Dell Data Protection | Personal Edition

Guida all'installazione v8.13

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.

© 2017 Dell Inc. Tutti i diritti riservati. Dell, EMC e gli altri marchi sono marchi commerciali di Dell Inc. o delle sue sussidiarie. Gli altri marchi possono essere marchi dei rispettivi proprietari.

I marchi registrati e i marchi commerciali utilizzati nella suite di documenti Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise e Dell Data Guardian: Dell™ e il logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ sono marchi commerciali di Dell Inc. Cylance®, CylancePROTECT, e il logo Cylance sono marchi registrati di Cylance, Inc. negli Stati Uniti e in altri Paesi. McAfee® e il logo McAfee sono marchi commerciali o marchi registrati di McAfee, Inc. negli Stati Uniti e in altri Paesi. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® sono marchi registrati di Intel Corporation negli Stati Uniti e in altri Paesi. Adobe®, Acrobat® e Flash® sono marchi registrati di Adobe Systems Incorporated. Authen Tec® e Eikon® sono marchi registrati di Authen Tec. AMD® è un marchio registrato di Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® e Visual C++® sono marchi commerciali o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. VMware® è un marchio registrato o marchio commerciale di VMware, Inc. negli Stati Uniti o in altri Paesi. Box® è un marchio registrato di Box. DropboxSM è un marchio di servizio di Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play sono marchi commerciali o marchi registrati di Google Inc. negli Stati Uniti e in altri Paesi. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® sono marchi di servizio, marchi commerciali o marchi registrati di Apple, Inc. negli Stati Uniti e/o in altri Paesi. GO ID®, RSA® e SecurID® sono marchi registrati di Dell EMC. EnCase™ e Guidance Software® sono marchi commerciali o marchi registrati di Guidance Software. Entrust® è un marchio registrato di Entrust®, Inc. negli Stati Uniti e in altri Paesi. InstallShield® è un marchio registrato di Flexera Software negli Stati Uniti, in Cina, nella Comunità Europea, ad Hong Kong, in Giappone, a Taiwan e nel Regno Unito. Micron® e RealSSD® sono marchi registrati di Micron Technology, Inc. negli Stati Uniti e in altri Paesi. Mozilla® Firefox® è un marchio registrato di Mozilla Foundation negli Stati Uniti e/o in altri Paesi. iOS® è un marchio commerciale o un marchio registrato di Cisco Systems, Inc. negli Stati Uniti e in alcuni altri Paesi ed è concesso in licenza. Oracle® e Java® sono marchi registrati di Oracle e/o suoi affiliate. Altri nomi possono essere marchi commerciali dei rispettivi proprietari. SAMSUNG™ è un marchio commerciale di SAMSUNG negli Stati Uniti o in altri Paesi. Seagate® è un marchio registrato di Seagate Technology LLC negli Stati Uniti e/o in altri Paesi. Travelstar® è un marchio registrato di HGST, Inc. negli Stati Uniti e in altri Paesi. UNIX® è un marchio registrato di The Open Group. VALIDITY™ è un marchio commerciale di Validity Sensors, Inc. negli Stati Uniti e in altri Paesi. VeriSign® e altri marchi correlati sono marchi commerciali o marchi registrati di VeriSign, Inc. o sue affiliate o filiali negli Stati Uniti e in altri Paesi, ed è concesso in licenza a Symantec Corporation. KVM on IP® è un marchio registrato di Video Products. Yahoo!® è un marchio registrato di Yahoo! Inc. In questo prodotto vengono utilizzate parti del programma 7-Zip. Il codice sorgente è disponibile all'indirizzo 7-zip.org. La gestione delle licenze è basata sulla licenza GNU LGPL + restrizioni unRAR (7-zip.org/license.txt).

Guida all'installazione di Personal Edition

2017 - 04

Rev. A01

Sommario

1

Panoramica di Personal Edition

La presente guida presuppone l'installazione di Security Tools con Personal Edition.

Personal Edition

Lo scopo di Personal Edition è quello di proteggere i dati nel computer, anche nel caso venga rubato o sia perduto.

Per garantire la protezione dei dati riservati, Personal Edition crittografa i dati presenti nel computer Windows. L'utente può sempre accedere ai dati se connesso al computer, ma i dati protetti saranno invece inaccessibili agli utenti non autorizzati. I dati rimarranno sempre crittografati nell'unità ma, dato che la crittografia è trasparente, l'utente potrà continuare a lavorare come di sua abitudine con dati e applicazioni.

Normalmente, il client di crittografia decrittografa i dati durante il normale utilizzo. Occasionalmente, un'applicazione può provare ad accedere ad un file nello stesso momento in cui il client di crittografia lo sta crittografando o decrittografando. Se ciò avviene, dopo un secondo o due il client di crittografia visualizza una finestra di dialogo in cui viene data la possibilità di restare in attesa o annullare la crittografia/decrittografia. Se si sceglie di attendere, il client di crittografia rilascia il file non appena la procedura viene completata (generalmente entro pochi secondi).

Security Tools

L'obiettivo di Security Tools è di fornire una soluzione di protezione end-to-end per il supporto di Autenticazione avanzata.

Security Tools offre supporto a più fattori nell'autenticazione di Windows con password, lettori di impronte digitali e smart card (sia “senza contatto” che “con contatto”) nonché nell'autoregistrazione, Password monouso (OTP) e Accesso singolo (Single Sign-On [SSO]).

La Security Console è l'interfaccia di Security Tools che guida gli utenti nella configurazione delle loro credenziali e delle domande di autoripristino, in base al criterio impostato dall'amministratore locale.

Lo strumento Impostazioni amministratore è a disposizione degli utenti con privilegi di amministratore ed è utilizzato per impostare i criteri di autenticazione e le opzioni di ripristino, gestire gli utenti e configurare le impostazioni avanzate e le impostazioni specifiche delle credenziali supportate per l'accesso a Windows.

Consultare Configurare le impostazioni di amministratore di Security Tools e fare riferimento alla *Guida per l'utente di Dell Console* per informazioni sull'utilizzo delle applicazioni di Security Tools.

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

Requisiti di Personal Edition

Questi requisiti descrivono in dettaglio tutto il necessario per l'installazione di Personal Edition.

Client di crittografia

- Per installare correttamente Personal Edition sono necessari i diritti. I diritti vengono forniti all'acquisto di Personal Edition. A seconda della modalità di acquisto di Personal Edition, potrebbe essere necessario installare manualmente i diritti. In tal caso, seguire le semplici istruzioni relative ai diritti. Se Personal Edition viene installato usando Dell Digital Delivery, l'installazione dei diritti viene eseguita dal servizio Dell Digital Delivery (per Enterprise Edition e Personal Edition vengono utilizzati gli stessi binari; i diritti comunicano al programma di installazione quale versione installare).
- Dell consiglia vivamente di utilizzare una password di Windows (se non ne esiste già una) per proteggere l'accesso ai dati crittografati. La creazione di una password per il computer impedisce ad altri di accedere al proprio account utente.
  a Andare al Pannello di controllo di Windows (**Start** > **Pannello di controllo**).
  b Fare clic sull'icona **Account utente**.
  c Fare clic su **Crea una password per l'account**.
  d Immettere una nuova password e reinserirla.
  e Aggiungere facoltativamente un suggerimento per la password.
  f Fare clic su **Crea password**.
  g Riavviare il sistema.
- Durante la distribuzione è opportuno seguire le procedure consigliate. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e distribuzioni scaglionate agli utenti.
- L'account utente che esegue l'installazione/l'aggiornamento/la disinstallazione deve essere un utente amministratore del dominio o locale, che può essere assegnato temporaneamente tramite uno strumento di distribuzione, ad esempio Microsoft SMS o Dell KACE. Non sono supportati gli utenti non amministratori con privilegi elevati.
- Prima di iniziare l'installazione/la disinstallazione/l'aggiornamento, eseguire il backup di tutti i dati importanti.
- Durante l'installazione/la disinstallazione/l'aggiornamento non apportare modifiche al computer, quali l'inserimento o la rimozione di unità esterne (USB).
- Per ridurre la durata iniziale del processo di crittografia (o la durata del processo di decrittografia se si esegue la disinstallazione), eseguire Pulizia disco di Windows per rimuovere i file temporanei e tutti i dati non necessari.
- Per evitare che un computer non utilizzato da un utente passi alla modalità di sospensione durante la ricerca crittografia iniziale, disattivare tale modalità. La crittografia, o la decrittografia, non può essere eseguita in un computer in modalità di sospensione.
- Il client di crittografia non supporta le configurazioni di avvio doppio poiché è possibile crittografare file di sistema dell'altro sistema operativo, il che interferirebbe con il suo funzionamento.
- Il programma di installazione principale non supporta aggiornamenti da componenti di una versione precedente alla v8.0. Estrarre i programmi di installazione figlio dal programma di installazione principale e aggiornare singolarmente i componenti. In caso di domande o problemi, contattare Dell ProSupport.
- Il client di crittografia ora supporta la modalità Controllo. La modalità Controllo consente agli amministratori di distribuire il client di crittografia come parte dell'immagine aziendale, piuttosto che usare soluzioni SCCM di terzi o simili per distribuire il client di crittografia. Per istruzioni su come installare il client Encryption in un'immagine aziendale, vedere http://www.dell.com/support/article/us/en/19/SLN304039.
- Il TPM è usato per sigillare la GPK. Pertanto, se si esegue il client di crittografia, cancellare il TPM nel BIOS prima di installare un nuovo sistema operativo nel computer client.
- Il client di crittografia è stato testato ed è compatibile con McAfee, client Symantec, Kaspersky e MalwareBytes. Le esclusioni hardcoded sono utilizzate da questi provider di antivirus per impedire le incompatibilità tra crittografia e scansione antivirus. Il client di crittografia è stato testato anche con il Microsoft Enhanced Mitigation Experience Toolkit.

Se la propria organizzazione utilizza un provider di antivirus non in elenco, consultare l'articolo della KB SLN298707 o Contattare Dell ProSupport per assistenza.

- L'aggiornamento del sistema operativo sul posto non è supportato con il client di crittografia installato. Eseguire la disinstallazione e la decrittografia del client di crittografia, l'aggiornamento al nuovo sistema operativo, quindi reinstallare il client di crittografia.

  Inoltre, la reinstallazione del sistema operativo non è supportata. Per reinstallare il sistema operativo, eseguire un backup del computer di destinazione, cancellarne i dati, installare il sistema operativo e quindi ripristinare i dati crittografati seguendo le procedure di ripristino stabilite.
- Visitare periodicamente www.dell.com/support per la documentazione più recente e i suggerimenti tecnici.

Prerequisiti del client di crittografia

- Microsoft .Net Framework 4.5.2 (o versione successiva) è richiesto per il programma di installazione principale e i client del programma di installazione figlio.

  Tutti i computer spediti dalla fabbrica Dell sono dotati di Microsoft .Net Framework 4.5.2 (o versione successiva) preinstallato. Tuttavia, se non si sta installando il client in un hardware Dell o si sta aggiornando il client negli hardware Dell precedenti, è necessario verificare la versione di Microsoft .Net installata e aggiornare la versione, **prima di installare il client**, al fine di prevenire errori di installazione/aggiornamento. Per verificare la versione di Microsoft .Net installata, seguire queste istruzioni nel computer destinato all'installazione: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Per installare Microsoft .Net Framework 4.5.2, andare all'indirizzo https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Il programma di installazione principale installa Microsoft Visual C++ 2012 Update 4 se non è già installato nel computer. **Se si usa il programma di installazione figlio**, è necessario installare questo componente prima di installare il client di crittografia.

Prerequisito
• Visual C++ 2012 Update 4 o Redistributable Package (x86 e x64) successivo • Microsoft SQL Server Compact 3.5 SP2 (x86 e x64)

Hardware del client di crittografia

- La tabella seguente descrive in dettaglio l'hardware del computer supportato.

Hardware
• I requisiti hardware minimi devono soddisfare le specifiche minime del sistema operativo

- La tabella seguente descrive in dettaglio l'hardware facoltativo del computer supportato.

Hardware integrato facoltativo
• TPM 1.2 o 2.0

Sistemi operativi dei client di crittografia

- La tabella seguente descrive in dettaglio i sistemi operativi supportati.

Sistemi operativi Windows (a 32 e 64 bit)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate • Windows Embedded Standard 7 con modello Application Compatibility (la crittografia hardware non è supportata) • Windows 8: Enterprise, Pro

Sistemi operativi Windows (a 32 e 64 bit)

- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (la crittografia hardware non è supportata)
- Windows 10: Education, Enterprise, Pro
- VMware Workstation 5.5 e versioni successive

N.B.: La modalità UEFI non è supportata in Windows 7, Windows Embedded Standard 7 o Windows Embedded 8.1 Industry Enterprise.

Sistemi operativi per External Media Shield (EMS)

- La tabella seguente descrive in dettaglio i sistemi operativi supportati quando si esegue l'accesso a supporti protetti da EMS.

N.B.: Per ospitare l'EMS, il supporto esterno deve disporre di circa 55 MB di spazio, più una quantità di spazio libero equivalente alle dimensioni del file più grande da crittografare.

N.B.:
Windows XP è supportato solo quando si utilizza EMS Explorer.

Sistemi operativi Windows supportati per l'accesso a supporti protetti da EMS (a 32 e 64 bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Sistemi operativi Mac supportati per l'accesso a supporti protetti da EMS (kernel a 64 bit)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.0

Supporto lingue del client di crittografia

- Il client di crittografia è compatibile con l'interfaccia utente multilingue (MUI, Multilingual User Interface) e supporta le lingue seguenti.

Supporto lingue

- EN - Inglese
- ES - Spagnolo
- FR - Francese
- IT - Italiano
- DE - Tedesco
- JA - Giapponese
- KO - Coreano
- PT-BR - Portoghese (Brasile)
- PT-PT - Portoghese (Portogallo)

Client di autenticazione avanzata

- Se si usa Autenticazione avanzata, l'accesso degli utenti al computer verrà protetto utilizzando credenziali di autenticazione avanzata gestite e registrate tramite Security Tools. Security Tools sarà il gestore primario delle credenziali di autenticazione per l'accesso a

Windows, incluse password, impronte digitali e smart card di Windows. Le credenziali per la password grafica, per il PIN e per le impronte digitali registrate tramite sistema operativo Microsoft non verranno riconosciute durante l'accesso a Windows.

Per continuare a usare il sistema operativo Microsoft per la gestione delle credenziali, non installare o disinstallare Security Tools.

