Dell Encryption Personal

Installation Guide v11.9

January 2024
Rev. A01

DELL Technologies

Messaggi di N.B., Attenzione e Avvertenza

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

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

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

Contents

1

Panoramica

In base a questa guida, Advanced Authentication viene installato con Encryption Personal.

Encryption Personal

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

Per garantire la protezione dei dati riservati, Encryption Personal crittografa i dati presenti nel computer Windows. L'utente può sempre accedere ai dati se connesso al computer, ma i dati protetti sono 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, l'applicazione decrittografa i dati durante il normale utilizzo. Occasionalmente, un'applicazione può provare ad accedere a un file nello stesso momento in cui l'applicazione lo sta crittografando o decrittografando. Se ciò avviene, dopo un secondo o due viene visualizzata una finestra di dialogo in cui viene data la possibilità di restare in attesa o annullare la crittografia/decrittografia. Se si sceglie di attendere, l'applicazione rilascia il file non appena la procedura viene completata (generalmente entro pochi secondi).

Advanced Authentication

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

Consultare Configurare le impostazioni amministratore di Advanced Authentication e fare riferimento alla *Dell Data Security Console User Guide* (Guida per l'utente di Dell Data Security Console) per informazioni sull'utilizzo di Advanced Authentication.

Contattare Dell ProSupport for Software

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

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

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

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

2

Requisiti

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

Crittografia

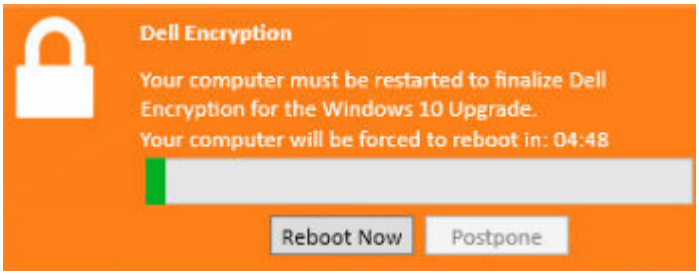
- Per installare correttamente Encryption Personal, sono necessari appositi diritti. I diritti vengono forniti all'acquisto di Encryption Personal. A seconda di come si acquista Encryption Personal, è possibile installare manualmente l'autorizzazione, utilizzando le semplici istruzioni in dotazione. È inoltre possibile immettere l'autorizzazione nella riga di comando. Se Encryption Personal viene installato usando Dell Digital Delivery, l'installazione dei diritti viene eseguita dal servizio Dell Digital Delivery. Gli stessi file binari vengono utilizzati per Encryption Enterprise e Encryption Personal. i diritti comunicano al programma di installazione quale versione installare).
- Gli account Microsoft e Office 365 sono supportati quando è in esecuzione Encryption Personal v11.0 o versioni successive su Windows 10.
- Per attivare un account Microsoft Live con Encryption Personal, consultare l'articolo della KB 124722.
- È necessario 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. Encryption Personal non potrà essere attivato se non viene creata una password.
- Non è possibile aggiornare Dell Encryption a v10.7.0 dalle versioni precedenti a v8.16.0. Gli endpoint in cui sono in esecuzione versioni precedenti a v8.16.0 devono eseguire l'aggiornamento a v8.16.0 e poi eseguire l'aggiornamento a v10.7.0.
- Dell Encryption utilizza set di istruzioni di crittografia Integrated Performance Primitives (IPP) di Intel. Per ulteriori informazioni, consultare l'articolo della KB 126015.

1. Andare al Pannello di controllo di Windows (**Start** > **Pannello di controllo**).
2. Cliccare sull'icona **Account utente**.
3. Cliccare su **Crea una password per l'account**.
4. Immettere una nuova password e reinserirla.
5. Aggiungere facoltativamente un suggerimento per la password.
6. Cliccare su **Crea password**.
7. Riavviare il sistema.

- Durante l'implementazione è opportuno seguire le procedure consigliate. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e implementazioni 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 implementazione, come ad esempio Microsoft SMS. 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 implementare il client di crittografia come parte dell'immagine aziendale, piuttosto che usare soluzioni SCCM di terze parti o simili per implementare il client di crittografia. Per istruzioni su come installare il client di crittografia in un'immagine aziendale, vedere l'articolo della KB 129990.
- Il TPM è utilizzato per sigillare la General Purpose Key. Pertanto, se si esegue il client di crittografia, cancellare il TPM nel BIOS prima di installare un nuovo sistema operativo nel computer di destinazione.

- Il client di crittografia è testato e compatibile con diversi antivirus basati su firma e soluzioni antivirus basate su intelligenza artificiale di ampio utilizzo, tra cui McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense e molti altri. Per impostazione predefinita, le esclusioni hardcoded sono incluse per molti provider di soluzioni antivirus al fine di evitare problemi di incompatibilità tra scansione antivirus e crittografia.

  Se l'organizzazione utilizza un provider di soluzioni antivirus che non è presente nell'elenco o si registrano eventuali problemi di compatibilità, consultare l'articolo della KB 126046 o Contattare Dell ProSupport per assistenza sulla convalida della configurazione per l'interoperabilità tra le soluzioni software e le soluzioni Dell Data Security.
- 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 dell.com/support per la documentazione più recente e le Avvertenze tecniche.
- Dopo l'aggiornamento delle funzionalità di Windows 10, è **necessario** il riavvio per finalizzare Dell Encryption. Di seguito viene visualizzato il messaggio nell'area di notifica dopo l'aggiornamento di funzione di Windows 10:



Prerequisiti

- È richiesto Microsoft .Net Framework 4.5.2 (o versioni successive) per il programma di installazione principale e figlio. Il programma di installazione non installa il componente Microsoft .Net Framework.

  N.B.: In modalità FIPS, è richiesto .Net Framework 4.6 (o versione successiva).

- Il programma di installazione principale installa i seguenti prerequisiti se non sono già installati nel computer. **Se si usa il programma di installazione figlio**, è necessario installare questo componente prima di installare la crittografia.

Prerequisito
○ Visual C++ 2012 Update 4 o Redistributable Package (x86 o x64) versione successiva ○ Visual C++ 2017 Update 3 o Redistributable Package (x86 o x64) versione successiva ○ Le applicazioni e i pacchetti di installazione firmati con i certificati SHA1 funzioneranno, ma verrà visualizzato un errore sull'endpoint durante l'installazione o l'esecuzione dell'applicazione, se non sono stati installati questi aggiornamenti

Hardware

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

Hardware
○ Processore Intel Pentium o AMD ○ 110 MB di spazio disponibile su disco ○ 512 MB di RAM **N.B.:** È richiesto spazio aggiuntivo sul disco per crittografare i file sull'endpoint. La quantità di spazio varia in base ai criteri e alle dimensioni dell'unità.

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

Hardware integrato facoltativo
○ TPM 1.2 o 2.0

Sistemi operativi

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

Sistemi operativi Windows (a 32 e 64 bit)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 - November 2022 Update/22H2) **Nota:** OEM e ODM non inviano Windows 10 v2004 (May 2020 Update/20H1 e versioni successive) con architettura a 32 bit. Per ulteriori informazioni, consultare https://docs.microsoft.com/it-it/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Sistemi operativi per Encryption External Media

- Per ospitare Encryption External Media, 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.
- Di seguito i sistemi operativi supportati durante l'accesso ai supporti protetti da Dell.

Sistemi operativi Windows supportati per l'accesso a media cifrati (a 32 e 64 bit)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 - November 2022 Update/22H2) **Nota:** OEM e ODM non inviano Windows 10 v2004 (May 2020 Update/20H1 e versioni successive) con architettura a 32 bit. Per ulteriori informazioni, consultare https://docs.microsoft.com/it-it/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Sistemi operativi Mac supportati per l'accesso a media cifrati (kernel a 64 bit)
○ macOS High Sierra 10.13.5 - 10.13.6 ○ macOS Mojave 10.14.0 - 10.14.4 ○ macOS Catalina 10.15.5 - 10.15.6

Localizzazione

- La crittografia è compatibile con l'interfaccia utente multilingue (MUI, Multilingual User Interface) ed è localizzata nelle lingue seguenti.

