Windows (a 32 e 64 bit)
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional
N.B. La modalità di avvio Legacy è supportata in Windows 7. UEFI non è supportato in Windows 7.
• Microsoft Windows 8 - Enterprise - Pro - Windows 8 (Consumer)

N.B. Windows 8 è supportato in modalità UEFI quando usato con Unità autocrittografanti compatibili con Opal e con Modelli di computer Dell - Supporto UEFI.

Sistemi operativi Windows (a 32 e 64 bit)
• Microsoft Windows 8.1 - 8.1 Update 1 - Enterprise Edition - Pro Edition
N.B. Windows 8,1 è supportato in modalità UEFI quando usato con Unità autocrittografanti compatibili con Opal e con Modelli di computer Dell - Supporto UEFI.
• Microsoft Windows 10 - Education Edition - Enterprise Edition - Pro Edition
N.B. Windows 10 è supportato in modalità UEFI quando usato con Unità autocrittografanti compatibili con Opal e con Modelli di computer Dell - Supporto UEFI.

Sistemi operativi dei dispositivi mobili

I seguenti sistemi operativi dei dispositivi mobili sono supportati con la funzionalità Password monouso (OTP) di Security Tools.

Sistemi operativi Android
• 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
Sistemi operativi iOS
• iOS 7.x
• iOS 8.x
Sistemi operativi Windows Phone
• Windows Phone 8.1
• Windows 10 Mobile

Hardware

Autenticazione

La tabella seguente descrive in dettaglio l'hardware di autenticazione supportato.

Lettori di impronte digitali
• Validity VFS495 in modalità protetta
• Lettore di bande magnetiche Broadcom ControlVault
• UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
• Lettori USB Authentec Eikon e Eikon To Go

N.B. Quando si utilizza un lettore di impronte digitali esterno, è necessario scaricare e installare i driver più recenti specifici per il lettore.

Schede senza contatti
• Schede senza contatti che utilizzano lettori per schede senza contatti integrati nei portatili Dell specificati
Smart card
• Smart card PKCS #11 che utilizzano il client ActivIdentity **N.B.** Il client ActivIdentity non è precaricato e deve essere installato separatamente.
• Common Access Card (CAC, Scheda di accesso comune) **N.B.** Con le CAC che dispongono di più di un certificato, all'accesso l'utente seleziona il certificato corretto da un elenco.
• Schede per provider del servizio di crittografia (CSP, Cryptographic Service Provider)
• Schede classe B/SIPR Net

La tabella seguente descrive in dettaglio i modelli di computer Dell che supportano le schede SIPR Net.

Modelli di computer Dell - Supporto schede Classe B/SIPR Net
• Latitude E6440
• Latitude E6540
• Precision M2800
• Precision M4800
• Precision M6800
• Latitude 14 Rugged Extreme
• Latitude 12 Rugged Extreme
• Latitude 14 Rugged

Modelli di computer Dell - Supporto UEFI

Le funzionalità di autenticazione sono supportate in modalità UEFI in computer Dell selezionati in cui sono in esecuzione Microsoft Windows 8, Microsoft Windows 8.1 e Microsoft Windows 10 e dispongono di Unità autocrittografanti compatibili con Opal qualificate. Altri computer in cui sono in esecuzione Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1 e Microsoft Windows 10 supportano la modalità di avvio Legacy.

La tabella seguente mostra in dettaglio i modelli di computer Dell supportati con UEFI.

Modelli di computer Dell - Supporto UEFI
• Latitude E7240
• Latitude E7250
• Latitude E7350
• Latitude E7440
• Latitude E7450
• Precision M4800
• Precision M6800
• Precision T7810
• OptiPlex 7020
• OptiPlex 9020 Micro
• Venue Pro 11 (modello 7139)

N.B. In un computer compatibile con UEFI, dopo aver selezionato **Riavvia** dal menu principale, il computer verrà riavviato e in seguito visualizzerà una delle due possibili schermate di accesso. La schermata di accesso che appare è determinata da differenze di architettura della piattaforma del computer. Alcuni modelli visualizzano la schermata di accesso PBA, altri modelli invece visualizzano la schermata di accesso Windows. Entrambe le schermate di accesso sono dotate dello stesso livello di sicurezza.

N.B. Assicurarsi che l'impostazione Enable Legacy Option ROMs (Abilita ROM di opzione legacy) sia disabilitata nel BIOS.

Per disabilitare le ROM di opzione legacy:

1. Riavviare il sistema.
2. Premere ripetutamente **F12** durante il riavvio per visualizzare le impostazioni di avvio del computer UEFI.
3. Premere la freccia verso il basso, evidenziare l'opzione **BIOS Settings** (Impostazioni BIOS) e premere **Invio**.
4. Selezionare **Settings > General > Advanced Boot Options** (Impostazioni > Generali > Opzioni di avvio avanzate).
5. Deselezionare la casella di controllo **Enable Legacy Option ROMs** (Abilita ROM opzioni di legacy) e fare clic su **Apply** (Applica).

Unità autocrittografanti compatibili con Opal

Le unità supportate presentano una "X", ma non sono qualificate per i sistemi Dell né incluse in dotazione.

Unità	Disponibilità	Standard
Seagate ST320LT009 (FIPS Julius 320 GB)	✓	Opal 1
Seagate ST320LT014 (Julius 320 GB)	✓	Opal 1
Seagate ST500LM001 (Kahuna 500 GB)	✓	Opal 2/eDrive
Seagate ST1000LM015 (Kahuna 1000 GB)	✓	Opal 2/eDrive
Seagate ST500LT012 (Yarra 1D non FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST500LT015 (Yarra 1D FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST500LM020 (Kahuna V FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST1000LM028 (Kahuna V FIPS 1000 GB)	✓	Opal 2/eDrive
Seagate ST500LM023 (Yarra X)	✓	Opal 2/eDrive
Seagate ST500LM024 (Yarra X FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST500LT025 (Yarra R)	✓	Opal 2/eDrive
Seagate ST500LT033 (Asagana)	✓	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3,5 pollici 1000 GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3,5 pollici 2000 GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3,5 pollici 3000GB)	X	Opal 2/eDrive
Travelstar serie 5K750	X	Opal 1
Travelstar serie 7K750	X	Opal 1
Travelstar serie Z5K320	X	Opal 1
Toshiba serie MKxx61GSYD	X	Opal 1
Toshiba serie MKxx61GSYG	X	Opal 1
Samsung SM840 EVO MZ-MTEXXXBW	X	Opal 2
SSD Samsung SM841 OPAL	✓	Opal 2
SSD Samsung SM841N OPAL	✓	Opal 2
Samsung SM850 PRO 2,5 pollici MZ-7KE128 – MZ-7KE2T0 (SSD SED 2,5 pollici da 128 GB a 2000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO 2,5 pollici MZ-75E120 – MZ-75E2T0 (SSD SED 2,5 pollici da 120 GB a 2000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO mSATA MZ-M5E120 – MZ-M5E1T0 (SSD SED mSATA da 120 GB a 1000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO M.2 MZ-N5E120 – MZ-N5E500 (SSD SED M.2. da 120 GB a 500 GB)	X	Opal 2/eDrive
SSD Samsung PM851 OPAL – 2,5 pollici (2,5 pollici 128 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM851 OPAL – mSATA (mSATA 128 GB - 512 GB)	✓	Opal 2/eDrive

