Dell Encryption Enterprise

Advanced Installation Guide v11.9

January 2023
Rev. A01

DELL Technologies

Messaggi di N.B., Attenzione e Avvertenza

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

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

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

Contents

1

Introduzione

Questa guida descrive in dettaglio la procedura per installare e configurare Encryption, SED Management, Full Disk Encryption, Protezione Web e Firewall client e BitLocker Manager.

Tutte le informazioni sui criteri e le relative descrizioni sono reperibili nella Guida dell'amministratore.

Prima di iniziare

1. Installare il Dell Server prima di procedere con la distribuzione dei client. Individuare la guida corretta come mostrato di seguito, seguire le istruzioni, quindi tornare a questa guida.
   - *Security Management Server Installation and Migration Guide (Guida alla migrazione e all'installazione di Security Management Server)*
   - *Security Management Server Virtual Quick Start Guide and Installation Guide (Guida introduttiva e all'installazione di Security Management Server Virtual)*
   - Verificare che i criteri siano impostati come desiderato. Sfogliare la Guida dell'amministratore, disponibile da **?** nella parte in alto destra della schermata. La Guida dell'amministratore è una guida a livello di pagina progettata per aiutare l'utente a impostare e modificare i criteri e comprendere le opzioni a disposizione con il Dell Server.
2. Leggere attentamente il capitolo Requisiti del presente documento.
3. Distribuire i client agli utenti.

Uso di questa guida

Usare questa guida nell'ordine seguente:

- Per prerequisiti del client, informazioni su hardware e software del computer, limitazioni, e modifiche di registro specifiche necessarie per le funzioni, consultare Requisiti.
- Se necessario, consultare Configurazione di pre-installazione per UEFI unità autocrittografante e BitLocker.
- Se i client ricevono i diritti usando Dell Digital Delivery (DDD), consultare Impostare l'oggetto criterio di gruppo nel controller di dominio per attivare i diritti.
- Se si installano i client tramite il programma di installazione principale di consultare:
  - Eseguire l'installazione interattiva usando il programma di installazione principale

    Oppure
  - Eseguire l'installazione dalla riga di comando usando il programma di installazione principale
- Se si installano i client usando i programmi di installazione figlio, i rispettivi file eseguibili devono essere estratti dal programma di installazione principale. Consultare Estrarre i programmi di installazione figlio dal programma di installazione principale, quindi tornare qui.
  - Installare i programmi di installazione figlio dalla riga di comando:
    - Installare crittografia - Utilizzare queste istruzioni per installare la crittografia, che è il componente che applica il criterio di protezione quando un computer è connesso alla rete, disconnesso dalla rete, perso o rubato.
    - Installare il client di Full Disk Encryption - Utilizzare queste istruzioni per installare Full Disk Encryption, che è un componente che applica il criterio di protezione quando un computer è connesso alla rete, disconnesso dalla rete, perso o rubato.
    - Installare SED Manager - Utilizzare queste istruzioni per installare il software di crittografia per le SED. Sebbene le unità autocrittografanti forniscano la propria crittografia, non dispongono di una piattaforma per la gestione di crittografia e criteri. Con SED Manager, tutti i criteri, i dispositivi di archiviazione e il recupero delle chiavi di crittografia sono disponibili da un'unica console, riducendo il rischio che i computer non siano protetti in caso di perdita o accesso non autorizzato.
    - Installare BitLocker Manager - Utilizzare queste istruzioni per installare BitLocker Manager, progettato per migliorare la sicurezza delle implementazioni BitLocker e semplificare e ridurre il costo di proprietà.

N.B.:

La *maggior parte* dei programmi di installazione figlio può essere installata in maniera interattiva, ma tali installazioni non sono descritte in questa guida.

- Consultare Scenari più comuni per prendere visione degli script degli scenari più comunemente usati.

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

Tutti i client

Questi requisiti si applicano a tutti i client. I requisiti elencati in altre sezioni si applicano a client specifici.

- 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, ad esempio Microsoft SCCM. Non sono supportati gli utenti non amministratori con privilegi elevati.
- Prima di iniziare l'installazione/la disinstallazione, eseguire il backup di tutti i dati importanti.
- Durante l'installazione non apportare modifiche al computer, quali l'inserimento o la rimozione di unità esterne (USB).
- Gli amministratori devono assicurarsi che tutte le porte necessarie siano disponibili.
- Visitare periodicamente dell.com/support per la documentazione più recente e le Avvertenze tecniche.
- La linea di prodotti Dell Data Security non supporta le versioni di Windows Insider Preview.

Prerequisiti

- Microsoft .Net Framework 4.5.2 (o versioni successive) è richiesto per i client del programma di installazione principale e del programma di installazione figlio di . Il programma di installazione *non* installa i componenti Microsoft .Net Framework.
- Per verificare la versione di Microsoft .Net installata, seguire queste istruzioni nel computer destinato all'installazione. Consultare queste istruzioni per installare Microsoft .Net Framework 4.5.2.
- Se si installa la crittografia in modalità FIPS, è richiesto Microsoft .NET Framework 4.6.

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. Lo spazio varia in base a criteri attivati e capacità dell'unità.

Localizzazione

- Dell Encryption, SED Manager, PBA Advanced Authentication, e BitLocker Manager sono compatibili con l'interfaccia utente multilingue e sono localizzati nelle lingue seguenti.

Supporto lingue		
EN - Inglese	IT - Italiano	KO - Coreano
ES - Spagnolo	DE - Tedesco	PT-BR - Portoghese (Brasile)

Supporto lingue		
FR - Francese	JA - Giapponese	PT-PT - Portoghese (Portogallo)

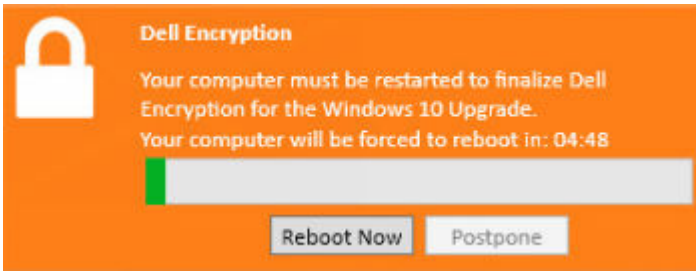
Crittografia

- Per essere attivato, il computer client deve essere dotato della connettività di rete.
- Per attivare un account Microsoft Live con Dell Encryption, fare riferimento a questo articolo della KB: 124722.
- Per ridurre la durata iniziale del processo di crittografia, eseguire Pulizia disco di Windows per rimuovere i file temporanei e tutti i dati non necessari.
- Il supporto di Windows Hello for Business richiede Encryption Enterprise v11.0 o versioni successive in esecuzione su Windows 10.
- Windows Hello for Business richiede l'attivazione su un server Dell su cui è in esecuzione la versione v11.0 o successiva.
- 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.
- La 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.
- 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.
- 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. Per le istruzioni di estrazione, consultare Estrarre i programmi di installazione figlio dal programma di installazione principale.
- La crittografia ora supporta la modalità Controllo. La modalità Controllo consente agli amministratori di implementare la crittografia come parte dell'immagine aziendale, piuttosto che usare soluzioni SCCM di terze parti o simili. Per istruzioni su come installare la crittografia in un'immagine aziendale, vedere l'articolo della KB 129990.
- 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.
- Dell Encryption utilizza i set di istruzioni di crittografia, Integrated Performance Primitives (IPP) di Intel. Per ulteriori informazioni, consultare l'articolo della KB 126015.
- Il TPM è utilizzato per sigillare la General Purpose Key. Pertanto, se si esegue la crittografia, cancellare il TPM nel BIOS prima di installare un nuovo sistema operativo nel computer di destinazione.
- La reinstallazione del sistema operativo sul posto 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.
- Il programma di installazione principale installa questi componenti se non sono già installati nel computer di destinazione. **Se si usa il programma di installazione figlio**, è necessario installare questi componenti prima di installare i client.

Prerequisito
○ Visual C++ 2012 Update 4 o Redistributable Package (x86 o x64) versione successiva ○ Visual C++ 2017 o Redistributable Package (x86 o x64) versione successiva ○ A partire da gennaio 2020, i certificati di firma SHA1 non sono più validi e non possono essere rinnovati. Per i dispositivi che eseguono Windows Server 2008 R2, è necessario installare gli aggiornamenti Microsoft KB https://support.microsoft.com/it-it/help/4474419 e https://support.microsoft.com/it-it/help/4490628 per convalidare i certificati di firma SHA256 su applicazioni e pacchetti di installazione. 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
- I criteri di *File in ibernazione sicura su Windows* e *Impedisci ibernazione non sicura* non sono supportati in modalità UEFI.

- L'attivazione posposta consente all'account utente dell'Active Directory utilizzato durante l'attivazione di essere indipendente dall'account utilizzato per accedere all'endpoint. Anziché avere il provider di rete che acquisisce le informazioni di autenticazione, l'utente deve specificare manualmente l'account basato su Active Directory, quando richiesto. Una volta inserite le credenziali, le informazioni di autenticazione vengono inviate in modo sicuro al Dell Server, che le convalida per i domini di Active Directory configurati. Per ulteriori informazioni, consultare l'articolo della KB 124736.
- 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:



Hardware

- La tabella seguente descrive in dettaglio l'hardware 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 ○ L'**attivazione posposta** include il supporto per tutte le risposte precedenti

Encryption External Media

Sistemi operativi

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

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)

Sistemi operativi Windows supportati per l'accesso a media cifrati (a 32 e 64 bit)
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 ○ L'**attivazione posposta** include il supporto per tutte le risposte precedenti

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

Full Disk Encryption

- Full Disk Encryption richiede l'attivazione su un Dell Server su cui è in esecuzione la versione 9.8.2 o successiva.
- Full Disk Encryption non è attualmente supportato sui computer host virtualizzati.
- Full Disk Encryption richiede un TPM hardware dedicato. PTT e i TPM basati su firmware non sono supportati al momento.
- I fornitori di credenziali di terze parti non funzioneranno con le funzionalità FDE installate e tutti i provider di credenziali di terze parti verranno disattivati quando il PBA viene abilitato.
- Per essere attivato, il computer client deve disporre della connettività di rete o del codice di accesso.
- Il computer deve essere dotato di una connessione di rete cablata per un utente smart card, per accedere mediante Autenticazione di preavvio per la prima volta.
- Gli aggiornamenti delle funzioni del sistema operativo non sono supportati con Full Disk Encryption.
- Una connessione cablata è richiesta per la PBA per comunicare con il Dell Server.
- Una SED non può essere presente sul computer di destinazione.
- La funzione Full Disk Encryption non è supportata con BitLocker o BitLocker Manager. Non installare Full Disk Encryption su un computer su cui è installato BitLocker o BitLocker Manager.
- Dell consiglia di installare il driver Intel Rapid Storage Technology più recente con le unità NVMe.
- 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.
- Full Disk Encryption Management 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.
- La reinstallazione del sistema operativo sul posto 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.
- 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 FDE. 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.
- Tutti i dischi devono essere inizializzati e formattati prima di abilitare Full Disk Encryption.
- Le configurazioni di crittografia su più dischi con Full Disk Encryption richiedono quanto segue:
  - Tutti i dischi nel sistema di destinazione devono avere la seguente configurazione:
    - Unità non SED
    - Configurato nella stessa modalità di avvio

    - Inizializzato come tabella di partizione GUID (GPT)
    - I dischi devono essere partizioni primarie
    - Ai dischi deve essere assegnata una lettera dell'unità
  - È necessario riavviare il sistema per crittografare i nuovi dischi dopo la configurazione iniziale.
  - È possibile crittografare un massimo di 16 dischi.
  - 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.

    Abilitare la crittografia multi-disco nella console di gestione. Vedere Impostazioni di registro per visualizzare i valori del Registro di sistema di Windows per la crittografia multi-disco e la ricerca multi-sweep.
  - Full Disk Encryption 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 Full Disk Encryption, 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.
- Il programma di installazione principale installa questi componenti se non sono già installati nel computer di destinazione. **Se si usa il programma di installazione figlio**, è necessario installare questi componenti prima di installare i client.

Prerequisito
○ Visual C++ 2017 o Redistributable Package (x86 o x64) versione successiva ○ A partire da gennaio 2020, i certificati di firma SHA1 non sono più validi e non possono essere rinnovati. Per i dispositivi che eseguono Windows Server 2008 R2, è necessario installare gli aggiornamenti Microsoft KB https://support.microsoft.com/it-it/help/4474419 e https://support.microsoft.com/it-it/help/4490628 per convalidare i certificati di firma SHA256 su applicazioni e pacchetti di installazione. 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

- **N.B.:** Con l'autenticazione di preavvio è obbligatoria una password. Dell consiglia di utilizzare una password minima con impostazione conforme alle policy di sicurezza interne.
- **N.B.:** Quando viene utilizzata la PBA, il criterio di Sincronizzazione di tutti gli utenti deve essere attivato se un computer ha più utenti. Inoltre, tutti gli utenti devono avere le password. Gli utenti di password di lunghezza zero verranno bloccati dal computer dopo l'attivazione.
- **N.B.:** I computer protetti da Full Disk Encryption 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.

N.B.: Full Disk Encryption deve essere configurato con gli algoritmi di crittografia impostati su AES-256 e con la modalità di crittografia impostata su CBC.

Hardware

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

Hardware integrato facoltativo
○ TPM 1.2 o 2.0

Opzioni di autenticazione con client Full Disk Encryption

- Per utilizzare le smart card e per eseguire l'autenticazione su computer UEFI, è necessario un hardware specifico. È necessaria la configurazione per utilizzare smart card con l'autenticazione di preavvio. Le seguenti tabelle mostrano le opzioni di autenticazione disponibili a seconda del sistema operativo, quando i requisiti hardware e di configurazione vengono soddisfatti.

UEFI				
	PBA - su computer Dell supportati			
	Password	Impronta	Smart card con contatti	Scheda SIPR
Windows 10	X[1]		X[1]	
Windows 11	X[1]		X[1]	
1. Disponibile con computer UEFI supportati.				

Modelli di computer Dell supportati con modalità di avvio UEFI

- Per l'elenco più aggiornato delle piattaforme supportate con Full Disk Encryption, consultare l'articolo della Knowledge Base 126855.
- Per un elenco delle docking station e degli adattatori supportati con Full Disk Encryption, consultare l'articolo della Knowledge Base 124241.

Sistemi operativi

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

Sistemi operativi Windows (a 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

Crittografia sui sistemi operativi del server

La crittografia dei sistemi operativi del server è destinata all'utilizzo nei computer che hanno in esecuzione la modalità server, in particolare i file server.

- La crittografia sui sistemi operativi del server è compatibile solo con Encryption Enterprise e Endpoint Security Suite Enterprise.
- La crittografia su sistemi operativi del server offre:
  - Crittografia del software
  - Crittografia dei supporti rimovibili
  - Controllo porte

    N.B.:

    Il server deve supportare il controllo delle porte.

    I criteri di sistema del controllo delle porte influenzano i supporti rimovibili sui server protetti, per esempio, controllando l'accesso e l'utilizzo delle porte USB del server da parte di dispositivi USB. Il criterio delle porte USB si applica alle porte USB esterne. La funzionalità delle porte USB interne non è influenzata dal criterio delle porte USB. Se il criterio delle porte USB viene disabilitato, la tastiera e il mouse USB del client non funzionano e l'utente non è in grado di usare il computer a meno che venga impostata una connessione al desktop in remoto prima che venga applicato il criterio.

- Il programma di installazione principale installa questi componenti se non sono già installati nel computer di destinazione. **Se si usa il programma di installazione figlio**, è necessario installare questi componenti prima di installare i client.

Prerequisito
○ Visual C++ 2012 Update 4 o Redistributable Package (x86 o x64) versione successiva ○ Visual C++ 2017 o Redistributable Package (x86 o x64) versione successiva ○ A partire da gennaio 2020, i certificati di firma SHA1 non sono più validi e non possono essere rinnovati. Per i dispositivi che eseguono Windows Server 2008 R2, è necessario installare gli aggiornamenti Microsoft KB https://support.microsoft.com/it-it/help/4474419 e https://support.microsoft.com/it-it/help/4490628 per convalidare i certificati di firma SHA256 su applicazioni e pacchetti di installazione. 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 crittografia dei sistemi operativi del server è da utilizzare con:

- File server con unità locali
- Guest di Virtual Machine (VM, Macchina virtuale) che hanno in esecuzione un sistema operativo server o non server come un semplice file server
- Configurazioni supportate:
  - I server dotati di unità RAID 5 o 10; RAID 0 (striping) e RAID 1 (mirroring) sono supportati indipendenti l'uno dall'altro.
  - I server dotati di unità Multi TB RAID
  - I server dotati di unità che possono essere sostituite senza spegnere il computer
  - Server Encryption viene convalidato per soluzioni antivirus leader del settore. Le esclusioni hardcoded sono utilizzate da questi provider di antivirus per impedire le incompatibilità tra crittografia e scansione antivirus. Se l'organizzazione utilizza un provider di antivirus non in elenco, consultare l'articolo della KB 126046 o contattare Dell ProSupport per assistenza.

La crittografia dei sistemi operativi del server non è adatta per l'uso con:

- Security Management Server Security Management Server Virtual o i server che eseguono i database per Security Management Server Security Management Server Virtual.
- Encryption Personal.
- SED Manager, PBA Advanced Authentication o BitLocker Manager.
- Server che fanno parte di Dell Financial Services (DFS).
- Migrazione da e verso la crittografia su un sistema operativo del server. L'aggiornamento da External Media Edition a crittografia dei sistemi operativi del server richiede che il prodotto precedente sia completamente rimosso prima di installare la crittografia sui sistemi operativi del server.
- Host di VM (un host di VM generalmente contiene guest di VM multipli)
- Controller di dominio
- Server Exchange
- Server che ospitano database (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange, ecc.)
- Server che utilizzano una qualunque delle seguenti tecnologie:
  - Resilient file system
  - Fluid file system
  - Spazi di archiviazione di Microsoft
  - Soluzioni di storage su rete SAN/NAS
  - Dispositivi connessi iSCSI
  - Software di deduplicazione
  - Deduplicazione dell'hardware
  - Split RAID (volumi multipli in un unico RAID)
  - SED (RAID e NON RAID)
  - Microsoft Storage Server 2012
- La crittografia sul sistema operativo del server 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.
- Le reinstallazioni del sistema operativo sul posto non sono supportate. 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. Per maggiori informazioni sul ripristino dei dati crittografati, fare riferimento alla *Guida al ripristino*.