- Per la funzionalità Password monouso (OTP) di Security Tools è necessario che il computer sia dotato di TPM abilitato e di proprietà. L'OTP non è supportata con TPM 2.0. Per cancellare e impostare la proprietà del TPM, consultare https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Hardware del client di autenticazione avanzata

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

Lettori di impronte digitali e di smart card

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

Schede senza contatto

- 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.
- Schede per provider del servizio di crittografia (CSP, Cryptographic Service Provider)
- Schede di accesso comune (CAC, Common Access Card)
- Schede classe B/SIPR Net

- Driver e firmware per Dell ControlVault, lettori di impronte e smart card (come mostrato di seguito) non sono inclusi nei file eseguibili del programma di installazione principale o del programma di installazione figlio. I driver e il firmware devono essere sempre aggiornati ed è possibile scaricarli dal sito http://www.dell.com/support selezionando il modello del computer desiderato. Scaricare i driver e il firmware appropriati in base all'hardware di autenticazione.

  - Dell ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity Fingerprint Reader 495 Driver
  - O2Micro Smart Card Driver

  Se si installa in hardware diverso da Dell, scaricare i driver e il firmware aggiornati dal sito Web del fornitore. Le istruzioni per l'installazione dei driver di Dell ControlVault sono indicate in Driver di Dell ControlVault.
- 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

Sistemi operativi del client di autenticazione avanzata

Sistemi operativi Windows

- La tabella seguente descrive in dettaglio i sistemi operativi supportati.

Sistemi operativi Windows (a 32 e 64 bit)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate • Windows 8: Enterprise, Pro • Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition • Windows 10: Education, Enterprise, Pro

N.B.: La modalità UEFI non è supportata in Windows 7.

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

Supporto lingue per client di autenticazione avanzata

- Il client di autenticazione avanzata è compatibile con l'interfaccia utente multilingue (MUI, Multilingual User Interface) e supporta le lingue seguenti. La modalità UEFI e l'autenticazione di preavvio non sono supportate in russo, cinese tradizionale e 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

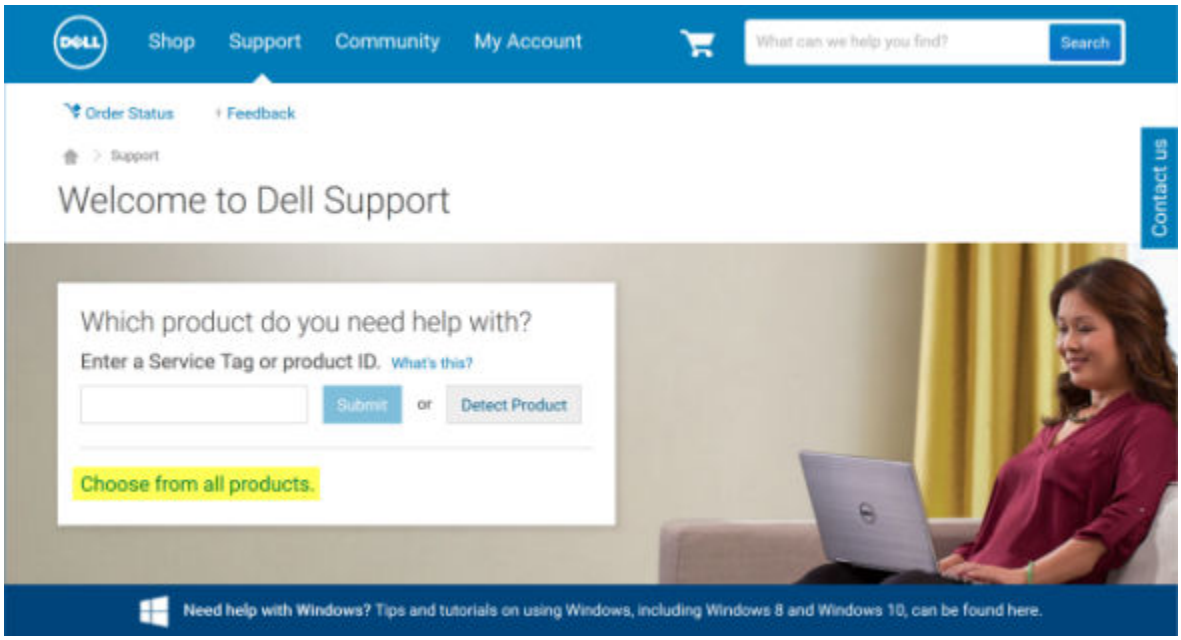
Passare a Come ottenere il software.

Scaricare il software

Questa sezione descrive in dettaglio come ottenere il software dal sito dell.com/support. Se l'utente dispone già del software è possibile ignorare questa sezione.

Accedere a dell.com/support per iniziare.

1 Nella pagina del supporto Dell, selezionare **Scegli tra tutti i prodotti**.



2 Selezionare **Software e sicurezza** dall'elenco di prodotti.

3 Selezionare **Soluzioni per la sicurezza degli endpoint** nella sezione *Software e sicurezza*.
Dopo aver effettuato la selezione una volta, il sito Web la memorizzerà.

4 Selezionare il prodotto Dell Data Protection.
Esempi:

Dell Encryption

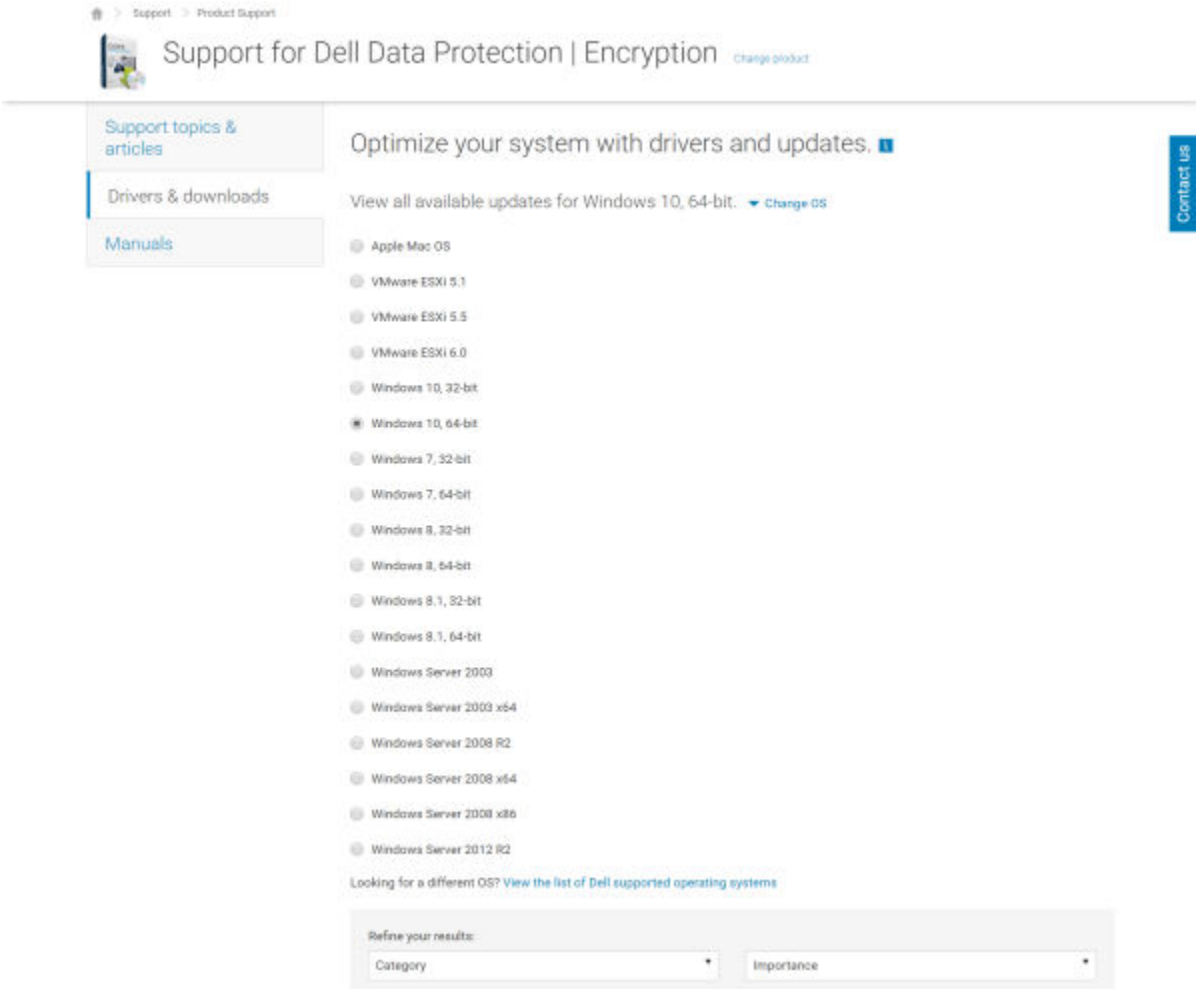
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Selezionare **Driver e download**.

6 Selezionare il tipo di sistema operativo del client desiderato.

7 Selezionare **Dell Data Protection (4 file)** nelle corrispondenze. Questo è solo un esempio, è probabile che si presenti in modo leggermente differente. Per esempio, potrebbero non esserci 4 file tra cui scegliere.



8 Selezionare **Scarica file** o **Aggiungi all'elenco dei download n. XX**.
Passare a Installare Personal Edition.

4

Installare Personal Edition

È possibile installare Personal Edition utilizzando il programma di installazione principale (scelta consigliata) o estraendo i programmi di installazione figlio dal programma di installazione principale. In entrambi i casi, è possibile installare Personal Edition dall'interfaccia utente, dalla riga di comando o da script, e utilizzando qualsiasi tecnologia push disponibile alla propria organizzazione.

Gli utenti devono prendere visione dei seguenti file della guida per assistenza sull'applicazione:

- Consultare la *Guida alla crittografia di Dell* per istruzioni sull'utilizzo della funzione del client di crittografia. Accedere alla guida da **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
- Consultare la *Guida a EMS* per istruzioni sulle funzioni dell'External Media Shield. Accedere alla guida da **<Install dir>:\Program Files\Dell \Dell Data Protection\Encryption\EMS**.
- Consultare la *Guida a Security Tools* per istruzioni sull'utilizzo delle funzioni di Autenticazione avanzata. Accedere alla guida da **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.

Scegliere un metodo di installazione

Vi sono due metodi per installare il client, selezionare **uno** dei seguenti:

- Installare Personal Edition usando il programma di installazione principale (SCELTA CONSIGLIATA)
- Installare Personal Edition usando i programmi di installazione figlio

Installare Personal Edition usando il programma di installazione principale (SCELTA CONSIGLIATA)

Per installare Personal Edition, il programma di installazione deve individuare i diritti appropriati nel sistema. Se non è possibile individuarli, l'installazione di Personal Edition non andrà a buon fine.

Il programma di installazione di Dell Data Protection è noto anche come programma di installazione principale, in quanto installa più client. Nel caso di Personal Edition, installa il client di crittografia e il client di Autenticazione avanzata.

Se si esegue l'installazione usando l'interfaccia utente del programma di installazione principale, è possibile installare Personal Edition in un computer alla volta.

I file di registro del programma di installazione principale si trovano in **C:\ProgramData\Dell\Dell Data Protection\Installer.**

Selezionare un metodo:

Installazione usando l'interfaccia utente

Installazione usando la riga di comando

Installazione usando l'interfaccia utente

Installare i diritti nel computer di destinazione, se necessario.

Copiare DDPSetup.exe nel computer locale.

Fare doppio clic su DDPSetup.exe per avviare il programma di installazione.

Viene visualizzata una finestra di dialogo che informa l'utente sullo stato di installazione dei prerequisiti. L'operazione richiede alcuni minuti.

Fare clic su **Avanti** nella schermata iniziale.

Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.

Fare clic su **Avanti** per installare Personal Edition nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection\.**

Security Tools è installato per impostazione predefinita e non è possibile deselezionarlo. Nel programma di installazione queste opzioni sono indicate come Security Framework.

L'Autenticazione avanzata è installata per impostazione predefinita e non è possibile deselezionarla.

Fare clic su **Avanti**.

Fare clic su **Installa** per avviare l'installazione.

Viene visualizzata una finestra di stato. L'operazione richiede alcuni minuti.

Selezionare **Sì, riavvia ora** e fare clic su **Fine**.

Al riavvio del sistema, autenticarsi in Windows.

L'installazione di Personal Edition + Security Tools è completa.

L'installazione e la configurazione guidate di Personal Edition sono trattate separatamente.

Quando l'installazione e la configurazione guidate di Personal Edition sono complete, avviare la console di amministrazione di Security Tools.

La parte rimanente di questa sezione descrive in dettaglio altre attività di installazione e può essere ignorata. Passare alle Installazioni guidate di Security Tools e Personal Edition

Installazione usando la riga di comando

Installare i diritti nel computer di destinazione, se necessario.

Opzioni:

Per eseguire l'installazione dalla riga di comando è necessario innanzitutto specificare le opzioni. La tabella seguente descrive in dettaglio le opzioni disponibili per l'installazione.

Opzione	Significato
-y -gm2	Trasmettere i dati all'autoestrattore
/S	Modalità non interattiva
/z	Trasmettere i dati alla CMDLINE della variabile di sistema InstallScript

Parametri:

La tabella seguente descrive in dettaglio i parametri disponibili per l'installazione.

Parametri
InstallPath=percorso di installazione alternativo.
FEATURE=PE

Esempio di installazione dalla riga di comando

Sebbene non sia incluso in questi esempi, potrebbe essere necessario un riavvio. La crittografia non può iniziare finché il computer non è stato riavviato.

È importante ricordare che tutti i valori contenenti uno o più caratteri speciali, ad esempio uno spazio, devono essere racchiusi tra virgolette con escape.

Le righe di comando fanno distinzione tra maiuscole/minuscole.

Nell'esempio seguente vengono installati Personal Edition e Security Tools (installazione invisibile all'utente, nessun riavvio e installati nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection**).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE\""
```

Nell'esempio seguente vengono installati Personal Edition e Security Tools (installazione invisibile all'utente, nessun riavvio e installati in un percorso alternativo **C:\Program Files\Dell\My_New_Folder**).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
```

Al riavvio del sistema, autenticarsi in Windows.

L'installazione di Personal Edition + Security Tools è completa.

L'installazione e la configurazione guidate di Personal Edition sono trattate separatamente.

Quando l'installazione e la configurazione guidate di Personal Edition sono complete, avviare la console di amministrazione di Security Tools.