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

SED Manager

- IPv6 non è supportato.
- Arrestare e riavviare il sistema dopo aver applicato i criteri per renderli effettivi.
- I computer dotati di unità autocrittografanti non possono essere utilizzati con le schede HCA. Sono presenti incompatibilità che impediscono il provisioning dell'HCA. Dell non vende computer con unità autocrittografanti che supportano il modulo HCA. Questa configurazione non supportata potrebbe essere una configurazione post vendita.
- Se il computer destinato alla crittografia è dotato di un'unità self-encrypting drive, assicurarsi che l'opzione di Active Directory, *Cambiamento obbligatorio password all'accesso successivo*, sia disabilitata. L'autenticazione di preavvio non supporta questa opzione di Active Directory.
- SED Manager non è supportato con le configurazioni multiunità.
- **N.B.:**

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

- Il programma di installazione principale installa i seguenti prerequisiti se non sono già installati nel computer. **Se si usa il programma di installazione figlio**, è necessario installare questo componente prima di installare SED Manager.

Prerequisito
○ Visual C++ 2017 Update 3 o Redistributable Package (x86 o x64) versione successiva ○ Le applicazioni e i pacchetti di installazione firmati con i certificati SHA1 funzioneranno, ma verrà visualizzato un errore sull'endpoint durante l'installazione o l'esecuzione dell'applicazione, se non sono stati installati questi aggiornamenti

- La configurazione delle unità autocrittografanti per SED Manager è diversa tra unità NVMe e non NVMe (SATA) nel seguente modo.
  - Qualsiasi unità NVMe che viene utilizzata al meglio per la PBA:
    - Se il dispositivo Dell è stato prodotto nel 2018 o successivamente: RAID ON o AHCI possono essere utilizzati con le unità NVMe.
    - La modalità di avvio del BIOS deve essere impostata su Unified Extensible Firmware Interface (UEFI). Le ROM legacy devono essere disabilitate.
  - Qualsiasi unità non NVMe che viene utilizzata al meglio per la PBA:
    - L'operazione SATA del BIOS può essere impostata su AHCI o RAID ON.
    - Il sistema operativo si arresta quando è impostato da RAID ON ad AHCI, se i driver del controller AHCI non sono stati preinstallati. Per istruzioni su come passare da RAID > AHCI (o viceversa), vedere l'articolo della KB 124714.

  Le SED compatibili con OPAL supportate richiedono driver Intel Rapid Storage Technology aggiornati, disponibili all'indirizzo www.dell.com/support. Dell consiglia di installare il driver Intel Rapid Storage Technology più recente con le unità NVMe.

  N.B.: I driver Intel Rapid Storage Technology dipendono dalla piattaforma. È possibile trovare il driver per il sistema in uso al collegamento riportato in precedenza, in base al modello del computer.

- Le configurazioni di crittografia su più dischi con SED Manager richiedono quanto segue:
  - Tutti i dischi nel sistema di destinazione devono essere SED.
  - Tutti i dischi nel sistema di destinazione devono essere configurati nella stessa modalità di avvio.
  - In modalità di avvio UEFI, il sistema operativo può essere installato su qualsiasi disco di destinazione.
  - In modalità di avvio Legacy, il sistema operativo deve essere installato sul primo disco (Disco #0). Se il sistema operativo non è installato su primo disco, la crittografia su più dischi è disabilitata.
- Alcune versioni del BIOS possono abilitare il blocco SID per impostazione predefinita, il che può inibire SED Manager. Per ulteriori informazioni, consultare l'articolo della KB 126083.
- Gli aggiornamenti delle funzionalità diretti da Windows 10 v1607 (Anniversary Update/Redstone 1) a Windows 10 v1903 (May 2019 Update/19H1) non sono supportati con Dell Encryption. Dell consiglia di scegliere un aggiornamento delle funzionalità

più recente, se si esegue l'aggiornamento a Windows 10 v1903. Qualsiasi tentativo di aggiornare direttamente da Windows 10 v1607 a v1903 genera un messaggio di errore e l'aggiornamento viene bloccato.

- **N.B.:** Con l'autenticazione di preavvio è obbligatoria una password. Dell consiglia di configurare una password minima di 9 o più caratteri.

- **N.B.:** È obbligatoria una password per tutti gli utenti aggiunti nel pannello *Aggiungi utente*. Gli utenti di password di lunghezza zero verranno bloccati dal computer dopo l'attivazione.
- **N.B.:** I computer protetti da SED Manager devono essere aggiornati a Windows 10 v1703 (Creators Update/Redstone 2) o versione successiva, prima dell'aggiornamento a Windows 10 v1903 (May 2019 Update/19H1) o versione successiva. Se si segue questo percorso di aggiornamento, viene visualizzato un messaggio di errore.
- SED Manager richiede l'utilizzo del provider di credenziali personalizzato Dell per sincronizzare le modifiche della password di Windows e le chiavi di crittografia dei dati. Per utilizzare applicazioni di terze parti che utilizzano provider di credenziali personalizzate su computer protetti da SED Manager, è necessario avviare le modifiche della password di Windows tramite Data Security Console. Per informazioni sulla modifica della password in Data Security Console, consultare il capitolo *Password* nella Guida utente di Data Security Console.

Hardware

- Per l'elenco più aggiornato di unità autocrittografanti (SED) conformi con Opal supportate con SED Manager, consultare l'articolo della Knowledge Base 126855.
- Per l'elenco più aggiornato di piattaforme supportate con SED Manager, consultare l'articolo della Knowledge Base 126855.
- Per un elenco di docking station e adattatori supportati con SED Manager, consultare l'articolo della Knowledge Base 124241.

Tastiere internazionali

Nella tabella seguente vengono elencate le tastiere internazionali supportate con l'autenticazione di preavvio su computer UEFI e non UEFI.

Supporto tastiere internazionali - UEFI	
DE-FR - (Svizzera francese)	EN-GB - Inglese (Regno Unito)
DE-CH - (Svizzera tedesca)	EN-CA - Inglese (Canada)
EN-US - Inglese (Stati Uniti)	

Supporto tastiere internazionali - Non-UEFI	
AR - Arabo (utilizza l'alfabeto latino)	EN-US - Inglese (Stati Uniti)
DE-FR - (Svizzera francese)	EN-GB - Inglese (Regno Unito)
DE-CH - (Svizzera tedesca)	EN-CA - Inglese (Canada)

Sistemi operativi

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

Sistemi operativi Windows (a 32 e 64 bit)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (November 2019 Update/19H2 - November 2022 Update/22H2) **Nota:** OEM e ODM non inviano Windows 10 v2004 (May 2020 Update/20H1 e versioni successive) con architettura a 32 bit. Per ulteriori informazioni, consultare https://docs.microsoft.com/it-it/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC

Sistemi operativi Windows (a 32 e 64 bit)
○ Windows 11: Enterprise, Pro v21H2 - 22H2

Le funzioni di autenticazione sono disponibili solo quando è attivata l'Autenticazione di preavvio.