Sistemi operativi

La tabella seguente descrive in dettaglio i sistemi operativi supportati.

Sistemi operativi (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 • L'**attivazione posposta** include il supporto per tutte le risposte precedenti

Sistemi operativi server supportati
• Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition • Windows Server 2012: Standard Edition, Essentials Edition, Datacenter Edition (Server Core non supportato) • Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition (Server Core non supportato) • Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition (Server Core non supportato) • Windows Server 2019: Standard Edition, Datacenter Edition • Windows Server 2022: Standard Edition, Datacenter Edition

Sistemi operativi supportati in modalità UEFI
• 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

N.B.:

In un computer compatibile con UEFI, dopo aver selezionato **Riavvia** dal menu principale, il computer verrà riavviato e in seguito visualizzerà una delle due possibili schermate di accesso. La schermata di accesso che viene visualizzata è determinata da differenze di architettura della piattaforma del computer.

Encryption External Media

Sistemi operativi

- 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.
- La tabella seguente descrive in dettaglio i sistemi operativi supportati quando si accede ai media 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.

Sistemi operativi Windows supportati per l'accesso a media cifrati (a 32 e 64 bit)
○ Windows 10 2019 LTSC ○ Windows 10 2021 LTSC ● Windows 11: Enterprise, Pro v21H2 - 22H2 ● L'**attivazione posposta** include il supporto per tutte le risposte precedenti

Sistemi operativi server supportati
● Windows Server 2012 R2

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 10.15.1 - 10.15.4

SED Manager

- Per installare correttamente SED Manager, il computer deve disporre di una connessione di rete cablata.
- Il computer deve essere dotato di una connessione di rete cablata per un utente smart card per accedere mediante l'autenticazione di preavvio la prima volta.
- I provider di credenziali di terze parti non funzioneranno con SED Manager installato e tutti i provider di credenziali di terze parti verranno disattivati se il PBA è abilitato.
- IPv6 non è supportato.
- SED Manager non è attualmente supportato sui computer host virtualizzati.
- 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.
- Dell consiglia di non modificare il metodo di autenticazione quando la PBA è stata attivata. Se è necessario passare ad un diverso metodo di autenticazione, occorre:
  - Rimuovere tutti gli utenti dalla PBA.

    Oppure
  - Disattivare la PBA, modificare il metodo di autenticazione, quindi riattivare la PBA.
- 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.

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.

- 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.
- Il programma di installazione principale installa questi componenti se non sono già installati nel computer di destinazione. **Se si usa il programma di installazione figlio**, è necessario installare questi componenti prima di installare i client.

Prerequisito
○ Visual C++ 2017 o Redistributable Package (x86 o x64) versione successiva ○ A partire da gennaio 2020, i certificati di firma SHA1 non sono più validi e non possono essere rinnovati. Per i dispositivi che eseguono Windows Server 2008 R2, è necessario installare gli aggiornamenti Microsoft KB https://support.microsoft.com/it-it/help/4474419 e https://support.microsoft.com/it-it/help/4490628 per convalidare i certificati di firma SHA256 su applicazioni e pacchetti di installazione. 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

- SED Manager non è supportato da Encryption sui sistemi operativi del server .
- Le configurazioni di crittografia su più dischi con SED Manager richiedono quanto segue:
  - Tutti i dischi nel sistema di destinazione devono avere la seguente configurazione:
    - Unità SED
    - Ai dischi deve essere assegnata una lettera dell'unità
  - 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.

    Abilitare la crittografia multi-disco nella console di gestione. Vedere Impostazioni di registro per visualizzare i valori del Registro di sistema di Windows per la crittografia multi-disco e la ricerca multi-sweep.
- **N.B.:** Con l'autenticazione di preavvio è obbligatoria una password. Dell consiglia di utilizzare una password minima con impostazione conforme alle policy di sicurezza interne.
- **N.B.:** Quando viene utilizzata la PBA, il criterio di Sincronizzazione di tutti gli utenti deve essere attivato se un computer ha più utenti. Inoltre, tutti gli utenti devono avere le password. 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.
-

Hardware

Unità autocrittografanti compatibili con OPAL

- Per l'elenco più aggiornato di SED compatibili con Opal supportate da SED Manager, fare riferimento all'articolo della KB: 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.

Opzioni di autenticazione di preavvio con SED Manager

- Per utilizzare le smart card e per eseguire l'autenticazione su computer UEFI, è necessario un hardware specifico. È necessaria la configurazione per utilizzare smart card con l'autenticazione di preavvio. Le seguenti tabelle mostrano le opzioni di autenticazione disponibili a seconda del sistema operativo, quando i requisiti hardware e di configurazione vengono soddisfatti.

Non UEFI				
	PBA			
	Password	Impronta	Smart card con contatti	Scheda SIPR
Windows 10	X[1]		X[1 2]	
Windows 11	X[1]		X[1 2]	
1. Disponibile quando i driver di autenticazione vengono scaricati dal sito dell.com/support 2. Disponibile con una SED OPAL supportata				

UEFI				
	PBA - su computer Dell supportati			
	Password	Impronta	Smart card con contatti	Scheda SIPR
Windows 10	X[1]		X[1]	
Windows 11	X[1]		X[1]	
1. Disponibile con una SED OPAL supportata su computer UEFI supportati				

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.

Sistemi operativi Windows (a 32 e 64 bit)
▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Localizzazione

SED Manager è un'interfaccia utente multilingue (MUI, Multilingual User Interface) ed è localizzata nelle lingue seguenti. La modalità UEFI e PBA Advanced Authentication 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	

BitLocker Manager

- Se BitLocker non è ancora distribuito nel proprio ambiente, è consigliabile verificare i requisiti di Microsoft BitLocker.
- Verificare che la partizione PBA sia già stata configurata. Se BitLocker Manager viene installato prima di configurare la partizione PBA, non sarà possibile attivare BitLocker e BitLocker Manager non sarà in funzione. Consultare Configurazione di preinstallazione per impostare una partizione PBA di BitLocker.
- Un Dell Server è necessario per utilizzare BitLocker Manager.
- Garantire la disponibilità di un certificato di firma all'interno del database. Per ulteriori informazioni, consultare l'articolo della KB 124931.
- I componenti di dispositivi video, mouse e tastiera devono essere collegati direttamente al computer. Non usare un'opzione KVM per gestire le periferiche, poiché essa può interferire con la corretta identificazione dell'hardware da parte del computer.
- Accendere e abilitare il TPM. BitLocker Manager assume la proprietà del dispositivo TPM senza richiedere il riavvio. Tuttavia, se esiste già una proprietà TPM, BitLocker Manager inizia il processo di configurazione della crittografia (senza richiedere il riavvio). È necessario che il TPM sia di proprietà e venga attivato.
- BitLocker Manager utilizza gli algoritmi validati AES FIPS approvati se è attivata la modalità FIPS per l'impostazione di sicurezza del GPO per la "Crittografia del sistema: utilizzo degli algoritmi conformi al FIPS per crittografia, hash e firma" nel dispositivo, sarà possibile gestire tale dispositivo attraverso il nostro prodotto. BitLocker Manager non viene impostato come predefinito per i client crittografati da BitLocker perché Microsoft al momento sconsiglia ai clienti di usare la crittografia convalidata FIPS a causa di numerosi problemi con compatibilità delle applicazioni, ripristino e crittografia dei supporti: http://blogs.technet.com.
- BitLocker Manager non è supportato da crittografia del sistema operativo del server.
- Quando si utilizza una connessione remota del desktop con BitLocker Manager che sfrutta un endpoint, Dell consiglia l'esecuzione di eventuali sessioni di desktop in remoto in modalità di console per evitare eventuali problemi di interazione dell'interfaccia utente con la sessione esistente dell'utente tramite il seguente comando:

  ```
  mstsc /admin /v:<target_ip_address>
  ```

- Il programma di installazione principale installa questi componenti se non sono già installati nel computer di destinazione. **Se si usa il programma di installazione figlio**, è necessario installare questi componenti prima di installare i client.

Prerequisito
○ Visual C++ 2017 o Redistributable Package (x86 o x64) versione successiva

Prerequisito
○ A partire da gennaio 2020, i certificati di firma SHA1 non sono più validi e non possono essere rinnovati. Per i dispositivi che eseguono Windows Server 2008 R2, è necessario installare gli aggiornamenti Microsoft KB https://support.microsoft.com/it-it/help/4474419 e https://support.microsoft.com/it-it/help/4490628 per convalidare i certificati di firma SHA256 su applicazioni e pacchetti di installazione. 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

- **N.B.:** I computer protetti da Bitlocker 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.
- **N.B.:** Gli aggiornamenti del sistema operativo sul posto a una versione più recente, ad esempio da o Windows 10 a Windows 11, non sono supportati.

Hardware

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

Hardware integrato facoltativo
○ TPM 1.2 o 2.0

Sistemi operativi

- Le tabelle seguenti descrivono in dettaglio i sistemi operativi supportati.

Sistemi operativi Windows
○ 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 Windows Server
○ Windows Server 2008 R2: Standard Edition, Enterprise Edition (a 64 bit) ○ Windows Server 2012 R2: Standard Edition, Enterprise Edition (a 64 bit) ○ Windows Server 2016: Standard Edition, Datacenter Edition (a 64 bit) ○ Windows Server 2019: Standard Edition, Datacenter Edition (64 bit) ○ Windows Server 2022: Standard Edition, Datacenter Edition

3

Impostazioni di registro

- Questa sezione descrive in dettaglio tutte le impostazioni di registro approvate da Dell ProSupport per i computer **client** locali, indipendentemente dal motivo di tale impostazione. Se un'impostazione di registro è sovrapposta in due prodotti, viene elencata in ciascuna categoria.
- Queste modifiche di registro devono essere effettuate solo da parte degli amministratori e potrebbero non essere appropriate o non funzionare in tutti gli scenari.

Crittografia

- Se un certificato autofirmato è utilizzato sul Dell Server. Per Windows, la convalida dell'attendibilità del certificato deve rimanere disabilitata nel computer client (la convalida dell'attendibilità è *disabilitata* per impostazione predefinita con Dell Server). Prima di *abilitare* la convalida dell'attendibilità nel computer client, devono essere soddisfatti i seguenti requisiti:
  - Un certificato firmato da un'autorità radice, come EnTrust o Verisign, deve essere importato nel Dell Server.
  - La catena di attendibilità completa del certificato deve essere archiviata nell'archivio chiavi Microsoft nel computer client.
  - Per *abilitare* la convalida dell'affidabilità della crittografia, modificare il valore della seguente voce di registro su 0 nel computer di destinazione.

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

    "IgnoreCertErrors"=DWORD:00000000

    0 = Non prosegue se viene riscontrato un errore del certificato

    1= Ignora gli errori

- Per creare un file di registro di Encryption Removal Agent, creare la seguente voce di registro nel computer destinato alla decrittografia: Consultare Creare un file di registro dell'Encryption Removal Agent (facoltativo).

  [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

- Per disabilitare il prompt all'utente di riavviare il computer dopo che l'Encryption Removal Agent ha terminato il suo stato finale nel processo di decrittografia, modificare il seguente valore di registro o modificare la policy *Imponi riavvio in presenza di aggiornamenti* nella console di gestione.

  [HKLM\Software\Dell\Dell Data Protection]

  "ShowDecryptAgentRebootPrompt"=DWORD

  1 = abilitato (visualizza il prompt)

  0 = disabilitato (nasconde il prompt)

- Per impostazione predefinita, durante l'installazione viene visualizzata l'icona dell'area di notifica. Usare la seguente impostazione di registro per nascondere l'icona dell'area di notifica per tutti gli utenti gestiti in un computer dopo l'installazione originale. Creare o modificare l'impostazione di registro:

  [HKLM\Software\CREDANT\CMGShield]

  "HIDESYSTRAYICON"=DWORD:1

- 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.

- La crittografia visualizza il prompt *Durata di ciascun ritardo di aggiornamento criteri* per cinque minuti ogni volta. Se l'utente non risponde alla richiesta, inizia il ritardo successivo. La richiesta di ritardo finale include una barra di conto alla rovescia e di stato che viene visualizzata finché l'utente risponde, oppure il ritardo finale scade e si verifica la disconnessione o il riavvio richiesto.

  È possibile modificare il comportamento della richiesta dell'utente di iniziare o ritardare la crittografia per impedire l'elaborazione della crittografia in seguito alla mancata risposta dell'utente alla richiesta. Per eseguire questa operazione, impostare il valore:

  [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])

- Usare l'impostazione di registro per fare eseguire alla crittografia il polling del Dell Server per un aggiornamento forzato dei criteri. Creare o modificare l'impostazione di registro:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  L'impostazione di registro scomparirà automaticamente al termine dell'operazione.

- Utilizzare le impostazioni del registro per consentire alla crittografia di inviare un inventario ottimizzato e completo (utenti attivati e non attivati) o completo (solo gli utenti attivati) al Dell Server.
  - Inviare l'inventario ottimizzato al Dell Server:

    Creare o modificare l'impostazione di registro:

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

    "OnlySendInvChanges"=REG_DWORD:1

    Se non è presente alcuna voce, l'inventario ottimizzato viene inviato al Dell Server.

  - Inviare l'inventario completo al Dell Server:

    Creare o modificare l'impostazione di registro:

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

    "OnlySendInvChanges"=REG_DWORD:0

    Se non è presente alcuna voce, l'inventario ottimizzato viene inviato al Dell Server.

  - Inviare l'inventario completo per tutti gli utenti attivati:

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

    "RefreshInventory"=REG_DWORD:1

    Questa voce viene eliminata dal registro nel momento in cui viene elaborata. Il valore viene salvato nel vault in modo che, anche se il computer viene riavviato prima del caricamento dell'inventario, la crittografia soddisferà questa richiesta al caricamento dell'inventario successivo.

Questa voce sostituisce il valore di registro OnlySendInvChanges.

- L'Attivazione in slot è una funzione che consente all'utente di diffondere le attivazioni dei client in un determinato periodo di tempo al fine di facilitare il caricamento del Dell Server durante un'implementazione di massa. Le attivazioni vengono ritardate in base a slot di tempo generati tramite algoritmi per fornire una distribuzione uniforme dei tempi di attivazione.

  Per gli utenti che richiedono l'attivazione tramite VPN, potrebbe essere necessaria una configurazione di attivazione in slot per il client, al fine di ritardare l'attivazione iniziale per un tempo sufficiente a consentire al client VPN di stabilire una connessione di rete.

  Per l'applicazione degli aggiornamenti, queste voci di registro richiedono un riavvio del computer.

  - **Attivazione in slot**

    Per abilitare o disabilitare questa funzione, creare una DWORD con il nome **SlottedActivation** sotto la parent key:

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

  - **Slot di attivazione**

    Per abilitare o disabilitare questa funzione, creare una subkey con il nome **ActivationSlot** sotto la parent key:

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

    Attivazione in slot - una stringa che definisce il periodo entro il quale la crittografia tenta di attivarsi con il Dell Server. Questi valori sono definiti in secondi e la sintassi è definita da <lowervalue>,<uppervalue>, ad esempio 120,300. Ciò significa che la crittografia tenta di attivarsi in un momento casuale compreso tra i 2 e i 5 minuti dall'accesso dell'utente.

    - **Ripetizione calendario**

      Per abilitare o disabilitare questa funzione, creare una subkey con il nome **CalRepeat** sotto la parent key:

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

      CalRepeat - Una DWORD che definisce il periodo di tempo in secondi in cui ha luogo l'intervallo dello slot di attivazione. Usare questa impostazione per sovrascrivere il periodo di tempo in secondi in cui ha luogo l'intervallo di slot di attivazione. In un periodo di sette ore, sono disponibili 25200 secondi per le attivazioni in slot. L'impostazione predefinita è 86400 secondi, che rappresenta una ripetizione giornaliera. Il valore decimale consigliato è 600, che rappresenta 10 minuti.

    - **Intervallo di slot**

      Per abilitare o disabilitare questa funzione, creare una subkey con il nome **SlotInterval** sotto la parent key:

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

      Intervallo di slot - Un valore di stringa che definisce gli intervalli tra le attivazioni di slot. L'impostazione suggerita è 45,120. Ciò rappresenta il tempo di attivazione assegnato casualmente tra 45 e 120 secondi.

    - **Soglia comunicazioni perse**

      Per abilitare o disabilitare questa funzione, creare una subkey con il nome **MissThreshold** sotto la parent key:

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

      MissThreshold - Un valore DWORD che contiene un numero intero positivo che definisce il numero di tentativi di attivazione prima della disconnessione. Se si raggiunge MissThreshold, i tentativi di attivazione cessano fino all'accesso successivo dell'utente non attivo. Il conteggio per MissThreshold viene sempre resettato alla disconnessione.

      Le chiavi di registro raccolgono i dati dell'utente dell'attivazione in slot:

      [HKCU/Software/CREDANT/ActivationSlot] (dati per utente)

      Periodo di tempo di rinvio per il tentativo di attivazione in slot, che è impostato quando l'utente accede alla rete per la prima volta dopo che è stata abilitata l'attivazione in slot. Lo slot di attivazione viene ricalcolato per ciascun tentativo di attivazione.

      [HKCU/Software/CREDANT/SlotAttemptCount] (dati per utente)

      Numero di tentativi non riusciti o persi quando giunge la scadenza dello slot di tempo e viene tentata l'attivazione, ma senza successo. Quando questo numero raggiunge il valore impostato in ACTIVATION_SLOT_MISSTHRESHOLD, il computer tenta l'attivazione immediata in seguito alla connessione alla rete.

- Per rilevare gli utenti non gestiti nel computer client, impostare in esso il valore di registro:

  [HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

  "UnmanagedUserDetected"=DWORD value:1

Rileva gli utenti non gestiti in questo computer=1

Non rilevare gli utenti non gestiti in questo computer=0

- L'accesso al supporto esterno crittografato con Encryption External Media può essere limitato ai computer che hanno accesso al Dell Server che ha prodotto le chiavi di crittografia con cui è stato crittografato il supporto.