La parte rimanente di questa sezione descrive in dettaglio altre attività di installazione e può essere ignorata. Passare alle Installazioni guidate di Security Tools e Personal Edition

Installare Personal Edition usando i programmi di installazione figlio

Per installare Personal Edition usando i programmi di installazione figlio, occorre prima estrarre i file eseguibili figlio dal programma di installazione principale. Consultare Estrarre i programmi di installazione figlio dal programma di installazione principale Al termine dell'operazione, tornare a questa sezione.

Installazione dalla riga di comando

Le opzioni e i parametri della riga di comando fanno distinzione tra maiuscole e minuscole.

È importante ricordare che tutti i valori contenenti uno o più caratteri speciali, ad esempio uno spazio nella riga di comando, devono essere racchiusi tra virgolette con escape.

Usare questi programmi di installazione per installare i client usando un'installazione tramite script, file batch o qualsiasi altra tecnologia push a disposizione della propria organizzazione.

Negli esempi delle righe di comando il riavvio è stato eliminato, ma un riavvio finale sarà necessario perché la crittografia non può iniziare finché il computer non è stato riavviato.

Windows crea file di registro di installazione dei programmi di installazione figlio univoci per l'utente che ha effettuato l'accesso a %temp % e si trovano nel percorso **C:\Users\<UserName>\AppData\Local\Temp.**

Se si decide di aggiungere un file di registro separato al momento dell'esecuzione del programma di installazione, accertarsi che il file di registro abbia un nome univoco, in quanto i file di registro dei programmi di installazione figlio non vengono aggiunti. Il comando .msi standard può essere utilizzato per creare un file di registro usando **/l*v C:\<qualsiasi directory>\<qualsiasi nome file di registro>.log**.

Per le installazioni dalla riga di comando, tutti i programmi di installazione figlio usano le stesse opzioni di visualizzazione e .msi di base, tranne dove indicato diversamente. È necessario specificare prima le opzioni. L'opzione /v è obbligatoria e richiede un argomento. Gli altri parametri devono essere inseriti nell'argomento che viene passato all'opzione /v.

Le opzioni di visualizzazione possono essere specificate in fondo all'argomento passato all'opzione /v per ottenere il comportamento desiderato. Non usare /q e /qn insieme nella stessa riga di comando. Usare solo ! e - dopo /qb.

Opzione	Significato
/v	Consente di passare variabili al file .msi all'interno di *.exe
/s	Modalità non interattiva
/i	Modalità di installazione

Opzione	Significato
/q	La finestra di dialogo non viene visualizzata e il sistema si riavvia automaticamente al termine del processo
/qb	Viene visualizzata una finestra di dialogo con il pulsante **Annulla** e viene richiesto di riavviare il sistema
/qb-	Viene visualizzata una finestra di dialogo con il pulsante **Annulla** e il sistema si riavvia automaticamente al termine del processo
/qb!	Viene visualizzata una finestra di dialogo senza il pulsante **Annulla** e viene richiesto di riavviare il sistema
/qb!-	Viene visualizzata una finestra di dialogo senza il pulsante **Annulla** e il sistema si riavvia automaticamente al termine del processo
/qn	L'interfaccia utente non viene visualizzata

Installare i driver

Driver e firmware per Dell ControlVault, lettori di impronte e smart card **non** sono inclusi nei file eseguibili del programma di installazione principale o del programma di installazione figlio. I driver e il firmware devono essere sempre aggiornati ed è possibile scaricarli dal sito http://www.dell.com/support selezionando il modello del computer desiderato. Scaricare i driver e il firmware appropriati in base all'hardware di autenticazione.

Dell ControlVault

NEXT Biometrics Fingerprint Driver

Validity Fingerprint Reader 495 Driver

O2Micro Smart Card Driver

Se si installa in hardware diverso da Dell, scaricare i driver e il firmware aggiornati dal sito Web del fornitore.

Quindi:

Installare i client di autenticazione avanzata

Gli utenti accederanno alla PBA utilizzando le proprie credenziali di Windows.

Il file si trova in **C:\extracted\Security Tools** e **C:\extracted\Security Tools\Authentication.**

Esempio di installazione dalla riga di comando

\Security Tools

Nell'esempio seguente viene installato Security Framework (installazione invisibile all'utente, nessun riavvio e installato nel percorso predefinito C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"/norestart /qn"
```

:

Questo client è necessario per l'autenticazione avanzata in v8.x.

Quindi:

\Security Tools\Authentication

Nell'esempio seguente viene installato Security Tools (installazione invisibile all'utente, nessun riavvio, installato nel percorso predefinito C:\Program Files\Dell\Dell Data Protection).

```
setup.exe /s /v"/norestart /qn"
```

Quindi:

Installare il client di crittografia

Se la propria organizzazione sta usando un certificato firmato da un'autorità radice, come EnTrust o Verisign, consultare i Requisiti del Client di crittografia. Per abilitare la convalida del certificato, è necessario modificare le impostazioni di registro nel computer client.

Il file si trova in **C:\extracted\Encryption.**

Esempio di installazione dalla riga di comando

Nell'esempio seguente vengono installati Personal Edition ed Encrypt for Sharing, vengono nascoste le icone sovrapposte, nessuna finestra di dialogo, nessuna barra di stato e viene eliminato il riavvio.

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

Al riavvio del sistema, autenticarsi in Windows.

L'installazione di Personal Edition + Security Tools è completa. L'installazione e la configurazione guidate di Personal Edition sono trattate separatamente.

Passare alle Installazioni guidate di Security Tools e Personal Edition

Installazioni guidate di Security Tools e Personal Edition

Accedere a Windows con il proprio nome utente e password. Verrà effettuato l'accesso a Windows. L'interfaccia potrebbe apparire diversa da quella che l'utente è abituato a vedere.

1 È possibile che il controllo dell'account utente richieda di eseguire l'applicazione. In tal caso, fare clic su Sì.

2 Dopo il riavvio dell'installazione iniziale viene visualizzata la procedura guidata di attivazione di Security Tools. Fare clic su **Avanti**.

3 Digitare e immettere nuovamente una nuova Password di amministratore per crittografia (EAP). Fare clic su **Avanti**.

4 Inserire un percorso di backup in un'unità di rete o in un supporto rimovibile per archiviare le informazioni di ripristino e fare clic su **Avanti**.

5 Fare clic su **Applica** per iniziare l'attivazione di ST.

6 Quando la procedura guidata di attivazione di Security Tools ha completato l'operazione, avviare l'installazione guidata di Personal Edition dall'icona di DDP nell'area di notifica (potrebbe avviarsi da sola).

   Questa procedura di configurazione guidata fornisce assistenza nell'utilizzo della crittografia per proteggere le informazioni sul computer. Se questa procedura guidata non viene completata, la crittografia non può iniziare.

   Leggere la schermata iniziale e fare clic su **Avanti**.

7 Selezionare un modello criteri. Il modello criteri stabilisce le impostazioni di criterio predefinite per la crittografia.

   Al completamento della configurazione iniziale, è possibile applicare facilmente un diverso modello criteri o personalizzare il modello selezionato nella console di gestione locale.

   Fare clic su **Avanti**.

8 Leggere e confermare l'avviso password di Windows. Se si desidera creare ora una password di Windows, consultare Requisiti.

9 Creare una Password di amministratore per crittografia (EAP) compresa fra 9 e 32 caratteri e confermarla. La password deve contenere caratteri alfabetici, numerici e speciali. Questa password può essere uguale all'EAP impostata per Security Tools, ma non è collegata ad essa. **Registrare e salvare la password in un luogo sicuro.** Fare clic su **Avanti**.

10 Fare clic su **Sfoglia** per scegliere un'unità di rete o un dispositivo di archiviazione rimovibile per eseguire il backup delle chiavi di crittografia (contenute in un'applicazione denominata LSARecovery_[hostname].exe).

   Queste chiavi sono utilizzate per ripristinare i dati in caso di determinati guasti al computer.

   Inoltre, future modifiche dei criteri talvolta richiedono di eseguire di nuovo il backup delle chiavi di crittografia. Se l'unità di rete o il dispositivo di archiviazione rimovibile è disponibile, il backup delle chiavi di crittografia viene eseguito in background. Tuttavia, se la posizione non è disponibile (ad esempio perché il dispositivo di archiviazione rimovibile non è inserito nel computer), le modifiche dei criteri saranno effettive solo dopo il backup manuale delle chiavi di crittografia.

   > **N.B.: Per istruzioni sul backup manuale delle chiavi di crittografia, fare clic su "? > Guida" nell'angolo superiore destro della console di gestione locale o fare clic su Start > Tutti i programmi > Dell > Dell Data Protection > Crittografia > Guida alla crittografia.**

   Fare clic su **Avanti**.

11 Nella schermata Conferma impostazioni di crittografia viene visualizzato un elenco di impostazioni di crittografia. Rivedere le voci e, al termine della selezione delle impostazioni, fare clic su **Conferma**.

   Viene avviata la configurazione del computer. Una barra di stato indica l'avanzamento della configurazione.

12 Fare clic su **Fine** per completare la configurazione.

13 Al termine della configurazione del computer per la crittografia è necessario riavviare il sistema. Fare clic su **Riavvia ora** oppure è possibile posporre di 20 minuti il riavvio per 5 volte.

14 Al termine del riavvio del computer, aprire la console di gestione locale dal menu Start per verificare lo stato di crittografia.

La crittografia viene eseguita in background. La console di gestione locale può essere aperta o chiusa, la crittografia dei file procede in entrambi i casi. Durante la crittografia è possibile continuare a utilizzare normalmente il computer.

15 Al termine della scansione, il computer verrà riavviato ancora una volta.

Al termine di tutte le ricerche di crittografia e i riavvii, è possibile verificare lo stato di conformità avviando la console di gestione locale. L'unità verrà etichettata come "Conforme".

Passare a Configurare le impostazioni amministratore di Security Tools.

Configurare le impostazioni amministratore per Security Tools

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 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 tale percorso non è disponibile (ad esempio perché l'unità USB di backup non è inserita), Security Tools richiederà un percorso per il backup dei dati. Per poter iniziare la crittografia sarà richiesto l'accesso ai dati di ripristino.

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:

Nel riquadro sinistro, in Autenticazione, selezionare **Opzioni di accesso**.

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.

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**.

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.

: 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 sotto Opzioni di ripristino, 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 entrambe le caselle di controllo sotto Opzioni di ripristino: Domande di ripristino e Password monouso.

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*.

:

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.

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:

Nel riquadro sinistro, sotto Autenticazione, selezionare **Password Manager**.

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.

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.

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**.

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

: 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:

Nel riquadro sinistro, in Autenticazione, selezionare **Domande di ripristino**.

Nella pagina Domande di ripristino, selezionare almeno tre domande di ripristino predefinite.

Facoltativamente, possono essere aggiunte fino a tre domande personalizzate nell'elenco mostrato all'utente per la selezione.

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:

Nel riquadro sinistro, in Autenticazione, selezionare **Impronte**.

In Registrazioni, impostare il numero minimo e massimo di dita che un utente può registrare.

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.

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.

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

Configurare l'autenticazione della Password monouso

: Per la funzionalità Password monouso (OTP) è necessario che il computer sia dotato di TPM abilitato e di proprietà. Per istruzioni sull'impostazione del TPM, consultare Configurazione di preinstallazione per password monouso.

Per avvalersi della funzione Password monouso, l'utente genera nel proprio dispositivo mobile una password monouso con l'applicazione Security Tools Mobile, quindi immette 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 una password.

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:

Nel riquadro sinistro, in Autenticazione, selezionare **Dispositivo mobile**.

Per richiedere all'utente di inserire una password per accedere all'applicazione Security Tools Mobile dal dispositivo mobile, selezionare **Richiedi password.**

: **Se si abilita il criterio *Richiedi password* dopo aver registrato i dispositivi mobili in 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 la casella di controllo **Richiedi password** è stata selezionata, gli utenti devono sbloccare il dispositivo mobile per accedere all'applicazione Security Tools Mobile. Se non è presente un blocco dispositivo nel dispositivo mobile, sarà richiesta la password.

Per selezionare la lunghezza della Password monouso (OTP), in **Lunghezza password monouso**, selezionare il numero di caratteri della password da richiedere.

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.

: **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

: **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:

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

Configurare le autorizzazioni avanzate

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.

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.

: 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.

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

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

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

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

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

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

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

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:

In Impostazioni amministratore, fare clic sulla scheda **Utenti**.

Nella pagina Utenti, fare clic su **Registra**.

Nella pagina iniziale, fare clic su **Avanti**.

Nella finestra di dialogo Autenticazione richiesta, accedere con la password Windows dell'utente e fare clic su **OK**.

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**.

Seguire le istruzioni presenti in ogni pagina e fare clic sul pulsante appropriato: **Avanti**, **Ignora** o **Indietro**.

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 *Guida per l'utente della console*.

Rimuovere una credenziale registrata

Fare clic sul riquadro **Impostazioni amministratore**.

Fare clic sulla scheda **Utenti** e trovare l'utente da modificare.

Passare il mouse sul segno di spunta verde della credenziale che si desidera rimuovere. Il segno di spunta cambierà nel simbolo .

Fare clic sul simbolo , quindi fare clic su **Sì** per confermare l'eliminazione.

: 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

Fare clic sul riquadro **Impostazioni amministratore**.

Fare clic sulla scheda **Utenti** e trovare l'utente che si desidera rimuovere.

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.

Eseguire la disinstallazione usando il programma di installazione principale

- Ciascun componente deve essere disinstallato separatamente, seguito dalla disinstallazione del programma di installazione principale. I client devono essere disinstallati secondo un **ordine specifico per impedire errori durante la disinstallazione**.
- Seguire le istruzioni in Estrarre i programmi di installazione figlio dal programma di installazione principale per ottenere i programmi di installazione figlio.
- Per la disinstallazione accertarsi di usare la stessa versione del programma di installazione principale (e quindi dei client) usata per l'installazione.
- Questo capitolo fa riferimento ad un altro capitolo che contiene istruzioni *dettagliate* sulla disinstallazione dei programmi di installazione figlio. Questo capitolo spiega **solo** l'ultima fase di disinstallazione del programma di installazione principale.

Disinstallare i client nell'ordine seguente:

1 Disinstallare il client di crittografia.
2 Disinstallare Client Security Framework.
3 Disinstallare l'autenticazione avanzata.

Non è necessario disinstallare il pacchetto di driver.

Passare a Scegliere un metodo di disinstallazione.

Scegliere un metodo di disinstallazione

Vi sono due metodi per disinstallare il programma di installazione principale, selezionare **uno** dei seguenti:

- Eseguire la disinstallazione da Installazione applicazioni
- Eseguire la disinstallazione dalla riga di comando

Eseguire la disinstallazione da Installazione applicazioni

Andare a Disinstalla un programma nel Pannello di controllo di Windows (**Start** > **Pannello di controllo** > **Programmi e funzionalità** > **Disinstalla un programma.**).

Evidenziare **Dell Data Protection Installer** e fare clic con il pulsante sinistro del mouse su **Modifica** per avviare l'installazione guidata.

Leggere la schermata iniziale e fare clic su **Avanti**.

Seguire le istruzioni per la disinstallazione e fare clic su **Fine**.

Riavviare il sistema e accedere a Windows.

Il programma di installazione principale è stato disinstallato.

Eseguire la disinstallazione dalla riga di comando

Nell'esempio seguente viene eseguita la disinstallazione automatica del programma di installazione principale.