Localizzazione

SED Manager è un'interfaccia utente multilingue (MUI, Multilingual User Interface) ed è localizzata nelle lingue seguenti. La modalità UEFI e l'Autenticazione di preavvio sono supportate nelle lingue seguenti:

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

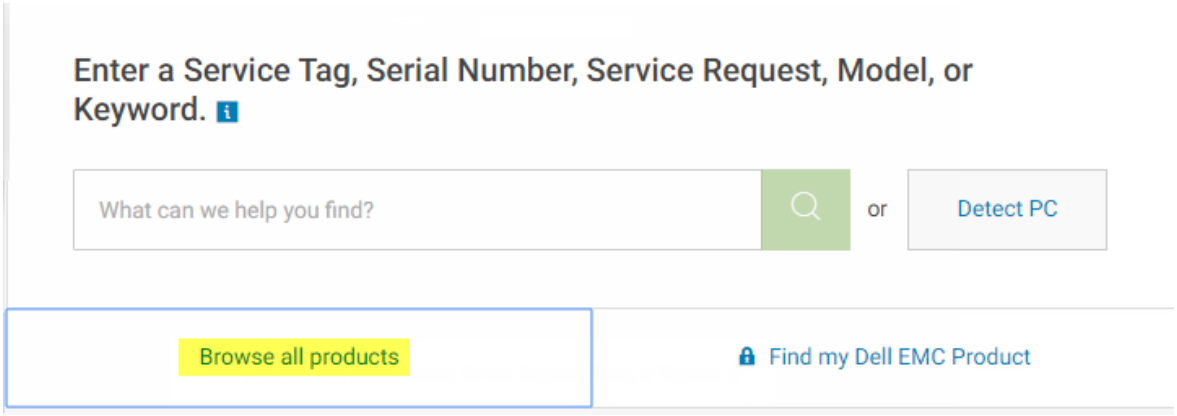
3

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 **Sicurezza** dall'elenco di prodotti.
3. Selezionare **Dell Data Security**.

   Dopo aver effettuato la selezione una volta, il sito Web la memorizza.
4. Selezionare il prodotto Dell.

   Esempi:

   Dell Encryption Enterprise

   Dell Endpoint Security Suite Enterprise
5. Selezionare **Driver e download**.
6. Selezionare il tipo di sistema operativo del client desiderato.
7. Selezionare **Dell Encryption** nei risultati. Questo è solo un esempio, è probabile che si presenti in modo leggermente differente. Per esempio, potrebbero non esserci quattro file tra cui scegliere.
8. Selezionare **Scarica**.

   Andare in Installa Encryption Personal.

4

Installazione

È possibile installare Encryption Personal 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 Encryption Personal dall'interfaccia utente, dalla riga di comando o dagli script e utilizzando qualsiasi tecnologia push disponibile nella propria organizzazione.

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

N.B.: Se la Crittografia basata su criteri viene installata prima di Encryption Management Agent, può verificarsi un arresto anomalo del computer. Questo problema è causato dal mancato caricamento del driver di sospensione della crittografia che gestisce l'ambiente PBA. Come soluzione alternativa, utilizzare il programma di installazione principale o verificare che la Crittografia basata su criteri venga installata dopo Encryption Management Agent.

- Consultare la *Guida alla crittografia di Dell* per istruzioni sull'utilizzo della funzione della crittografia. Accedere alla guida da `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
- Consultare la Encryption External Media per istruzioni sulle funzioni di Encryption External Media. Accedere alla guida da `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption`.
- Consultare la *Encryption Personal* per istruzioni sull'utilizzo delle funzioni di Advanced Authentication. Accedere alla guida da `<Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help`.

Importare i diritti

L'installazione di Encryption Personal richiede una chiave di registro sul computer di destinazione. Questa chiave di registro viene aggiunta tramite l'interfaccia della riga di comando durante l'installazione o tramite la GUI prima dell'installazione.

Per aggiungere la chiave di registro tramite l'interfaccia della riga di comando, consultare Installazione dalla riga di comando.

Per aggiungere la chiave di registro tramite la GUI:

1. Aprire un editor di testo.
2. Aggiungere il seguente testo.

   ```
   [HKEY_LOCAL_MACHINE\Software\Dell\Dell Data Protection\Entitlement]

   "SaEntitlement"="1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-
   XXXXXXXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX="
   ```

3. Salvare il file di testo con l'estensione `.reg`.
4. Cliccare due volte sul file di registro salvato per importare il diritto Encryption Personal.

Scegliere un metodo di installazione

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

- Installazione interattiva - CONSIGLIATA
- Installazione dalla riga di comando

Installazione interattiva

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

- Il programma di installazione principale installa client multipli. Nel caso di Encryption Personal, installa la crittografia e la gestione SED.

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

1. Installare i diritti nel computer di destinazione, se necessario. Le istruzioni per l'aggiunta dei diritti al computer sono incluse con il messaggio di posta elettronica che illustra le informazioni sulla licenza.
2. Copiare DDSSetup.exe nel computer locale.
3. Cliccare due volte su DDSSetup.exe per avviare il programma di installazione.
4. Viene visualizzata una finestra di dialogo che informa l'utente sullo stato di installazione dei prerequisiti. L'operazione richiede alcuni minuti.
5. Cliccare su **Avanti** nella schermata iniziale.
6. Leggere il contratto di licenza, accettare i termini, quindi cliccare su **Avanti**.
7. Cliccare su **Avanti** per installare Encryption Personal nel percorso predefinito di `C:\Program Files\Dell\Dell Data Protection\`.
8. L'Autenticazione è installata per impostazione predefinita e non è possibile deselezionarla. Nel programma di installazione queste opzioni sono indicate come Security Framework.

   Cliccare su **Avanti**.
9. Cliccare su **Installa** per avviare l'installazione.

   Viene visualizzata una finestra di stato. L'operazione richiede alcuni minuti.
10. Selezionare **Sì, riavvia ora** e cliccare su **Fine**.
11. Al riavvio del sistema, autenticarsi in Windows.

L'installazione di Encryption Personal e Advanced Authentication è completa.

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

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

La parte rimanente di questa sezione descrive in dettaglio altre attività di installazione e può essere ignorata. Procedere con la sezione Installazioni guidate di Advanced Authentication e Encryption Personal.

Installazione dalla riga di comando

Per installare Encryption Personal usando la riga di comando, 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.

- Installare i diritti nel computer di destinazione, se necessario.
- **N.B.:** I registri di Dell Encryption non specificano se lo spazio non sufficiente sul disco ha causato o meno un errore durante l'installazione.
- 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.

Switch	Significato
/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.

Parametri
FEATURE=PE
DIRITTI=1:PE:{codice di licenza di Encryption Personal qui} **N.B.:** Questo parametro può essere usato **solo** con Encryption Personal

- Esempio di installazione dalla riga di comando

  Negli esempi delle righe di comando il riavvio è stato eliminato, ma un riavvio finale sarà necessario perché

  La Crittografia basata su criteri 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 viene installato il Encryption client (installazione automatica, nessun riavvio e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`) passando il codice di licenza direttamente al programma di installazione.

  DDPE_XXbit_setup.exe /s /v"ENTITLEMENT=1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-XXXXX-XXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX= /l*v c:\Shieldinstall.log /qn /norestart"

- Nell'esempio seguente vengono installati Encryption Personal e Advanced Authentication (installazione automatica, nessun riavvio e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE\""
  ```

- Nell'esempio seguente vengono installati Encryption Personal e Advanced Authentication (installazione automatica, nessun riavvio e installazione nel percorso alternativo `C:\Program Files\Dell\My_New_Folder`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
  ```

  Al riavvio del sistema, autenticarsi in Windows.

  L'installazione di Encryption Personal e Advanced Authentication è completa.

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

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

  La parte rimanente di questa sezione descrive in dettaglio altre attività di installazione e può essere ignorata. Procedere con la sezione Installazioni guidate di Advanced Authentication e Personal Edition.

5

Installazioni guidate di Advanced Authentication e Encryption Personal

Accedere a Windows con il proprio nome utente e password. Viene 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 Advanced Authentication. Cliccare su **Avanti**.
3. Digitare e immettere nuovamente una nuova Password di amministratore per crittografia (EAP). Cliccare su **Avanti**.

   Nota: la password di amministratore per Encryption deve essere di almeno otto caratteri e non può superare 127 caratteri.
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 Advanced Authentication.

   Al termine della procedura guidata di attivazione di Advanced Authentication, procedere al passaggio successivo.
6. Avviare l'installazione guidata di Encryption Personal dall'icona di Dell Data Encryption 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 cliccare 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.

   Cliccare 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 8 e 127 caratteri e confermarla. La password deve contenere caratteri alfabetici, numerici e speciali. Questa password può essere uguale all'EAP impostata per Advanced Authentication, ma non è collegata ad essa. **Registrare e salvare la password in un luogo sicuro.** Cliccare su **Avanti**.