  È possibile abilitare questa funzione impostando il registro:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

  "EnterpriseUsage"=DWORD:0

  Disattivato (predefinito)=0

  Accesso ai file limitato a enterprise=1

  Se questo valore viene modificato successivamente alla crittografia dei file nel supporto esterno, i file vengono crittografati nuovamente in base al valore della chiave di registro aggiornata quando il supporto verrà collegato al computer in cui l'impostazione di registro è stata aggiornata.

- Per abilitare una riattivazione automatica invisibile all'utente nel raro caso in cui un utente diventi disattivato, è necessario impostare il valore di registro nel computer client.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=DWORD:00000001

  0 =Disabilitata; impostazione predefinita

  1=Abilitata

- 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 il registro nel computer:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=DWORD:00000000

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

  Per ulteriori informazioni su SDUser, consultare l'articolo di KB 131035

- Durante l'impostazione della voce di registro EnableNGMetadata, se si verificano problemi correlati agli aggiornamenti di Microsoft sui computer con dati crittografati mediante chiavi comuni o alla crittografia, decrittografia o decompressione di elevati numeri di file all'interno di una cartella.

  Impostare la voce di registro EnableNGMetadata nel seguente percorso:

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = DWORD:1

  0 =Disabilitata; impostazione predefinita

  1=Abilitata

- È possibile abilitare la funzione di attivazione fuori dominio contattando Dell ProSupport e richiedendo le relative istruzioni.
- 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\

  " DumpPolicies" = DWORD

  Valore = 1

  Nota: i registri vengono scritti in C:\ProgramData\Dell\Dell Data Protection\Policy.

- 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

SED Manager

- Per impostare l'intervallo tra tentativi quando il Dell Server non è disponibile a comunicare con SED Manager, aggiungere il seguente valore del Registro di sistema:

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  Questo valore corrisponde al numero di secondi per cui SED Manager attende prima di provare a contattare il Dell Server se questo non è disponibile a comunicare. Il valore predefinito è 300 secondi (5 minuti).

- Se viene usato un certificato autofirmato nel Dell Server per SED Manager, la convalida dell'attendibilità SSL/TLS deve rimanere disabilitata nel computer client (la convalida dell'attendibilità SSL/TLS è *disabilitata* per impostazione predefinita in SED Manager). Prima di *abilitare* la convalida dell'attendibilità SSL/TLS nel computer client, devono essere soddisfatti i seguenti requisiti:
  - Un certificato firmato da un'autorità radice, come EnTrust o Verisign, deve essere importato nel Dell Server.
  - La catena di attendibilità completa del certificato deve essere archiviata nell'archivio chiavi Microsoft nel computer client.
  - Per *abilitare* la convalida dell'attendibilità SSL/TLS per SED Manager, modificare il valore della seguente voce del Registro di sistema su 0 nel computer client.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Abilitata

    1 = Disabilitata

- 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.

- 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

- Per impedire a SED Manager 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

NOTA: questo valore può impedire al provider di credenziali Dell di sincronizzare correttamente le credenziali inizialmente a causa della disabilitazione dei provider di credenziali di terze parti. Assicurarsi che i dispositivi che utilizzano questa chiave del Registro di sistema possano comunicare correttamente con il Dell Server.

- Per impostare l'intervallo in cui SED Manager prova a contattare il Dell Server quando non è disponibile a comunicare, impostare il valore seguente nel computer di destinazione:

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD Value:300

  Questo valore corrisponde al numero di secondi per cui SED Manager attende prima di provare a contattare il Dell Server se questo non è disponibile a comunicare. Il valore predefinito è 300 secondi (5 minuti).

- Se necessario, l'host del Security Server può essere modificato dal percorso di installazione originale. Le informazioni sull'host vengono lette ogni volta che si verifica il polling di un criterio. Modificare il seguente valore di registro nel computer client:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- Se necessario, la porta del Security Server può essere modificata dal percorso di installazione originale. Questo valore viene letto ogni volta che si verifica il polling di un criterio. Modificare il seguente valore di registro nel computer client:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888

- Se necessario, l'URL del Security Server può essere modificato dal percorso di installazione originale. Questo valore viene letto dal computer client ogni volta che si verifica il polling di un criterio. Modificare il seguente valore di registro nel computer client:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

- (Solo con autenticazione di preavvio) Se **non** si desidera che PBA Advanced Authentication modifichi i servizi associati alle smart card e ai dispositivi biometrici in un tipo di avvio "automatico", disabilitare la funzione di avvio del servizio. La disabilitazione di questa funzione comporta anche l'annullamento degli avvisi associati ai servizi richiesti non in esecuzione.

  Se **disabilitato**, PBA Advanced Authentication non tenterà di avviare i servizi seguenti:

  - 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.

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Abilitata

    1 = Disabilitata

- Per usare le smart card con autenticazione di preavvio delle SED, è necessario impostare il seguente valore di registro nel computer client dotato di SED.

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

  "MSSmartcardSupport"=DWORD:1

  Impostare il criterio Metodo di autenticazione su Smart card nella console di gestione ed eseguire il commit della modifica.

- 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

Full Disk Encryption

- Questa sezione descrive in dettaglio tutte le impostazioni di registro approvate da Dell ProSupport per i computer locali, indipendentemente dal motivo di tale impostazione. Se un'impostazione di registro è sovrapposta in due prodotti, viene elencata in ciascuna categoria.
- Queste modifiche di registro devono essere effettuate solo da parte degli amministratori e potrebbero non essere appropriate o non funzionare in tutti gli scenari.
- Per impostare l'intervallo tra tentativi quando il Dell Server non è disponibile a comunicare con Full Disk Encryption, aggiungere il seguente valore di registro.

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  Questo valore è il numero di secondi che Full Disk Encryption attende prima di provare a contattare il Dell Server se questo non è disponibile a comunicare con Full Disk Encryption. Il valore predefinito è 300 secondi (5 minuti).

- Se viene usato un certificato autofirmato nel Dell Server per Full Disk Encryption, la convalida dell'affidabilità SSL/TLS deve rimanere disabilitata nel computer client (la validazione dell'attendibilità SSL/TLS è *disabilitata* per impostazione predefinita in Full Disk Encryption). Prima di *abilitare* la convalida dell'attendibilità SSL/TLS nel computer client, devono essere soddisfatti i seguenti requisiti:
  - Un certificato firmato da un'autorità radice, come EnTrust o Verisign, deve essere importato nel Dell Server.
  - La catena di attendibilità completa del certificato deve essere archiviata nell'archivio chiavi Microsoft nel computer client.
  - Per *abilitare* la convalida dell'attendibilità SSL/TLS per Dell Encryption Management, modificare il valore della seguente voce di registro su 0 nel computer client.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Abilitata

    1 = Disabilitata

- 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

- Se necessario, l'host del Security Server può essere modificato dal percorso di installazione originale. Queste informazioni sull'host vengono lette dal computer client ogni volta che si verifica il polling di un criterio. Modificare il seguente valore di registro nel computer client:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- Se necessario, la porta del Security Server può essere modificata dal percorso di installazione originale. Questo valore viene letto dal computer client ogni volta che si verifica il polling di un criterio. Modificare il seguente valore di registro nel computer client:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888

- (Solo con autenticazione di preavvio) Se **non** si desidera che PBA Advanced Authentication modifichi i servizi associati alle smart card e ai dispositivi biometrici in un tipo di avvio "automatico", disabilitare la funzione di avvio del servizio. La disabilitazione di questa funzione comporta anche l'annullamento degli avvisi associati ai servizi richiesti non in esecuzione.

  Se **disabilitato**, PBA Advanced Authentication non tenterà di avviare i servizi seguenti:

  - 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.

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Abilitata

    1 = Disabilitata

- Per impedire che Full Disk Encryption venga disabilitato, creare la seguente chiave del Registro di sistema:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 =Disabilitata; impostazione predefinita

  1=Abilitata

  NOTA: questo valore può impedire al provider di credenziali Dell di sincronizzare correttamente le credenziali inizialmente a causa della disabilitazione dei provider di credenziali di terze parti. Assicurarsi che i dispositivi che utilizzano questa chiave del Registro di sistema possano comunicare correttamente con il Dell Server.

- 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

- Per consentire l'installazione di Full Disk Encryption con Policy Based Encryption, è necessario impostare il seguente valore del registro sul computer client.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

" EnableFDE" = DWORD: 1

0 =Disabilitata; impostazione predefinita

1=Abilitata

BitLocker Manager

- Se viene usato un certificato autofirmato nel Dell Server per BitLocker Manager, la convalida dell'attendibilità SSL/TLS deve rimanere disabilitata nel computer client (la convalida dell'attendibilità SSL/TLS è *disabilitata* per impostazione predefinita in BitLocker Manager). Prima di *abilitare* la convalida dell'attendibilità SSL/TLS nel computer client, devono essere soddisfatti i seguenti requisiti:
  - Un certificato firmato da un'autorità radice, come EnTrust o Verisign, deve essere importato nel Dell Server.
  - La catena di attendibilità completa del certificato deve essere archiviata nell'archivio chiavi Microsoft nel computer client.
  - Per *abilitare* la convalida dell'attendibilità SSL/TLS per BitLocker Manager, modificare il valore della seguente voce di registro su 0 nel computer client.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Abilitata

    1 = Disabilitata

  - Per impedire a Bitlocker Manager di rilevare dischi rimovibili come dischi fissi, aggiungere la seguente chiave del Registro di sistema:

    HKLM\Software\Dell\Dell Data Protection\

    "UseEncryptableVolumeType" = DWORD:1

    0 =Disabilitata; impostazione predefinita

    1=Abilitata

4

Installazione tramite il programma di installazione principale

- Le opzioni e i parametri della riga di comando fanno distinzione tra maiuscole e minuscole.
- Per eseguire l'installazione usando porte non predefinite, usare i programmi di installazione figlio al posto del programma di installazione principale.
- I file di registro del programma di installazione principale di si trovano al percorso `C:\ProgramData\Dell\Dell Data Protection\Installer`.

  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.

- Indicare agli utenti di prendere visione del seguente documento e file della guida per assistenza sull'applicazione:
  - 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\EMS`.
  - Consultare la Encryption Enterprise Endpoint Security Suite Pro Endpoint Security Suite Enterprise per istruzioni sull'utilizzo delle funzioni di . Accedere alla guida da `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.
- Al completamento dell'installazione, gli utenti devono aggiornare i propri criteri cliccando con il pulsante destro del mouse sull'icona di Dell Encryption nell'area di notifica e selezionando **Verificare la disponibilità di aggiornamenti ai criteri**.
- Il programma di installazione principale installa l'intera suite di prodotti. Vi sono due metodi per eseguire l'installazione tramite il programma di installazione principale. Scegliere uno dei seguenti:
  - Eseguire l'installazione interattiva usando il programma di installazione principale

  Oppure
  - Eseguire l'installazione dalla riga di comando usando il programma di installazione principale

Eseguire l'installazione interattiva usando il programma di installazione principale

- Il programma di installazione principale di può trovarsi in:
  - **Da dell.com/support** - se necessario, ottenere il software da **dell.com/support**
  - **Dall'account Dell FTP** - Individuare il pacchetto di installazione in Dell-Encryption-8.x.x.xxx.zip
- Utilizzare queste istruzioni per installare o aggiornare Dell Encryption Enterprise in modo interattivo tramite il programma di installazione principale di . Il presente metodo può essere utilizzato per installare la suite di prodotti in un computer alla volta.

1. Individuare **DDSSetup.exe** nel supporto di installazione Dell. Copiarlo nel computer locale.
2. Cliccare due volte su per avviare il programma di installazione. L'operazione potrebbe richiedere alcuni minuti.
3. Cliccare su **Avanti** nella finestra di dialogo Introduzione.
4. Leggere il contratto di licenza, accettare i termini, e cliccare su **Avanti**.
5. Nel campo *Nome Dell Server On-Prem*, inserire il nome host completo del Dell Server che gestirà l'utente di destinazione.

   Inserire i valori delle porte nella *porta del Core Server* e nella *porta di Security Server* se l'organizzazione utilizza porte non standard.

   Cliccare su **Avanti.**

6. Cliccare su **Avanti** per installare il prodotto nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\. Dell recommends installing in the default location only`, in quanto potrebbero verificarsi problemi con l'installazione in altri percorsi.
7. Selezionare i componenti da installare.

   Il *Framework di sicurezza* consente di installare il framework di sicurezza sottostante, l'Encryption Management Agent e l'autenticazione PBA.

   BitLocker Manager installa il client di BitLocker Manager, progettato per potenziare la protezione delle distribuzioni di BitLocker semplificando e riducendo il costo di proprietà tramite la gestione centralizzata dei criteri di crittografia di BitLocker.

   La *crittografia* installa il componente che applica il criterio di protezione quando un computer è connesso alla rete, disconnesso dalla rete, perso o rubato.

   Encryption External Media installa il componente che applica Encryption External Media.

   Full Disk Encryption installa il componente che applica Full Disk Encryption.

   Cliccare su **Avanti** al termine delle selezioni.
8. Cliccare su **Installa** per avviare l'installazione. L'installazione richiede alcuni minuti.
9. Selezionare **Sì, riavvia ora** e cliccare su **Fine**.

   L'installazione è completata.

Eseguire l'installazione dalla riga di comando usando il programma di installazione principale

- È necessario prima specificare gli switch in un'installazione dalla riga di comando. Gli altri parametri devono essere inseriti nell'argomento che viene passato all'opzione `/v`.

  Opzioni
- La seguente tabella descrive gli switch utilizzabili con il programma di installazione principale di .

  N.B.: Se l'azienda richiede l'utilizzo di provider di credenziali di terze parti, è necessario installare o aggiornare Encryption Management Agent con il parametro FEATURE=BLM o FEATURE=BASIC.

Switch	Descrizione
/s	Installazione automatica
/z	Consente di passare variabili al file .msi all'interno di DDSSetup.exe

Parametri

- La seguente tabella descrive i parametri utilizzabili con il programma di installazione principale di .

Parametro	Descrizione
SUPPRESSREBOOT	Sopprime il riavvio automatico al termine dell'installazione. Può essere usato in MODALITÀ NON INTERATTIVA.
SERVER	Specifica l'URL del Dell Server.
InstallPath	Specifica il percorso di installazione. Può essere usato in MODALITÀ NON INTERATTIVA.
FEATURES	Specifica i componenti che è possibile installare in MODALITÀ NON INTERATTIVA. DE = solo client di crittografia unità EME = solo Encryption External Media BLM = BitLocker Manager

Parametro	Descrizione
	SED = SED Manager (Encryption Management, Agent/Manager, driver PBA/GPE)
BLM_ONLY=1	Deve essere usato con FEATURES=BLM nella riga di comando per escludere il plug-in SED Manager.

Esempio di riga di comando

- I parametri della riga di comando fanno distinzione tra maiuscole e minuscole.
- In questo esempio, vengono installati tutti i componenti usando il programma di installazione principale di tramite porte standard, installazione automatica, nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\` e configurati per usare il Dell Server specificato.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com\""
  ```
- In questo esempio, vengono installati SED Manager ed Encryption External Media usando il programma di installazione principale tramite porte standard, installazione automatica, nessun riavvio, nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\` e configurati per usare il Dell Server specificato.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=EME-SED,
  SUPPRESSREBOOT=1\""
  ```
- In questo esempio, viene installato SED Manager usando il programma di installazione principale tramite porte standard, installazione automatica, nessun riavvio, nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\` e configurato per usare il Dell Server specificato.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=SED, SUPPRESSREBOOT=1\""
  ```
- In questo esempio, viene installato SED Manager usando il programma di installazione principale tramite porte standard, installazione automatica, nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\` e configurato per usare il Dell Server specificato.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=SED\""
  ```
- In questo esempio, vengono installati Encryption e BitLocker Manager (senza il plug-in SED Management) usando il programma di installazione principale tramite porte standard, con installazione automatica, nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\` e configurati per usare il Dell Server specificato.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
  ```
- In questo esempio, vengono installati BitLocker Manager (con il plug-in SED Manager) ed Encryption External Media usando il programma di installazione principale tramite porte standard, con installazione automatica, nessun riavvio, nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\` e configurati per usare il Dell Server specificato.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=BLM-EME,
  SUPPRESSREBOOT=1\""
  ```
- In questo esempio, vengono installati BitLocker Manager (senza il plug-in SED Manager) ed Encryption External Media usando il programma di installazione principale tramite porte standard, con installazione automatica, nessun riavvio, nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\` e configurati per usare il Dell Server specificato.

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1,
  SUPPRESSREBOOT=1\""
  ```

5

Disinstallare il programma di installazione principale

- Dell consiglia di utilizzare il Programma di disinstallazione di Data Security per rimuovere la suite Data Security.
- Ciascun componente deve essere disinstallato separatamente, seguito dalla disinstallazione del programma di installazione principale di . 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.
- Accertarsi che la stessa versione del programma di installazione principale di (e quindi dei client) venga utilizzata per la disinstallazione come per l'installazione.
- Questo capitolo fa riferimento ad altri capitoli che contengono 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 Encryption.
  2. Disinstallare SED Manager.
  3. Disinstallare Full Disk Encryption
  4. Disinstallare BitLocker Manager.
- Passare a Disinstallare il programma di installazione principale.

Disinstallare il programma di installazione principale di

Ora che tutti i singoli client sono stati disinstallati, può essere disinstallato il programma di installazione principale.

Disinstallazione dalla riga di comando

- Nel seguente esempio, viene eseguita la disinstallazione automatica del programma di installazione principale di .