Unità	Disponibilità	Standard
SSD Samsung PM851 OPAL - M.2. (M.2. 128 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - 2,5 pollici (2,5 pollici 256 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - mSATA (mSATA 256 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - M.2. (M.2. 256 GB - 512 GB)	✓	Opal 2/eDrive
SanDisk X300s	X	Opal 2
SSD LiteOn L9M OPAL	✓	Opal 2
SSD LiteOn serie M3	✓	Opal 1
SSD LiteOn serie M6	✓	Opal 2
SSD LiteOn serie V2M	✓	Opal 2
SSD Crucial RealSSD C400	X	Opal 1
SSD Micron RealSSD C400	X	Opal 1
SSD Micron M500 2,5 pollici (120 GB - 960 GB)	X	Opal 2/eDrive
SSD Micron M500 mSATA (120 GB - 480 GB)	X	Opal 2/eDrive

Supporto lingue

DDP|ST è compatibile con l'interfaccia utente multilingue (MUI) e supporta le seguenti lingue.

N.B. La localizzazione PBA non supporta la lingua russa, cinese tradizionale o cinese semplificato.

Supporto lingue	
• EN - Inglese	• KO - Coreano
• FR - Francese	• ZH-CN - Cinese semplificato
• IT - Italiano	• ZH-TW - Cinese tradizionale/Taiwan
• DE - Tedesco	• PT-BR - Portoghese (Brasile)
• ES - Spagnolo	• PT-PT - Portoghese (Portogallo)
• JA - Giapponese	• RU - Russo

Opzioni di autenticazione

Le seguenti opzioni di autenticazione richiedono hardware specifici: Impronte digitali, Smart card, Schede senza contatti, Schede Class B/SIPRNet e autenticazione in computer UEFI.

La funzione Password monouso richiede che il TPM sia presente, abilitato e di proprietà. Per maggiori informazioni, consultare Cancellare la proprietà e attivare il TPM.

Le seguenti tabelle mostrano le opzioni di autenticazione disponibili con Security Tools a seconda del sistema operativo, quando i requisiti hardware e di configurazione vengono soddisfatti.

Non UEFI

	PBA					Autenticazione di Windows				
	Password	Impronta	Smart card con contatti	OTP	Scheda SIPR	Password	Impronta	Smart card	OTP	Scheda SIPR
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. Disponibile con una SED Opal supportata.

UEFI

	PBA - nei computer Dell supportati					Autenticazione di Windows				
	Password	Impronta	Smart card con contatti	OTP	Scheda SIPR	Password	Impronta	Smart card	OTP	Scheda SIPR
Windows 7										
Windows 8	X[2]					X	X	X	X	X
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. Disponibile con una SED OPAL supportata in computer UEFI supportati.

Interoperabilità

Effettuare il deprovisioning e disinstallare Dell Data Protection | Access

Se DDP|A è stato appena installato o è stato installato in precedenza nel proprio computer, **prima** di installare Security Tools effettuare il deprovisioning dell'hardware gestito da DDP|-A e poi disinstallare DDP|A. Se DDP|A non è stato utilizzato, si può semplicemente disinstallare DDP|A e riavviare il processo di installazione.

Il deprovisioning dell'hardware gestito da DDP|A include il lettore di impronte, il lettore di smart card, le password del BIOS, il TPM e l'unità autocrittografante.

N.B. Se sono in esecuzione prodotti con crittografia DDP|E, interrompere o mettere in pausa la ricerca della crittografia. Se si esegue Microsoft BitLocker, sospendere il criterio di crittografia. Una volta disinstallato DDP|A e sospeso il criterio Microsoft BitLocker, inizializzare il TPM seguendo le istruzioni riportate in http://technet.microsoft.com/en-us/library/cc753140.aspx.

Effettuare il deprovisioning dell'hardware gestito da DDP|A

1. Avviare DDP|A e fare clic sulla scheda *Avanzate*.
2. Selezionare **Reimposta sistema**. Per verificare la propria identità, sarà necessario immettere eventuali credenziali di provisioning. Dopo la verifica delle credenziali, DDP|A eseguirà le azioni seguenti:

   - Rimozione di tutte le credenziali sottoposte a provisioning da Dell ControlVault (se presente)
   - Rimozione della password del proprietario di Dell ControlVault (se presente)
   - Rimozione di tutte le impronte digitali sottoposte a provisioning dal lettore integrato (se presente)
   - Rimozione di tutte le password BIOS (password di sistema BIOS, amministratore del BIOS e HDD)
   - Cancellazione del Trusted Platform Module
   - Rimozione del provider di credenziali DDP|A

   Una volta effettuato il deprovisioning, il DDP|A riavvierà il computer per ripristinare il provider di credenziali predefinite di Windows.

Disinstallare DDP|A

Al termine del deprovisioning dell'hardware di autenticazione, disinstallare DDP|A.

1. Avviare DDP|A e scegliere Reimposta sistema.

   Questa operazione rimuove tutte le credenziali e le password di gestione di DDP|A ed elimina il Trusted Platform Module (TPM).
2. Fare clic su **Disinstalla** per avviare il programma di installazione.
3. Una volta terminata la disinstallazione, fare clic su **Sì** per riavviare.

N.B. La rimozione di DDP|A sbloccherà anche l'unità autocrittografante e rimuoverà l'autenticazione di preavvio.

Inizializzare il TPM

1. Seguire le istruzioni all'indirizzo http://technet.microsoft.com/en-us/library/cc753140.aspx.

Cancellare la proprietà e attivare il TPM

Per cancellare e impostare la proprietà del TPM, consultare https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Procedere con Installazione e attivazione.

3

Installazione e attivazione

Questa sezione illustra l'installazione di DDP|ST in un computer locale. Per installare e attivare DDP|ST, è necessario accedere al computer come amministratore.

PROCEDURA CONSIGLIATA: Durante l'installazione non apportare modifiche al computer, quali l'inserimento o la rimozione di unità esterne (USB).

Installare DDP|ST

Per installare Security Tools:

1. Individuare il file di installazione nel supporto di installazione di DDP|ST. Copiarlo nel computer locale.

N.B. Il supporto di installazione è disponibile all'indirizzo www.dell.com/support > Soluzioni per la sicurezza degli endpoint.