   Nota: la password di amministratore per Encryption deve essere di almeno otto caratteri e non può superare 127 caratteri.
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 sono 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 > Dell > Guida alla crittografia**.

    Cliccare 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 viene 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 viene etichettata come "Conforme".

6

Configurare le impostazioni della console

Le impostazioni predefinite consentono ad amministratori e utenti di utilizzare Advanced Authentication 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 Advanced Authentication. Tuttavia, per impostazione predefinita, non è abilitata l'autenticazione di Windows a più fattori.

Per configurare le funzioni di Advanced Authentication, è necessario accedere al computer come amministratore.

Modificare la password di amministratore e il percorso di backup

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

1. In qualità di amministratore, avviare Dell Data Security Console 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, per 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.

   Viene 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), Advanced Authentication richiederà un percorso per il backup dei dati. Per poter iniziare la crittografia è richiesto l'accesso ai dati di ripristino.

Configurazione dell'autenticazione di preavvio

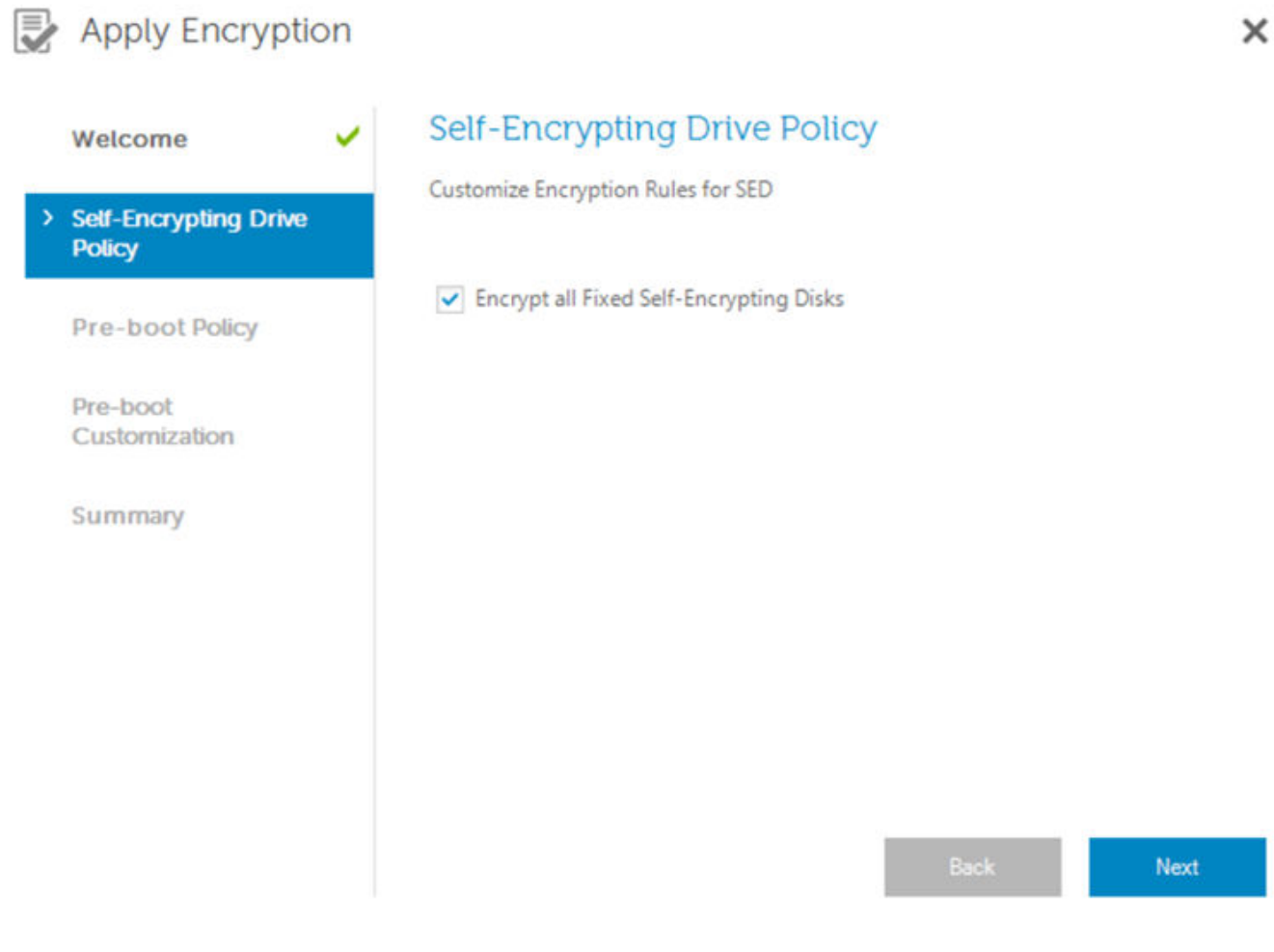
L'autenticazione di preavvio (PBA) è disponibile se il computer è dotato di una SED. La PBA è configurata tramite la scheda Crittografia. Quando SED Manager assume la proprietà della SED, la PBA viene attivata.

Per attivare la gestione SED:

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

   Se viene visualizzato *Percorso di backup non trovato* e il percorso di backup si trova in un'unità USB, è possibile che l'unità non sia connessa oppure che sia connessa a uno slot diverso da quello utilizzato durante il backup. Se viene visualizzato il messaggio e il percorso di backup si trova in un'unità di rete, quest'ultima risulta inaccessibile dal computer. Se è necessario modificare il percorso di backup, dalla scheda **Impostazioni amministratore** selezionare **Modifica percorso di backup** per modificare il percorso dello slot o dell'unità accessibile corrente. Qualche secondo dopo aver riassegnato il percorso, è possibile procedere con l'abilitazione della crittografia.
3. Fare clic sulla scheda **Crittografia** e quindi su **Crittografa**.
4. Nella schermata iniziale, fare clic su **Avanti**.

5. Selezionare **Crittografa tutti i dischi self-encrypting fissi** per abilitare la crittografia multi-disco.



6. Nella pagina Criterio di preavvio, modificare o confermare i seguenti valori, quindi fare clic su **Avanti**.

Tentativi di accesso per gli utenti non memorizzati nella cache	Numero di tentativi di accesso consentiti agli utenti sconosciuti, ossia agli utenti che non hanno mai effettuato l'accesso al computer in precedenza e le cui credenziali non sono memorizzate nella cache.
Tentativi di accesso per gli utenti memorizzati nella cache	Numero di volte per cui un utente conosciuto può tentare l'accesso.
Tentativi di risposta alle domande di ripristino	Numero di volte per cui un utente può tentare di inserire la risposta corretta.
Attiva password di cancellazione con crittografia	Selezionare per abilitare.
Immetti password di cancellazione con crittografia	Come meccanismo di sicurezza FailSafe viene utilizzato un codice o una parola con lunghezza massima di 100 caratteri. L'inserimento di questa parola o codice nel campo Nome utente o Password durante l'autenticazione di preavvio avvia la cancellazione con crittografia, che elimina le chiavi dall'archiviazione sicura. Una volta richiamato il processo, il disco è irrecuperabile. Lasciare vuoto questo campo se non si desidera rendere disponibile alcuna password di cancellazione con crittografia in caso di emergenza. Lasciare vuoto questo campo se non si desidera rendere disponibile alcuna password di cancellazione con crittografia in caso di emergenza.

Memorizza profilo utente	Abilita o disabilita la possibilità per l'utente di selezionare l'opzione Memorizza credenziali sulla schermata di accesso PBA.