```
"DDPSetup.exe" -y -gm2 /S /x
```

Al termine, riavviare il sistema.

Il programma di installazione principale è stato disinstallato.

Passare a Eseguire la disinstallazione usando i programmi di installazione figlio.

Eseguire la disinstallazione usando i programmi di installazione figlio

- L'utente che esegue la decrittografia e la disinstallazione deve essere un amministratore del dominio o locale. Se si esegue la disinstallazione dalla riga di comando sono necessarie le credenziali di amministratore del dominio.
- Se Personal Edition è stato installato con il programma di installazione principale, prima di eseguire la disinstallazione occorre prima estrarre i file eseguibili figlio dal programma di installazione principale, come mostrato in Estrarre i programmi di installazione figlio dal programma di installazione principale.
- Per la disinstallazione accertarsi di usare la stessa versione di client usata per l'installazione.
- Se possibile, eseguire la decrittografia di notte.
- Per evitare che un computer non utilizzato da un utente passi alla modalità di sospensione, disattivare tale modalità. La decrittografia non può essere eseguita in un computer in modalità di sospensione.
- Arrestare tutti i processi e le applicazioni per ridurre al minimo gli errori dovuti a file bloccati.

Disinstallare il client di crittografia

- **Prima di iniziare il processo di disinstallazione**, Creare un file di registro dell'Encryption Removal Agent (facoltativo). Questo file di registro è utile per risolvere eventuali problemi di un'operazione di disinstallazione/decrittografia. Se non si desidera decrittografare file durante il processo di disinstallazione, non è necessario creare un file di registro di Encryption Removal Agent.
- Eseguire WSScan per accertarsi che tutti i dati siano decrittografati al termine della disinstallazione, ma prima di riavviare il sistema. Per istruzioni, consultare Usa WSScan.
- Periodicamente Verificare lo stato dell'Encryption Removal Agent. La decrittografia dei dati è ancora in corso se il servizio Encryption Removal Agent è ancora presente nel pannello Servizi.

Scegliere un metodo di disinstallazione

Vi sono due metodi per disinstallare il client di crittografia, selezionare **uno** dei seguenti:

Eseguire la disinstallazione usando l'interfaccia utente

Eseguire la disinstallazione dalla riga di comando

Eseguire la disinstallazione usando l'interfaccia utente

Andare a Disinstalla un programma nel Pannello di controllo di Windows (**Start** > **Pannello di controllo** > **Programmi e funzionalità** > **Disinstalla un programma.**).

Evidenziare **Encryption** e fare clic con il pulsante sinistro del mouse su **Cambia** per avviare l'Installazione guidata di Personal Edition.

Leggere la schermata iniziale e fare clic su **Avanti**.

Nella schermata di installazione di Encryption Removal Agent, selezionare una delle voci seguenti:

: La seconda opzione è abilitata per impostazione predefinita. Se si desidera eseguire la decrittografia dei file, accertarsi di selezionare la prima opzione.

Encryption Removal Agent - Importa chiavi da file

Per la crittografia SDE, Utente o Comune, questa opzione decrittografa i file e disinstalla il client di crittografia. ***Questa è la scelta consigliata.***

Non installare Encryption Removal Agent

Questa opzione disinstalla il client di crittografia, *ma non esegue la decrittografia dei file*. Utilizzare questa opzione **solo** per la risoluzione dei problemi, come indicato da Dell ProSupport.

Fare clic su **Avanti**.

Nella casella di testo *File di backup*, immettere il percorso all'unità di rete o alla posizione del supporto rimovibile del file di backup o fare clic su **...** per scegliere la posizione. Il formato del file è LSARecovery_[nomehost].exe.

Immettere la Password di amministratore per crittografia nella casella di testo Password. È la password impostata nella configurazione guidata quando è stato installato il software.

Fare clic su **Avanti**.

Nella schermata *Accesso a Dell Decryption Agent Service come* sono disponibili due opzioni. Selezionare **Account di sistema locale**. Fare clic su **Fine**.

Nella schermata Rimuovi il programma fare clic su **Rimuovi**.

Nella schermata Configurazione completata fare clic su **Fine**.

Riavviare il sistema e accedere a Windows.

La decrittografia è ora in corso.

Il processo di decrittografia potrebbe richiedere diverse ore, a seconda del numero di unità da decrittografare e della quantità di dati in quelle unità. Per controllare il processo di decrittografia, consultare Verificare lo stato dell'Encryption Removal Agent.

Eseguire la disinstallazione dalla riga di comando

Le opzioni e i parametri della riga di comando fanno distinzione tra maiuscole e minuscole.

È importante ricordare che tutti i valori contenenti uno o più caratteri speciali, ad esempio uno spazio nella riga di comando, devono essere racchiusi tra virgolette con escape. I parametri della riga di comando fanno distinzione tra maiuscole e minuscole.

Usare questi programmi di installazione per disinstallare i client usando un'installazione tramite script, file batch o qualsiasi altra tecnologia push disponibile alla propria organizzazione.

File di registro

Windows crea file di registro di disinstallazione dei programmi di installazione figlio univoci per l'utente che ha effettuato l'accesso a %temp%, e si trovano nel percorso C:\Users\<UserName>\AppData\Local\Temp.

Se si decide di aggiungere un file di registro separato al momento dell'esecuzione del programma di installazione, accertarsi che il file di registro abbia un nome univoco, in quanto i file di registro dei programmi di installazione figlio non vengono aggiunti. Il comando .msi standard può essere utilizzato per creare un file di registro usando /l C:\<qualsiasi directory>\<qualsiasi nome file di registro>.log. Dell sconsiglia di usare "/l*v" (registrazione dettagliata) durante la disinstallazione da una riga di comando, poiché nome utente/password sono registrati nel file di registro.

Per le disinstallazioni dalla riga di comando, tutti i programmi di installazione figlio usano le stesse opzioni di visualizzazione e .msi di base, tranne dove indicato diversamente. È necessario specificare prima le opzioni. L'opzione /v è obbligatoria e richiede un argomento. Gli altri parametri devono essere inseriti nell'argomento che viene passato all'opzione /v.

Le opzioni di visualizzazione possono essere specificate in fondo all'argomento passato all'opzione /v per ottenere il comportamento desiderato. Non usare /q e /qn insieme nella stessa riga di comando. Usare solo ! e - dopo /qb.

Opzione	Significato
/v	Consente di passare variabili al file .msi all'interno di setup.exe
/s	Modalità non interattiva
/x	Modalità di disinstallazione

Opzione	Significato
/q	La finestra di dialogo non viene visualizzata e il sistema si riavvia automaticamente al termine del processo
/qb	Viene visualizzata una finestra di dialogo con il pulsante **Annulla** e viene richiesto di riavviare il sistema
/qb-	Viene visualizzata una finestra di dialogo con il pulsante **Annulla** e il sistema si riavvia automaticamente al termine del processo
/qb!	Viene visualizzata una finestra di dialogo senza il pulsante **Annulla** e viene richiesto di riavviare il sistema
/qb!-	Viene visualizzata una finestra di dialogo senza il pulsante **Annulla** e il sistema si riavvia automaticamente al termine del processo
/qn	L'interfaccia utente non viene visualizzata

Una volta estratto dal programma di installazione principale, il programma di installazione del client di crittografia è disponibile al percorso C:\extracted\Encryption\DDPE_XXbit_setup.exe.

La tabella seguente descrive in dettaglio i parametri disponibili per la disinstallazione.

Parametro	Selezione
CMG_DECRYPT	Proprietà che consente di selezionare il tipo di installazione di Encryption Removal Agent: 2 - Ottenere le chiavi usando un bundle di chiavi Forensic 0 - Non installare Encryption Removal Agent
CMGSILENTMODE	Proprietà che consente di eseguire la disinstallazione invisibile all'utente: 1 - Invisibile all'utente 0 - Visibile all'utente
DA_KM_PW	Password dell'account amministratore di dominio.
DA_KM_PATH	Percorso per il bundle di materiale delle chiavi.

Nell'esempio seguente viene eseguita la disinstallazione del client Encryption senza installare Encryption Removal Agent.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:\FullPathToLSA.exe
DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

Nell'esempio seguente viene eseguita la disinstallazione del client Encryption usando un bundle di chiavi Forensic. Copiare il bundle di chiavi Forensic nel disco locale, quindi eseguire questo comando.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:
\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

Al termine, riavviare il sistema.

Il processo di decrittografia potrebbe richiedere diverse ore, a seconda del numero di unità da decrittografare e della quantità di dati in quelle unità. Per controllare il processo di decrittografia, consultare Verificare lo stato dell'Encryption Removal Agent.

Disinstallare Autenticazione avanzata

Scegliere un metodo di disinstallazione

Vi sono due metodi per disinstallare il client di crittografia, selezionare **uno** dei seguenti:

- Eseguire la disinstallazione usando l'interfaccia utente
- Eseguire la disinstallazione dalla riga di comando

Eseguire la disinstallazione usando l'interfaccia utente

1. Andare a Disinstalla un programma nel Pannello di controllo di Windows (**Start** > **Pannello di controllo** > **Programmi e funzionalità** > **Disinstalla un programma.**).
2. Evidenziare **Security Tools Authentication** e fare clic con il pulsante sinistro del mouse su **Cambia** per avviare l'installazione guidata.
3. Leggere la schermata iniziale e fare clic su **Avanti**.
4. Immettere la password amministratore.
5. Seguire le istruzioni per la disinstallazione e fare clic su **Fine**.
6. Riavviare il sistema e accedere a Windows.

Security Tools Authentication è stato disinstallato.

Eseguire la disinstallazione dalla riga di comando

1. Una volta estratto dal programma di installazione principale, il programma di installazione del client di Autenticazione avanzata è disponibile al percorso C:\extracted\Security Tools\Authentication\<x64/x86>\setup.exe.
2. Nell'esempio seguente viene eseguita la disinstallazione automatica del client di Autenticazione avanzata.