2. Fare doppio clic sul file per avviare il programma di installazione.
3. Selezionare la lingua desiderata e fare clic su **OK**.
4. Fare clic su **Avanti** quando viene visualizzata la pagina Introduzione.
5. Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.
6. Fare clic su **Avanti** per installare Security Tools nel percorso predefinito C:\Program Files\Dell\Dell Data Protection. Selezionare **Avanti** nella pagina Selezione funzionalità.
7. Fare clic su **Installa** per avviare l'installazione.
8. Al termine dell'installazione sarà necessario riavviare il sistema. Selezionare **Sì** per riavviare il sistema e fare clic su **Fine**.

   L'installazione è completata.

Attivare DDP|ST

La prima volta che si esegue la DDP Security Console e si seleziona Impostazioni amministratore, la procedura guidata di attivazione accompagna l'utente in questo processo.

Se la DDP Security Console non è ancora attivata, l'utente finale potrà comunque eseguirla. Quando l'utente finale è la prima persona ad utilizzare DDP Security Console prima che l'amministratore abbia attivato DDP|ST e personalizzato le impostazioni, verranno utilizzati i valori predefiniti.

Per attivare Security Tools:

1. Come amministratore, avviare Security Tools dal collegamento sul desktop.

N.B. Se è stato effettuato l'accesso come utente standard (tramite un account standard di Windows), per l'avvio lo strumento Impostazioni amministratore richiederà l'elevazione del controllo account utente. L'utente standard in primo luogo inserirà le credenziali di amministratore per accedere allo strumento e in seguito, quando richiesto, inserirà la password di amministratore (la password salvata in Impostazioni amministratore).

2. Fare clic sul riquadro **Impostazioni amministratore**.
3. Nella schermata iniziale, fare clic su **Avanti**.
4. Creare la password di DDP|ST e fare clic su **Avanti**.

   Prima di configurare Security Tools, è necessario creare una password amministratore di DDP|ST. La password scelta verrà richiesta ad ogni esecuzione dello strumento Impostazioni amministratore. La password deve essere compresa fra gli 8 e i 32 caratteri e deve contenere almeno una lettera, un numero e un carattere speciale.

5. In **Percorso di backup,** specificare la posizione in cui il file di backup deve essere scritto e fare clic su **Avanti**.
   Il file di backup deve essere salvato in un'unità di rete o in un supporto rimovibile. Il file di backup contiene le chiavi necessarie per il ripristino dei dati nel computer. Il Supporto Dell deve avere accesso a questo file per fornire assistenza durante il ripristino dei dati.

   Verrà automaticamente eseguito il backup dei dati di ripristino nel percorso specificato. Se la posizione non è disponibile (per esempio se l'unità USB di backup non è inserita), DDP|ST suggerirà una posizione per il backup dei dati. Per poter iniziare la crittografia sarà richiesto l'accesso ai dati di ripristino.

6. Nella pagina di riepilogo, fare clic su **Applica**.

L'attivazione di Security Tools è completata.

Gli amministratori e gli utenti possono subito iniziare ad utilizzare le funzioni di Security Tools in base alle impostazioni predefinite.

4

Attività di configurazione per amministratori

Le impostazioni predefinite di Security Tools consentono ad amministratori e utenti di utilizzare Security Tools immediatamente dopo la sua attivazione, senza necessità di ulteriore configurazione. Al momento dell'accesso al computer con le rispettive password di Windows gli utenti sono automaticamente aggiunti come utenti di Security Tools. Tuttavia, per impostazione predefinita, non è abilitata l'autenticazione a più fattori di Windows. Per impostazione predefinita, anche la crittografia e l'autenticazione di preavvio non sono attive.

Per configurare le funzioni di Security Tools è necessario accedere al computer come amministratore.

Modificare la password di amministratore e il percorso di backup

Una volta attivato Security Tools, è possibile modificare la password di amministratore e il percorso di backup, se necessario.

1. Come amministratore, avviare Security Tools dal collegamento sul desktop.
2. Fare clic sul riquadro **Impostazioni amministratore**.
3. Nella finestra di dialogo Autenticazione, inserire la password di amministratore impostata in fase di attivazione e fare clic su **OK**.
4. Fare clic sulla scheda **Impostazioni amministratore**.
5. Nella pagina Modifica password amministratore, se si desidera cambiare la password, inserire una nuova password che contenga 8-32 caratteri e includa almeno una lettera, un numero e un carattere speciale.
6. Immettere la password una seconda volta per confermarla, quindi fare clic su **Applica**.
7. Per modificare il percorso in cui è archiviata la chiave di ripristino, nel riquadro sinistro selezionare **Modifica percorso di backup**.
8. Selezionare un nuovo percorso per il backup e fare clic su **Applica**.

   Il file di backup deve essere salvato in un'unità di rete o in un supporto rimovibile. Il file di backup contiene le chiavi necessarie per il ripristino dei dati nel computer. Dell ProSupport deve avere accesso a questo file per assistere l'utente nel ripristino dei dati.

   Verrà automaticamente eseguito il backup dei dati di ripristino nel percorso specificato. Se la posizione non è disponibile (per esempio se l'unità USB di backup non è inserita), DDP|ST suggerirà una posizione per il backup dei dati. Per poter iniziare la crittografia sarà richiesto l'accesso ai dati di ripristino.

Configurare la crittografia e l'autenticazione di preavvio

La crittografia e l'autenticazione di preavvio (PBA) sono disponibili se il computer è dotato di un'unità autocrittografante (SED). Vengono configurati entrambi tramite la scheda Crittografia, visualizzabile solo se il computer è dotato di un'unità autocrittografante. Abilitando la crittografia o la PBA, verrà abilitata anche l'altra funzione.

Prima di attivare la crittografia e la PBA, Dell consiglia di registrare e abilitare le domande di ripristino come Opzione di ripristino in modo da poter recuperare la password in caso di smarrimento. Per maggiori informazioni, consultare Configurare le opzioni di accesso.

Per configurare la crittografia o l'autenticazione di preavvio:

1. Nella DDP Security Console, fare clic sul riquadro **Impostazioni amministratore**.
2. Assicurarsi che il percorso di backup sia accessibile dal computer.

N.B. Quando la crittografia è abilitata, se viene visualizzato il messaggio "Percorso di backup non trovato" e il percorso di backup si trova in un'unità USB, è possibile che l'unità non sia connessa oppure che sia connessa a uno slot diverso da quello utilizzato durante il backup. Se viene visualizzato il messaggio e il percorso di backup si trova in un'unità di rete, quest'ultima risulta inaccessibile dal computer. Se è necessario modificare il percorso di backup, dalla scheda **Impostazioni amministratore** selezionare **Modifica percorso di backup** per modificare il percorso dello slot o dell'unità accessibile corrente. Qualche secondo dopo aver riassegnato il percorso, è possibile procedere con l'abilitazione della crittografia.