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

Testo del Titolo di preavvio	Questo testo viene visualizzato nella parte superiore della schermata PBA. Se si lascia vuoto questo campo non verrà visualizzato alcun titolo. Il testo non va a capo, pertanto l'immissione di più di 17 caratteri potrebbe comportare il troncamento del testo.
Testo informazioni supporto	Testo da visualizzare nella schermata PBA contenente le informazioni per il supporto. Personalizzare il messaggio in modo da includere indicazioni specifiche su come contattare l'help desk o l'amministratore della sicurezza. Il mancato inserimento di testo in questo campo comporta la mancata disponibilità all'utente delle informazioni per contattare il supporto tecnico. Il testo viene mandato a capo a livello di parola, non di carattere. Se una singola parola ha una lunghezza di oltre 50 caratteri, tale parola non viene mandata a capo e non viene aggiunta alcuna barra di scorrimento. Il testo risulta pertanto troncato.
Testo note legali	Questo testo viene visualizzato prima che l'utente possa accedere al dispositivo. Ad esempio: “Facendo clic su OK, l'utente accetta di osservare i criteri di utilizzo del computer”. Non inserendo del testo in questo campo non verrà visualizzato alcun testo o verranno visualizzati i pulsanti OK/Annulla. Il testo viene mandato a capo a livello di parola, non di carattere. Se ad esempio è presente una singola parola con lunghezza di oltre 50 caratteri, tale parola non viene mandata a capo e non viene aggiunta alcuna barra di scorrimento. Il testo risulta pertanto troncato.

8. Nella pagina di riepilogo, fare clic su **Applica**.
9. Quando richiesto, fare clic su **Arresta il sistema**.

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

10. Dopo l'arresto, riavviare il sistema.

    L'autenticazione viene ora gestita da Encryption Management Agent. Gli utenti devono accedere alla schermata di PBA con le relative password di Windows.

Modifica della gestione SED e delle impostazioni PBA

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

- Modifica criterio o personalizzazione di preavvio - Fare clic sulla scheda **Crittografia** quindi fare clic su **Modifica**.
- Disattivazione della gestione SED (ad es. per la disinstallazione): fare clic su **Decrittografa**.

Dopo aver prima attivato la gestione SED e configurato il criterio e la personalizzazione di preavvio, sono disponibili le seguenti azioni nella scheda Impostazioni di preavvio:

- Modifica criterio o personalizzazione di preavvio - Cliccare sulla scheda **Impostazioni di preavvio** e selezionare **Criterio self-encrypting drive**, **Criterio di preavvio** o **Personalizzazione preavvio**.

Gestione degli utenti e della loro autenticazione

Aggiungi utente

Gli utenti di Windows diventano automaticamente utenti di Encryption Personal quando effettuano l'accesso a Windows o registrano una credenziale.

Il computer deve essere collegato al dominio per aggiungere un utente del dominio dalla scheda Aggiungi utente della Data Security Console.

1. Nel riquadro sinistro dello strumento Impostazioni amministratore, selezionare **Utenti**.
2. Nella parte superiore destra della pagina Utente, fare clic su **Aggiungere utenti** per iniziare il processo di registrazione per un utente Windows esistente.
3. Quando viene visualizzata la finestra di dialogo Seleziona utente, selezionare **Tipi di oggetto**.
4. Immettere il nome di un oggetto utente nella casella di testo e fare clic su **Controlla nomi**.
5. Al termine fare clic su **OK**.

Elimina utente

1. Nel riquadro sinistro dello strumento Impostazioni amministratore, selezionare **Utenti**.
2. Per eliminare un utente, individuare la colonna utente e fare clic su **Rimuovi**. (per visualizzare l'opzione Rimuovi scorrere fino alla fine della colonna utente).

Rimuovere tutte le credenziali registrate di un utente

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

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

7

Disinstallazione del 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 Encryption Management Agent.

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

Disinstallazione in modo interattivo

1. Selezionare *Disinstalla un programma* nel Pannello di controllo di Windows (nella barra delle applicazioni per la ricerca, digitare **Pannello di controllo**, quindi selezionare Pannello di controllo dai risultati).
2. Evidenziare **Dell Installer** e fare clic con il pulsante sinistro del mouse su **Modifica** 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.