```
setup.exe /x /s /v" /qn"
```

3. Al termine, arrestare e riavviare il sistema.

Passare a Criteri e descrizioni dei modelli.

Disinstallare Client Security Framework

Scegliere un metodo di disinstallazione

Vi sono due metodi per disinstallare il client di crittografia, selezionare **uno** dei seguenti:

- Eseguire la disinstallazione usando l'interfaccia utente
- Eseguire la disinstallazione dalla riga di comando

Eseguire la disinstallazione usando l'interfaccia utente

1. Andare a Disinstalla un programma nel Pannello di controllo di Windows (**Start** > **Pannello di controllo** > **Programmi e funzionalità** > **Disinstalla un programma.**).
2. Evidenziare **Client Security Framework** e fare clic con il pulsante sinistro del mouse su **Cambia** per avviare l'installazione guidata.
3. Leggere la schermata iniziale e fare clic su **Avanti**.
4. Seguire le istruzioni per la disinstallazione e fare clic su **Fine**.
5. Riavviare il sistema e accedere a Windows.

Client Security Framework è stato disinstallato.

Eseguire la disinstallazione dalla riga di comando

Una volta estratto dal programma di installazione principale, il programma di installazione del client di Client Security Framework è disponibile al percorso C:\extracted\Security Tools\EMAgent_.

Nell'esempio seguente viene eseguita la disinstallazione automatica del client dell'unità autocrittografante.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

Al termine, arrestare e riavviare il sistema.

9

Criteri e descrizioni dei modelli

I suggerimenti vengono visualizzati al passaggio del mouse su un criterio nella console di gestione locale.

Criteri

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Criteri dei dispositivi di archiviazione fissi										
Crittografia SDE abilitata	Vero								Falso	È il "criterio principale" per tutti gli altri criteri di System Data Encryption (SDE). Se il criterio è Falso, la crittografia SDE non viene eseguita, indipendentemente dai valori degli altri criteri. Se il criterio è Vero, tutti i dati non crittografati tramite altri criteri Intelligent Encryption verranno crittografati in base al criterio Regole di crittografia SDE. Se si modifica il valore di questo criterio, è necessario riavviare il sistema.
Algoritmo crittografia SDE	AES256									AES 256, AES 128, 3DES
Regole di crittografia SDE										Regole di crittografia da utilizzare per includere o escludere dalla crittografia determinate unità, directory e cartelle. Contattare Dell ProSupport in caso di dubbi sulla modifica dei valori predefiniti.
Criteri delle impostazioni generali										

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Crittografia abilitata	Vero							Falso		È il "criterio principale" per tutti i criteri delle impostazioni generali. Se impostato su Falso, la crittografia non viene eseguita, indipendentemente dai valori degli altri criteri. Se impostato su Vero, tutti i criteri di crittografia sono abilitati. Cambiando il valore di questo criterio, si avvia una nuova ricerca per la crittografia/decrittografia dei file.
Cartelle crittografate comuni										Stringa: massimo 100 voci di 500 caratteri ognuna (fino a un massimo di 2.048 caratteri) Un elenco di cartelle nelle unità endpoint che si desidera crittografare o escludere dalla crittografia e a cui in seguito possono accedere tutti gli utenti gestiti autorizzati ad accedere all'endpoint. Le lettere delle unità disponibili sono: #: si riferisce a tutte le unità f#: si riferisce a tutte le unità fisse r#: si riferisce a tutte le unità rimovibili Importante: ignorare la protezione della directory può causare il mancato avvio del computer e/o richiedere la riformattazione delle unità. Se una stessa cartella è specificata sia in questo criterio sia nel criterio Cartelle crittografate utente, prevarrà questo criterio.
Algoritmo crittografia comune	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES I file di paging del sistema sono crittografati usando l'algoritmo AES 128.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Elenco Application Data Encryption	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									Stringa: massimo 100 voci di 500 caratteri ognuna Dell sconsiglia di aggiungere explorer.exe o iexplorer.exe all'elenco crittografia dati applicazioni (ADE), poiché potrebbero verificarsi risultati inaspettati o indesiderati. Tuttavia, explorer.exe è il processo utilizzato per creare un nuovo file Blocco note sul desktop utilizzando il menu di scelta rapida. Impostare la crittografia in base all'estensione del file, piuttosto che all'elenco ADE, garantisce una protezione più estesa. Elencare i nomi dei processi delle applicazioni (senza percorsi) di cui si desidera crittografare i nuovi file, separati da ritorni a capo. Non usare caratteri jolly. Dell sconsiglia di aggiungere all'elenco applicazioni/ programmi di installazione che scrivono file di importanza critica per il sistema. In questo modo, infatti, si rischia di crittografare importanti file di sistema, causando il mancato avvio di un computer. Nomi di processi comuni: outlook.exe, winword.exe, frontpg.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe I seguenti nomi di processo dei programmi di installazione e del sistema con codifica permanente vengono ignorati se specificato in questo criterio: hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Chiave di Application Data Encryption	Comune									Comune o utente Scegliere una chiave che indica chi dovrebbe avere accesso ai file crittografati con Elenco Application Data Encryption e dove. Comune: se si desidera che questi file siano accessibili a tutti gli utenti gestiti nell'endpoint in cui sono stati creati (stesso livello di accesso delle Cartelle crittografate comuni) e crittografati con l'Algoritmo crittografia comune. Utente: se si desidera che questi file siano accessibili solo all'utente che li ha creati, solo nell'endpoint in cui sono stati creati (stesso livello di accesso delle Cartelle crittografate utente), e crittografati con l'Algoritmo crittografia utente. Eventuali modifiche apportate a questo criterio non si ripercuotono sui file precedentemente crittografati in virtù di questo criterio.
Crittografa cartelle personali Outlook	Vero							Falso		Se impostato su Vero, si esegue la crittografia delle cartelle personali di Outlook.
Crittografa file temporanei	Vero							Falso		Se impostato su Vero, si esegue la crittografia dei percorsi elencati nelle variabili di ambiente TEMP e TMP con la chiave di crittografia dati utente.
Crittografa file temporanei Internet	Vero	Falso								Se impostato su Vero, si esegue la crittografia del percorso elencato nelle variabili di ambiente CSIDL_INTERNET_CACHE con la chiave di crittografia dati utente. Per ridurre i tempi della ricerca di crittografia, il client elimina i contenuti di

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										CSIDL_INTERNET_CACHE per eseguire la crittografia iniziale, nonché gli aggiornamenti di questo criterio. Questo criterio è applicabile esclusivamente quando si utilizza Microsoft Internet Explorer.
Crittografa documenti profilo utente	Vero								Falso	Se impostato su Vero, crittografa: · Il profilo utente (**C:\Users \jsmith**) con la chiave di crittografia dati utente · \Users\Public con la chiave di crittografia comune
Crittografia file di paging Windows	Vero								Falso	Vero permette di crittografare il file di paging Windows. Se si modifica questo criterio, è necessario riavviare il sistema.
Servizi gestiti										Stringa: massimo 100 voci di 500 caratteri ognuna (fino a un massimo di 2.048 caratteri) I servizi gestiti da questo criterio vengono avviati solo dopo che l'utente ha effettuato l'accesso e il client è stato sbloccato. Inoltre, questo criterio garantisce che il servizio gestito dal criterio venga interrotto prima del blocco del client durante la chiusura della sessione. Il criterio può infine impedire la chiusura di una sessione da parte dell'utente se il servizio non risponde. La sintassi prevede un nome di servizio per riga. Gli spazi nel nome del servizio sono supportati. I caratteri jolly non sono supportati. I servizi gestiti non vengono avviati se effettua l'accesso un utente non gestito.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Pulitura sicura post-crittografia	Sovrascrittura a tre passaggi	Sovrascrittura a passaggio singolo							Senza sovrascrittura	Senza sovrascrittura, Sovrascrittura a passaggio singolo, Sovrascrittura a tre passaggi, Sovrascrittura a sette passaggi Una volta crittografate le cartelle specificate da altri criteri in questa categoria, questo criterio stabilisce cosa fare con la parte non crittografata dei file originali: · Senza sovrascrittura la cancella. Questo valore fornisce il processo di crittografia più rapido. · Sovrascrittura a passaggio singolo la sovrascrive con dati casuali. · Sovrascrittura a tre passaggi la sovrascrive con un modello standard binario, successivamente con il relativo complemento e infine con dati casuali. · Sovrascrittura a sette passaggi la sovrascrive con uno schema standard binario, successivamente con il relativo complemento e infine con dati casuali per cinque volte. Con questo valore ripristinare i file originali dalla memoria è più difficile e il processo di crittografia è più sicuro.
Proteggi file di sospensione di Windows	Vero					Falso		Vero	Falso	Se questo criterio è abilitato, il file di sospensione viene crittografato solo quando il computer passa allo stato di sospensione. Il client disattiva la protezione quando il sistema esce dallo stato di sospensione, assicurando la protezione senza influire sull'attività di utenti o applicazioni mentre il sistema è in uso.
Impedisci sospensione non protetta	Vero					Falso		Vero	Falso	Quando questo criterio è abilitato, il client non consente la sospensione del computer se il client non è in grado di

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										crittografare i dati di sospensione.
Priorità scansione workstation	Alta	Normale								Massima, Alta, Normale, Bassa, Minima Specifica la priorità relativa di Windows del processo di scansione della cartella crittografata.
Cartelle crittografate utente										Stringa: massimo 100 voci di 500 caratteri ognuna (fino a un massimo di 2.048 caratteri) Un elenco di cartelle nel disco rigido endpoint che si desidera crittografare con la chiave di crittografia dati utente o escludere dalla crittografia. Questo criterio è valido per tutte le unità classificate come Unità disco rigido da Windows. Non è possibile utilizzare questo criterio per crittografare un'unità o un supporto esterno classificato come Disco rimovibile, in questo caso utilizzare EMS - Crittografa il supporto esterno.
Algoritmo crittografia utente	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES Algoritmo di crittografia utilizzato per crittografare i dati a livello di singolo utente. È possibile specificare valori diversi per utenti diversi dello stesso endpoint.
Chiave di crittografia dati utente	Utente	Comune		Utente	Comune				Utente	Comune o utente Scegliere una chiave che indica chi dovrebbe avere accesso ai file crittografati in base ai seguenti criteri, e dove: · Cartelle crittografate utente · Crittografa cartelle personali Outlook · Crittografa file temporanei (solo in \Documents and

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										Settings\username\Local Settings\Temp) · Crittografa file temporanei Internet · Crittografa documenti profilo utente Selezionare: · Comune: se si desidera che le cartelle/i file crittografati utente siano accessibili a tutti gli utenti gestiti nell'endpoint in cui sono stati creati (stesso livello di accesso delle Cartelle crittografate comuni), e crittografati con l'Algoritmo crittografia comune. · Utente: se si desidera che questi file siano accessibili solo all'utente che li ha creati, solo nell'endpoint in cui sono stati creati (stesso livello di accesso delle Cartelle crittografate utente), e crittografati con l'Algoritmo crittografia utente. Se si sceglie di includere un criterio di crittografia per crittografare le partizioni dell'intero disco, si consiglia di usare il criterio di crittografia SDE predefinito, piuttosto che i criteri Comune o Utente. In questo modo tutti i file crittografati del sistema operativo sono accessibili anche quando l'utente gestito non ha effettuato l'accesso.
Hardware Crypto Accelerator (supportato solo con i client Encryption da v8.3 a v8.9.1)										
Hardware Crypto Accelerator (HCA)	Falso									È il "criterio principale" per tutti gli altri criteri di Hardware Crypto Accelerator (HCA). Se il criterio è Falso, la crittografia HCA non viene eseguita, indipendentemente dai valori degli altri criteri. I criteri HCA possono essere utilizzati solo nei computer che dispongono di un Hardware Crypto Accelerator.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Volumi destinati alla crittografia	Tutti i volumi fissi									Tutti i volumi fissi o solo il volume di sistema Specificare il/i volume/i da crittografare.
Metadati forensi disponibili in unità con crittografia HCA	Falso									Vero o Falso Se impostato su Vero, i metadati forensi sono inclusi nell'unità per facilitare le attività forensi. Metadati inclusi: • ID del computer (MCID) attualmente in uso • ID del dispositivo (DCID/SCID) dell'installazione dello Shield corrente Se impostato su Falso, i metadati forensi non sono inclusi nell'unità. Passando da Falso a Vero si avvierà nuovamente la ricerca in base ai criteri HCA per l'aggiunta dei metadati forensi.
Consenti approvazione utente per crittografia unità secondaria	Falso									Vero consente agli utenti di decidere se eseguire o meno la crittografia di ulteriori unità.
Algoritmo di crittografia	AES256									AES 256 o AES 128
Criteri di controllo delle porte										
Sistema di controllo porte	Disabilitato									Abilita o disabilita tutti i criteri di Sistema di controllo porte. Se il criterio è impostato su Disabilita, non viene applicato alcun criterio di Sistema di controllo porte, indipendentemente dagli altri suoi criteri. **N.B.** I criteri PCS richiedono il riavvio del sistema affinché le nuove impostazioni abbiano effetto.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Porta: slot scheda Express	Abilitata									Consente di abilitare, disabilitare o ignorare le porte esposte tramite lo slot scheda Express.
Porta: eSATA	Abilitata									Abilita, disabilita o ignora l'accesso alle porte SATA esterne.
Porta: PCMCIA	Abilitata									Abilita, disabilita o ignora l'accesso alle porte PCMCIA.
Porta: FireWire (1394)	Abilitata									Abilita, disabilita o ignora l'accesso alle porte Firewire (1394) esterne.
Porta: SD	Abilitata									Abilita, disabilita o ignora l'accesso alle porte per schede SD.
Sottoclasse Memorizzazione: Controllo unità esterne	Bloccato	Sola lettura			Accesso completo			Sola lettura	Accesso completo	FIGLIO di Classe: Memorizzazione. Classe: Memorizzazione deve essere impostato su Abilitato per utilizzare questo criterio. Questo criterio ha interazioni con il Sistema di controllo porte. Consultare Interazioni tra EMS e il Sistema di controllo porte Accesso completo: la porta dell'unità esterna non include restrizioni di accesso in lettura/scrittura Sola lettura: consente la lettura dei dati. La scrittura dei dati è disabilitata Bloccato: l'accesso in lettura/scrittura alla porta è bloccato Questo criterio è basato sull'endpoint e non può essere sostituito da un criterio utente.
Porta: dispositivi di trasferimento memoria (MTD)	Abilitata									Abilita, disabilita o ignora l'accesso alle porte per Memory Transfer Device (MTD, Dispositivi di trasferimento memoria).

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Classe: archiviazione	Abilitata									PADRE dei prossimi 3 criteri. Impostare questo criterio su Abilitato per utilizzare i successivi tre criteri Sottoclasse memorizzazione. L'impostazione di questo criterio su Disabilitato disabilita i tre criteri di Sottoclasse memorizzazione, indipendentemente dal relativo valore.
Sottoclasse Memorizzazione: Controllo unità ottiche	Sola lettura	Solo UDF				Accesso completo		Solo UDF	Accesso completo	FIGLIO di Classe: Memorizzazione. Classe: Memorizzazione deve essere impostato su Abilitato per utilizzare questo criterio. Accesso completo: la porta del lettore ottico non include restrizioni di accesso in lettura/scrittura Solo UDF: blocca la scrittura di dati che non sono in formato UDF (masterizzazione CD/DVD e ISO). La lettura dei dati è abilitata. Sola lettura: consente la lettura dei dati. La scrittura dei dati è disabilitata Bloccato: l'accesso in lettura/scrittura alla porta è bloccato Questo criterio è basato sull'endpoint e non può essere sostituito da un criterio utente. Universal Disk Format (UDF) è un'implementazione della specifica nota come ISO/IEC 13346 e ECMA-167 ed è un file system aperto e indipendente dal fornitore per l'archiviazione di dati per un'ampia gamma di supporti. Questo criterio ha interazioni con il Sistema di controllo porte. Consultare Interazioni tra EMS e il Sistema di controllo porte

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Sottoclasse Memorizzazione: Controllo unità floppy	Bloccato	Sola lettura				Accesso completo		Sola lettura	Accesso completo	FIGLIO di Classe: Memorizzazione. Classe: Memorizzazione deve essere impostato su Abilitato per utilizzare questo criterio. Accesso completo: la porta dell'unità floppy non riporta restrizioni di accesso in lettura/scrittura Sola lettura: consente la lettura dei dati. La scrittura dei dati è disabilitata Bloccato: l'accesso in lettura/scrittura alla porta è bloccato Questo criterio è basato sull'endpoint e non può essere sostituito da un criterio utente.
Classe: Dispositivi portatili Windows (WPD)	Abilitata									PADRE del criterio successivo. Impostare questo criterio su Attivato per utilizzare il criterio Sottoclasse Dispositivi portatili Windows (WPD): Memorizzazione. L'impostazione di questo criterio su Disattivato disabilita il criterio Sottoclasse Dispositivi portatili Windows (WPD): Memorizzazione, indipendentemente dal relativo valore. Controlla l'accesso a tutti i dispositivi portatili Windows.