  ```
  "DDSSetup.exe" /s /x
  ```

  Al termine, riavviare il sistema.

6

Eseguire l'installazione usando i programmi di installazione figlio

- Per installare o aggiornare ciascun client singolarmente, i file eseguibili figlio devono essere prima estratti dal programma di installazione principale di , come mostrato in Estrarre i programmi di installazione figlio dal programma di installazione principale.
- Gli esempi di comandi inclusi in questa sezione presumono che i comandi vengano eseguiti da `C:\extracted`.
- Le opzioni e i parametri della riga di comando fanno distinzione tra maiuscole e minuscole.
- È importante ricordare che tutti i valori contenenti uno o più caratteri speciali, ad esempio uno spazio nella riga di comando, devono essere racchiusi tra virgolette con escape.
- Usare questi programmi di installazione per installare i client usando un'installazione tramite script, file batch o qualsiasi altra tecnologia push a disposizione della propria organizzazione.
- Negli esempi delle righe di comando il riavvio è stato eliminato, ma un riavvio finale sarà necessario perché

  Nota: la crittografia basata su criteri non può iniziare finché il computer non è stato riavviato.

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

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

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

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

Opzione	Significato
/v	Consente di passare variabili al file .msi all'interno di setup.exe. Il contenuto deve sempre essere racchiuso tra virgolette con testo normale.
/s	Modalità non interattiva
/x	Modalità di disinstallazione

N.B.:

Con /v, sono disponibili le opzioni predefinite di Microsoft. Per un elenco di opzioni, consultare questo articolo.

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

Opzione	Significato
/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
/norestart	Viene eliminato il riavvio

- Indicare agli utenti di prendere visione del seguente documento e file della guida per assistenza sull'applicazione:
  - Consultare la *Dell Encrypt Help* (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 *Help* (Guida di Encryption External Media) per istruzioni sulle funzioni di Encryption External Media. Accedere alla guida da `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS`.
  - Consultare la Guida di *Encryption Enterprise* per istruzioni sull'utilizzo delle funzioni di Autenticazione PBA . Accedere alla guida da `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.

Installare i driver

- I driver e il firmware per ControlVault, lettori di impronte e smart card non sono inclusi nei file eseguibili del programma di installazione principale o programma di installazione figlio di . I driver e il firmware devono essere sempre aggiornati ed è possibile scaricarli dal sito http://www.dell.com/support selezionando il modello del computer desiderato. Scaricare i driver e il firmware appropriati in base all'hardware di autenticazione.
  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity Fingerprint Reader 495 Driver
  - O2Micro Smart Card Driver

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

Installare la crittografia

- Se la propria organizzazione sta usando un certificato firmato da un'autorità root, come EnTrust o Verisign, consultare i Requisiti di crittografia. Per abilitare la convalida del certificato, è necessario modificare le impostazioni di registro nel computer client.
- Al completamento dell'installazione, gli utenti devono aggiornare i propri criteri facendo clic con il pulsante destro del mouse sull'icona di Dell Encryption nell'area di notifica e selezionando *Verificare la disponibilità di aggiornamenti ai criteri*.
- Il programma di installazione della crittografia è disponibile su:
  - **Da dell.com/support** - Se necessario, consultare Ottenere il software da dell.com/support e poi consultare Estrarre i programmi di installazione figlio dal programma di installazione principale. Dopo l'estrazione, il file si trova in `C:\extracted\Encryption`.
  - **Dall'account Dell FTP** - Individuare il bundle di installazione in Encryption-Enterprise-10.x.x.xxx.zip e poi consultare Estrarre i programmi di installazione figlio dal programma di installazione principale. Dopo l'estrazione, il file si trova in `C:\extracted\Encryption`.
  - **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.

Installazione dalla riga di comando

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

Parametri
SERVERHOSTNAME=<ServerName> (FQDN del Dell Server per la riattivazione)
POLICYPROXYHOSTNAME=<RGKName> (FQDN del Policy Proxy predefinito)
MANAGEDDOMAIN=<MyDomain> (dominio da utilizzare per il dispositivo)
DEVICESERVERURL=<DeviceServerName/SecurityServerName> (URL utilizzato per l'attivazione, che solitamente include nome server, porta e lo standard xAPI)
GKPORT=<NewGKPort> (porta Gatekeeper)
MACHINEID=<MachineName> (nome computer)
RECOVERYID=<RecoveryID> (ID di ripristino)
REBOOT=ReallySuppress (Null consente i riavvii automatici, ReallySuppress li disabilita)
HIDEOVERLAYICONS=1 (0 abilita le icone di sovrapposizione, 1 le disabilita)
HIDESYSTRAYICON=1 (0 abilita l'icona nell'area di notifica, 1 disabilita l'icona nell'area di notifica)
ENABLE_FDE_LM=1 (Consente l'installazione di Dell Encryption su un computer con Full Disk Encryption attivo)
EME=1 (installare la modalità Encryption External Media)

Per un elenco di opzioni e opzioni di visualizzazione .msi base che possono essere utilizzate nelle righe di comando, fare riferimento a Eseguire l'installazione usando i programmi di installazione figlio.

- Nella tabella seguente vengono descritti i parametri opzionali relativi all'attivazione.

Parametri
SLOTTEDACTIVATON=1 (0 disabilita le attivazioni ritardate/pianificate, 1 le abilita)
SLOTINTERVAL=45.120 (consente di pianificare le attivazioni mediante l'annotazione x,x dove il primo valore rappresenta il limite inferiore della pianificazione e il secondo il limite superiore, in secondi)
CALREPEAT=600 (DEVE essere uguale o maggiore del limite superiore impostato in SLOTINTERVAL. Il numero di secondi che la crittografia attende prima di generare un tentativo di attivazione in base a SLOTINTERVAL.)

Esempio di riga di comando

N.B.: Sostituire `DEVICESERVERURL=https://server.organization.com:8081/xapi` (senza la barra finale) se la versione di Security Management Server è precedente alla 7.7.

- Nell'esempio seguente viene installato Dell Encryption con i parametri predefiniti (crittografia, Encrypt for Sharing, nessuna finestra di dialogo, nessun barra di stato, riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- Nell'esempio seguente, vengono installati Encryption ed Encrypt for Sharing, vengono nascoste l'icona dell'area di notifica di Dell Encryption e le icone sovrapposte, nessuna finestra di dialogo, nessuna barra di avanzamento, il riavvio viene eliminato e l'installazione avviene nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ HIDESYSTRAYICON=1
  HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
  ```

  Esempio di riga di comando per installare solo Encryption External Media

- Installazione automatica, nessuna barra di stato, riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- Installazione automatica, nessun riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" EME="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
  ```

- **N.B.:**

  Anche se la finestra Informazioni nel client mostra informazioni sul numero di versione del software, non specifica se è stata installata la crittografia (installazione completa) o soltanto Encryption External Media. Per individuare queste informazioni, accedere a `C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log` e trovare la seguente voce:

  [<date/timestamp> DeviceInfo: < >] ***Shield Information - SM=External Media Only***, SB=DELL, UNF=FQUN, last sweep={0, 0}

  Esempio di riga di comando per convertire Encryption External Media in crittografia (installazione completa)

  N.B.: La conversione di Encryption External Media in Encryption (installazione completa) non è supportata con gli aggiornamenti.

- La decrittografia non è necessaria durante la conversione di Encryption External Media a una versione completa della crittografia.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL EME=0
  REINSTALLMODE=vamus /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  ```

```
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
REINSTALL="ALL" EME="0" REINSTALLMODE="vamus"
```

- **Esempio di riga di comando per installare Dell Encryption con Full Disk Encryption**

  \Encryption

- Nell'esempio seguente viene installato Dell Encryption con i parametri predefiniti (crittografia, Encrypt for Sharing, nessuna finestra di dialogo, nessun barra di stato, riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  Quindi:

  \Encryption Management Agent

  Nell'esempio seguente viene installata Full Disk Encryption gestita in remoto e viene consentita l'installazione su un computer protetto Dell Encryption (con installazione automatica, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Esempio di riga di comando per installare Encryption External Media e Full Disk Encryption.**

  \Encryption

  Nell'esempio seguente viene installato Encryption External Media con installazione automatica, nessuna barra di avanzamento, nessun riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption.`

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Quindi:

  \Encryption Management Agent

  Nell'esempio seguente viene installata una funzione Full Disk Encryption gestita in remoto e viene consentita l'installazione su un computer protetto Dell Encryption (installazione invisibile all'utente, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Esempio di riga di comando per installare Encryption External Media su un'installazione Full Disk Encryption esistente.**

  Nell'esempio seguente viene installato Encryption External Media su un'installazione Full Disk Encryption esistente con installazione invisibile all'utente, senza indicatore di stato, riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection.`

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
  norestart /qn"
  ```

- **Esempio di riga di comando per installare un client di crittografia gestito in remoto su un'installazione Full esistente.**

  Nell'esempio seguente, viene abilitata l'installazione di Dell Encryption su un'installazione Full Disk Encryption esistente con i parametri predefiniti (client di crittografia, Encrypt for Sharing, nessuna finestra di dialogo, nessuna barra di avanzamento, riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`) e registri di installazione in `C:\Dell`. **Nota:** per la riuscita della generazione dei registri, la directory `C:\Dell` deve esistere prima di procedere all'installazione.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
norestart /qn /l*v C:\Dell\DellEncryptionInstall.log"
```

NOTA: alcune versioni meno recenti potrebbero richiedere caratteri di \" intorno ai valori dei parametri. Per esempio:

DDPE_XXbit_setup.exe /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\" DA_RUNAS=\"domain\username\" DA_RUNASPWD=\"password\" /qn

Installare Full Disk Encryption

- Se l'organizzazione sta usando un certificato firmato da un'autorità root, come EnTrust o Verisign, consultare la sezione Requisiti di Full Disk Encryption. Per abilitare la convalida del certificato SSL/TLS, è necessario modificare le impostazioni di registro nel computer client.
- Gli utenti accederanno alla PBA utilizzando le proprie credenziali di Windows.

Installazione dalla riga di comando

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

Parametri
CM_EDITION=1 (gestione remota)
INSTALLDIR=(modifica la destinazione di installazione)
SERVERHOST=(securityserver.organization.com)
SERVERPORT=8888
SECURITYSERVERHOST=(securityserver.organization.com)
SECURITYSERVERPORT=8443
FEATURE=FDE
ENABLE_FDE_LM=1 (consente l'installazione di Full Disk Encryption su un computer con Dell Encryption attivo)

Per un elenco di opzioni e opzioni di visualizzazione .msi base che possono essere utilizzate nelle righe di comando, fare riferimento a Eseguire l'installazione usando i programmi di installazione figlio.

Esempio di riga di comando

Encryption Management Agent

- Nell'esempio seguente viene installato Full Disk Encryption gestita (installazione automatica, nessun riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 FEATURE=FDE SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /
norestart /qn"
```

- **Encryption Management Agent**
- Nell'esempio seguente viene installato Full Disk Encryption gestito in remoto e viene consentita l'installazione su un computer protetto Dell Encryption (installazione automatica, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

- **Esempio di riga di comando per installare Full Disk Encryption ed Encryption External Media.**

  Crittografia

  Nell'esempio seguente viene installato Encryption External Media con installazione automatica, nessuna barra di avanzamento, nessun riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Quindi:

  Encryption Management Agent

  Nell'esempio seguente viene installata Full Disk Encryption gestita in remoto e viene consentita l'installazione su un computer protetto Dell Encryption (con installazione automatica, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
  ```

Installare Encryption sul sistema operativo del server

Sono disponibili due metodi per installare Encryption sul sistema operativo del server. Scegliere uno dei seguenti metodi:

- Installare Encryption sul sistema operativo del server in modo interattivo

  La crittografia sul sistema operativo del server può essere installata in maniera interattiva solo nei computer in cui sono in esecuzione i sistemi operativi del server. L'installazione nei computer in cui sono in esecuzione i sistemi operativi non server deve essere eseguita dalla riga di comando, con il parametro SERVERMODE=1 specificato.

- Installare Encryption sul sistema operativo del server utilizzando la riga di comando

Account utente virtuale

- Come parte dell'installazione, viene creato un **account utente del server virtuale** per l'uso esclusivo della crittografia sul sistema operativo del server. La password e l'autenticazione DPAPI sono disabilitate in modo che solo l'utente virtuale del server possa accedere alle chiavi di crittografia.

Prima di iniziare

- L'account utente che esegue l'installazione deve essere un utente di dominio con autorizzazioni di livello amministratore.
- Per ignorare questa esigenza, o per eseguire la crittografia sul sistema operativo del server su server non dominio o multi dominio, impostare la *ssos.domainadmin.verify* property su *falso* nel file application.properties. Il file viene archiviato nei seguenti percorsi di file, in base al Dell Server che si sta utilizzando:

  Security Management Server - *<cartella di installazione>*/Security Server/conf/application.properties

  Security Management Server Virtual - /opt/dell/server/security-server/conf/application.properties

- Il server deve supportare il controllo delle porte.

  I criteri di sistema del controllo delle porte influenzano i supporti rimovibili sui server protetti, per esempio, controllando l'accesso e l'utilizzo delle porte USB del server da parte di dispositivi USB. Il criterio delle porte USB si applica alle porte USB esterne. La funzionalità delle porte USB interne non è influenzata dal criterio delle porte USB. Se il criterio delle porte USB viene disabilitato, la tastiera e il mouse USB non funzionano e l'utente non è in grado di usare il computer a meno che venga impostata una connessione al desktop in remoto prima che venga applicato il criterio.

- Per attivarsi correttamente, il computer deve disporre di connettività di rete.
- Quando il Trusted Platform Module (TPM) è disponibile, viene usato per sigillare la GPK nell'hardware Dell. Se non è disponibile un TPM, l'API del Data Protection (DPAPI) di Microsoft è utilizzato per proteggere la General Purpose Key.

  Quando si installa un nuovo sistema operativo in un computer Dell con un TPM che ha in esecuzione Server Encryption, cancellare il TPM nel BIOS. Consultare questo articolo per istruzioni.

- Il file di registro per l'installazione si trova nella directory %temp% dell'utente, disponibile al percorso `C:\Users\<user name>\AppData\Local\Temp`. Per individuare il file di registro corretto, cercare un nome di file che inizi con MSI e

termini con un'estensione .log. Il file contiene una data/timestamp corrispondente al momento in cui è stato eseguito il programma di installazione.

- Encryption non è supportato sui server che fanno parte di sistemi di file system distribuiti (DFS).

Estrarre il programma di installazione figlio

- Per installare Encryption sul sistema operativo del server, è prima necessario estrarre il programma di installazione figlio **DDPE_xxbit_setup.exe** dal programma di installazione principale. Consultare Estrarre i programmi di installazione figlio dal programma di installazione principale

Installare in modo interattivo

- Utilizzare le istruzioni riportate di seguito per installare Encryption sul sistema operativo del server in modo interattivo. Questo programma di installazione include i componenti necessari per la crittografia del software.

1. Individuare **DDPE_XXbit_setup.exe** nella cartella `C:\extracted\Encryption`. Copiarlo nel computer locale.
2. Se si sta installando la crittografia sul sistema operativo del server, fare doppio clic su **DDPE_XXbit_setup.exe** per avviare il programma di installazione.

   N.B.:

   Quando la crittografia sul sistema operativo del server è installata in un computer che ha in esecuzione un sistema operativo del server come Windows Server 2012 R2, il programma di installazione installa automaticamente la crittografia in SERVERMODE.

3. Nella schermata iniziale, fare clic su **Avanti**.
4. Nella schermata del Contratto di licenza leggere il contratto, accettare i termini e fare clic su **Avanti**.
5. Selezionare *On-Prem Dell Management Server* , quindi fare clic su **Avanti**.

6. Fare clic su **Avanti** per installare nel percorso predefinito.
7. Fare clic su **Avanti** per ignorare la finestra di dialogo *Tipo di gestione*.
8. Nel *Nome Security Management Server*, immettere/validare il nome host qualificato completo del Dell Server per gestire l'utente di destinazione (ad esempio, *server.organization.com)*.

   Immettere il nome di dominio nel campo *Dominio gestito* (ad esempio, organizzazione). Fare clic su **Avanti**.
9. Nell'hostname e nella porta di Policy Proxy, immettere/validare le informazioni, quindi fare clic **Avanti**.

10. Nell'URL Device Server, immettere/validare le informazioni, quindi fare clic su **Avanti**.
11. Fare clic su **Installa** per avviare l'installazione.

    L'installazione potrebbe richiedere alcuni minuti.
12. Una volta completata la configurazione, fare clic su **Fine**.

    L'installazione è completata.
13. Riavviare il sistema. Dell consiglia di posporre il riavvio solo se è necessario tempo per salvare il lavoro svolto e chiudere le applicazioni. la crittografia non può iniziare finché il computer non è stato riavviato.

Installare usando la riga di comando

Il programma di installazione si trova in `C:\extracted\Encryption`

- Usare **DDPE_xxbit_setup.exe** per eseguire l'installazione o l'aggiornamento mediante file batch, un'installazione tramite script o qualsiasi altra tecnologia push disponibile alla propria organizzazione.

Opzioni

La tabella seguente descrive in dettaglio le opzioni disponibili per l'installazione.

Opzione	Significato
/v	Consente di passare variabili al file .msi all'interno di DDPE_XXbit_setup.exe
/a	Installazione amministrativa
/s	Modalità non interattiva

Parametri

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

Componente	File di registro	Parametri della riga di comando
Tutti	/l*v [percorso completo] [nome file].log *	SERVERHOSTNAME=<Security Management Server Name>
		SERVERMODE=1
		POLICYPROXYHOSTNAME=<RGK Name>
		MANAGEDDOMAIN=<My Domain>
		DEVICESERVERURL=<Activation Server Name>
		GKPORT=<New GK Port>
		MACHINEID=<Machine Name>
		RECOVERYID=<Recovery ID>
		REBOOT=ReallySuppress
		HIDEOVERLAYICONS=1
		HIDESYSTRAYICON=1
		EME=1

N.B.:

Componente	File di registro	Parametri della riga di comando
Anche se può essere soppresso, il riavvio è comunque necessario. la crittografia non può iniziare finché il computer non è stato riavviato.		

Opzioni

La tabella seguente descrive in dettaglio le opzioni di visualizzazione che possono essere specificate in fondo all'argomento passato all'opzione /v.

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

N.B.:

Non usare **/q** e **/qn** insieme nella stessa riga di comando. Usare solo **!** e - dopo **/qb**.

- Il parametro della riga di comando, SERVERMODE=1, viene rispettato solo nel corso di nuove installazioni. Il parametro viene ignorato per le disinstallazioni.
- Racchiudere un valore contenente uno o più caratteri speciali, ad esempio uno spazio, tra virgolette con escape.
- Il parametro DEVICESERVERURL rileva la distinzione tra maiuscole e minuscole.

Esempio di installazione dalla riga di comando

- Nell'esempio seguente viene installato Encryption in modalità del sistema operativo del server con i parametri predefiniti (crittografia, Encrypt for Sharing, nessuna finestra di dialogo, nessuna barra di avanzamento, riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn
  REBOOT="ReallySuppress" SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
  POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- Nell'esempio seguente viene installato Encryption in modalità del sistema operativo del server con un file di registro e parametri predefiniti (crittografia, Encrypt for Sharing, installazione automatica, nessuna finestra di dialogo, nessuna barra di avanzamento, nessun riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`) e viene specificato un nome del file di registro personalizzato che termina con un numero (DDP_ssos-090.log) che deve essere aumentato se la riga di comando viene eseguita più di una volta nello stesso server. Per specificare un percorso del registro diverso da quello predefinito in cui si trova l'eseguibile, inserire il percorso completo nella riga di comando. Per esempio, /l*v C:\Logs\DDP_ssos-090.log creerà registri di installazione nella cartella C:\Logs.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /l*v DDP_ssos-090.log /
  norestart/qn"
  ```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/
xapi/" /l*v DDP_ssos-090.log /norestart/qn"
```

Riavviare il computer dopo l'installazione. Dell consiglia di posporre il riavvio solo se è necessario tempo per salvare il lavoro svolto e chiudere le applicazioni. la crittografia non può iniziare finché il computer non è stato riavviato.

Attiva

- Assicurarsi che il nome del computer del server sia il nome endpoint che si desidera visualizzare nella Management Console.
- Un utente interattivo con credenziali di amministratore di dominio deve effettuare l'accesso al server almeno una volta per l'attivazione iniziale. L'utente che effettua l'accesso al server può essere di qualsiasi tipo: utente di dominio o non di dominio, connesso al desktop in remoto o interattivo, ma l'attivazione richiede credenziali di amministratore di dominio.
- Dopo il riavvio che segue l'installazione, viene visualizzata la finestra di dialogo Attivazione. L'amministratore deve immettere le credenziali di amministratore di dominio con un nome utente in formato Nome principale utente (UPN). La crittografia dei sistemi operativi del server non si attiva automaticamente.
- Durante l'attivazione iniziale, viene creato un account utente del server virtuale. Dopo l'attivazione iniziale, il computer viene riavviato in modo che possa iniziare l'attivazione del dispositivo.
- Durante la fase di autenticazione e attivazione del dispositivo, al computer viene assegnato un ID della macchina univoco, le chiavi di crittografia vengono create e raggruppate in pacchetti, e si stabilisce un rapporto tra il pacchetto chiavi di crittografia e l'utente del server virtuale. Il pacchetto chiavi di crittografia associa le chiavi di crittografia e i criteri al nuovo utente del server virtuale per creare una relazione indissolubile tra i dati crittografati, il computer specifico e l'utente del server virtuale. Dopo l'attivazione del dispositivo, l'utente del server virtuale appare nella Management Console come UTENTE-SERVER@<*fully qualified server name*>. Per maggiori informazioni sull'attivazione, consultare Attivazione nel sistema operativo di un server.

N.B.:

Se si rinomina il server dopo l'attivazione, il nome visualizzato non si modificherà nella Management Console. Tuttavia, se la crittografia dei sistemi operativi del server si attiva nuovamente dopo che il nome del server viene modificato, il nuovo nome del server viene visualizzato nella Management Console.

Una finestra di dialogo Attivazione viene visualizzata una volta dopo ogni riavvio per richiedere all'utente di attivare la crittografia sul sistema operativo del server. Per completare l'attivazione, attenersi alla seguente procedura:

1. Effettuare l'accesso al server o al server oppure usando la Connessione desktop remoto.
2. Immettere il nome utente di un amministratore di dominio in formato UPN e la password e fare clic su **Attiva**. È la stessa finestra di dialogo di Attivazione che appare ogni volta che viene riavviato un sistema non attivato.

   Il Dell Server emette una chiave di crittografia per l'ID della macchina, crea l'**account utente del server virtuale**, crea una chiave di crittografia per l'account utente, raggruppa in pacchetti le chiavi di crittografia e crea la relazione tra il pacchetto di crittografia e l'account utente del server virtuale.

3. Fare clic su **Chiudi**.

   Al termine dell'attivazione, viene avviata la crittografia.

4. Al termine della ricerca della crittografia, riavviare il sistema per elaborare i file che erano in uso in precedenza. Si tratta di un passaggio importante ai fini della sicurezza.

   N.B.:

   Se il criterio *Credenziali Windows di protezione* è attivato, la crittografia del sistema operativo del server crittografa i file `\Windows\system32\config`, che includono le credenziali di Windows. I file in `\Windows\system32\config` vengono cifrati se il criterio *Crittografia SDE abilitata* non è selezionato. Per impostazione predefinita, il criterio *Credenziali Windows di protezione* è selezionato.

   N.B.:

   Dopo il riavvio del computer, l'autenticazione per la chiave di crittografia comune richiede *sempre* la chiave di macchina del server protetto. Il Dell Server restituisce una chiave di sblocco per accedere alle chiavi di crittografia e ai criteri nel vault (le chiavi e i criteri sono per il server, non per l'utente). Senza la chiave di macchina del server, la chiave di crittografia comune del file non può essere sbloccata e il computer non può ricevere gli aggiornamenti dei criteri.

Confermare l'attivazione

Dalla console locale, aprire la finestra di dialogo **Informazioni** per confermare che la crittografia del server è installata, autenticata e in modalità server. Se l'ID di Encryption Client è **rosso**, la crittografia non è stata ancora attivata.

Utente del server virtuale

- Nella Management Console, è possibile trovare un server protetto con il suo nome della macchina. Inoltre, ogni server protetto ha il proprio account utente del server virtuale. Ogni account ha un nome utente statico e un nome della macchina univoci.
- L'account utente del server virtuale viene usato solo dalla crittografia del sistema operativo del server ed è altrimenti trasparente per il funzionamento del server protetto. L'utente del server virtuale è associato al pacchetto chiavi di crittografia e al policy proxy.
- Dopo l'attivazione, l'account utente del server virtuale è l'account utente che viene attivato e associato al server.
- Dopo che l'account utente del server virtuale viene attivato, tutte le notifiche di accesso/fine sessione del server vengono ignorate. Al contrario, durante l'avvio, il computer effettua automaticamente l'autenticazione con l'utente del server virtuale, quindi scarica la chiave di macchina dal Dell Server.

Installare SED Manager e PBA Advanced Authentication

- Se la propria organizzazione sta usando un certificato firmato da un'autorità root, come EnTrust o Verisign, consultare i Requisiti SED. Per abilitare la convalida del certificato SSL/TLS, è necessario modificare le impostazioni di registro nel computer client.
- Gli utenti accederanno alla PBA utilizzando le proprie credenziali di Windows.
- I programmi di installazione di SED Manager e PBA Advanced Authentication si trovano in:
  - **Da dell.com/support** - Se necessario, consultare Ottenere il software da dell.com/support e poi consultare Estrarre i programmi di installazione figlio dal programma di installazione principale. Dopo l'estrazione, il file si trova in `C:\extracted\Encryption Management Agent`.
  - **Dall'account Dell FTP** - Individuare il bundle di installazione in Encryption-Enterprise-10.x.x.xxx.zip e poi consultare Estrarre i programmi di installazione figlio dal programma di installazione principale. Dopo l'estrazione, il file si trova in `C:\extracted\Encryption Management Agent`.

Installazione dalla riga di comando

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

Parametri
CM_EDITION=1 <remote management>
INSTALLDIR=<change the installation destination>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Per un elenco di opzioni e opzioni di visualizzazione .msi base che possono essere utilizzate nelle righe di comando, fare riferimento a Eseguire l'installazione usando i programmi di installazione figlio.

I seguenti comandi di esempio consentono di installare o aggiornare Encryption Management Agent.

Esempio di riga di comando

\Encryption Management Agent

- Nell'esempio seguente, vengono installati SED Manager, Encryption Management Agent e la console di sicurezza locale in modalità remota (installazione automatica, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

Installare BitLocker Manager

- **N.B.:** Se l'azienda richiede l'utilizzo di provider di credenziali di terze parti, è necessario installare o aggiornare Encryption Management Agent con il parametro FEATURE=BLM o FEATURE=BASIC.

- Se la propria organizzazione sta usando un certificato firmato da un'autorità radice, come EnTrust o Verisign, consultare i Requisiti del client di BitLocker Manager. Per abilitare la convalida del certificato SSL/TLS, è necessario modificare le impostazioni di registro nel computer client.
- I programmi di installazione del client di BitLocker Manager sono disponibili su:
  - **Da dell.com/support** - Se necessario, consultare Ottenere il software da dell.com/support e poi consultare Estrarre i programmi di installazione figlio dal programma di installazione principale. Dopo l'estrazione, il file si trova in `C:\extracted\Encryption Management Agent`.
  - **Dall'account Dell FTP** - Individuare il bundle di installazione in Encryption-Enterprise-10.x.x.xxx.zip e poi consultare Estrarre i programmi di installazione figlio dal programma di installazione principale. Dopo l'estrazione, il file si trova in `C:\extracted\Encryption Management Agent`.

Installazione dalla riga di comando

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

Parametri
CM_EDITION=1 <remote management>
INSTALLDIR=<change the installation destination>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
FEATURE=BLM <install BitLocker Manager only>
FEATURE=BLM,SED <install BitLocker Manager with SED>
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Per un elenco di opzioni e opzioni di visualizzazione .msi base che possono essere utilizzate nelle righe di comando, fare riferimento a Eseguire l'installazione usando i programmi di installazione figlio.

Esempio di riga di comando

- Nell'esempio seguente, viene installato solo BitLocker Manager (installazione invisibile all'utente, nessun riavvio, nessuna voce nell'elenco Programmi del Pannello di controllo e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
FEATURE=BLM /norestart /qn"
```

- Nell'esempio seguente, viene installato BitLocker Manager con un'unità autocrittografante (installazione invisibile all'utente, nessun riavvio, nessuna voce nell'elenco Programmi del Pannello di controllo e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`)

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM,SED /norestart /qn"
  ```

- **Esempio di riga di comando per installare BitLocker Manager e Dell Encryption**

  Nell'esempio seguente, viene installato solo BitLocker Manager (installazione invisibile all'utente, nessun riavvio, nessuna voce nell'elenco Programmi del Pannello di controllo e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`)

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Quindi:

  Nell'esempio seguente viene installato il client con i parametri predefiniti (client di crittografia ed Encrypt for Sharing, senza finestra di dialogo, senza barra di stato, riavvio automatico, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

7

Eseguire la disinstallazione usando i programmi di installazione figlio

- Dell consiglia di utilizzare il Programma di disinstallazione di Data Security per rimuovere la suite Data Security.
- Per disinstallare ciascun client singolarmente, i file eseguibili figlio devono essere prima estratti dal programma di installazione principale di , come mostrato in Estrarre i programmi di installazione figlio dal programma di installazione principale. In alternativa, eseguire un'installazione amministrativa per estrarre il file .msi.
- Per la disinstallazione accertarsi di usare le stesse versioni di client usate per l'installazione.
- 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.

Opzione	Significato
/v	Consente di passare variabili al file .msi all'interno di setup.exe. Il contenuto deve sempre essere racchiuso tra virgolette con testo normale.
/s	Modalità non interattiva
/x	Modalità di disinstallazione
/a	Installazione amministrativa (tutti i file all'interno del file .msi vengono copiati)

N.B.:

Con /v, sono disponibili le opzioni predefinite di Microsoft. Per un elenco delle opzioni, fare riferimento a https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

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

Opzione	Significato
/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

Disinstallare la crittografia e la crittografia sul sistema operativo del server

- Per ridurre la durata del processo di decrittografia, eseguire Pulizia disco di Windows per rimuovere i file temporanei e altri dati non necessari.
- 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 di decrittografia dovuti a file bloccati.
- Al termine della disinstallazione e mentre la decrittografia è in corso, disabilitare la connettività di rete. In caso contrario potrebbero essere acquisiti nuovi criteri che riattivano la crittografia.
- Seguire il processo esistente per la decrittografia dei dati, ad esempio impostare l'aggiornamento di un criterio.
- La crittografia ed Encryption External Media aggiornano il Dell Server per modificare lo stato di *Non protetto* all'inizio di un processo di disinstallazione di un client. Tuttavia, se il client non riesce a contattare il Dell Server per qualsiasi motivo, non è possibile aggiornare lo stato. In questo caso sarà necessario selezionare manualmente l'opzione *Rimuovi endpoint* nella Management Console. Se l'organizzazione utilizza questo workflow ai fini della conformità, Dell consiglia di verificare che lo stato *Non protetto* sia stato impostato come previsto nella Management Console o nei Report gestiti.

Procedura

- **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.
- È necessario configurare Key Server (e Security Management Server) prima della disinstallazione se si usa l'opzione **Scarica chiavi dal server di Encryption Removal Agent**. Per istruzioni, consultare Configurare un Key Server per la disinstallazione di Encryption client attivato per Security Management Server. Non è necessaria alcuna azione precedente se il client da disinstallare è stato attivato per un Security Management Server Virtual, in quanto Security Management Server Virtual non utilizza il Key Server.
- Se si sta usando l'opzione **Importa chiavi da file di Encryption Removal Agent**, prima di avviare l'Encryption Removal Agent è necessario usare la Dell Administrative Utility (CMGAd). Questa utilità è usata per ottenere il bundle di chiavi di crittografia. Per istruzioni, consultare Usare l'Administrative Download Utility (CMGAd). L'utilità può trovarsi nel supporto di installazione Dell.
- 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.

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale , il programma di installazione di Encryption si trova in `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: 3 - Utilizzare il pacchetto LSARecovery 2 - Utilizzare il materiale della chiave Forensic scaricato in precedenza 1 - Scaricare le chiavi dal Dell Server 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
Proprietà richieste	
DA_KM_PATH	Il percorso qualificato completo per il keybundle.
DA_KM_PW	La password impostata nel keybundle.
DA_SERVER	FQHN per il Security Management Server che ospita la sessione di negoziazione.
DA_PORT	Porta in Security Management Server per la richiesta (predefinita 8050).
SVCPN	Nome utente in formato UPN con cui il servizio Key Server ha effettuato l'accesso a Security Management Server.
DA_RUNAS	Nome utente in formato compatibile con SAM nel cui contesto viene effettuata la richiesta di ripristino delle chiavi. Questo utente deve essere incluso nell'elenco Key Server in Security Management Server.
DA_RUNASPWD	Password per l'utente runas.
FORENSIC_ADMIN	L'account amministratore Forensic sul Dell Server, che può essere utilizzato per le richieste Forensic di disinstallazioni o chiavi.
FORENSIC_ADMIN_PWD	Password dell'account amministratore Forensic.
Proprietà facoltative	
SVCLOGONUN	Nome utente in formato UPN per l'accesso al servizio Encryption Removal Agent come parametro.
SVCLOGONPWD	Password per l'accesso come utente.

- Nell'esempio seguente viene disinstallato Encryption in modo invisibile all'utente e vengono scaricate le chiavi di crittografia dal Security Management Server.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  DA_SERVER=server.organization.com DA_PORT=8050 SVCPN=administrator@organization.com
  DA_RUNAS=domain\username DA_RUNASPWD=password /qn"
  ```

  Comando MSI:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
```

Al termine, riavviare il sistema.

- Nell'esempio seguente viene disinstallato Encryption in modo invisibile all'utente e vengono scaricate le chiavi di crittografia usando un account amministratore Forensic.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn
  CMG_DECRYPT=1 CMGSILENTMODE=1 FORENSIC_ADMIN=forensicadmin@organization.com
  FORENSIC_ADMIN_PWD=tempchangeit REBOOT=REALLYSUPPRESS
  ```

  Al termine, riavviare il sistema.

- Nell'esempio seguente Encryption viene disinstallato in modo invisibile all'utente mediante le chiavi precedentemente scaricate reperibili in C:\Users\administrator\Desktop\Admin\ utilizzando la password dell'amministratore Forensic e i registri di scrittura in C:\SheildUninstall.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENT=1 DA_KM_PATH=C:
  \Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v c:
  \ShieldUninstall.log /qn /norestart"
  ```

  Comando MSI

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" CMG_DECRYPT=2 CMGSILENT=1
  DA_KM_PATH=C:\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v
  c:\ShieldUninstall.log /qn /norestart
  ```

N.B.:

Dell consiglia di effettuare le seguenti azioni quando si utilizza una password amministratore Forensic sulla riga di comando:

1. Creare un account amministratore Forensic nella Management Console allo scopo di eseguire la disinstallazione invisibile all'utente.
2. Usare una password temporanea univoca per quell'account e per un periodo di tempo specifico.
3. Al termine della disinstallazione invisibile all'utente, rimuovere l'account temporaneo dall'elenco degli amministratori o modificarne la password.