   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.

  ```
  "DDSSetup.exe" /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.

8

Eseguire la disinstallazione usando i programmi di installazione figlio

- Dell consiglia di utilizzare Data Security Uninstaller per rimuovere Encryption Personal.
- 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 Encryption Personal 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 la crittografia

- **Prima di iniziare il processo di disinstallazione**, Creare 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 un file di registro di Encryption Removal Agent.

  N.B.: Prima di disinstallare, accertarsi che tutti i modelli di policy siano impostati su Disabilitato e inserire un qualsiasi supporto esterno crittografato per la decodifica automatica.

  Questo video descrive la modifica dei modelli di policy nella Local Management Console.

- 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 di 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:

- Disinstallazione in modo interattivo
- Eseguire la disinstallazione dalla riga di comando

Disinstallazione in modo interattivo

1. Selezionare *Disinstalla un programma* nel Pannello di controllo di Windows (nella barra delle applicazioni per la ricerca, digitare **Pannello di controllo**, quindi selezionare **Pannello di controllo** dai risultati).
2. Evidenziare **Dell Encryption a XX bit** e cliccare con il pulsante sinistro del mouse su **Cambia** per avviare l'installazione guidata di Encryption Personal.
3. Leggere la schermata iniziale e cliccare su **Avanti**.
4. Nella schermata di installazione di Encryption Removal Agent, selezionare una delle voci seguenti:

N.B.: 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.

  Cliccare su **Avanti**.

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

   Immettere la password di amministratore per crittografia. Si tratta della password della procedura di configurazione guidata al momento dell'installazione del software.

   Cliccare su **Avanti**.

6. In *Accesso a Dell Decryption Agent Service come* selezionare **Account di sistema locale** e cliccare su **Fine**.
7. Nella schermata Rimuovi il programma cliccare su **Rimuovi**.
8. Nella schermata Configurazione completata cliccare su **Fine**.
9. 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:\<any directory>\<any log file name>.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.

Switch	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 pacchetto di chiavi Forensic 0 - Non installare Encryption Removal Agent
CMGSILENTMODE	Proprietà che consente di eseguire la disinstallazione invisibile all'utente: 1 - Invisibile all'utente - opzione richiesta per l'esecuzione con variabili msiexec contenenti /q o /qn 0 - Visibile all'utente - possibile solo quando le variabili msiexec con /q non sono presenti nella sintassi della riga di comando
DA_KM_PW	Password dell'account amministratore di dominio.
DA_KM_PATH	Percorso per il pacchetto 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 pacchetto di chiavi Forensic. Copiare il pacchetto 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 Encryption Management Agent

Scegliere un metodo di disinstallazione

Vi sono due metodi per disinstallare Encryption Management Agent, selezionare **uno** dei seguenti:

- Disinstallazione in modo interattivo
- Eseguire la disinstallazione dalla riga di comando

Disinstallazione in modo interattivo

1. Selezionare *Disinstalla un programma* nel Pannello di controllo di Windows (nella barra delle applicazioni per la ricerca, digitare **Pannello di controllo**, quindi selezionare **Pannello di controllo** dai risultati).
2. Evidenziare **Dell Encryption Management Agent** e fare clic con il pulsante sinistro del mouse su **Modifica** per avviare l'installazione guidata.
3. Leggere la schermata iniziale e cliccare 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 di Encryption Management Agent è disponibile al percorso `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- Nell'esempio seguente viene eseguita la disinstallazione invisibile all'utente di SED Management.

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

  Al termine, arrestare e riavviare il sistema.

9

Programma di disinstallazione Data Security

Disinstallare Encryption Personal

Dell fornisce Data Security Uninstaller come principale programma di disinstallazione. Questa utilità raccoglie i prodotti attualmente installati e li rimuove nell'ordine appropriato.

Il programma di disinstallazione Data Security è disponibile in: `C:\Program Files (x86)\Dell\Dell Data Protection`

Per ulteriori informazioni o per utilizzare l'interfaccia della riga di comando (CLI), vedere l'articolo della KB 125052.

I registri vengono generati in `C:\ProgramData\Dell\Dell Data Protection\` per tutti i componenti rimossi.

Per eseguire l'utilità, aprire la cartella che la contiene, fare clic con il pulsante destro del mouse su **DataSecurityUninstaller.exe** e selezionare **Avvia come amministratore.**

Cliccare su **Avanti**.

Se lo si desidera, deselezionare qualsiasi applicazione per la rimozione, quindi fare clic su **Avanti**.

Le dipendenze necessarie vengono automaticamente selezionate o deselezionate.

Per rimuovere le applicazioni senza dover installare Encryption Removal Agent, scegliere **Non installare Encryption Removal Agent** e selezionare **Avanti**.

Selezionare **Encryption Removal Agent - Importa chiavi da file**, quindi fare clic su **Avanti**.

Individuare la posizione delle chiavi di ripristino, quindi immettere la passphrase per il file e fare clic su **Avanti**.

Selezionare **Rimuovi** per avviare la disinstallazione.

Fare clic su **Fine** per completare la rimozione e riavviare il computer. L'opzione **Riavvia il computer al termine** è selezionata per impostazione predefinita.

La disinstallazione e la rimozione sono state completate.

10

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 di crittografia basati su criteri vengono crittografati in base al criterio Regole di crittografia SDE. Se si modifica il valore di questo criterio, è necessario riavviare il sistema.
Algoritmo di crittografia SDE	AES256									AES-256, AES-128
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

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
										sulla modifica dei valori predefiniti.
Criteri delle impostazioni generali										
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

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
										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 I file di paging del sistema sono crittografati usando l'algoritmo AES-128.
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

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
										di crittografare importanti file di sistema, causando il mancato avvio di un computer. Nomi di processi comuni: outlook.exe, winword.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
Chiave di Application Data Encryption	Comune									Comune o utente Scegliere una chiave che indica chi può accedere ai file crittografati con Elenco Application Data Encryption e dove. Comune: questi file sono 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: questi file sono 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

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
										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 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

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
										· \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.
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

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
										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.
File Ibernazione sicura 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 computer esce dallo stato di sospensione, assicurando la protezione senza influire sull'attività di utenti o applicazioni mentre il computer è in uso.

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
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 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 rimovibile 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 Algoritmo di crittografia utilizzato per crittografare i dati a livello di singolo utente. È possibile specificare valori diversi per utenti diversi dello stesso endpoint.

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 crittografia dati utente	Utente	Comune		Utente	Comune				Utente	Comune o utente Scegliere una chiave che indica chi può accedere ai file crittografati in base ai seguenti criteri, e dove: · Cartelle crittografate utente · Crittografa cartelle personali Outlook · Crittografa file temporanei (solo in \Documents and Settings\nome utente\Impostazioni locali\Temp) · Crittografa file temporanei Internet · Crittografa documenti profilo utente Selezionare: · Comune: perché 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: affinché 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	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
										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)										
L'Hardware Crypto Accelerator (HCA)	Falso									È il "criterio principale" per tutti gli altri criteri di Hardware Crypto Accelerator (HCA). Se impostato su 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.
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) in cui è installato l'Encryption client corrente Se impostato su Falso, i metadati forensi non sono inclusi nell'unità.

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
										Passando da Falso a Vero si avvia nuovamente la ricerca in base ai criteri 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 criteri di Sistema di controllo porte. Tutti i criteri PCS richiedono il riavvio del sistema affinché le nuove impostazioni abbiano effetto. **N.B.:** Bloccando le operazioni dei dispositivi, i nomi dei dispositivi vengono visualizzati come vuoti.
Porta: slot scheda Express	Abilitata									Consente di abilitare, disabilitare o ignorare le porte esposte tramite lo slot scheda Express.

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: 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 Encryption External Media e 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	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
memoria (MTD)										
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

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
										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 Encryption External Media e Sistema di controllo porte.
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.

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
										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.
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

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 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 Encryption External Media e 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 Encryption External Media e 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 porte. Consultare Encryption External Media e 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

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
										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 consente 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
EMS - Esegui scansione del supporto esterno	Vero	Falso								Il criterio Vero consente ai supporti rimovibili di essere analizzati ogni volta che vengono inseriti. Quando questo criterio è impostato su Falso e il criterio EMS - Crittografa il supporto esterno è impostato su Vero, vengono crittografati solo i file nuovi e modificati. Una scansione viene eseguita a ogni inserimento in modo da poter rilevare tutti i file aggiunti al supporto rimovibile senza autenticazione. Se l'autenticazione viene rifiutata, i file possono essere aggiunti al supporto, ma i dati crittografati non sono

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
										accessibili. In questo caso, i file aggiunti non vengono crittografati e la volta successiva che si esegue l'autenticazione del supporto (per utilizzare i dati crittografati) tutti i file eventualmente aggiunti sono sottoposti a scansione e crittografati.
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 rimovibili da non includere nella crittografia. Tutti i dispositivi multimediali rimovibili non presenti in questo elenco vengono 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 crittografato. 2. Aprire l' EMSService.log C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3. Trovare "PNPDeviceID="

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
										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	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
contenere lettere										
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

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
										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. 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 2.048 caratteri vengono ignorate. I dispositivi di archiviazione dotati di connessioni multi-interfaccia, quali Firewire, USB, eSATA e così via, possono richiedere l'utilizzo sia di Encryption External Media sia delle regole 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 Encryption External Media.
EMS - Blocca accesso a supporti non protetti	Vero								Falso	Bloccare l'accesso ai supporti rimovibili da meno di 55 MB, ovvero con una capacità di archiviazione insufficiente per contenere Encryption External Media (come un floppy da 1,44 MB). L'accesso è bloccato quando sia il criterio EMS che questo criterio sono impostati su Vero. Se EMS - Crittografa il supporto esterno è impostato su Vero, ma questo criterio

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 impostato su Falso, si dispone di accesso in lettura al supporto non crittografabile, ma l'accesso in scrittura al supporto è bloccato. Se EMS - Crittografa il supporto esterno è Falso, questo criterio non ha alcun effetto e l'accesso al supporto non crittografabile resta invariato.
Criteri di controllo dell'esperienza utente										
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 viene 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	Falso		Vero					Falso		Se si imposta il valore su Vero, l'utente visualizza

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
elaborazione crittografia locale										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 la crittografia). Permettendo a un utente di mettere in pausa la crittografia, si potrebbe consentirgli di impedire al Encryption client di crittografare o decrittografare completamente i dati in base al 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 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 supporti 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 supporti 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 supporti 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 supporti 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 supporti 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 supporti rimovibili.

Protezione base per unità esterne

Questo modello criteri:

- Protegge i supporti 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.

11

Estrarre i programmi di installazione figlio

- 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`DDSSetup.exe`.
2. Nello stesso percorso del file `DDSSetup.exe` aprire un prompt dei comandi e inserire:

   ```
   DDSSetup.exe /s /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.

12

Risoluzione dei problemi

Aggiornamento tramite Aggiornamenti funzionalità di Windows 10 o Windows 11

Per aggiornare Windows 10 o Windows 11 utilizzando Aggiornamenti funzionalità, attenersi alle istruzioni riportate nell'articolo della KB 125419.

Risoluzione dei problemi di Dell Encryption

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 gli 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 Encryption External Media e il sistema di controllo delle 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 > Sottoclasse memorizzazione: Controllo unità esterne. Se si intende impostare il criterio EMS - Accesso a supporto non protetto su *Accesso completo*, accertarsi che anche il criterio Sottoclasse 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 Crittografia dei supporti Windows = attivata.
- Impostare EMS - Escludi crittografia CD/DVD = non selezionata.
- Sottoclasse memorizzazione: Controllo unità ottiche = Solo UDF

Usare WSScan

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

N.B.: WSScan deve essere eseguito in modalità sistema con lo strumento PsExec se un file di destinazione è di proprietà dell'account di sistema.