3. Fare clic sulla scheda **Crittografia** e quindi su **Crittografa**.
4. Nella schermata iniziale, fare clic su Avanti.
5. Nella pagina Criterio di preavvio, modificare o confermare i seguenti valori, quindi fare clic su **Avanti**.

Tentativi di accesso per gli utenti non memorizzati nella cache	Numero di tentativi di accesso consentiti agli utenti sconosciuti, ossia agli utenti che non hanno mai effettuato l'accesso al computer in precedenza e le cui credenziali non sono memorizzate nella cache.
Tentativi di accesso per gli utenti memorizzati nella cache	Numero di volte per cui un utente conosciuto può tentare l'accesso.
Tentativi di risposta alle domande di ripristino	Numero di volte per cui un utente può inserire la risposta corretta.
Attiva password di cancellazione con crittografia	Selezionare per abilitare.
Immetti password di cancellazione con crittografia	Come meccanismo di sicurezza FailSafe viene utilizzato un codice o una parola con lunghezza massima di 100 caratteri. Immettendo questa parola o codice nel campo nome utente o password durante l'autenticazione PBA, il dispositivo viene cancellato in modo definitivo. Se questo campo viene lasciato vuoto, in caso di emergenza non sarà disponibile alcuna password di cancellazione con crittografia.

6. Nella pagina Personalizzazione preavvio, inserire un testo personalizzato da visualizzare nella schermata Autenticazione di preavvio (PBA) e fare clic su **Avanti**.

Testo titolo di preavvio	Questo testo viene visualizzato nella parte superiore della schermata PBA. Se si lascia vuoto questo campo non verrà visualizzato alcun titolo. Il testo non va a capo, pertanto l'immissione di più di 17 caratteri potrebbe comportare il troncamento del testo.
Testo informazioni supporto	Questo testo viene visualizzato nella pagina delle informazioni sul supporto PBA. Dell consiglia di personalizzare il messaggio e includere indicazioni specifiche su come contattare l'helpdesk o l'amministratore della sicurezza. Il mancato inserimento di testo in questo campo comporta la mancata disponibilità all'utente delle informazioni per contattare il supporto tecnico. Il testo viene mandato a capo a livello di parola, non di carattere. Se ad esempio è presente una singola parola con lunghezza di oltre 50 caratteri, tale parola non viene mandata a capo e non viene aggiunta alcuna barra di scorrimento. Il testo risulta pertanto troncato.

Testo note legali	Questo testo viene visualizzato prima che l'utente possa accedere al dispositivo. Per esempio: "Facendo clic su OK l'utente accetta di osservare i criteri di uso del computer". Il mancato inserimento di testo in questo campo comporta la mancata visualizzazione del testo o dei pulsanti OK/Annulla. Il testo viene mandato a capo a livello di parola, non di carattere. Se ad esempio è presente una singola parola con lunghezza di oltre 50 caratteri, tale parola non viene mandata a capo e non viene aggiunta alcuna barra di scorrimento. Il testo risulta pertanto troncato.

7 Nella pagina di riepilogo, fare clic su **Applica**.

8 Quando richiesto, fare clic su **Arresta il sistema**.

Prima di poter avviare la crittografia è necessario l'arresto completo del sistema.

9 Dopo l'arresto, riavviare il computer.

L'autenticazione è ora gestita da Security Tools. Gli utenti devono accedere alla schermata Autenticazione di preavvio con le relative password di Windows.

Modificare le impostazioni di crittografia e autenticazione di preavvio

Dopo aver abilitato la crittografia per la prima volta e configurato il criterio o la personalizzazione di preavvio, sono disponibili le seguenti azioni dalla scheda Crittografia:

- Modifica criterio o personalizzazione di preavvio - Fare clic sulla scheda **Crittografia** quindi fare clic su **Modifica**.
- Decrittografia dell'unità autocrittografante, ad esempio per la disinstallazione - Fare clic su **Decrittografa**.

Dopo aver abilitato la crittografia per la prima volta e configurato il criterio o la personalizzazione di preavvio, sono disponibili le seguenti azioni dalla scheda Impostazioni preavvio:

- Modifica criterio o personalizzazione di preavvio - Fare clic sulla scheda **Impostazioni preavvio** quindi selezionare **Personalizzazione preavvio** o **Criteri accesso preavvio**.

  Per le istruzioni di disinstallazione, consultare Attività di disinstallazione.

Configurare le opzioni di autenticazione

I controlli nella scheda Autenticazione di Impostazioni amministratore consentono all'utente di impostare le opzioni di accesso e personalizzare le impostazioni per ciascuna di esse.

N.B. L'opzione Password monouso verrà visualizzata in Opzioni di ripristino solo in presenza di TPM abilitato e di proprietà.

Configurare le opzioni di accesso

Nella pagina Opzioni di accesso, è possibile configurare i criteri di accesso. Per impostazione predefinita, tutte le credenziali supportate sono elencate nella sezione Opzioni disponibili.

Per configurare le opzioni di accesso:

1. Nel riquadro sinistro, in Autenticazione, selezionare **Opzioni di accesso**.
2. Per scegliere il ruolo che si desidera impostare selezionarlo dall'elenco **Applica opzioni di accesso a**: **Utenti** o **Amministratori**. Tutte le modifiche apportate in questa pagina saranno applicate solo al ruolo selezionato.
3. Impostare Opzioni disponibili per l'autenticazione.

   Per impostazione predefinita, ogni metodo di autenticazione è configurato per essere utilizzato singolarmente e non in combinazione con altri metodi di autenticazione. Le impostazioni predefinite possono essere modificate nei seguenti modi:

   - Per impostare una combinazione di opzioni di autenticazione, in Opzioni disponibili, fare clic su per selezionare il primo metodo di autenticazione. Nella finestra di dialogo Opzioni disponibili, selezionare il secondo metodo di autenticazione, quindi fare clic su **OK**.

     Per esempio, è possibile impostare come credenziali di accesso sia un'impronta digitale sia una password. Nella finestra di dialogo, selezionare il secondo metodo di autenticazione che deve essere utilizzato in combinazione con l'autenticazione mediante impronta digitale.
   - Per consentire che ciascun metodo di autenticazione possa essere utilizzato singolarmente, nella finestra di dialogo Opzioni disponibili lasciare come impostazione del secondo metodo di autenticazione **Nessuno** e fare clic su **OK**.
   - Per rimuovere un'opzione di accesso, sotto Opzioni disponibili nella pagina Opzioni di accesso, fare clic sulla **X** per rimuovere il metodo.
   - Per aggiungere una nuova combinazione di metodi di autenticazione, fare clic su **Aggiungi un'opzione**.
4. Impostare le opzioni di ripristino per consentire agli utenti di recuperare l'accesso al computer, nel caso siano rimasti bloccati.
   - Per consentire agli utenti di definire un insieme di domande e risposte da utilizzare per ottenere nuovamente l'accesso al computer, selezionare **Domande di ripristino**.