Alcuni client meno recenti potrebbero richiedere caratteri di escape \" intorno ai valori dei parametri. Per esempio:

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\"
CMGSILENTMODE=\"1\" DA_SERVER=\"server.organization.com\" DA_PORT=\"8050\"
SVCPN=\"administrator@organization.com\" DA_RUNAS=\"domain\username\"
DA_RUNASPWD=\"password\" /qn"
```

Disinstallare Encryption External Media

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

Disinstallazione dalla riga di comando

Eseguire una riga di comando analoga alla seguente:

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

Al termine, riavviare il sistema.

Disinstallare Full Disk Encryption

- Per disattivare PBA è richiesta la connessione di rete al Dell Server.

Procedura

- Disattivare la PBA, che rimuove tutti i dati PBA dal computer e sblocca le chiavi Full Disk Encryption.
- Disinstallare Full Disk Encryption.

Disattivare la PBA

1. Eseguire l'accesso alla Management Console come amministratore Dell.
2. Nel riquadro sinistro, fare clic su **Popolamenti** > **Endpoint**.
3. Selezionare il Tipo endpoint appropriato.
4. Selezionare Mostra >*Visibili, Nascosti* o *Tutti*.
5. Se si conosce il nome host del computer, immetterlo nel campo Nome host (è supportato l'utilizzo dei caratteri jolly). È possibile lasciare il campo vuoto per visualizzare tutti i computer. Fare clic su **Cerca**.

   Se non si conosce il nome host, scorrere l'elenco per individuare il computer desiderato.

   A seconda del filtro di ricerca viene visualizzato un computer o un elenco di computer.
6. Selezionare il nome host del computer desiderato.
7. Fare clic su **Criteri di protezione** dal menu principale.
8. Selezionare **Full Disk Encryption** dal gruppo **Crittografia Windows**.
9. Modificare **Full Disk Encryption** e il criterio da `On` a ***`Off`***.
10. Fare clic su **Salva**.
11. Nel riquadro sinistro, fare clic sul banner **Commit criteri**.
12. Fare clic su **Commit criteri**.

    Attendere la propagazione del criterio dal Dell Server al computer da disattivare.

    Disinstallare Full Disk Encryption e PBA Advanced Authentication dopo aver disattivato la PBA.

Disinstallare il client di Full Disk Encryption

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale, Full Disk Encryption è disponibile al percorso `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
  - Nell'esempio seguente, viene eseguita la disinstallazione automatica di Full Disk Encryption.

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

    Al termine, arrestare e riavviare il sistema.

Disinstallare SED Manager

- Per disattivare PBA è richiesta la connessione di rete al Dell Server.

Procedura

- Disattivare la PBA, che rimuove tutti i dati di PBA dal computer e sblocca le chiavi delle unità autocrittografanti.
- Disinstallare SED Manager.

Disattivare la PBA

1. Eseguire l'accesso alla Management Console come amministratore Dell.
2. Nel riquadro sinistro, fare clic su **Popolamenti** > **Endpoint**.
3. Selezionare il Tipo endpoint appropriato.
4. Selezionare Mostra >*Visibili, Nascosti* o *Tutti*.

5. Se si conosce il nome host del computer, immetterlo nel campo Nome host (è supportato l'utilizzo dei caratteri jolly). È possibile lasciare il campo vuoto per visualizzare tutti i computer. Fare clic su **Cerca**.

   Se non si conosce il nome host, scorrere l'elenco per individuare il computer desiderato.

   A seconda del filtro di ricerca viene visualizzato un computer o un elenco di computer.

6. Selezionare il nome host del computer desiderato.
7. Fare clic su **Criteri di protezione** dal menu principale.
8. Selezionare **Unità autocrittografanti** dalla pagina **Categoria criteri**.
9. Modificare l'**Unità autocrittografante (SED)** e il criterio da *On* a ***Off***.
10. Fare clic su **Salva**.
11. Nel riquadro sinistro, fare clic sul banner **Commit criteri**.
12. Fare clic su **Commit criteri**.

    Attendere la propagazione del criterio dal Dell Server al computer da disattivare.

    Disinstallare SED Manager e PBA Advanced Authentication dopo aver disattivato la PBA.

Disinstallare il client dell'unità autocrittografante

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale, il programma di installazione di SED Manager 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 Manager.

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

    Al termine, arrestare e riavviare il sistema.

Disinstallare BitLocker Manager

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale di , il programma di installazione di BitLocker si trova in `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- L'esempio seguente disinstalla in modo invisibile all'utente BitLocker Manager.

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

  Al termine, riavviare il sistema.

8

Programma di disinstallazione Data Security

Disinstallare

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 **Scarica chiavi dal server di Encryption Removal Agent**.

Immettere le credenziali complete di un amministratore Forensic e selezionare **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.

9

Scenari di uso comune

- Per installare ciascun client singolarmente, i file eseguibili figlio devono essere prima estratti dal programma di installazione principale di come mostrato in Estrarre i programmi di installazione figlio dal programma di installazione principale.
- Le opzioni e i parametri della riga di comando fanno distinzione tra maiuscole e minuscole.
- È importante ricordare che tutti i valori contenenti uno o più caratteri speciali, ad esempio uno spazio nella riga di comando, devono essere racchiusi tra virgolette con escape.
- Usare questi programmi di installazione per installare i client usando un'installazione tramite script, file batch o qualsiasi altra tecnologia push a disposizione della propria organizzazione.
- Negli esempi delle righe di comando il riavvio è stato eliminato, ma un riavvio finale sarà necessario perché la crittografia non può iniziare finché il computer non è stato riavviato.
- File di registro - Windows crea file di registro di installazione dei programmi di installazione figlio univoci per l'utente che ha effettuato l'accesso a %temp% e si trovano nel percorso `C:\Users\<UserName>\AppData\Local\Temp`.

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

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

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

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

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

- Indicare agli utenti di prendere visione del seguente documento e file della guida per assistenza sull'applicazione:

- Consultare la *Dell Encrypt Help* (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* (Guida di Encryption External Media) per istruzioni sulle funzioni di Encryption External Media. Accedere alla guida da `<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS`
- Consultare *Encryption Enterprise Help* (Guida di Encryption Enterprise) (Guida diEndpoint Security Suite Pro) (Guida di Endpoint Security Suite Enterprise)per istruzioni sull'utilizzo delle funzioni di. Accedere alla guida da `<Install dir>:\Program Files\Dell\Dell Data Protection\Authentication \Help`.

Encryption Client

- Nell'esempio seguente vengono installati SED Management ed Encryption Management Agent (installazione automatica, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Quindi:

- Nell'esempio seguente viene installata la crittografia con i parametri predefiniti (crittografia ed Encrypt for Sharing, nessuna finestra di dialogo, nessuna barra di avanzamento, nessun riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

  Sostituire `DEVICESERVERURL=https://server.organization.com:`**`8081/xapi`** (senza la barra finale) se la versione di Security Management Server è precedente alla 7.7.

Client di SED Manager (inclusa Advanced Authentication) ed Encryption

- Nell'esempio seguente vengono installati i driver per il Trusted Software Stack (TSS) per il TPM e gli aggiornamenti rapidi di Microsoft nel percorso specificato, senza creare alcuna voce nell'elenco Programmi nel Pannello di controllo ed eliminando il riavvio.

  Questi driver devono essere installati durante l'installazione del client di crittografia.

  ```
  setup.exe /S /z"\"InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
  ```

  Quindi:

- Nell'esempio seguente, viene installato SED Manager gestito in remoto (installazione invisibile all'utente, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Quindi:

- Nell'esempio seguente viene installata l'Autenticazione avanzata (installazione invisibile all'utente, nessun riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Authentication`).

  ```
  setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
  ```

  Quindi:

- Nell'esempio seguente viene installato il client con i parametri predefiniti (client di crittografia ed Encrypt for Sharing, senza finestra di dialogo, senza barra di stato, senza riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

  Sostituire `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (senza la barra finale) se la versione di Security Management Server è precedente alla 7.7.

SED Manager ed Encryption External Media

- Nell'esempio seguente, vengono installati SED Manager, Encryption Management Agent e la console di sicurezza locale (installazione automatica, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Quindi:

- Nell'esempio seguente, viene installato solo Encryption External Media (installazione invisibile all'utente, nessun riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

  Sostituire `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (senza la barra finale) se la versione di Security Management Server è precedente alla 7.7.

BitLocker Manager ed Encryption External Media

- BitLocker Manager ed Encryption External Media interagiscono in base alla sequenza di crittografia. Se un'unità crittografata BitLocker Manager è inserita in un computer con Encryption External Media, la password BitLocker Manager **deve** essere immessa per consentire a Encryption External Media di leggere e crittografare l'unità.
- Se Encryption External Media è attivo su un'unità, la crittografia BitLocker Manager può essere applicata alla stessa unità.
- Nell'esempio seguente viene installato BitLocker Manager (installazione invisibile all'utente, nessun riavvio, nessuna voce nell'elenco Programmi nel Pannello di controllo e installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Quindi:

- Nell'esempio seguente, viene installato solo Encryption External Media (installazione invisibile all'utente, nessun riavvio, installazione nel percorso predefinito `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

Sostituire `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (senza la barra finale) se la versione di Security Management Server è precedente alla 7.7.

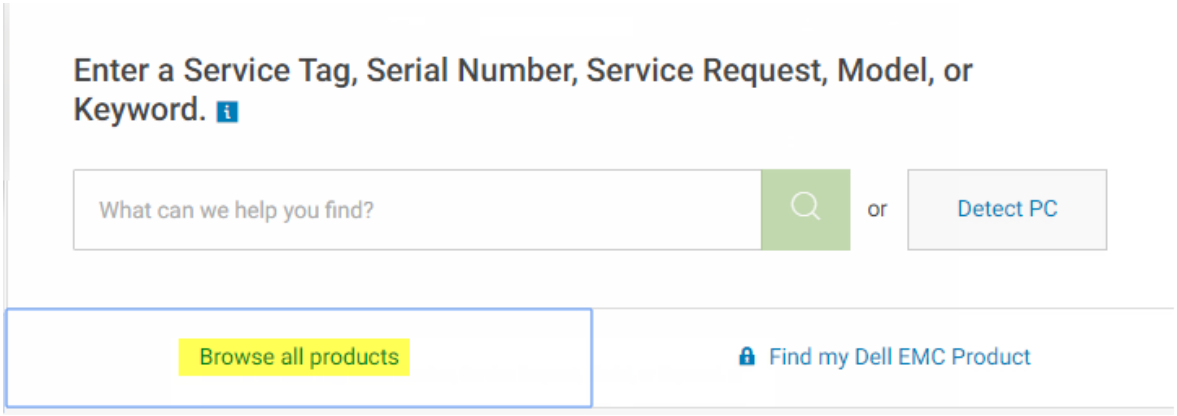
10

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**.

11

Configurazione di preinstallazione per UEFI unità autocrittografante e BitLocker Manager

Inizializzare il TPM

- È necessario essere membro del gruppo amministratori locali o avere un ruolo equivalente.
- È necessario che il computer disponga di un BIOS o TPM compatibili.
- Seguire le istruzioni all'indirizzo http://technet.microsoft.com/en-us/library/cc753140.aspx.

Configurazione di preinstallazione per computer UEFI

Abilitare la connettività di rete durante l'autenticazione di preavvio UEFI

Per eseguire l'autenticazione di preavvio in un computer con firmware UEFI, la PBA deve disporre della connettività di rete. Per impostazione predefinita, i computer con firmware UEFI non dispongono di connettività di rete fino al caricamento del sistema operativo, che avviene dopo la modalità PBA.

La procedura seguente abilita la connettività di rete durante la PBA per computer UEFI abilitati. Poiché la procedura di configurazione può variare in base al modello di computer UEFI, la procedura seguente è solo a titolo di esempio.

1. Avviare la configurazione firmware UEFI.
2. Premere continuamente F2 durante l'avvio fino alla visualizzazione di un messaggio nella schermata superiore destra analogo a "preparing one-time boot menu".
3. Se richiesto, immettere la password di amministratore del BIOS.

   N.B.:

   Se si tratta di un computer nuovo, questa richiesta non viene generalmente visualizzata poiché la password del BIOS non è stata ancora configurata.
4. Selezionare **Configurazione di sistema**.
5. Selezionare **NIC integrata**.
6. Selezionare la casella di controllo **Abilita stack di rete UEFI**.
7. Selezionare **Abilitato** o **Abilitato con PXE**.
8. Selezionare **Applica**.

   N.B.:

   I computer *non* dotati di firmware UEFI non richiedono configurazione.

Disabilitare le ROM di opzione legacy

Assicurarsi che l'impostazione **Abilita ROM di opzione legacy** sia disabilitata nel BIOS.

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

Configurazione di preinstallazione per impostare una partizione PBA di BitLocker

- La partizione PBA deve essere creata **prima** di installare BitLocker Manager.
- Accendere e attivare il TPM **prima** di installare BitLocker Manager. BitLocker Manager assume la proprietà del TPM (non è necessario il riavvio). Tuttavia, se esiste già una proprietà del TPM, BitLocker Manager inizia il processo di configurazione della crittografia. È necessario che il TPM sia di proprietà e venga attivato.
- Potrebbe essere necessario creare manualmente le partizioni del disco. Per ulteriori informazioni, consultare la Descrizione dello strumento Preparazione unità BitLocker.
- Per questa operazione usare il comando BdeHdCfg.exe. Il parametro predefinito indica che lo strumento della riga di comando segue la stessa procedura di configurazione guidata di BitLocker.

  ```
  BdeHdCfg -target default
  ```

  N.B.:

  Per maggiori informazioni sulle opzioni disponibili per il comando BdeHdCfg, consultare Riferimento al parametro BdeHdCfg.exe di Microsoft.

12

Designare il Dell Server tramite il registro

- Se i client vengono autorizzati tramite Dell Digital Delivery, attenersi a queste istruzioni per impostare un registro tramite Oggetti Criteri di gruppo per preconfigurare il Dell Server all'utilizzo al termine dell'installazione.
- La workstation deve essere un membro dell'unità organizzativa (OU) a cui sono applicati gli oggetti Criteri di gruppo, oppure è necessario impostare manualmente le impostazioni di registro sull'endpoint.
- Verificare che la porta 443 in uscita sia disponibile per comunicare con il Dell Server su cloud.dell.com. Se la porta 443 è bloccata (per qualsiasi motivo), l'acquisizione dell'autorizzazione non riesce e i diritti vengono utilizzati dal pool disponibile.

  N.B.: Se non si imposta questo valore del registro quando si tenta di eseguire l'installazione tramite Dell Digital Delivery o non si specifica un SERVER nel programma di installazione principale, l'URL di attivazione predefinito è 199.199.199.199.

Impostazione manuale della chiave di registro

Per gli endpoint che non sono collegati al dominio o per i quali non è stato possibile impostare un oggetto Criteri di gruppo, preimpostare una chiave di registro per l'attivazione su un Dell Server specifico durante l'installazione.

1. Nella casella di ricerca presente nella barra delle applicazioni, digitare **regedit**, quindi cliccare con il pulsante destro del mouse e selezionare **Esegui come amministratore**.
2. A questo punto, creare la seguente chiave di registro in questo percorso:

   HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection

   REG_SZ: Server

   Valore: <FQDN o indirizzo IP del Dell Server>

3. Installare Encryption tramite Dell Digital Delivery o il programma di installazione principale.

Creazione di un oggetto Criteri di gruppo

1. Nel controller di dominio per gestire i client, fare clic su **Start** > **Strumenti di amministrazione** > **Gestione Criteri di gruppo**.
2. Fare clic con il pulsante destro del mouse sull'unità organizzativa in cui dovrebbe essere applicato il criterio e selezionare **Crea un oggetto Criteri di gruppo in questo dominio** e **crea qui un collegamento**.
3. Immettere un nome per il nuovo oggetto criterio di gruppo, selezionare (nessuno) per l'Oggetto Criteri di gruppo Starter di origine e fare clic su **OK**.
4. Fare clic con il pulsante destro del mouse sull'oggetto criterio di gruppo creato e selezionare **Modifica**.
5. Viene caricato l'editor di gestione dei criteri di gruppo. Accedere a **Configurazione computer** > **Preferenze** > **Impostazioni di Windows** > **Registro**.
6. Fare clic con il pulsante destro del mouse sul Registro e selezionare **Nuovo** > **Elemento del registro**. Completare i campi seguenti:

   Azione: Create

   Hive: HKEY_LOCAL_MACHINE

   Percorso chiave: SOFTWARE\Dell\Dell Data Protection

   Nome valore: Server

   Tipo valore: REG_SZ

   Dati valore: <FQDN o indirizzo IP del Dell Server>

7. Cliccare su **OK**.
8. Effettuare la disconnessione e quindi accedere nuovamente alla workstation, oppure eseguire **`gpupdate /force`** per applicare il criterio di gruppo.

13

Estrarre i programmi di installazione figlio

- Per installare ciascun client individualmente, estrarre i file eseguibili figlio dal programma di installazione.
- Il programma di installazione principale non è un *programma di disinstallazione*. Ciascun client deve essere disinstallato singolarmente dopo la disinstallazione del programma di installazione principale. 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. Aprire un prompt dei comandi nello stesso percorso del file **DDSSetup.exe** e immettere:

   ```
   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\.`

14

Configurare il Key Server

- In questa sezione, viene spiegato come configurare i componenti da usare con l'autenticazione/autorizzazione Kerberos quando si utilizza un Security Management Server. Il Security Management Server Virtual non utilizza il Key Server.

  Il Key Server è un servizio in ascolto dei client per la connessione tramite un socket. Al momento della connessione di un client, una connessione sicura verrà negoziata, autenticata e crittografata mediante API Kerberos (se non è possibile negoziare una connessione sicura, il client verrà disconnesso).

  Il Key Server verificherà quindi con il Security Server (ex Device Server) se l'utente che esegue il client è autorizzato ad accedere alle chiavi. Questo tipo di accesso viene concesso mediante singoli domini nella Management Console.

- Se è necessario usare l'autenticazione/autorizzazione Kerberos, il server che contiene il componente Key Server dovrà essere parte del dominio coinvolto.
- Poiché il Security Management Server Virtual non usa il Key Server, non è possibile usare la disinstallazione tipica. Quando viene disinstallato un client di crittografia attivato per un Security Management Server Virtual, viene usato il recupero standard delle chiavi Forensic tramite Security Server al posto del metodo Kerberos del Key Server. Per maggiori informazioni consultare Disinstallazione dalla riga di comando.

Pannello servizi - Aggiungere un account utente di dominio

1. In Security Management Server, andare al pannello servizi (Start > Esegui > services.msc > OK).
2. Fare clic con il pulsante destro del mouse su Key Server e selezionare **Proprietà**.
3. Selezionare la scheda Connessione, quindi il pulsante di opzione **Account:**.

   In *Account:* aggiungere l'account utente di dominio. Questo utente di dominio dovrà disporre almeno dei diritti di amministratore locale per la cartella Key Server (deve essere in grado di scrivere nel file di configurazione di Key Server e nel file log.txt).

   Immettere e confermare la password per l'utente di dominio.

   Fare clic su **OK**.
4. Riavviare il servizio Key Server (lasciare aperto il pannello servizi per ulteriori operazioni).
5. Passare al file log.txt in <Key Server install dir> per verificare che il servizio sia stato avviato.

File di configurazione Key Server - Aggiungi utente per comunicazione del Security Management Server

1. Passare a <Key Server install dir>.
2. Aprire il file `Credant.KeyServer.exe.config` con un editor di testo.
3. Accedere a <add key="user" value="superadmin" /> e modificare il valore "superadmin" con il nome dell'utente appropriato (è possibile mantenere "superadmin").