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: *Tutte le unità, Tutte le unità fisse, Unità rimovibili* o *CDROM/ DVDROM*.
5. Selezionare il Tipo di rapporto di crittografia: *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 della 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 nel menu 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" è ancora crittografato con AES256

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 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, "**è ancora crittografato con AES256**" RIJNDAEL 128 RIJNDAEL 256 AES-128 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 aggiornarne lo stato.

- **In attesa della disattivazione di SDE** – La crittografia è ancora installata, configurata o entrambe le cose. La decrittografia inizia solo dopo la disinstallazione della 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, del driver, dell'eseguibile e dell'eseguibile del driver.

Come crittografare un iPod con Encryption External Media

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.

- Dell sconsiglia l'utilizzo dell'iPod Shuffle poiché potrebbero verificarsi problemi imprevisti.
- Queste informazioni variano di pari passo con l'uscita di nuovi modelli, pertanto è necessaria la massima cautela quando si consente l'utilizzo di iPod su computer in cui è attivato Encryption External Media.
- Poiché i nomi delle cartelle sugli iPod variano a seconda del modello di iPod, Dell 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 Encryption External Media non renda il dispositivo inutilizzabile, immettere le seguenti regole nel criterio Regole crittografia di Encryption External Media:

  -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. Accedere all'indirizzo web dell.com/support.
2. Selezionare il modello di computer.
3. Selezionare **Driver e download**.
4. Selezionare il **Sistema operativo** del computer di destinazione.
5. Selezionare 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

1. Passare alla cartella in cui è stato scaricato il file di installazione del driver.
2. Cliccare due volte sul driver di Dell ControlVault per avviare il file eseguibile autoestraente.

   N.B.:

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

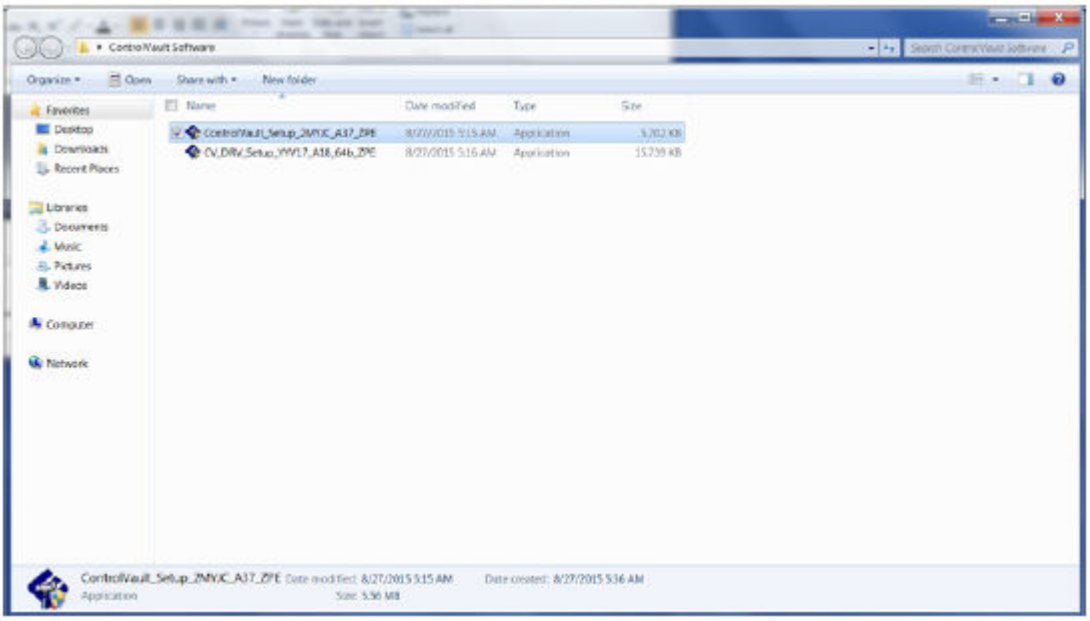
3. Cliccare su **Continua** per iniziare.
4. Cliccare su **OK** per decomprimere i file del driver nel percorso predefinito `C:\Dell\Drivers\<New Folder>`.
5. Cliccare su **Sì** per consentire la creazione di una nuova cartella.
6. Cliccare su **OK** quando viene visualizzato il messaggio di completamento 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. In questo caso, la cartella è **JW22F**.
8. Cliccare due volte 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)].
9. Cliccare su **Avanti** nella schermata iniziale.
10. Cliccare su **Avanti** per l'installazione dei driver nel percorso predefinito `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Selezionare l'opzione **Completata** e cliccare su **Avanti**.
12. Cliccare su **Installa** per avviare l'installazione dei driver.
13. È possibile, facoltativamente, selezionare la casella di controllo per visualizzare il file di registro del programma di installazione. Cliccare su **Fine** per uscire dalla procedura guidata.

Verificare l'installazione del driver

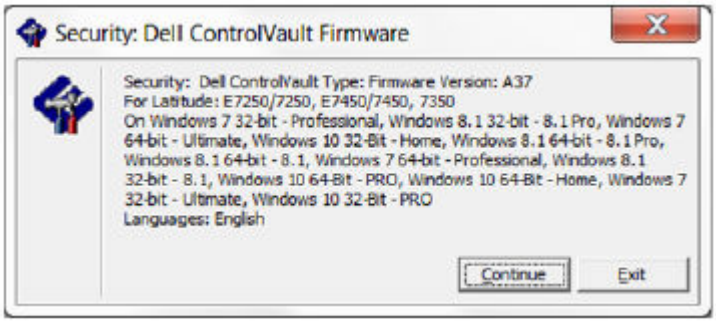
- Device Manager avrà un dispositivo Dell ControlVault (e altri dispositivi) a seconda del sistema operativo e della configurazione dell'hardware.

Installare il firmware di Dell ControlVault

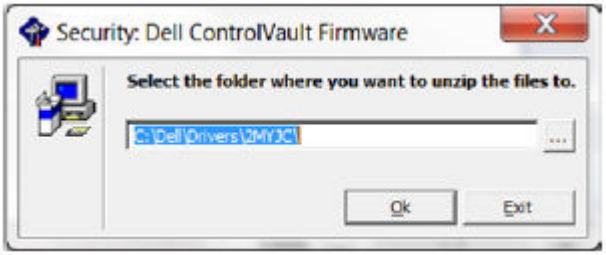
1. Passare alla cartella in cui è stato scaricato il file di installazione del firmware.



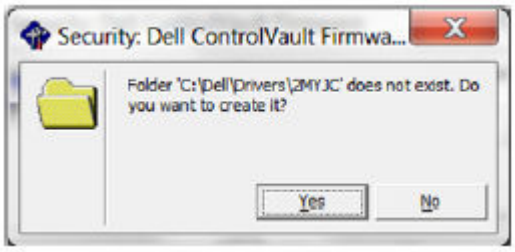
2. Cliccare due volte sul firmware di Dell ControlVault per avviare il file eseguibile autoestraente.
3. Cliccare su **Continua** per iniziare.



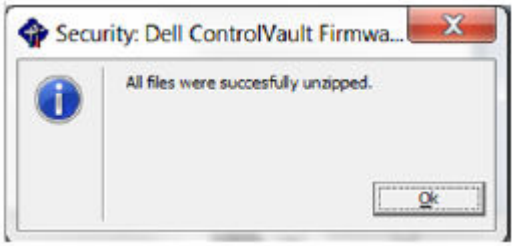
4. Cliccare su **OK** per decomprimere i file del driver nel percorso predefinito `C:\Dell\Drivers\<New Folder>`.