     Per non usare le Domande di ripristino, deselezionare l'opzione.
   - Per consentire agli utenti di recuperare l'accesso tramite dispositivo mobile, selezionare **Password monouso**. Se è stata scelta la Password monouso (OTP) come metodo di recupero, questa non sarà più selezionabile come opzione di accesso nella schermata di accesso Windows.

     Per avvalersi della funzione OTP per l'accesso, deselezionare l'opzione in Opzioni di ripristino. Quando la funzione non è più selezionata come metodo di ripristino, l'opzione OTP viene visualizzata nella pagina di accesso Windows qualora almeno un utente abbia registrato un'OTP.

N.B. L'amministratore può controllare le possibili modalità di utilizzo della funzione Password monouso (per autenticazione o per ripristino). La funzione OTP può essere utilizzata per l'autenticazione oppure per il ripristino, ma non per entrambi gli scopi. La configurazione interessa tutti gli utenti del computer o tutti gli amministratori, a seconda della selezione effettuata in **Applica opzioni di accesso a** nel campo Opzioni di accesso.

Se l'opzione Password monouso non è presente in elenco, significa che la configurazione del computer non la supporta. Per maggiori informazioni, consultare Requisiti.

- Per richiedere all'utente di chiamare l'helpdesk nel caso abbia dimenticato o perso le credenziali di accesso, deselezionare Domande di ripristino e Password monouso.

5 Per impostare un lasso di tempo per consentire agli utenti di registrare le proprie credenziali di autenticazione, selezionare **Periodo di tolleranza**.

La funzione Periodo di tolleranza permette all'amministratore di impostare la data in cui comincerà a essere applicata un'opzione di accesso configurata. È possibile configurare un'opzione di accesso prima della data in cui sarà applicata e impostare un lasso di tempo per consentire all'utente la registrazione. Per impostazione predefinita, il criterio è applicato immediatamente.

Per modificare la data di Applica opzione di accesso da *Immediatamente* nella finestra di dialogo Periodo di tolleranza, fare clic sul menu a discesa e selezionare **Data specificata**. Fare clic sulla freccia GIÙ sul lato destro del campo della data per visualizzare il calendario, quindi selezionare una data nel calendario. Il criterio viene applicato a partire dalle ore 00:01 circa della data selezionata.

Gli utenti possono ricevere un promemoria per la registrazione delle proprie credenziali richieste al successivo accesso a Windows (impostazione predefinita) oppure possono essere impostati promemoria periodici. Selezionare l'intervallo di tempo del promemoria dall'elenco a discesa *Promemoria utenti*.

N.B. Il promemoria visualizzato varia leggermente a seconda che al momento della sua attivazione l'utente si trovi nella schermata di accesso di Windows o in una sessione di Windows. I promemoria non vengono visualizzati nelle schermate di accesso all'Autenticazione di preavvio.

Funzionalità durante il periodo di tolleranza

Durante un periodo di tolleranza specificato, se l'utente non ha ancora registrato le credenziali minime necessarie per soddisfare i requisiti di un'Opzione di accesso modificata, dopo ogni accesso viene visualizzata la notifica Credenziali aggiuntive. Il contenuto del messaggio è: *Le credenziali aggiuntive sono disponibili per la registrazione.*

Se le credenziali aggiuntive sono disponibili, ma non obbligatorie, il messaggio viene visualizzato una volta sola dopo la modifica del criterio.

A seconda del contesto, quando si fa clic sulla notifica può verificarsi quanto segue:

- Se non sono presenti credenziali registrate, viene visualizzata l'installazione guidata che permette agli utenti con privilegi amministrativi di configurare impostazioni correlate al computer e offre agli utenti la possibilità di registrare le credenziali più comuni.
- Dopo la registrazione iniziale delle credenziali, quando si fa clic sulla notifica viene visualizzata l'installazione guidata nella DDP Security Console.

Funzionalità dopo la scadenza del periodo di tolleranza

In tutti i casi, dopo la scadenza del periodo di tolleranza gli utenti che non hanno registrato le credenziali richieste dall'Opzione di accesso non possono accedere al sistema. Se un utente tenta di effettuare l'accesso con credenziali o combinazioni di credenziali che non rispondono all'Opzione di accesso, sopra la schermata di accesso di Windows viene visualizzata l'installazione guidata.

- Se l'utente registra correttamente le credenziali necessarie, può effettuare l'accesso a Windows.
- Se l'utente non registra correttamente le credenziali necessarie o annulla la procedura guidata, torna alla schermata di accesso di Windows.

6 Per salvare le impostazioni per il ruolo selezionato, fare clic su **Applica**.

Configurare l'autenticazione in Password Manager

Nella pagina Password Manager è possibile configurare le modalità di autenticazione degli utenti in Password Manager.

Per configurare l'autenticazione in Password Manager:

1. Nel riquadro sinistro, sotto Autenticazione, selezionare **Password Manager**.
2. Per scegliere il ruolo che si desidera impostare selezionarlo dall'elenco **Applica opzioni di accesso a**: **Utenti** o **Amministratori**. Tutte le modifiche apportate in questa pagina saranno applicate solo al ruolo selezionato.
3. Facoltativamente, selezionare la casella di controllo **Non richiedere l'autenticazione** per consentire al ruolo utente selezionato di accedere automaticamente a tutte le applicazioni software e ai siti Web di Internet con le credenziali archiviate in Password Manager.
4. Impostare Opzioni disponibili per l'autenticazione.

   Per impostazione predefinita, ogni metodo di autenticazione è configurato per essere utilizzato singolarmente e non in combinazione con altri metodi di autenticazione. Le impostazioni predefinite possono essere modificate nei seguenti modi:

   - Per impostare una combinazione di opzioni di autenticazione, in Opzioni disponibili, fare clic su per selezionare il primo metodo di autenticazione. Nella finestra di dialogo Opzioni disponibili, selezionare il secondo metodo di autenticazione, quindi fare clic su **OK**.

     Per esempio, è possibile impostare come credenziali di accesso sia un'impronta digitale sia una password. Nella finestra di dialogo, selezionare il secondo metodo di autenticazione che deve essere utilizzato in combinazione con l'autenticazione mediante impronta digitale.
   - Per consentire che ciascun metodo di autenticazione possa essere utilizzato singolarmente, nella finestra di dialogo Opzioni disponibili lasciare come impostazione del secondo metodo di autenticazione **Nessuno** e fare clic su **OK**.
   - Per rimuovere un'opzione di accesso, sotto Opzioni disponibili nella pagina Opzioni di accesso, fare clic sulla **X** per rimuovere il metodo.
   - Per aggiungere una nuova combinazione di metodi di autenticazione, fare clic su **Aggiungi un'opzione**.
5. Per salvare le impostazioni per il ruolo selezionato, fare clic su **Applica**.