   Il formato di "superadmin" può essere qualsiasi metodo in grado di eseguire l'autenticazione al Security Management Server. È accettabile il nome dell'account SAM, l'UPN o il formato DOMINIO\Nome utente. È accettabile qualsiasi metodo in grado di eseguire l'autenticazione al Security Management Server, poiché la convalida è richiesta per l'account utente specifico ai fini dell'autorizzazione ad Active Directory.

   Per esempio, in un ambiente multidominio, se si immette solo un nome di account SAM come "jdoe", l'operazione potrebbe avere esito negativo. Il Security Management Server, infatti, non sarà in grado di autenticare "jdoe" poiché non riuscirà a trovarlo. In un ambiente multidominio è consigliabile usare l'UPN, sebbene sia accettabile anche il formato DOMINIO\Nome utente. In un ambiente con un solo dominio è accettabile l'utilizzo del nome dell'account SAM.

4. Accedere a <add key="epw" value="<encrypted value of the password>" /> e modificare "epw" in "password". Quindi modificare "<encrypted value of the password>" con la password dell'utente al punto 3. La password verrà nuovamente crittografata al riavvio di Security Management Server.

   Se si utilizza "superadmin" nel punto 3 e la password superadmin non è "changeit", dovrà essere modificata in questo punto. Salvare e chiudere i file.

File di configurazione di esempio

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="port" value="8050" /> [porta TCP su cui sarà in ascolto il Key Server. La porta predefinita è: 8050.]

<add key="maxConnections" value="2000" /> [numero di connessioni socket attive consentite dal Key Server]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [URL di Security Server (ex Device Server) (il formato è 8081/xapi per un Security Management Server precedente a v7.7)]

<add key="verifyCertificate" value="false" /> [true abilita la verifica dei certificati. Impostare su false per non eseguire la verifica o se si utilizzano certificati autofirmati.]

<add key="user" value="superadmin" /> [nome utente utilizzato per comunicare con il Security Server. Questo utente deve avere il ruolo di amministratore selezionato nella Management Console. Il formato di "superadmin" può essere qualsiasi metodo in grado di eseguire l'autenticazione al Security Management Server. È accettabile il nome dell'account SAM, l'UPN o il formato DOMINIO\Nome utente. È accettabile qualsiasi metodo in grado di eseguire l'autenticazione al Security Management Server, poiché la convalida è richiesta per l'account utente specifico ai fini dell'autorizzazione ad Active Directory. Per esempio, in un ambiente multidominio, se si immette solo un nome di account SAM come "jdoe", l'operazione potrebbe avere esito negativo. Il Security Management Server, infatti, non sarà in grado di autenticare "jdoe" poiché non riuscirà a trovarlo. In un ambiente multidominio è consigliabile usare l'UPN, sebbene sia accettabile anche il formato DOMINIO\Nome utente. In un ambiente con un solo dominio è accettabile l'utilizzo del nome dell'account SAM.]

<add key="cacheExpiration" value="30" /> [frequenza (in secondi) con cui il servizio verificherà quali utenti sono autorizzati a chiedere chiavi. Il servizio mantiene una cache e tiene traccia della data di creazione. Una volta che la data della cache avrà superato il valore indicato, verrà creato un nuovo elenco. Nel momento in cui un utente si connette, il Key Server dovrà scaricare gli utenti autorizzati dal Security Server. Se non è presente una memoria cache per questi utenti o l'elenco non è stato scaricato negli ultimi "x" secondi, verrà nuovamente effettuato il download. Non si verificherà alcun polling, ma questo valore configurerà il livello di obsolescenza consentito per l'elenco prima che quest'ultimo venga aggiornato.]

<add key="epw" value="encrypted value of the password" /> [password utilizzata per comunicare con il Security Management Server. Se la password superadmin è stata modificata, sarà necessario cambiarla in questo punto.]

</appSettings>

</configuration>

Pannello Servizi - Riavvia servizio Key Server

1. Tornare al pannello servizi (Start > Esegui > services.msc > OK).
2. Riavviare il servizio Key Server.
3. Passare al file log.txt in <Key Server install dir> per verificare che il servizio sia stato avviato.
4. Chiudere il pannello servizi.

Management Console - Aggiungi amministratore Forensic

1. Eseguire l'accesso alla Management Console come amministratore Dell.
2. Fare clic su **Popolamenti** > **Domini**.
3. Selezionare il dominio appropriato.

4. Fare clic sulla scheda **Key Server**.
5. In *Account*, aggiungere l'utente per eseguire le attività dell'amministratore. Il formato è DOMINIO\Nome utente. Fare clic su **Aggiungi account**.
6. Fare clic su **Utenti** nel menu a sinistra. Nell'apposita casella cercare il nome utente aggiunto al punto 5. Fare clic su **Cerca**.
7. Una volta individuato l'utente corretto, fare clic sulla scheda **Admin** tab.
8. Selezionare **Amministratore Forensic** e fare clic su **Aggiorna**.

   I componenti sono ora configurati per l'autenticazione/autorizzazione Kerberos.

15

Usare l'Administrative Download Utility (CMGAd)

- Questa utilità consente il download di un bundle di materiale delle chiavi da usare in un computer non connesso a un Dell Server.
- Questa utilità usa uno dei metodi seguenti per scaricare un bundle di materiale delle chiavi, a seconda del parametro della riga di comando trasferito all'applicazione:
  - Modalità Forensic - Usata se -f viene trasferito alla riga di comando o se non viene usato alcun parametro della riga di comando.
  - Modalità Amministratore - Usata se -a viene trasferito alla riga di comando.

    I file di registro sono disponibili al percorso `C:\ProgramData\CmgAdmin.log`

Utilizzo della modalità Forensic

1. Fare doppio clic su **`cmgad.exe`** per avviare l'utilità o aprire un prompt dei comandi in cui si trova CMGAd e digitare **`cmgad.exe -f`** (o **`cmgad.exe`**).
2. Immettere le seguenti informazioni (alcuni campi possono essere già popolati).

   URL del Device Server: URL completo del Security Server (Device Server). Il formato è https://securityserver.domain.com:8443/xapi/. Se il Dell Server in uso è precedente alla versione v7.7, il formato è https://deviceserver.domain.com:8081/xapi (numero di porta diverso, senza barra finale).

   Amministratore Dell: Nome dell'amministratore con credenziali di amministratore Forensic, ad esempio jdoe (attivato nella Management Console)

   Password: password dell'amministratore Forensic

   MCID: ID della macchina, come IDmacchina.dominio.com

   DCID: prime otto cifre dell'ID dello Shield a 16 cifre

   N.B.:

   Solitamente, è sufficiente specificare l'MCID *o* il DCID. Tuttavia, se sono noti, è utile immetterli entrambi. Ogni parametro contiene informazioni diverse utilizzate da questa utilità.

   Fare clic su **Avanti**.

3. Nel campo *Passphrase*, immettere una passphrase per proteggere il file di download. La passphrase deve contenere almeno otto caratteri, di cui almeno uno alfabetico e uno numerico. Confermare la passphrase.

   Accettare il nome e il percorso predefiniti in cui salvare il file, oppure fare clic sui tre puntini ("...") per selezionare un percorso diverso.

   Fare clic su **Avanti**.

   Viene visualizzato un messaggio che indica che il materiale delle chiavi è stato sbloccato. È ora possibile accedere ai file.

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

Utilizzo della modalità Amministratore

Il Security Management Server Virtual non usa il Key Server, quindi non è possibile usare la modalità Amministratore per ottenere un bundle di chiavi da un Security Management Server Virtual. Usare la modalità Forensic per ottenere il bundle di chiavi se il client è attivato per un Security Management Server Virtual.

1. Aprire un prompt dei comandi dove si trova CMGAd e digitare **`cmgad.exe -a`**.
2. Immettere le seguenti informazioni (alcuni campi possono essere già popolati).

   Server: nome host completo del Key Server, come serverchiavi.dominio.com

   Numero di porta: la porta predefinita è 8050

   Account server: l'utente del dominio in cui è in esecuzione Key Server. Il formato è DOMINIO\Nome utente. L'utente del dominio in cui l'utilità è in esecuzione deve essere autorizzato ad effettuare il download dal Key Server

   MCID: ID della macchina, come IDmacchina.dominio.com

   DCID: prime otto cifre dell'ID dello Shield a 16 cifre

   N.B.:

   Solitamente, è sufficiente specificare l'MCID *o* il DCID. Tuttavia, se sono noti, è utile immetterli entrambi. Ogni parametro contiene informazioni diverse utilizzate da questa utilità.

   Fare clic su **Avanti**.

3. Nel campo *Passphrase*, digitare una passphrase per proteggere il file di download. La passphrase deve contenere almeno otto caratteri, di cui almeno uno alfabetico e uno numerico.

   Confermare la passphrase.

   Accettare il nome e il percorso predefiniti in cui salvare il file, oppure fare clic sui tre puntini ("...") per selezionare un percorso diverso.

   Fare clic su **Avanti**.

   Viene visualizzato un messaggio che indica che il materiale delle chiavi è stato sbloccato. È ora possibile accedere ai file.

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

16

Configurare la crittografia sul sistema operativo di un server

Abilitare la crittografia sul sistema operativo del server

N.B.:

La crittografia dei sistemi operativi del server converte la crittografia dell'utente in crittografia comune.

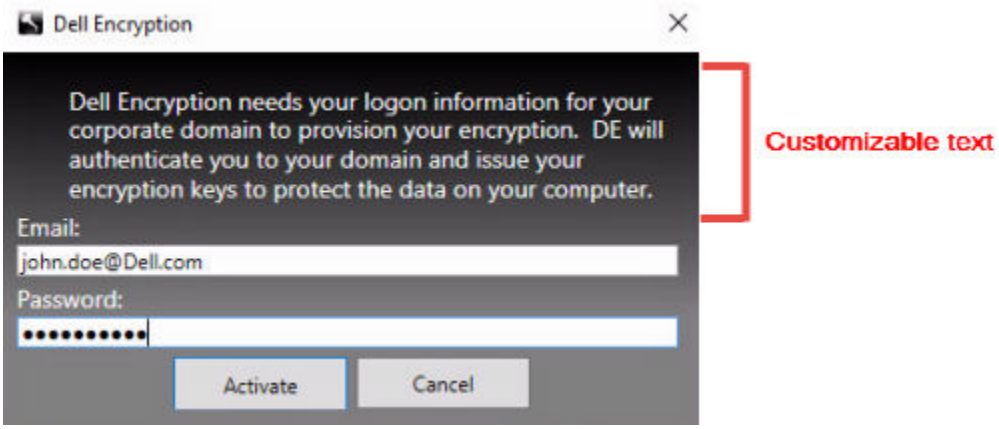
1. Eseguire l'accesso alla console di gestione come amministratore Dell.
2. Selezionare **Gruppo di endpoint** (oppure **Endpoint**), cercare l'endpoint o il gruppo di endpoint che si desidera abilitare, selezionare **Criteri di protezione**, quindi selezionare la categoria di criterio **Server Encryption**.
3. Impostare i seguenti criteri:
   - Server Encryption - **Selezionare** per abilitare la crittografia sul sistema operativo del server e i relativi criteri.
   - Crittografia SDE abilitata - **Selezionare** per attivare la crittografia SDE.
   - Crittografia abilitata - **Selezionare** per attivare la crittografia comune.
   - Credenziali Windows di protezione **-** Questo criterio è **Selezionato** per impostazione predefinita.

     Quando il criterio *Credenziali Windows di protezione* è **Selezionato** (predefinito), tutti i file nella cartella \Windows\system32\config files vengono crittografati, comprese le credenziali di Windows. Per evitare che le credenziali di Windows vengano crittografate, impostare il criterio *Credenziali Windows di protezione* su **Non selezionato**. La crittografia delle credenziali Windows avviene indipendentemente dall'impostazione del criterio *Crittografia SDE abilitata*.
4. Salvare i criteri ed eseguire il relativo commit.

Personalizzare la finestra di dialogo Accesso attivazione

La finestra di dialogo Accesso attivazione visualizza:

- Quando un utente non gestito effettua l'accesso.
- Quando l'utente seleziona Attiva Dell Encryption dal menu dell'icona Encryption, che si trova nell'area di notifica.



Configurare i criteri di Encryption External Media

Il ***computer crittografante originale*** è il computer che crittografa originariamente un dispositivo rimovibile. Quando il computer originale è un ***server protetto*** (un server con crittografia installata e attivata sul sistema operativo del server) e

il server protetto rileva per la prima volta la presenza di un dispositivo rimovibile, all'utente viene richiesto di crittografare il dispositivo rimovibile.

- I criteri di Encryption External Media controllano l'accesso dei supporti rimovibili al server, l'autenticazione, la crittografia e altre funzioni.
- I criteri di controllo delle porte influenzano i supporti rimovibili sui server protetti, per esempio, controllando l'accesso e l'utilizzo delle porte USB del server da parte di dispositivi USB.

È possibile trovare i criteri per la crittografia dei supporti rimovibili nella Management Console nel gruppo di tecnologia *Server Encryption*.

Crittografia sul sistema operativo del server e media esterni

Quando il criterio *EMS - Crittografa il supporto esterno* del server protetto è **Selezionato**, il supporto esterno è crittografato. Encryption collega il dispositivo al server protetto con la chiave di macchina e all'utente con la chiave Roaming utente del proprietario/utente del dispositivo rimovibile. Tutti i file aggiunti al dispositivo rimovibile vengono poi crittografati con quelle stesse chiavi, indipendentemente dal computer al quale viene collegato.

N.B.:

La crittografia sul sistema operativo del server converte la crittografia utente in crittografia comune, tranne che nei dispositivi rimovibili. Nei dispositivi rimovibili, la crittografia viene eseguita con la Chiave Roaming utente associata al computer.

Quando l'utente non accetta di crittografare un dispositivo rimovibile, l'accesso dell'utente al dispositivo può essere impostato su *bloccato* quando viene usato sul server protetto, *Sola lettura* mentre viene usato sul server protetto oppure *Accesso completo*. I criteri del server protetto determinano il livello di accesso ad un dispositivo rimovibile non protetto.

Quando il dispositivo rimovibile viene inserito di nuovo nel server protetto originale si verificano gli aggiornamenti del criterio.

Autenticazione e supporti esterni

I criteri del server protetto determinano la funzionalità di autenticazione.

Dopo che un dispositivo rimovibile è stato crittografato, solo il proprietario/utente può accedere al dispositivo rimovibile sul server protetto. Gli altri utenti non possono accedere ai file crittografati nel supporto rimovibile.

L'autenticazione automatica locale consente ai supporti rimovibili protetti di essere autenticati automaticamente quando vengono inseriti nel server protetto quando il proprietario di tale supporto ha eseguito l'accesso. Quando l'autenticazione automatica è disabilitata, il proprietario/utente deve eseguire l'autenticazione per accedere al dispositivo rimovibile protetto.

Se il computer crittografante originale di un dispositivo rimovibile è un server protetto, il proprietario/utente deve sempre effettuare l'accesso al dispositivo rimovibile quando lo usa su computer non crittografanti di origine, indipendentemente dalle impostazioni del criterio Encryption External Media definite negli altri computer.

Fare riferimento alla Guida dell'amministratore per informazioni sui criteri di controllo delle porte di Server Encryption e di Encryption External Media.

Sospensione della crittografia nel sistema operativo del server

La sospensione di un server crittografato impedisce l'accesso ai suoi dati crittografati dopo un riavvio. L'utente del server virtuale non può essere sospeso. Al contrario, la chiave di macchina del server crittografato è sospesa.

N.B.:

La sospensione dell'endpoint del server non sospende immediatamente il server. La sospensione si verifica alla richiesta successiva della chiave, generalmente al successivo riavvio del server.

N.B.:

Da utilizzare con cautela. La sospensione di un server crittografato potrebbe causare instabilità, a seconda delle impostazioni dei criteri e se il server protetto viene sospeso mentre è disconnesso dalla rete.

Prerequisiti

- Per sospendere un endpoint sono necessari i diritti di amministratore helpdesk, assegnati nella Management Console.
- L'amministratore deve aver effettuato l'accesso alla Management Console.

Nel riquadro sinistro della Management Console, fare clic su **Popolamenti** > **Endpoint**.

Ricercare o selezionare un hostname, quindi fare clic sulla scheda **Dettagli e azioni**.

In *Controllo dispositivo server*, fare clic su **Sospendi** quindi **Sì**.

N.B.:

Fare clic su **Ripristina** per permettere alla crittografia del server di accedere ai dati cifrati nel server dopo il riavvio.

17

Configurare l'Attivazione posposta

Encryption Client con l'attivazione posposta è diverso dall'attivazione del client di crittografia per due motivi:

Criteri di crittografia basati su dispositivo

I criteri di Encryption Client si basano sull'utente; i criteri di crittografia di Encryption Client con l'attivazione posposta si basano sul dispositivo. La crittografia utente viene convertita nella crittografia comune. Questa differenza consente all'utente di portare un dispositivo personale per utilizzarlo all'interno del dominio dell'organizzazione, mentre l'organizzazione mantiene inalterata la sicurezza gestendo centralmente i criteri di crittografia.

Attivazione

Con Encryption Client, l'attivazione è automatica. Quando con Attivazione posposta è installato, l'attivazione automatica è disattivata. Al contrario, l'utente decide se e quando attivare la crittografia.

N.B.:

Prima che lasci definitivamente l'organizzazione e mentre il suo indirizzo e-mail è ancora attivo, un utente deve eseguire Encryption Removal Agent e disinstallare il client di crittografia dal computer.