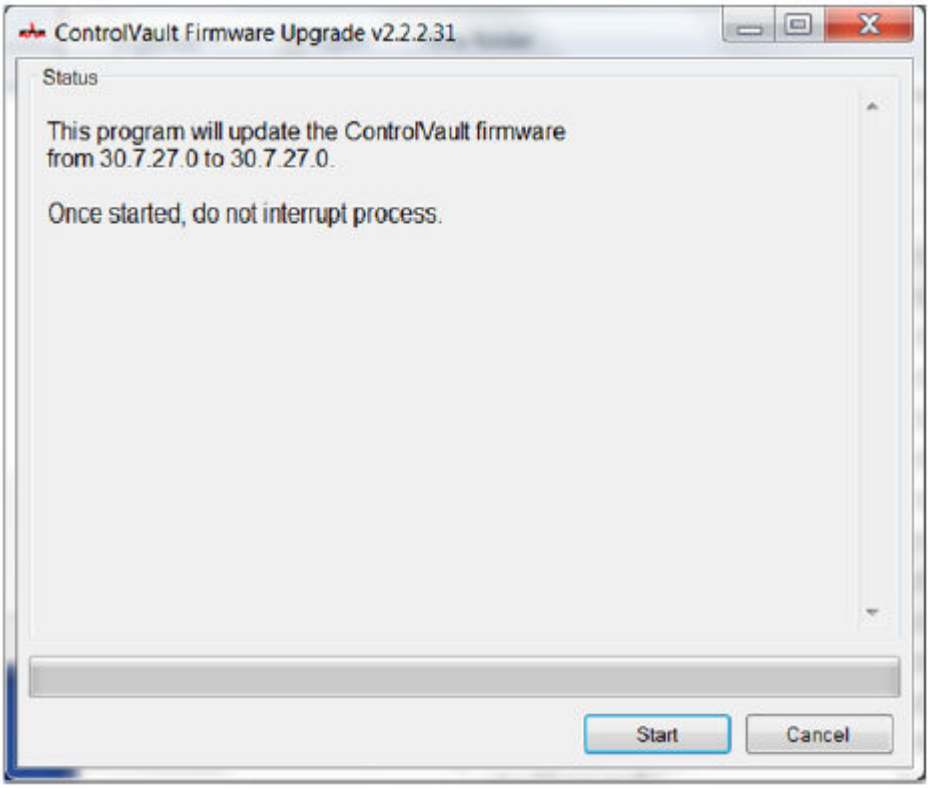
5. Cliccare su **Sì** per consentire la creazione di una nuova cartella.



6. Cliccare 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. Cliccare due volte su **ushupgrade.exe** per avviare il programma di installazione del firmware.
9. Cliccare su **Avvia** per avviare l'aggiornamento del firmware.



N.B.:

Se si tratta dell'aggiornamento di una versione precedente del firmware, all'utente potrebbe essere richiesto di immettere la password di amministratore. Immettere `Broadcom` come password e cliccare su **Invio** se viene visualizzata questa finestra di dialogo.

Vengono visualizzati alcuni messaggi di stato.

10. Cliccare 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.

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 gli 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 stabilire se è presente una smart card ed è attiva, accertarsi che sia impostato il seguente valore:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Se SmartcardEnabled è mancante o presenta un valore zero, il provider delle credenziali visualizzerà solo la password per l'autenticazione.

  Se SmartcardEnabled ha un valore diverso da zero, il provider delle credenziali visualizzerà le opzioni per la password e l'autenticazione smart card.

- Il seguente valore di registro indica se Winlogon debba generare una notifica per gli eventi di accesso da smart card.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = Disabilitata

  1 = Abilitata

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 mostra il prompt *`length of each policy update delay`* 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 modifica il comportamento predefinito della posposizione. In assenza di interazione dell'utente, l'elaborazione della crittografia viene 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 x [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 la crittografia sta elaborando un aggiornamento del criterio che include un criterio SDE attivo, la directory del profilo utente in uso viene cifrata 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 viene usata per crittografare queste directory dell'utente.

Disabilitare/Abilitare l'opzione Encrypt for Sharing nel menu di scelta rapida visualizzato cliccando con il pulsante destro del mouse

- Per disabilitare o abilitare l'opzione *Encrypt for Sharing* nel menu di scelta rapida visualizzato cliccando con il pulsante destro del mouse, utilizzare la seguente chiave del Registro di sistema:

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

  0 = disabilita l'opzione Encrypt for Sharing nel menu di scelta rapida visualizzato cliccando con il pulsante destro del mouse

  1 = abilita l'opzione Encrypt for Sharing nel menu di scelta rapida visualizzato cliccando con il pulsante destro del mouse

Disabilitare/Abilitare la notifica per l'attivazione di Encryption Personal

- HKCU\Software\Dell\Dell Data Protection\Encryption

  "HidePasswordPrompt"=DWORD

  1 = disabilita il prompt della password per l'attivazione di Encryption Personal

  0 = abilita il prompt della password per l'attivazione di Encryption Personal

Disabilitare/abilitare il prompt di riavvio dopo che Encryption Removal Agent ha terminato la fase finale di decrittografia

- Per disabilitare il prompt all'utente di riavvio del computer dopo che Encryption Removal Agent ha terminato lo stato finale del processo di decrittografia, modificare il seguente valore di registro.

  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  Impostazione predefinita = abilitato

  1 = abilitato (visualizza il prompt)

  0 = disabilitato (nasconde il prompt)

Autenticazione avanzata

Disabilitare smart card e servizi biometrici (facoltativo)

Se non si desidera che Advanced Authentication 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 disabilitata, l'autenticazione non tenta di avviare i seguenti tre servizi:

- SCardSvr - Gestisce l'accesso alle smart card lette dal computer. Se il servizio viene interrotto, questo computer non può 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 in hosting 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 determinare se la PBA è attivata, accertarsi che sia impostato il seguente valore:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

  "PBAIsActivated"=DWORD (32-bit):1

  Il valore 1 indica che la PBA è attivata. Il valore 0 indica che la PBA non è attivata.

  N.B.: L'eliminazione manuale di questa chiave può creare risultati indesiderati per gli utenti che effettuano la sincronizzazione con la PBA determinando la necessità di un ripristino manuale.

- Per stabilire se è presente una smart card ed è attiva, accertarsi che sia impostato il seguente valore:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Se SmartcardEnabled è mancante o presenta un valore zero, il provider delle credenziali visualizzerà solo la password per l'autenticazione.

  Se SmartcardEnabled ha un valore diverso da zero, il provider delle credenziali visualizzerà le opzioni per la password e l'autenticazione smart card.

- Il seguente valore di registro indica se Winlogon debba generare una notifica per gli eventi di accesso da smart card.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = Disabilitata

  1 = Abilitata

  Passare al Glossario.

- Per impedire a SED Management di disabilitare i provider di credenziali di terze parti, creare la seguente chiave del Registro di sistema:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 =Disabilitata; impostazione predefinita

1=Abilitata

- Per impostazione predefinita, Encryption Management Agent non restituisce più criteri. Per eseguire l'output dei criteri utilizzati in futuro, creare la seguente chiave del Registro di sistema:

  HKLM\Software\Dell\Dell Data Protection\

  DWORD: DumpPolicies

  Valore = 1

  Nota: per rendere effettive le modifiche, è necessario riavviare il sistema.

- Per eliminare tutte le notifiche Toaster da Encryption Management Agent, il seguente valore del registro deve essere impostato sul computer client.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Abilitata (impostazione predefinita)

  1 = Disabilitata

13

Glossario

Advanced Authentication - Il prodotto Advanced Authentication fornisce le opzioni del lettore di smart card. Advanced Authentication consente di gestire tali metodi di autenticazione, supporta l'accesso con unità autocrittografanti e SSO e gestisce le password e le credenziali dell'utente.

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 Management Console 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, la crittografia usa la chiave di crittografia 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 di crittografia Comune rende i file accessibili a tutti gli utenti gestiti nel dispositivo in cui sono stati creati. La chiave di crittografia Utente rende i file accessibili solo all'utente che li ha creati, solo nel dispositivo in cui sono stati creati. La chiave di crittografia Roaming utente rende i file accessibili solo all'utente che li ha creati, in qualsiasi dispositivo Windows o Mac crittografato.

Ricerca crittografia – Il processo di scansione delle cartelle da crittografare, 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 verifica 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 vengono analizzate a 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), attiva una ricerca. Anche abilitando e disabilitando la crittografia si attiva una ricerca crittografia.

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 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.