N.B. Selezionare il pulsante Impostazioni predefinite per ripristinare le impostazioni ai valori originali.

Configurare le domande di ripristino

Nella pagina Domande di ripristino, è possibile selezionare le domande da presentare agli utenti durante la definizione delle domande e risposte di ripristino personali. Le Domande di ripristino consentono agli utenti di recuperare l'accesso ai propri computer in caso di password scadute o smarrite.

Per configurare le domande di ripristino:

1. Nel riquadro sinistro, in Autenticazione, selezionare **Domande di ripristino**.
2. Nella pagina Domande di ripristino, selezionare almeno tre domande di ripristino predefinite.
3. Facoltativamente, possono essere aggiunte fino a tre domande personalizzate nell'elenco mostrato all'utente per la selezione.
4. Per salvare le Domande di ripristino, fare clic su **Applica**.

Configurare l'autenticazione con scansione dell'impronta digitale

Per configurare l'autenticazione con scansione dell'impronta digitale:

1. Nel riquadro sinistro, in Autenticazione, selezionare **Impronte**.
2. In Registrazioni, impostare il numero minimo e massimo di dita che un utente può registrare.

3 Impostare la sensibilità della scansione dell'impronta digitale.

Una bassa sensibilità aumenta la variazione accettabile e la probabilità che una scansione falsificata venga accettata. Con l'impostazione massima il sistema potrebbe rifiutare anche le impronte digitali legittime. L'impostazione Maggiore sensibilità abbassa la percentuale di accettazione di scansioni false a 1 su 10.000.

4 Per rimuovere tutte le scansioni delle impronte digitali e le registrazioni delle credenziali dal buffer del lettore biometrico, fare clic su **Cancella lettore**. Questa operazione rimuove solo i dati correnti aggiunti e non elimina le scansioni e le registrazioni archiviate nelle precedenti sessioni.

5 Per salvare le impostazioni, fare clic su **Applica**.

Configurare l'autenticazione della Password monouso

Per utilizzare la funzionalità Password monouso, l'utente genera una Password monouso con l'applicazione Dell Data Protection | Security Tools Mobile del proprio dispositivo mobile poi inserirà la password nel computer. La password può essere utilizzata solo una volta ed è valida solo per un periodo di tempo limitato.

Per incrementare la protezione, l'amministratore può garantire la sicurezza dell'applicazione mobile richiedendo un PIN.

Nella pagina Dispositivo mobile, è possibile configurare le impostazioni per aumentare ulteriormente la sicurezza del dispositivo mobile e della Password monouso.

Per configurare l'autenticazione con Password monouso:

1. Nel riquadro sinistro, in Autenticazione, selezionare **Dispositivo mobile**.
2. Per richiedere all'utente di inserire un PIN per accedere all'applicazione Security Tools Mobile dal dispositivo mobile, selezionare **Richiedi PIN**.

N.B. Se si abilita il criterio *Richiedi PIN* dopo aver registrato i dispositivi mobili con un computer, verrà annullata la registrazione di tutti i dispositivi mobili. Una volta attivato questo criterio, gli utenti dovranno registrare nuovamente i propri dispositivi mobili.

Se si seleziona la casella di controllo **Richiedi PIN**, gli utenti dovranno sbloccare il proprio dispositivo mobile per accedere all'app Security Tools Mobile. Se non è presente un blocco dispositivo nel dispositivo mobile, sarà richiesto il PIN.

3. Per selezionare la lunghezza della Password monouso (OTP), in **Lunghezza password monouso**, selezionare il numero di caratteri della password da richiedere.
4. Per selezionare il numero di tentativi che l'utente ha a disposizione per inserire correttamente la Password monouso, in **Tentativi di accesso utente consentiti**, selezionare un numero da **5** a **30**.

   Una volta raggiunto il limite massimo di tentativi consentiti, la funzione OPT sarà disabilitata finché l'utente non registrerà nuovamente il dispositivo mobile.

PROCEDURA CONSIGLIATA: Dell consiglia la configurazione di almeno un'altra modalità di autenticazione oltre alla Password monouso.

Configurare la registrazione delle smart card

DDP|Security Tools supporta due tipi di smart card: con contatti e senza contatti.

Le smart card con contatti richiedono l'uso di un lettore in cui inserire la scheda. Le smart card con contatti sono compatibili solo con i computer di dominio. Le smart card CAC e SIPRNet sono entrambe con contatti. A causa della tipologia avanzata di queste schede, all'utente sarà richiesto di scegliere un certificato dopo aver inserito la scheda per l'accesso.

- Le schede senza contatti sono supportate da computer non appartenenti al dominio e da computer configurati con specifiche di dominio.
- Gli utenti possono registrare una smart card con contatti per ciascun account utente oppure più schede senza contatti per account.
- Le smart card non sono supportate dall'Autenticazione di preavvio

N.B. Se si rimuove la registrazione di una smart card da un account con diverse schede registrate, verrà annullata la registrazione di tutte le schede allo stesso tempo.

Per configurare la registrazione di una smart card:

1. Nella scheda Autenticazione dello strumento Impostazioni amministratore, selezionare **Smart card**.

Configurare le autorizzazioni avanzate

1. Fare clic su **Avanzate** per modificare le opzioni avanzate per gli utenti finali. In *Avanzate* è possibile consentire agli utenti che lo desiderano di registrare autonomamente le credenziali o, facoltativamente, di modificare le credenziali registrate e abilitare l'accesso singolo.
2. Selezionare o deselezionare le caselle di controllo:

   Consenti agli utenti di registrare le credenziali - Questa casella di controllo è selezionata per impostazione predefinita. Gli utenti possono registrare le credenziali senza alcun intervento da parte dell'amministratore. Se la casella di controllo viene deselezionata, le credenziali dovranno essere registrate dall'amministratore.

   Consenti agli utenti di modificare le credenziali - Questa casella di controllo è selezionata per impostazione predefinita. Quando questa opzione è selezionata, gli utenti sono autorizzati a modificare o eliminare le proprie credenziali registrate, senza alcun intervento da parte dell'amministratore. Se si deseleziona la casella di controllo le credenziali non potranno essere modificate o eliminate da un utente ordinario, ma dovranno essere modificate o eliminate dall'amministratore.

N.B. Per registrare le credenziali di un utente, andare alla pagina *Utenti* dello strumento Impostazioni amministratore, selezionare un utente e fare clic su **Registra**.

   Consenti accesso singolo - L'accesso singolo equivale al Single Sign-on (SSO). Questa casella è selezionata per impostazione predefinita. Quando questa funzione è abilitata, gli utenti devono immettere le proprie credenziali solo nella schermata di Autenticazione di preavvio. Gli utenti accedono automaticamente a Windows. Se la casella di controllo viene deselezionata, può essere richiesto all'utente di effettuare l'accesso più volte.