Sottoclasse Dispositivi portatili Windows (WPD): Memorizzazione	Abilitata									FIGLIO di classe: Dispositivi portatili Windows (WPD) Per utilizzare questo criterio, Classe: Dispositivi portatili Windows (WPD) deve essere impostato su Attivato. Accesso completo: la porta non include restrizioni di accesso in lettura/scrittura. Sola lettura: consente la lettura dei dati. La scrittura dei dati è disabilitata. Bloccato: l'accesso in lettura/scrittura alla porta è bloccato.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Classe: Human Interface Device (HID)	Abilitata									Controlla l'accesso a tutti i dispositivi Human Interface (tastiere, mouse). **N.B.** Il blocco a livello di porta USB e il blocco a livello di classe HID vengono rispettati solo se è possibile identificare il tipo di telaio del computer come fattore di forma laptop/notebook. Ci si avvale del BIOS del computer per l'identificazione del telaio.
Classe: Altro	Abilitata									Controlla l'accesso a tutti i dispositivi non contemplati nelle altre classi.
Criteri dei dispositivi di archiviazione rimovibili										
EMS - Crittografa il supporto esterno	Vero					Falso		Vero	Falso	Questo criterio è il "criterio principale" per tutti i criteri dei dispositivi di archiviazione rimovibili. Se impostato su Falso, la crittografia dei dispositivi di archiviazione rimovibili non viene eseguita, indipendentemente dai valori degli altri criteri. Se impostato su Vero, tutti i criteri di crittografia dei dispositivi di archiviazione rimovibili sono abilitati. Questo criterio ha interazioni con il Sistema di controllo porte. Consultare Interazioni tra EMS e il Sistema di controllo porte
EMS - Escludi crittografia CD/DVD	Falso								Vero	Se impostato su Falso, si esegue la crittografia di CD/DVD. Questo criterio ha interazioni con il Sistema di controllo porte. Consultare Interazioni tra EMS e il Sistema di controllo porte
EMS - Accesso a supporto non protetto	Blocca	Sola lettura				Accesso completo		Sola lettura	Accesso completo	Blocca, Sola lettura, Accesso completo Questo criterio ha interazioni con il Sistema di controllo

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										porte. Consultare Interazioni tra EMS e il Sistema di controllo porte Quando questo criterio è impostato su Blocca accesso, l'utente non ha accesso ai dispositivi di archiviazione rimovibili a meno che non siano crittografati. Selezionando Sola lettura o Accesso completo è possibile decidere quale dispositivo di archiviazione rimovibile crittografare. Se si sceglie di non crittografare i dispositivi di archiviazione rimovibili e questo criterio è impostato su Accesso completo, si dispone di accesso completo in lettura e scrittura ai dispositivi di archiviazione rimovibili. Se si sceglie di non crittografare i dispositivi di archiviazione rimovibili e questo criterio è impostato su Sola lettura, non è possibile leggere o eliminare i file esistenti nei dispositivi di archiviazione rimovibili non crittografati e il client non consentirà la modifica o l'aggiunta di alcun file nel dispositivo di archiviazione rimovibile a meno che non sia crittografato.
EMS - Algoritmo crittografia	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES
EMS - Esegui scansione del supporto esterno	Vero	Falso								Se impostato su Vero, EMS può eseguire la scansione di un dispositivo di archiviazione rimovibile ogni volta che viene inserito. Quando è impostato su Falso e il criterio EMS - Crittografa il supporto esterno è impostato su Vero, EMS esegue solo la crittografia di file nuovi e modificati.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										La scansione ha luogo ogni volta che viene inserito un dispositivo di archiviazione rimovibile affinché EMS possa rilevare tutti i file aggiunti al dispositivo di archiviazione rimovibile senza eseguire l'autenticazione. Se l'utente rifiuta di eseguire l'autenticazione, è possibile aggiungere file al dispositivo di archiviazione rimovibile, ma non è possibile accedere ai dati crittografati. In questo caso, i file aggiunti non vengono crittografati e la volta successiva che si esegue l'autenticazione nel supporto rimovibile per utilizzare i dati crittografati, EMS ne esegue la scansione e crittografa tutti i file che sono stati aggiunti senza crittografia.
EMS - Accedi ai dati crittografati su dispositivo non protetto	Vero									Vero permette all'utente di accedere ai dati crittografati sul dispositivo di archiviazione rimovibile, indipendentemente dal fatto che l'endpoint sia crittografato o meno.
Elenco dispositivi EMS consentiti										Questo criterio consente di specificare i dispositivi con supporti esterni da non includere nella crittografia EMS. Tutti i dispositivi multimediali esterni non presenti in questo elenco verranno protetti. Sono consentiti un massimo di 150 dispositivi con un massimo di 500 caratteri per PNPDeviceID. È consentito un numero massimo di 2048 caratteri in totale. Per trovare il PNPDeviceID dei dispositivi di archiviazione rimovibili: 1 Inserire il dispositivo di archiviazione rimovibile in un computer protetto. 2 Aprire l'EMSService.log in C:\Programdata\Dell

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										\Dell Data Protection \Encryption\EMS. 3 Trovare "PNPDeviceID=" Ad esempio: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR \DISK&VEN_SEAGATE& PROD_USB&REV_0409\ 2HC015KJ&0 Specificare quanto segue nel criterio Elenco dispositivi EMS consentiti: VEN=Fornitore (ad esempio, USBSTOR \DISK&VEN_SEAGATE) PROD=Nome prodotto/ modello (ad esempio, &PROD_USB); esclude anche dalla crittografia EMS tutte le unità USB Seagate; un valore VEN (ad esempio, USBSTOR \DISK&VEN_SEAGATE) deve precedere questo valore REV=Revisione firmware (ad esempio, &REV_0409); esclude anche il modello specifico in uso; i valori VEN e PROD devono precedere questo valore Numero di serie (ad esempio, \2HC015KJ&0); esclude solo questo dispositivo; i valori VEN, PROD e REV devono precedere questo valore Delimitatori consentiti: tabulazioni, virgole, punti e virgola, carattere esadecimale 0x1E (carattere separatore di record)
EMS - La password deve contenere lettere	Vero									Vero richiede la presenza di una o più lettere nella password.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
EMS - La password deve contenere lettere maiuscole e minuscole	Vero	Falso								Vero richiede la presenza di almeno una lettera maiuscola e una minuscola nella password.
EMS - Numero di caratteri Richiesti per la password	8					6		8		Da 1 a 40 caratteri Numero minimo di caratteri richiesti per la password.
EMS - La password deve contenere numeri	Vero	Falso								Vero richiede la presenza di uno o più caratteri numerici nella password.
EMS - Tentativi password consentiti	2	3				4		3		Da 1 a 10 Numero di tentativi per immettere la password corretta consentiti all'utente.
EMS - La password deve contenere caratteri speciali	Vero	Falso							Vero	Vero richiede la presenza di uno o più caratteri speciali nella password.
EMS - Ritardo tempo di attesa tra tentativi	30									Da 0 a 5000 secondi Numero di secondi che l'utente deve attendere tra il primo e il secondo round di tentativi di accesso.
EMS - Incremento tempo di attesa tra tentativi	30	20				10	30	10		Da 0 a 5000 secondi Incremento di tempo da sommare al precedente tempo di attesa dopo ogni round di tentativi di accesso non riusciti.
Regole di crittografia EMS										Regole di crittografia per includere o escludere dalla crittografia determinate unità, directory e cartelle.

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										È consentito un massimo di 2048 caratteri. I caratteri Spazio e Invio usati per aggiungere righe vengono conteggiati tra i caratteri usati. Le regole che superano il limite di 2048 caratteri vengono ignorate. I dispositivi di archiviazione dotati di connessioni multi-interfaccia, quali Firewire, USB, eSATA, ecc., possono richiedere l'utilizzo delle regole EMS e di crittografia per eseguire la crittografia del dispositivo. Ciò è necessario poiché il sistema operativo Windows gestisce i dispositivi di archiviazione in modo diverso a seconda del tipo di interfaccia. Consultare Come crittografare un iPod con EMS
EMS - Blocca accesso a supporti non protetti	Vero								Falso	Blocca l'accesso ai dispositivi di archiviazione rimovibili da meno di 17 MB, ovvero con una capacità di archiviazione insufficiente per contenere la protezione del supporto rimovibile (come un floppy da 1,44 MB). L'accesso è bloccato quando sia Crittografa il supporto esterno che questo criterio sono impostati su Vero. Se Crittografa il supporto esterno è impostato su Vero, ma questo criterio è impostato su Falso, si dispone di accesso in lettura al dispositivo di archiviazione rimovibile non crittografabile, ma l'accesso in scrittura al supporto è bloccato. Se Crittografa il supporto esterno è impostato su Falso, questo criterio non ha alcun effetto e l'accesso al dispositivo di archiviazione rimovibile non crittografabile resta invariato.
Criteri di controllo dell'esperienza utente										

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
Imponi riavvio in presenza di aggiornamenti	Vero								Falso	Se si imposta il valore su Vero, il computer si riavvia immediatamente per consentire l'elaborazione della crittografia o gli aggiornamenti relativi ai criteri basati su dispositivi, come System Data Encryption (SDE).
Durata di ciascun ritardo di riavvio	5	10				20		15		Il numero di minuti di ritardo quando l'utente sceglie di ritardare il riavvio per il criterio basato su dispositivi.
Numero di ritardi di riavvio consentiti	1					5		3		Il numero di volte nelle quali verrà consentito all'utente di scegliere di ritardare il riavvio per il criterio basato su dispositivi.
Sopprimi notifica conflitti file	Falso									Questo criterio controlla la visualizzazione dei messaggi popup di notifica da parte degli utenti se un'applicazione tenta di accedere a un file durante l'elaborazione dello stesso da parte del client.
Visualizza controllo elaborazione crittografia locale	Falso		Vero					Falso		Se si imposta il valore su Vero, l'utente visualizza un'opzione di menu nell'icona dell'area di notifica che consente di sospendere/riprendere la crittografia/decrittografia (a seconda dell'operazione che sta effettuando lo Shield). **N.B.: Consentendo ad un utente di sospendere la crittografia potrebbe consentirgli di impedire allo Shield di crittografare o decrittografare completamente i dati per criterio.**
Consenti processo di crittografia solo quando lo schermo è bloccato	Falso		Facoltativo per l'utente					Falso		Vero, Falso, Facoltativo per l'utente Quando è impostato su Vero, non viene eseguito alcun processo di crittografia o decrittografia di dati quando

Criterio	Elevata protezione per tutte le unità fisse ed esterne	Normativa PCI	Normative sulla violazione dei dati	Normativa HIPAA	Protezione base per tutte le unità fisse ed esterne (predefinita)	Protezione base per tutte le unità fisse	Protezione base per la sola unità di sistema	Protezione base per unità esterne	Crittografia disattivata	Descrizione
										l'utente sta utilizzando il computer. Il client elabora i dati solo quando lo schermo è bloccato. Facoltativo per l'utente aggiunge un'opzione all'icona nell'area di notifica consentendo all'utente di attivare o disattivare questa funzionalità. Quando è impostato su Falso, il processo di crittografia può essere eseguito in qualsiasi momento, anche quando l'utente sta utilizzando il computer. Abilitando questa opzione si prolunga considerevolmente il tempo necessario per completare un processo di crittografia o decrittografia.

Descrizioni dei modelli

Elevata protezione per tutte le unità fisse ed esterne

Questo modello criteri è stato concepito per le organizzazioni che mirano a rafforzare il sistema di protezione e a minimizzare i rischi in tutta l'impresa. Tale soluzione è particolarmente adatta alle organizzazioni che privilegiano la sicurezza rispetto all'usabilità e che raramente necessitano di eccezioni meno sicure per gruppi, utenti o dispositivi specifici.

Questo modello criteri:

- Fornisce maggiore protezione grazie a una configurazione con un alto livello di restrizioni.
- Protegge l'unità di sistema e tutte le unità fisse.
- Crittografa tutti i dati di dispositivi di archiviazione rimovibili e impedisce l'utilizzo di dispositivi di archiviazione rimovibili non crittografati.
- Fornisce un controllo dei lettori ottici in modalità di sola lettura.

Mirato alla normativa PCI

Gli standard di protezione PCI sono standard di protezione dati su più livelli che includono requisiti per gestione della sicurezza, criteri, procedure, architettura di rete, progettazione di software e altre significative misure di protezione. Tale insieme di standard ha lo scopo di fornire alle organizzazioni le linee guida per proteggere in modo proattivo i dati relativi agli account dei clienti.

Questo modello criteri:

- Protegge l'unità di sistema e tutte le unità fisse.

Richiede agli utenti di crittografare i dispositivi di archiviazione rimovibili.

Consente di creare CD/DVD esclusivamente in formato UDF. La configurazione del controllo porte consente l'accesso in lettura a tutte le unità ottiche.

Mirato alle normative sulla violazione dei dati

Il Sarbanes-Oxley Act impone controlli adeguati nella gestione di informazioni di carattere finanziario. Poiché la maggior parte di tali informazioni è in formato elettronico, le funzionalità di crittografia sono fondamentali per il controllo dei dati archiviati o trasferiti. Le linee guida stabilite dal Gramm-Leach-Bliley (GLB) Act (conosciuto anche come Financial Services Modernization Act) non prevedono l'uso della crittografia. Tuttavia, il Federal Financial Institutions Examination Council (FFIEC) suggerisce che "gli istituti finanziari dovrebbero utilizzare funzioni di crittografia per ridurre il rischio di divulgazione o alterazione delle informazioni riservate archiviate o trasmesse". Il California Senate Bill 1386 (Database Security Breach Notification Act) ha lo scopo di proteggere i cittadini californiani da furti di identità, imponendo alle organizzazioni che subiscono violazioni della protezione informatica di avvisare tutti i soggetti interessati. Per evitare di avvisare tutti i clienti interessati, le organizzazioni devono essere in grado di dimostrare che tutte le informazioni personali erano state crittografate prima della violazione.

Questo modello criteri:

Protegge l'unità di sistema e tutte le unità fisse.

Richiede agli utenti di crittografare i dispositivi di archiviazione rimovibili.

Consente di creare CD/DVD esclusivamente in formato UDF. La configurazione del controllo porte consente l'accesso in lettura a tutte le unità ottiche.

Mirato alla normativa HIPAA

Lo Health Insurance Portability and Accountability Act (HIPAA) prevede che le organizzazioni di assistenza sanitaria adottino una serie di misure tecniche di sicurezza allo scopo di proteggere la riservatezza e l'integrità di tutte le informazioni sanitarie private e riconducibili a singoli pazienti.

Questo modello criteri:

Protegge l'unità di sistema e tutte le unità fisse.

Richiede agli utenti di crittografare i dispositivi di archiviazione rimovibili.

Consente di creare CD/DVD esclusivamente in formato UDF. La configurazione del controllo porte consente l'accesso in lettura a tutte le unità ottiche.

Protezione base per tutte le unità fisse ed esterne (predefinita)

Questo modello criteri fornisce la configurazione consigliata, che offre un alto livello di protezione senza compromettere l'usabilità del sistema in modo significativo.

Questo modello criteri:

Protegge l'unità di sistema e tutte le unità fisse.

Richiede agli utenti di crittografare i dispositivi di archiviazione rimovibili.

Consente di creare CD/DVD esclusivamente in formato UDF. La configurazione del controllo porte consente l'accesso in lettura a tutte le unità ottiche.

Protezione base per tutte le unità fisse

Questo modello criteri:

Protegge l'unità di sistema e tutte le unità fisse.

Consente di creare CD/DVD in tutti i formati supportati. La configurazione del controllo porte consente l'accesso in lettura a tutte le unità ottiche.

Questo modello criteri non consente di:

Fornire funzioni di crittografia per dispositivi di archiviazione rimovibili.

Protezione base per la sola unità di sistema

Questo modello criteri:

Protegge l'unità di sistema, generalmente l'unità C:, in cui è caricato il sistema operativo.

Consente di creare CD/DVD in tutti i formati supportati. La configurazione del controllo porte consente l'accesso in lettura a tutte le unità ottiche.

Questo modello criteri non consente di:

Fornire funzioni di crittografia per dispositivi di archiviazione rimovibili.

Protezione base per unità esterne

Questo modello criteri:

Protegge i dispositivi di archiviazione rimovibili.

Consente di creare CD/DVD esclusivamente in formato UDF. La configurazione del controllo porte consente l'accesso in lettura a tutte le unità ottiche.

Questo modello criteri non consente di:

Proteggere l'unità di sistema (generalmente l'unità C:, in cui è caricato il sistema operativo) o altre unità fisse.

Crittografia disattivata

Questo modello criteri non fornisce funzioni di protezione mediante crittografia. Adottare ulteriori misure per proteggere i dispositivi da perdita e furto quando si utilizza questo modello.

Questo modello è molto utile per le organizzazioni che preferiscono iniziare con sistemi di sicurezza che non prevedono l'uso di funzioni di crittografia. In seguito, quando l'organizzazione si è abituata al modello, è possibile abilitare gradualmente la funzionalità di crittografia modificando singoli criteri o applicando modelli più rigidi in tutta l'organizzazione o parte di essa.

Passare a Configurazione di preinstallazione per password monouso.

10

Configurazione di preinstallazione per password monouso

Queste funzioni di Personal Edition richiedono la configurazione **prima** dell'installazione.

Inizializzare il TPM

- È necessario essere membro del gruppo amministratori locali o avere un ruolo equivalente.
- È necessario che il computer disponga di un BIOS o TPM compatibili.

Questa operazione è necessaria se si utilizza Password monouso (OTP).

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

Estrarre i programmi di installazione figlio dal programma di installazione principale

- Per installare ciascun client individualmente, estrarre i file eseguibili figlio dal programma di installazione.
- Se per l'installazione è stato usato il programma di installazione principale, i client devono essere disinstallati singolarmente. Usare questa procedura per estrarre i client dal programma di installazione principale in modo da poterli utilizzare per la disinstallazione.

1 Dal supporto di installazione Dell, copiare nel computer locale il file`DDPSetup.exe`.

2 Nello stesso percorso del file`DDPSetup.exe` aprire un prompt dei comandi e immettere:

```
DDPSetup.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

Il percorso di estrazione non può superare i 63 caratteri.

Prima di iniziare l'installazione, accertarsi che siano stati soddisfatti tutti i prerequisiti e che tutti i software richiesti siano stati installati per ogni programma di installazione figlio che si intende installare. Per dettagli, fare riferimento a Requisiti.

I programmi di installazione figlio estratti si trovano in **C:\extracted\.**

Passare a Risoluzione dei problemi.

Risoluzione dei problemi

Aggiornamento a Windows 10 Anniversary Update

Per i computer nei quali è installato Encryption, è necessario usare un pacchetto di aggiornamento a Windows 10 appositamente configurato per l'aggiornamento a Windows 10 Anniversary Update. La versione configurata del pacchetto di aggiornamento garantisce che Dell Data Protection sia in grado di gestire l'accesso ai file crittografati dell'utente per proteggerli da danni durante il processo di aggiornamento.

Per eseguire l'aggiornamento alla versione Windows 10 Anniversary, seguire le istruzioni riportate nel seguente articolo:

http://www.dell.com/support/article/us/en/19/SLN298382

Risoluzione dei problemi del client di crittografia

Eseguire l'aggiornamento a Windows 10 Anniversary Update

Per effettuare l'aggiornamento alla versione Windows 10 Anniversary Update, seguire le istruzioni riportate nel seguente articolo: http://www.dell.com/support/article/us/en/19/SLN298382.

Creare un file di registro dell'Encryption Removal Agent (facoltativo)

- Prima di iniziare il processo di disinstallazione, è possibile creare facoltativamente un file di registro dell'Encryption Removal Agent. Questo file di registro è utile per risolvere eventuali problemi di un'operazione di disinstallazione/decrittografia. Se non si desidera decrittografare file durante il processo di disinstallazione, non è necessario creare il file di registro.
- Il file di registro dell'Encryption Removal Agent non viene creato finché viene eseguito il servizio Encryption Removal Agent, operazione che avviene solo dopo il riavvio del computer. Dopo la disinstallazione del client e la decrittografia completa del computer, il file di registro viene eliminato definitivamente.
- Il percorso del file di registro è **C:\ProgramData\Dell\Dell Data Protection\Encryption.**
- Creare la seguente voce di registro nel computer destinato alla decrittografia.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: nessuna registrazione

  1: registra errori che impediscono l'esecuzione del servizio

  2: registra errori che impediscono la decrittografia completa dei dati (livello consigliato)

  3: registra informazioni su tutti i file e i volumi di cui è in corso la decrittografia

  5: registra informazioni sul debug

Trovare la versione TSS

- TSS è un componente che si interfaccia con il TPM. Per trovare tale versione TSS, accedere a (percorso predefinito) **C:\Program Files \Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe**. Fare clic con il pulsante destro del mouse sul file e selezionare **Proprietà**. Verificare la versione del file nella scheda **Dettagli**.

Interazioni tra EMS e il Sistema di controllo porte

Per garantire che il supporto non sia di sola lettura e che la porta non sia bloccata

Il criterio EMS - Accesso a supporto non protetto interagisce con il criterio Sistema di controllo porte - Categoria memorizzazione: Controllo unità esterne. Se si intende impostare il criterio EMS - Accesso a supporto non protetto su *Accesso completo*, accertarsi che anche il criterio Categoria memorizzazione: Controllo unità esterne sia impostato su *Accesso completo* per garantire che il supporto non sia di sola lettura e che la porta non sia bloccata.

Per crittografare dati scritti su CD/DVD

- Impostare EMS - Crittografa il supporto esterno = Vero.
- Impostare EMS - Escludi crittografia CD/DVD = Falso.
- Sottoclasse memorizzazione: Controllo unità ottiche = Solo UDF

Usare WSScan

- WSScan consente di garantire che tutti i dati vengano decrittografati durante la disinstallazione del client di crittografia, nonché visualizzare lo stato della crittografia e individuare i file non crittografati che devono essere crittografati.
- Per eseguire questa utilità, sono richiesti privilegi di amministratore.

Eseguire WSScan

1. Dal supporto di installazione Dell, copiare WSScan.exe nel computer Windows che si desidera sottoporre a scansione.
2. Avviare una riga di comando dal percorso suindicato e immettere **wsscan.exe** al prompt dei comandi. WSScan si avvia.
3. Fare clic su **Avanzate**.
4. Selezionare il tipo di unità da analizzare dal menu a discesa: *Tutte le unità, Tutte le unità fisse, Unità rimovibili* o *CDROM/ DVDROM.*
5. Selezionare il Tipo di rapporto di crittografia desiderato dal menu a discesa: *file crittografati*, *file non crittografati*, *tutti i file* o *file non crittografati in violazione*:
   - *File crittografati* - per garantire che tutti i dati vengano decrittografati durante la disinstallazione del client di crittografia. Seguire il processo esistente per la decrittografia dei dati, ad esempio impostare l'aggiornamento di un criterio di decrittografia. Dopo la decrittografia dei dati, ma prima di eseguire il riavvio in preparazione per la disinstallazione, eseguire WSScan per verificare che tutti i dati siano stati decrittografati.
   - *File non crittografati* - Per individuare i file che non sono crittografati, con un'indicazione sulla necessità o meno di crittografare i file (S/N).
   - *Tutti i file* - Per visualizzare l'elenco di tutti i file crittografati e non crittografati, con un'indicazione sulla necessità o meno di crittografare i file (S/N).
   - *File non crittografati in violazione* - Per individuare i file che non sono crittografati che devono essere crittografati.
6. Fare clic su **Cerca**.

OPPURE

1. Fare clic su **Avanzate** per attivare/disattivare la visualizzazione su **Semplice** per sottoporre a scansione una cartella specifica.
2. Accedere a Impostazioni di scansione e inserire il percorso della cartella nel campo **Percorso di ricerca**. Se si utilizza questo campo, la selezione nella casella di riepilogo viene ignorata.
3. Se non si desidera scrivere i risultati della scansione di WSScan su file, disattivare la casella di controllo **Output su file**.

4 Modificare il percorso e il nome del file predefiniti in *Percorso*, se lo si desidera.

5 Selezionare **Aggiungi a file esistente** se non si desidera sovrascrivere nessun file di output WSScan esistente.

6 Scegliere il formato di output:

- Selezionare Formato rapporto per un elenco di tipo rapporto dell'output sottoposto a scansione. Questo è il formato predefinito.
- Selezionare File delimitato da valore per l'output che è possibile importare in un'applicazione per foglio di calcolo. Il delimitatore predefinito è "|", ma può essere sostituito da un massimo di 9 caratteri alfanumerici, spazi o segni di punteggiatura.
- Selezionare l'opzione Valori tra virgolette per delimitare ogni valore tra virgolette.
- Selezionare File a larghezza fissa per output non delimitati contenenti una linea continua di informazioni a lunghezza fissa per ciascun file crittografato.

7 Fare clic su **Cerca**.

Fare clic su **Interrompi la ricerca** per interromperla. Fare clic su **Cancella** per cancellare i messaggi visualizzati.

Output WSScan

I dati WSScan sui file crittografati contengono le seguenti informazioni.

Esempio di output:

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" is still AES256 encrypted

Output	Significato
Indicatore data e ora	La data e l'ora in cui il file è stato scansionato.
Tipo di crittografia	Il tipo di crittografia utilizzato per crittografare il file. **SysData**: chiave di crittografia SDE. **Utente**: chiave di crittografia utente. **Comune**: chiave di crittografia comune. WSScan non riporta i file crittografati tramite Encrypt for Sharing.
KCID	L'ID del computer principale. Come mostrato nell'esempio riportato sopra, "**7vdlxrsb**". Se si esegue la scansione di un'unità di rete mappata, il rapporto di scansione non genera un KCID.
UCID	L'ID utente. Come mostrato nell'esempio riportato sopra, "**_SDENCR_**". L'UCID è condiviso da tutti gli utenti del computer.
File	Il percorso del file crittografato. Come mostrato nell'esempio riportato sopra, "**c:\temp\Dell - test.log**".
Algoritmo	L'algoritmo di crittografia utilizzato per crittografare il file. Come mostrato nell'esempio riportato sopra, "**is still AES256 encrypted**" RIJNDAEL 128 RIJNDAEL 256 AES 128

Output	Significato
	AES 256
	3DES

Verificare lo stato dell'Encryption Removal Agent

Lo stato dell'Encryption Removal Agent viene visualizzato nell'area di descrizione del pannello Servizi (Start > Esegui > services.msc > OK) come segue. Aggiornare periodicamente il servizio (evidenziare il servizio > fare clic con il pulsante destro del mouse > Aggiorna) per aggiornare il relativo stato.

- **In attesa della disattivazione di SDE** – Il client di crittografia è ancora installato, configurato o entrambi. La decrittografia inizia solo dopo la disinstallazione del client di crittografia.
- **Ricerca iniziale** – Il servizio sta eseguendo una ricerca iniziale che calcola il numero di file e byte crittografati. La ricerca iniziale viene eseguita una volta sola.
- **Ricerca decrittografia** – Il servizio sta decrittografando file e probabilmente richiede di decrittografare file bloccati.
- **Decrittografa al riavvio (parziale)** - La ricerca della decrittografia è stata completata e alcuni file bloccati (ma non tutti) verranno decrittografati al riavvio successivo.
- **Decrittografa al riavvio** - La ricerca della decrittografia è stata completata e tutti i file bloccati verranno decrittografati al riavvio successivo.
- **Impossibile decrittografare tutti i file** - La ricerca della decrittografia è stata completata, ma non è stato possibile decrittografare tutti i file. Questo stato indica che si è verificato uno degli scenari seguenti:
  - Non è stato possibile pianificare la decrittografia per i file bloccati perché erano troppo grandi o perché si è verificato un errore durante la richiesta di sblocco.
  - Si è verificato un errore di input/output durante la decrittografia dei file.
  - Un criterio impediva di decrittografare i file.
  - I file sono contrassegnati come da crittografare.
  - Si è verificato un errore durante la ricerca della decrittografia.
  - In tutti i casi viene creato un file di registro (se è stata configurata la registrazione) quando viene impostato LogVerbosity=2 (o più alto). Per eseguire la risoluzione dei problemi, impostare il livello di dettaglio del registro su 2 e riavviare il servizio Encryption Removal Agent per forzare un'altra ricerca della decrittografia., .
- **Completata** - La ricerca della decrittografia è stata completata. Al riavvio successivo è pianificata l'eliminazione del servizio, dell'eseguibile, del driver e dell'eseguibile del driver.

Come crittografare un iPod con EMS

Queste regole disabilitano o abilitano la crittografia di tali cartelle e tipi di file per tutti i dispositivi rimovibili, oltre all'iPod. Prestare particolare attenzione quando si definiscono le regole.

- Si sconsiglia l'utilizzo di iPod Shuffle poiché si possono verificare problemi inattesi.
- Queste informazioni variano di pari passo con l'uscita di nuovi modelli, pertanto è necessario esercitare cautela quando si consente l'utilizzo di iPod in computer in cui è attivato EMS.
- Poiché i nomi delle cartelle variano a seconda del modello di iPod, si consiglia di creare un criterio di esclusione che comprenda tutti i nomi delle cartelle di tutti i modelli iPod.
- Per assicurarsi che la crittografia di un iPod tramite EMS non renda il dispositivo inutilizzabile, immettere le seguenti regole nel criterio Regole crittografia EMS:

  -R#:\Calendars

  -R#:\Contacts

  -R#:\iPod_Control

-R#:\Notes

-R#:\Photos

- È possibile anche forzare la crittografia di tipi di file specifici nelle directory di cui sopra. Aggiungendo le seguenti regole, i file ppt, pptx, doc, docx, xls e xlsx vengono crittografati nelle directory *escluse* dalla crittografia tramite le regole precedenti:

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- Sostituendo queste cinque regole con la seguente regola è possibile forzare la crittografia di file ppt, pptx, doc, docx, xls e xlsx in qualsiasi directory dell'iPod, tra cui Calendars, Contacts, iPod_Control, Notes e Photos:

  ^R#:\;ppt.doc.xls.pptx.docx.xlsx

- Le regole sono state testate sui questi iPod:

  iPod Video 30 GB di quinta generazione

  iPod Nano 2 GB di seconda generazione

  iPod Mini 4 GB di seconda generazione

Driver di Dell ControlVault

Aggiornare driver e firmware di Dell ControlVault

I driver e il firmware di Dell ControlVault che vengono preinstallati nei computer Dell sono obsoleti e devono essere aggiornati seguendo l'ordine della procedura seguente.