N.B. Questa opzione può essere selezionata solo se è selezionata anche l'impostazione **Consenti agli utenti di registrare le credenziali**.

3. Al termine, fare clic su **Applica**.

Smart card e servizi di biometria (facoltativo)

Se non si desidera che Security Tools modifichi i servizi associati alle smart card e ai dispositivi biometrici con un avvio "automatico", la funzione di avvio del servizio può essere disabilitata.

Se disabilitato, Security Tools non tenterà di avviare i seguenti tre servizi:

- SCardSvr - Gestisce l'accesso alle smart card lette dal computer. Se il servizio viene interrotto, questo computer non potrà leggere le smart card. Se il servizio viene disabilitato, non sarà possibile avviare gli eventuali servizi che dipendono direttamente da esso.
- SCPolicySvc - Consente al sistema di essere configurato per il blocco del desktop utente dopo la rimozione della smart card.
- WbioSrvc - Il servizio di biometria di Windows permette alle applicazioni client di acquisire, confrontare, modificare e archiviare dati biometrici senza l'accesso diretto ad hardware o campioni biometrici. Il servizio è ospitato in un processo SVCHOST privilegiato.

La disabilitazione di questa funzione comporta anche l'annullamento degli avvisi associati ai servizi richiesti non in esecuzione.

Disabilitare l'avvio del servizio in automatico

Per impostazione predefinita, se non esiste la chiave del registro di sistema o il valore è impostato su 0 questa funzione è abilitata.

1. Eseguire **Regedit**.

2 Individuare la seguente voce di registro:

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Impostare su 0 per abilitare.
Impostare su 1 per disabilitare.

Gestire l'autenticazione degli utenti

I controlli nella scheda Autenticazione di Impostazioni amministratore consentono di impostare le opzioni di accesso dell'utente e personalizzare le impostazioni per ciascuna di esse.

Per gestire l'autenticazione degli utenti:

1 In qualità di amministratore, fare clic sul riquadro **Impostazioni amministratore**.

2 Fare clic sulla scheda **Utenti** per gestire gli utenti e visualizzare lo stato delle registrazioni degli utenti. Da questa scheda è possibile:

- Registrare nuovi utenti
- Aggiungere o modificare le credenziali
- Rimuovere le credenziali di un utente

N.B. Le voci **Accesso** e **Sessione** mostrano lo stato di registrazione di un utente.

Quando lo stato **Accesso** è **OK,** tutte le registrazioni di cui l'utente necessita per poter effettuare l'accesso sono state portate a termine. Quando lo stato **Sessione** è **OK,** tutte le registrazioni di cui l'utente necessita per poter utilizzare Password Manager sono state portate a termine.

Se per uno degli stati risulta **No**, l'utente deve portare a termine altre registrazioni. Per vedere quali registrazioni sono ancora necessarie, selezionare lo strumento **Impostazioni amministratore** e aprire la scheda **Utenti**. I segni di spunta grigi rappresentano le registrazioni incomplete. In alternativa, fare clic sul riquadro **Registrazioni** e rivedere la colonna **Criterio** della scheda **Stato**, dove sono elencate le registrazioni richieste.

Aggiungere nuovi utenti

N.B. I nuovi utenti di Windows vengono aggiunti automaticamente quando accedono a Windows o registrano le credenziali.

1 Fare clic su **Aggiungi utente** per iniziare il processo di registrazione per un utente Windows già esistente.

2 Quando viene visualizzata la finestra di dialogo *Seleziona utente*, selezionare **Tipi di oggetto**.

3 Immettere il nome di un oggetto utente nella casella di testo e fare clic su **Controlla nomi**.

4 Al termine fare clic su **OK**.

Si apre la registrazione guidata.

Per istruzioni passare a Registrare o modificare le credenziali utente.

Registrare o modificare le credenziali utente

L'amministratore può registrare o modificare le credenziali di un utente per suo conto; tuttavia vi sono alcune attività correlate alla registrazione che richiedono la presenza dell'utente, come rispondere alle domande di ripristino o la scansione delle impronte digitali dell'utente.

Per registrare o modificare le credenziali dell'utente:

1. In Impostazioni amministratore, fare clic sulla scheda **Utenti**.
2. Nella pagina Utenti, fare clic su **Registra**.
3. Nella pagina iniziale, fare clic su **Avanti**.
4. Nella finestra di dialogo Autenticazione richiesta, accedere con la password Windows dell'utente e fare clic su **OK**.
5. Nella pagina Password, per modificare la password Windows dell'utente, immettere 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**.
6. Seguire le istruzioni presenti in ogni pagina e fare clic sul pulsante appropriato: **Avanti**, **Ignora** o **Indietro**.
7. 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 la modifica di una credenziale, consultare la *Guida dell'utente di Dell Data Protection | Console*.

Rimuovere una credenziale registrata

1. Fare clic sul riquadro **Impostazioni amministratore**.
2. Fare clic sulla scheda **Utenti** e trovare l'utente da modificare.
3. Passare il mouse sul segno di spunta verde della credenziale che si vuole rimuovere. Il segno di spunta cambierà nel simbolo ⊗.
4. Fare clic sul simbolo ⊗, quindi fare clic su **Sì** per confermare l'eliminazione.

N.B. Una credenziale non può essere rimossa in questo modo se costituisce l'unica credenziale registrata dell'utente. Inoltre, non è possibile rimuovere la password con questo metodo. Utilizzare il comando Rimuovi per rimuovere completamente un accesso utente al computer.

Rimuovere tutte le credenziali registrate di un utente

1. Fare clic sul riquadro **Impostazioni amministratore**.
2. Fare clic sulla scheda **Utenti** e trovare l'utente che si desidera rimuovere.
3. Fare clic su **Rimuovi** (il comando Rimuovi viene visualizzato in rosso in fondo alle impostazioni dell'utente).

Dopo la rimozione, l'utente non potrà accedere al computer a meno che effettui nuovamente la registrazione.

5

Attività di disinstallazione

Per disinstallare DDP|ST è necessario che il ruolo utente sia almeno quello di **Amministratore locale**.

Disinstallare DDP|ST

È necessario disinstallare le applicazioni in questo ordine:

1. DDP | Client Security Framework
2. DDP | Security Tools Authentication
3. DDP | Security Tools

Se si dispone di un computer con un'unità autocrittografante, seguire queste istruzioni per procedere con la disinstallazione:

1. Effettuare il deprovisioning dell'unità autocrittografante:
   a. Da Impostazioni amministratore > fare clic sulla scheda **Crittografia**.
   b. Fare clic su **Decrittografa** per disabilitare la crittografia.
   c. Una volta decrittografata l'unità autocrittografante, riavviare il computer.
2. Nel Pannello di controllo di Windows, passare a **Disinstalla un programma**.

N.B. Start > Pannello di controllo > Programmi e funzionalità > Disinstalla un programma.

3. Disinstallare **Client Security Framework** e riavviare il computer.
4. Dal Pannello di controllo di Windows, disinstallare **Security Tools Authentication**.

   Viene visualizzato un messaggio con la richiesta di conferma se mantenere i dati utente.

   Fare clic su **Sì** se si prevede di reinstallare Security Tools. In caso contrario, fare clic su **No**.

   Al termine della disinstallazione, riavviare il sistema.
5. Dal Pannello di controllo di Windows, disinstallare **Security Tools**.

   Viene visualizzato un messaggio con la richiesta se si desidera disinstallare completamente l'applicazione e i suoi componenti.

   Fare clic su **Sì**.

   Viene visualizzata la finestra di dialogo *Disinstallazione completata*.
6. Fare clic su **Sì, riavvia ora** quindi su **Fine**.
7. Il computer viene riavviato e l'installazione completata.

6

Ripristino

Le opzioni di ripristino sono disponibili nel caso in cui le credenziali utente siano scadute o smarrite:

- **Password monouso (OTP):** Per poter effettuare nuovamente l'accesso, l'utente dovrà generare una OTP tramite l'app Security Tools Mobile in un dispositivo mobile registrato ed inserire l'OTP nella schermata di accesso Windows. Questa opzione è disponibile solo se l'utente ha effettuato la registrazione di un dispositivo mobile nel computer tramite Security Tools. Per utilizzare la funzione OTP per il ripristino, l'utente non deve aver utilizzato l'OTP per accedere al computer.

N.B. La funzione Password monouso (OTP) richiede la presenza del TPM attivato e di proprietà. Seguire le istruzioni in Cancellare la proprietà e attivare il TPM.
È possibile utilizzare una OTP per l'autenticazione o il ripristino, ma non per entrambi. Per ulteriori dettagli, consultare Configurare le opzioni di accesso.

- **Domande di ripristino:** Per poter accedere nuovamente al computer, l'utente dovrà rispondere correttamente ad una serie di domande personali. Questa opzione è disponibile solo nel caso in cui l'amministratore abbia configurato, abilitato e registrato le Domande di ripristino. Utilizzare l'opzione per ottenere nuovamente l'accesso al computer tramite la schermata Autenticazione di preavvio e la schermata di accesso di Windows.

Entrambi i metodi di ripristino necessitano di una preparazione da parte dell'utente mediante la registrazione delle domande di ripristino oppure mediante la registrazione nel computer di un dispositivo mobile con Security Tools.

Ripristino autonomo, domande di ripristino dell'accesso a Windows

Per rispondere alle domande di ripristino e ripristinare l'accesso alla schermata di accesso di Windows:

1. Per utilizzare le domande di ripristino, fare clic su **Non è possibile accedere al proprio account?**

   Verranno visualizzate le Domande di ripristino scelte in fase di registrazione.

2. Immettere le risposte e fare clic su **OK**.

   Rispondendo in modo appropriato alle domande, si passa alla modalità di ripristino dell'accesso. I passaggi successivi dipendono dalle credenziali non corrette.

   - Se è stata inserita una password di Windows non corretta, viene visualizzata la schermata Modifica password.
   - Se un'impronta digitale non viene riconosciuta, viene visualizzata la pagina di registrazione delle impronte digitali per poter registrare nuovamente le impronte digitali.

Ripristino autonomo, domande di ripristino di PBA

Per rispondere alle domande di ripristino e ripristinare l'accesso alla schermata Autenticazione di preavvio:

1. Nella schermata Autenticazione di preavvio, inserire il nome utente.
2. Nell'angolo inferiore sinistro della schermata, selezionare **Opzioni**.
3. Nel menu Opzioni, selezionare **Password dimenticata**.
4. Rispondere alle domande di ripristino e fare clic su **Accedi**.

Ripristino autonomo, Password monouso

La presente procedura descrive le modalità di utilizzo della funzione di Password monouso (OTP) per ripristinare l'accesso al computer nel caso in cui, ad esempio, la password di Windows sia scaduta, venga dimenticata o si superi il limite massimo di tentativi di accesso consentiti. L'opzione Password monouso (OTP) è disponibile solo nel caso in cui l'utente abbia effettuato la registrazione del dispositivo mobile e solo se l'OTP non sia stata utilizzata per eseguire l'accesso a Windows l'ultima volta.

N.B. La funzione Password monouso (OTP) richiede la presenza del TPM abilitato e di proprietà. L'OTP può essere utilizzata per l'autenticazione di Windows o per il ripristino, ma non per entrambi. L'amministratore può impostare il criterio per consentire la Password monouso per il ripristino, l'autenticazione o per disabilitare la funzione.

Per utilizzare la Password monouso per accedere al computer:

1. 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 Windows, DDP | Security Tools 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 che entrambi possano riconoscere la stessa password contemporaneamente. 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**.
6. Nel computer, nella schermata della modalità di ripristino, selezionare **Password di Windows dimenticata** e seguire le istruzioni visualizzate per reimpostare la password.

Glossario

Accesso singolo (SSO) - SSO semplifica il processo 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.

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

Deprovisioning - Il deprovisioning rimuove il database di PBA e disattiva la PBA. Affinché il deprovisioning abbia effetto, è necessario arrestare il sistema.

Password monouso (OTP) - La Password monouso è una password che può essere utilizzata una sola volta ed è valida per un periodo di tempo limitato. L'OTP richiede che il TPM sia presente, abilitato e di proprietà. Per abilitare l'OTP, deve essere associato un dispositivo mobile al computer tramite la DDP Security Console e l'app Security Tools Mobile. L'app Security Tools Mobile genererà una password nel dispositivo mobile utilizzato per accedere al computer nella schermata di accesso di Windows. A seconda dei criteri, la funzione OTP può essere utilizzata per ripristinare l'accesso al computer in caso di password scaduta o smarrita, 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. Il livello di sicurezza fornito dall'OTP è maggiore rispetto ad altri metodi di autenticazione in quanto la password generata può essere usata una sola volta e scade in breve tempo.

Trusted Platform Module (TPM) - Il TPM è un chip di protezione che svolge tre funzioni principali: archiviazione protetta, misurazioni e attestazione. DDP|E utilizza il TPM per la sua funzione di archiviazione protetta. Inoltre, il TPM è in grado di fornire contenitori crittografati per il software Vault di DDP|E e di proteggere la chiave di crittografia dell'HCA di DDP|E. Dell consiglia di eseguire il provisioning del TPM. L'utilizzo dell'HCA di DDP|E e della Password monouso prevede la presenza del TPM.


0XXXXXA0X