Se, durante l'installazione del client, l'utente riceve un messaggio di errore che richiede di uscire dal programma di installazione per aggiornare i driver di Dell ControlVault, tale messaggio può essere ignorato per procedere con l'installazione del client. I driver (e il firmware) di Dell ControlVault possono essere aggiornati dopo aver completato l'installazione del client.

Scaricare le versioni più recenti dei driver

1. Visitare il sito support.dell.com.
2. Selezionare il modello di computer.
3. Selezionare **Driver e download**.
4. Selezionare il **Sistema operativo** del computer di destinazione.
5. Espandere la categoria **Sicurezza**.
6. Scaricare e salvare i driver di Dell ControlVault.
7. Scaricare e salvare il firmware di Dell ControlVault.
8. Copiare i driver e il firmware nei computer di destinazione, se necessario.

Installare il driver di Dell ControlVault

Passare alla cartella in cui è stato scaricato il file di installazione del driver.

Fare doppio clic sul driver di Dell ControlVault per avviare il file eseguibile autoestraente.

:

Assicurarsi di installare prima il driver. Il nome file del driver *al momento della creazione del documento* è ControlVault_Setup_2MYJC_A37_ZPE.exe.

Fare clic su **Continua** per iniziare.

Fare clic su **OK** per decomprimere i file del driver nel percorso predefinito C:\Dell\Drivers\<Nuova cartella>.

Fare clic su **Sì** per consentire la creazione di una nuova cartella.

Fare clic su **OK** quando viene visualizzato il messaggio di completamento della decompressione.

Al termine dell'estrazione, viene visualizzata la cartella contenente i file. Se ciò non accade, passare alla cartella in cui sono stati estratti i file. In questo caso, la cartella è **JW22F**.

Fare doppio clic su **CVHCI64.MSI** per avviare il programma di installazione del driver [in questo esempio si tratta di **CVHCI64.MSI** (CVHCI per un computer a 32 bit)].

Fare clic su **Avanti** nella schermata iniziale.

Fare clic su **Avanti** per installare i driver nel percorso predefinito C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.

Selezionare l'opzione **Completata** e fare clic su **Avanti**.

Fare clic su **Installa** per avviare l'installazione dei driver.

È possibile, facoltativamente, selezionare la casella di controllo per visualizzare il file di registro del programma di installazione. Fare clic su **Fine** per uscire dalla procedura guidata.

Verificare l'installazione del driver

Device Manager avrà un dispositivo Dell ControlVault (e altri dispositivi) a seconda del sistema operativo e della configurazione dell'hardware.

Installare il firmware di Dell ControlVault

1 Passare alla cartella in cui è stato scaricato il file di installazione del firmware.
2 Fare doppio clic sul firmware di Dell ControlVault per avviare il file eseguibile autoestraente.
3 Fare clic su **Continua** per iniziare.
4 Fare clic su **OK** per decomprimere i file del driver nel percorso predefinito C:\Dell\Drivers\<Nuova cartella>.
5 Fare clic su **Sì** per consentire la creazione di una nuova cartella.
6 Fare clic su **OK** quando viene visualizzato il messaggio di completamento della decompressione.
7 Al termine dell'estrazione, viene visualizzata la cartella contenente i file. Se ciò non accade, passare alla cartella in cui sono stati estratti i file. Selezionare la cartella **firmware**.
8 Fare doppio clic su **ushupgrade.exe** per avviare il programma di installazione del firmware.
9 Fare clic su **Avvia** per avviare l'aggiornamento del firmware.

:

Se si tratta dell'aggiornamento di una versione precedente del firmware, all'utente potrebbe essere richiesto di immettere la password di amministratore. In tal caso, immettere la password **`Broadcom`** e fare clic su **Invio**.

Vengono visualizzati alcuni messaggi di stato.

10 Fare clic su **Riavvia** per completare l'aggiornamento del firmware.

L'aggiornamento dei driver e del firmware di Dell ControlVault è stato completato.

Impostazioni di registro

Questa sezione descrive in dettaglio tutte le impostazioni di registro approvate da Dell ProSupport per i computer client locali.

Client di crittografia

Creare un file di registro dell'Encryption Removal Agent (facoltativo)

Prima di iniziare il processo di disinstallazione, è possibile creare facoltativamente un file di registro dell'Encryption Removal Agent. Questo file di registro è utile per risolvere eventuali problemi di un'operazione di disinstallazione/decrittografia. Se non si desidera decrittografare file durante il processo di disinstallazione, non è necessario creare il file di registro.

Il file di registro dell'Encryption Removal Agent non viene creato finché viene eseguito il servizio Encryption Removal Agent, operazione che avviene solo dopo il riavvio del computer. Dopo la disinstallazione del client e la decrittografia completa del computer, il file di registro viene eliminato definitivamente.

Il percorso del file di registro è **C:\ProgramData\Dell\Dell Data Protection\Encryption.**

Creare la seguente voce di registro nel computer destinato alla decrittografia.

[HKLM\Software\Credant\DecryptionAgent]

"LogVerbosity"=dword:2

0: nessuna registrazione

1: registra errori che impediscono l'esecuzione del servizio

2: registra errori che impediscono la decrittografia completa dei dati (livello consigliato)

3: registra informazioni su tutti i file e i volumi di cui è in corso la decrittografia

5: registra informazioni sul debug

Usare le smart card con l'accesso a Windows

Per usare le smart card con l'Autenticazione di Windows, è necessario impostare il seguente valore di registro nel computer client:

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

Conservare i file temporanei durante l'installazione

Per impostazione predefinita, tutti i file temporanei nella directory c:\windows\temp vengono automaticamente eliminati durante l'installazione. L'eliminazione dei file temporanei velocizza la crittografia iniziale ed ha luogo prima della ricerca crittografia iniziale.

Tuttavia, se l'organizzazione utilizza un'applicazione di terzi che richiede di conservare la struttura dei file nella directory \temp, è opportuno evitare l'eliminazione di questi file.

Per disabilitare l'eliminazione dei file temporanei, creare o modificare l'impostazione di registro come segue:

[HKLM\SOFTWARE\CREDANT\CMGShield]

"DeleteTempFiles"=REG_DWORD:0

La mancata eliminazione dei file temporanei aumenta il tempo di crittografia iniziale.

Modificare il comportamento predefinito della richiesta dell'utente di iniziare o ritardare la crittografia

Il client di crittografia visualizza il prompt *Durata di ciascun ritardo di aggiornamento criteri* per cinque minuti ogni volta. Se l'utente non risponde alla richiesta, inizia il ritardo successivo. La richiesta di ritardo finale include una barra di conto alla

rovescia e di stato che viene visualizzata finché l'utente risponde, oppure il ritardo finale scade e si verifica la disconnessione o il riavvio richiesto.

È possibile modificare il comportamento della richiesta dell'utente di iniziare o ritardare la crittografia, per impedire l'elaborazione della crittografia in seguito alla mancata risposta dell'utente alla richiesta. A tal fine, impostare il seguente valore di registro:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

Un valore diverso da zero modificherà il comportamento predefinito della posposizione. In assenza di interazione dell'utente, l'elaborazione della crittografia verrà ritardata fino al numero di ritardi configurabili consentiti. L'elaborazione della crittografia inizia alla scadenza del ritardo finale.

Calcolare il ritardo massimo possibile nel modo seguente (un ritardo massimo implica che l'utente non ha risposto ad alcuna richiesta di ritardo visualizzata per 5 minuti):

(NUMERO DI RITARDI DI AGGIORNAMENTO CRITERI CONSENTITI x DURATA DI CIASCUN RITARDO DI AGGIORNAMENTO CRITERI) + (5 MINUTI [NUMERO DI RITARDI DI AGGIORNAMENTO CRITERI CONSENTITI - 1])

Modificare l'uso predefinito della chiave SDUser

System Data Encryption (SDE) viene applicato in base al valore del criterio per Regole di crittografia SDE. Le directory aggiuntive sono protette per impostazione predefinita quando il criterio Crittografia SDE abilitata è Selezionato. Per maggiori informazioni, cercare "Regole di crittografia SDE" nella Guida dell'amministratore. Quando il client di crittografia sta elaborando un aggiornamento del criterio che include un criterio SDE attivo, la directory del profilo utente in uso viene crittografata per impostazione predefinita con la chiave SDUser (una chiave utente) piuttosto che con la chiave SDE (una chiave dispositivo). La chiave SDUser viene anche usata per crittografare file o cartelle che vengono copiate (non spostate) in una directory dell'utente che non è crittografata con SDE.

Per disabilitare la chiave SDUser e usare la chiave SDE per crittografare queste directory dell'utente, creare la seguente voce di registro nel computer:

[HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

"EnableSDUserKeyUsage"=dword:00000000

Se questa chiave di registro non è presente o è impostata su un valore diverso da 0, la chiave SDUser verrà usata per crittografare queste directory dell'utente.

Client di autenticazione avanzata

Disabilitare smart card e servizi biometrici (facoltativo)

Se non si desidera che Security Tools modifichi i servizi associati alle smart card e ai dispositivi biometrici in un tipo di avvio "automatico", è possibile disabilitare la funzione di avvio del servizio.

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.

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

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Impostare su 0 per abilitare.

Impostare su 1 per disabilitare.

Usare le smart card con l'accesso a Windows

Per usare le smart card con l'Autenticazione di Windows, è necessario impostare il seguente valore di registro nel computer client:

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

Passare al Glossario.

13

Glossario

Autenticazione avanzata - Il prodotto Autenticazione avanzata fornisce le opzioni integrate complete del lettore di impronte, smart card e smart card senza contatti. Autenticazione avanzata consente di gestire tali metodi di autenticazione hardware, supporta l'accesso con unità autocrittografanti e SSO, e gestisce le password e le credenziali dell'utente. Inoltre, l'Autenticazione avanzata può essere usata per accedere non solo ai PC, ma a qualsiasi sito Web, SaaS o applicazione. Nel momento in cui gli utenti registrano le proprie credenziali, Autenticazione avanzata consente l'utilizzo di tali credenziali per accedere al dispositivo e sostituire la password.

Password di amministratore per crittografia (EAP, Encryption Administrator Password) - L'EAP è una password amministrativa univoca per ogni computer. La maggior parte delle modifiche di configurazione effettuate nella console di gestione locale richiede questa password. Si tratta anche della stessa password richiesta se si utilizza il file LSARecovery_[nomehost].exe per ripristinare i dati. Registrare e salvare la password in un luogo sicuro.

Client di crittografia – Il client di crittografia è il componente nel dispositivo che applica i criteri di protezione quando un endpoint è connesso alla rete, disconnesso dalla rete, perso o rubato. Creando un ambiente di elaborazione affidabile per gli endpoint, il client di crittografia opera come strato nel sistema operativo del dispositivo e fornisce autenticazione, crittografia e autorizzazione applicate costantemente per massimizzare la protezione delle informazioni sensibili.

Chiavi di crittografia - Nella maggior parte dei casi, il client di crittografia usa la chiave utente più due chiavi di crittografia aggiuntive. Tuttavia esistono delle eccezioni: tutti i criteri di SDE e il criterio Credenziali Windows di protezione usano la chiave SDE. Il criterio Crittografia file di paging Windows e il criterio Proteggi file di sospensione di Windows usano la propria chiave, la General Purpose Key (GPK). La chiave Comune rende i file accessibili a tutti gli utenti gestiti nel dispositivo in cui sono stati creati. La chiave Utente rende i file accessibili solo all'utente che li ha creati, solo nel dispositivo in cui sono stati creati. La chiave Roaming utente rende i file accessibili solo all'utente che li ha creati, in qualsiasi dispositivo Windows (o Mac) protetto.

Ricerca crittografia – La ricerca crittografia è il processo di scansione delle cartelle da crittografare in un endpoint protetto, al fine di garantire l'adeguato stato di crittografia dei file contenuti. Le normali operazioni di creazione e ridenominazione dei file non attivano una ricerca crittografia. È importante comprendere quando può avvenire una ricerca crittografia e quali fattori possono influenzare i tempi di ricerca risultanti, come segue: - Una ricerca crittografia si verificherà alla ricezione iniziale di un criterio che ha la crittografia abilitata. Ciò può verificarsi immediatamente dopo l'attivazione se il criterio ha la crittografia abilitata. - Se il criterio Esegui scansione workstation all'accesso è abilitato, le cartelle specificate per la crittografia verranno analizzate ad ogni accesso dell'utente. - È possibile riattivare una ricerca in base a determinate modifiche successive di un criterio. Qualsiasi modifica di criterio relativa a definizione di cartelle di crittografia, algoritmi di crittografia, utilizzo delle chiavi di crittografia (utente comune), attiverà una ricerca. Anche abilitando e disabilitando la crittografia si attiverà una ricerca crittografia.

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. 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.

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.

System Data Encryption (SDE) – L'SDE è progettato per eseguire la crittografia di sistema operativo e file di programma. A tal fine, SDE deve essere in grado di aprire la relativa chiave quando è in corso l'avvio del sistema operativo. Lo scopo è evitare modifiche o attacchi offline al sistema operativo. L'SDE non è concepito per i dati degli utenti. I modelli di crittografia Comune e Utente sono concepiti per dati riservati, in quanto per sbloccare le chiavi di crittografia è necessaria la password dell'utente. I criteri SDE non eseguono la crittografia dei file necessari affinché il sistema operativo possa iniziare il processo di avvio. I criteri SDE non richiedono l'autenticazione di preavvio né interferiscono in alcun modo con il record di avvio principale. Quando è in corso l'avvio del sistema, i file crittografati sono disponibili prima dell'accesso degli utenti (per abilitare gli strumenti di gestione delle patch, SMS, backup e ripristino). Disabilitando la crittografia SDE si attiva la decrittografia automatica di tutte le directory e i file crittografati con SDE per i relativi utenti, indipendentemente dagli altri criteri SDE, come le Regole di crittografia SDE.

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).