Personalizzazione dell'Attivazione posposta

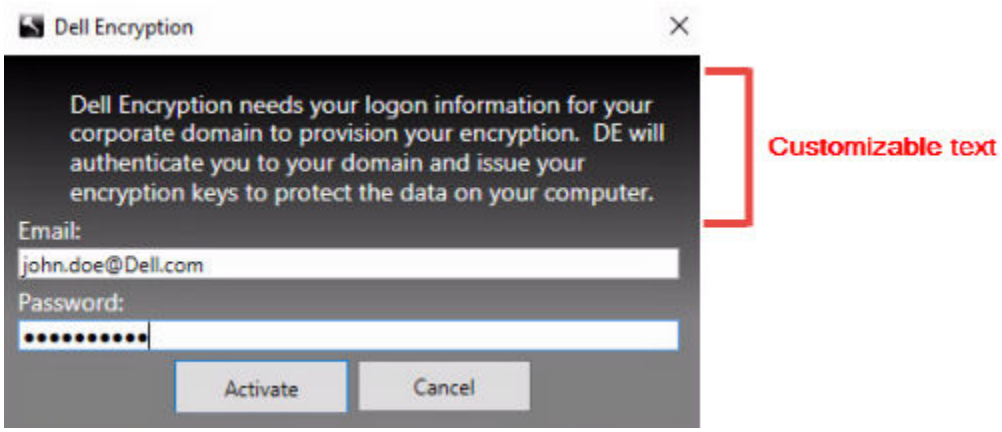
Le seguenti attività lato client consentono di personalizzare l'Attivazione posposta.

- Aggiungere una dichiarazione di non responsabilità alla finestra di dialogo Accesso attivazione
- Disattivare la riattivazione automatica (opzionale)

Aggiungere una dichiarazione di non responsabilità alla finestra di dialogo Accesso attivazione

La finestra di dialogo Accesso attivazione viene visualizzata nelle seguenti condizioni:

- Quando un utente non gestito effettua l'accesso.
- Quando l'utente seleziona Attiva Dell Encryption dal menu dell'icona Encryption, che si trova nell'area di notifica.



Preparare il computer per l'installazione

Se i dati vengono crittografati con un prodotto di crittografia non Dell, prima di procedere all'installazione del client di crittografia, decrittografare i dati utilizzando il software per la crittografia esistente, per poi disinstallarlo. Riavviare il computer se non si riavvia automaticamente.

Creare una password di Windows

Dell consiglia vivamente di creare 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.

Disinstallare le versioni precedenti del client di crittografia

Prima di disinstallare una versione precedente del client di crittografia, arrestare o sospendere la ricerca dei dati da crittografare, se necessario.

Se sul computer è in esecuzione una versione di Dell Encryption precedente alla v8.6, disinstallare il client di crittografia dalla riga di comando. Per istruzioni, vedere *Disinstallare il client di crittografia e di crittografia server*.

N.B.:

Se si intende installare l'ultima versione del client di crittografia immediatamente dopo la disinstallazione, non è necessario eseguire Encryption Removal Agent per decrittografare i file.

Per aggiornare una versione precedente del client di crittografia installata con l'Attivazione posposta, usare il programma di disinstallazione di Data Security o i programmi di installazione figlio. Questi metodi di disinstallazione sono possibili anche se il parametro OPTIN è disabilitato.

N.B.:

Se gli utenti non sono stati attivati in precedenza, il client di crittografia cancella l'impostazione del parametro OPTIN dall'archivio SDE poiché viene mantenuta da un'installazione precedente. Il client di crittografia blocca le attivazioni posposte se gli utenti hanno effettuato l'attivazione in precedenza, ma il parametro OPTIN non è impostato nell'archivio SDE.

Installare la crittografia con attivazione posposta

Per installare il client di crittografia con l'Attivazione posposta, procedere utilizzando il parametro OPTIN=1. Per ulteriori informazioni sull'installazione del client con il parametro OPTIN=1, consultare Installare la crittografia.

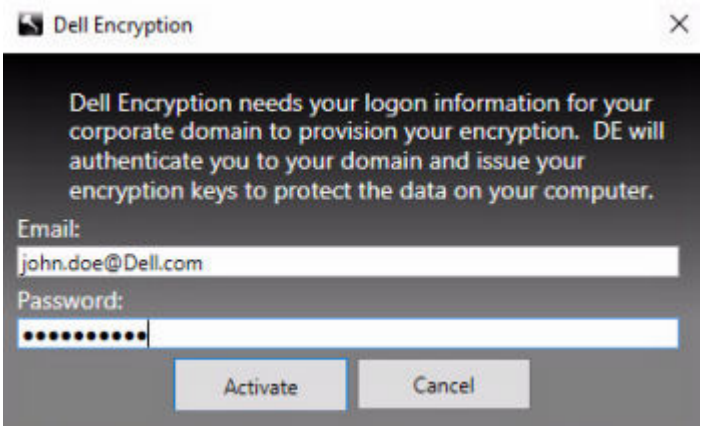
Attivare la crittografia con attivazione posposta

- L'attivazione associa un utente di dominio a un account utente locale e un computer specifico.
- Più utenti possono effettuare l'attivazione sullo stesso computer, a condizione che utilizzino account locali univoci e abbiano indirizzi e-mail di dominio univoci.
- Un utente può attivare il client di crittografia solo una volta per ogni account di dominio.

Prima di attivare il client di crittografia:

- Accedere all'account locale che si utilizza più spesso. I dati associati a questo account sono quelli che verranno crittografati.
- Connettersi alla rete dell'organizzazione.

1. Accedere alla workstation o al server.
2. Immettere l'indirizzo e-mail di dominio e la password e fare clic su **Attiva**.



N.B.:

Gli indirizzi e-mail non di dominio o personali non possono essere utilizzati per l'attivazione.

3. Fare clic su **Chiudi**.

   Il Dell Server associa il pacchetto chiavi di crittografia alle credenziali dell'utente e all'ID univoco del computer (ID del computer), creando una relazione indissolubile tra il pacchetto chiavi, il computer specifico e l'utente.

4. Riavviare il computer per iniziare la ricerca dei dati da crittografare.

N.B.:

La Management Console locale, accessibile utilizzando l'icona dell'area notifiche, mostra i criteri inviati dal server e non il criterio effettivo.

Risolvere i problemi dell'Attivazione posposta

Risolvere i problemi di attivazione

Problema: impossibile accedere a determinati file e cartelle

L'impossibilità di accedere a determinati file e cartelle è un sintomo dell'accesso con un account diverso da quello con cui l'utente ha effettuato l'attivazione.

Nella finestra di dialogo Accesso attivazione viene anche visualizzato se l'utente ha effettuato l'attivazione in precedenza.

Soluzione possibile

Disconnettersi ed effettuare nuovamente l'accesso con le credenziali dell'account attivato e provare ad accedere nuovamente ai file.

Nel raro caso in cui il client di crittografia non riesca ad autenticare l'utente, nella finestra Accesso attivazione viene richiesto all'utente di immettere le credenziali per effettuare l'autenticazione e l'accesso alle chiavi di crittografia. Per utilizzare la funzione di riattivazione automatica, le chiavi del Registro di sistema *AutoReactivation* e *AutoPromptForActivation* devono essere ENTRAMBE attivate. Anche se la funzione è attivata per impostazione predefinita, è possibile disattivarla manualmente. Per ulteriori informazioni, vedere Disattivare la riattivazione automatica.

Messaggio di errore: Autenticazione server non riuscita

Il server non è stato in grado di autenticare l'indirizzo e-mail e la password.

Soluzioni possibili

- Utilizzare l'indirizzo e-mail associato all'organizzazione. Gli indirizzi e-mail personali non possono essere utilizzati per l'attivazione.
- Immettere nuovamente l'indirizzo e-mail e la password e accertarsi che non vi siano errori di battitura.
- Chiedere all'amministratore di verificare che l'account e-mail sia attivo e non bloccato.
- Chiedere all'amministratore di reimpostare la password di dominio dell'utente.

Messaggio di errore: Errore della connessione di rete

Il client di crittografia non è riuscito a comunicare con il Dell Server.

Soluzioni possibili

- Connettersi direttamente alla rete dell'organizzazione e riprovare ad effettuare l'attivazione.
- Se per connettersi alla rete è necessario l'accesso VPN, controllare la connessione VPN e riprovare.
- Controllare l'URL del Dell Server per accertarsi che corrisponda all'URL fornito dall'amministratore.

  L'URL e altri dati immessi dall'utente nel programma di installazione sono archiviati nel registro. Controllare la precisione dei dati in [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

- Disconnettersi e riconnettersi:

  Disconnettere il computer dalla rete.

  Ricollegare alla rete.

  Riavviare il sistema.

Tentare di nuovo di connettersi alla rete.

Messaggio di errore: Server legacy non supportato

Encryption non può essere attivato con un server legacy; la versione del Dell Server deve essere la v9.1 o successiva.

Soluzione possibile

- Controllare l'URL del Dell Server per accertarsi che corrisponda all'URL fornito dall'amministratore.

  L'URL e altri dati immessi dall'utente nel programma di installazione sono archiviati nel registro.

- Controllare la precisione dei dati in [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

  Messaggio di errore: Utente di dominio già attivato

  Un secondo utente ha effettuato l'accesso al computer locale e ha tentato di effettuare l'attivazione con un account di dominio già attivato.

  Un utente può attivare il client di crittografia solo una volta per ogni account di dominio.

  Soluzione possibile

  Decrittografare e disinstallare il client di crittografia mentre è stato effettuato l'accesso come secondo utente attivato.

  Messaggio di errore: Errore del server generale

  Si è verificato un errore sul server.

  Soluzione possibile

  L'amministratore deve controllare i registri dei server per verificare che i servizi siano in esecuzione.

  L'utente deve tentare di effettuare l'attivazione in un secondo momento.

Strumenti

CMGAd

Utilizzare l'utilità CMGAd prima di avviare Encryption Removal Agent al fine di ottenere il pacchetto chiavi di crittografia. L'utilità CMGAd e le relative istruzioni si trovano nel supporto di installazione Dell (Dell-Offline-Admin-XXbit)

File di registro

In `C:\ProgramData\Dell\Dell Data Protection\Encryption`, cercare il file di registro denominato **CmgSysTray**.

Cercare la frase "Manual activation result".

Il codice di errore è sulla stessa riga, seguito da " status = "; lo stato indica cosa non ha funzionato.

18

Risoluzione dei problemi

Tutti i client - Risoluzione dei problemi

- I file di registro del programma di installazione principale di **Master Suite** si trovano nel percorso `C:\ProgramData\Dell\Dell Data Protection\Installer`.
- Windows crea **file di registro di installazione dei programmi di installazione figlio** univoci per l'utente che ha effettuato l'accesso a %temp%, e si trovano nel percorso `C:\Users\<Nomeutente>\AppData\Local\Temp`.
- Windows crea file di registro per i prerequisiti del client, come ad esempio Visual C++, per l'utente che ha effettuato l'accesso a %temp%, e si trovano nel percorso `C:\Users\<Nomeutente>\AppData\Local\Temp`. Ad esempio, `C:\Users\<Nomeutente>\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log`
- Seguire le istruzioni in http://msdn.microsoft.com per verificare la versione di Microsoft .Net installata nel computer destinato all'installazione.

  Andare a https://www.microsoft.com/en-us/download/details.aspx?id=30653 per scaricare la versione completa di Microsoft .Net Framework 4.5.2 o versione successiva.
- Consultare *questo documento* se nel computer destinato all'installazione è (o è stato in passato) installato Dell Access. Dell Access non è compatibile con questa suite di prodotti.

Tutti i client - Stato di protezione

In Dell Security Management Server v9.8.2, è stato implementato un nuovo metodo per rilevare lo stato protetto di un dispositivo. In precedenza, l'area di stato protetta dell'endpoint nella dashboard della Management Console denotava solo lo stato della crittografia a seconda del dispositivo.

Ora, con Dell Server v9.8.2, viene indicato lo stato protetto, se uno di questi criteri viene soddisfatto:

- Advanced Threat Prevention è installato e abilitato.
- Protezione Web o Firewall client sono installati e il criterio di uno dei due è attivato.
- Self-Encrypting Drive Manager è installato, abilitato e la PBA è attiva.
- Full Disk Encryption è installato, abilitato e la PBA è attiva.
- BitLocker Manager è installato, abilitato e la crittografia è stata completata.
- Dell Encryption (Mac) è installato e abilitato e la *Crittografia tramite FileVault per Mac* è stata applicata.
- Dell Encryption (Windows) è installato e attivato, la crittografia basata su criteri è stata impostata per l'endpoint e le ricerche del dispositivo sono completate.

Risoluzione dei problemi di Dell Encryption (client e server)

Attivazione nel sistema operativo di un server

Quando la crittografia viene installata nel sistema operativo di un server, l'attivazione richiede due fasi di attivazione: attivazione iniziale e attivazione dispositivo.

Risoluzione dei problemi di attivazione iniziale

L'attivazione iniziale non riesce quando:

- Un UPN valido non può essere costruito usando le credenziali fornite.
- Le credenziali non sono reperibili nell'insieme di credenziali aziendale.
- Le credenziali usate per attivare non sono le credenziali dell'amministratore di dominio.

Messaggio di errore: nome utente sconosciuto o password errata

Il nome utente o la password non corrispondono.

Soluzione possibile: cercare nuovamente di effettuare l'accesso accertandosi di digitare il nome utente e la password in modo corretto.

Messaggio di errore: attivazione non riuscita perché l'account utente non ha diritti di amministratore di dominio.

Le credenziali usate per effettuare l'attivazione non hanno diritti di amministratore di dominio, oppure il nome utente dell'amministratore non era nel formato UPN.

Soluzione possibile**:** nella finestra di dialogo Attivazione, immettere le credenziali di un amministratore di dominio in formato UPN.

Messaggio di errore: impossibile stabilire una connessione con il server.

oppure

`The operation timed out.`

Server Encryption non è riuscito a comunicare con la porta 8449 su HTTPS con il Dell Server.

Soluzioni possibili

- Connettersi direttamente con la propria rete e riprovare ad effettuare l'attivazione.
- Se la connessione è tramite VPN, provare a connettersi direttamente alla rete e riprovare ad effettuare l'attivazione.
- Controllare l'URL del Dell Server per accertarsi che corrisponda all'URL fornito dall'amministratore. L'URL e altri dati immessi dall'utente nel programma di installazione sono archiviati nel registro. Controllare la precisione dei dati in [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].
- Disconnettere il server dalla rete. Riavviare il server e riconnetterlo alla rete.

Messaggio di errore: attivazione non riuscita perché il server non è in grado di supportare questa richiesta.

Soluzioni possibili

- Server Encryption non può essere attivato con un server legacy; la versione del Dell Server deve essere la 9.1 o successiva. Se necessario, aggiornare il Dell Server alla versione 9.1 o successiva.
- Controllare l'URL del Dell Server per accertarsi che corrisponda all'URL fornito dall'amministratore. L'URL e altri dati immessi dall'utente nel programma di installazione sono archiviati nel registro.
- Controllare la precisione dei dati in [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].

Processo di attivazione iniziale

Il diagramma seguente illustra una attivazione iniziale con esito positivo.

Il processo di attivazione iniziale della crittografia dei sistemi operativi del server richiede che un utente acceda al server in tempo reale. L'utente può essere di qualsiasi tipo: utente di dominio o non di dominio, connesso al desktop in remoto o interattivo, purché abbia accesso a credenziali di amministratore di dominio.

Viene visualizzata la finestra di dialogo di attivazione quando si verifica uno dei due workflow:

- Un nuovo utente (non gestito) effettua l'accesso al computer.
- Quando un nuovo utente fa clic con il tasto destro del mouse sull'icona di *crittografia* nell'area di notifica e seleziona *Attiva Dell Encryption*.

  Il processo di attivazione iniziale è come segue:

1. Effettuare l'accesso.
2. Quando viene rilevato un nuovo utente (non gestito), viene visualizzata la finestra di dialogo *Attiva*. Fare clic su **Annulla**.
3. Aprire la finestra Informazioni sulla crittografia del server per confermare che è in esecuzione in modalità server.
4. Fare clic con il tasto destro del mouse sull'icona di *crittografia* nell'area di notifica e selezionare *Attiva Dell Encryption*.
5. Immettere le credenziali di amministratore di dominio nella finestra di dialogo Attiva.

   N.B.:

   Il requisito per le credenziali di amministratore di dominio è una misura di sicurezza che impedisce di implementare la crittografia dei sistemi operativi per server in ambienti server non supportati. Per disabilitare la richiesta di credenziali di amministratore di dominio, consultare Prima di iniziare.
6. Il Dell Server controlla le credenziali nell'insieme di credenziali aziendale (Active Directory o equivalente) per verificare che le credenziali siano credenziali di amministratore di dominio.
7. Un UPN è costruito usando le credenziali.

8. Con l'UPN, il Dell Server crea un nuovo account utente per l'utente virtuale del server e memorizza le credenziali nell'insieme di credenziali del Dell Server.

   L'**account utente virtuale del server** è ad uso esclusivo del client di crittografia. Viene utilizzato per l'autenticazione con il server, per gestire le chiavi di crittografia comune e per ricevere aggiornamenti dei criteri.

   N.B.:

   La password e l'autenticazione DPAPI sono disabilitate per tale account in modo che *solo* l'utente virtuale del server possa accedere alle chiavi di crittografia nel computer. L'account non corrisponde a nessun altro account utente nel computer o nel dominio.
9. Quando l'attivazione è completata, l'utente riavvia il sistema, cosa che lancia la seconda fase, l'autenticazione e l'attivazione del dispositivo.

Risoluzione dei problemi di autenticazione e attivazione del dispositivo

L'attivazione del dispositivo non riesce quando:

- L'attivazione iniziale non è riuscita.
- Non è stato possibile stabilire la connessione con il server.
- Non è stato possibile convalidare il certificato di attendibilità.

Dopo l'attivazione, quando il computer viene riavviato, la crittografia per i sistemi operativi del server effettua automaticamente l'accesso come utente del server virtuale e richiede la chiave di computer al Dell Server. Questo avviene anche prima che qualsiasi utente possa effettuare l'accesso.

- Aprire la finestra di dialogo Informazioni per confermare che la crittografia per i sistemi operativi del server è autenticata e in modalità server.
- Se l'ID di Encryption client è rosso, la crittografia non è stata ancora attivata.
- Nella Management Console, la versione di un server in cui sia installato Server Encryption è elencata come *Shield per Server*.
- Se il recupero della chiave di computer non riesce a causa di un errore di rete, Server Encryption si registra nel sistema operativo per le notifiche di rete.
- Se il recupero della chiave di computer non riesce:
  - L'accesso dell'utente virtuale del server viene ancora eseguito.
  - Impostare il criterio *Intervallo tra tentativi a seguito di un errore di rete* per effettuare tentativi di recupero della chiave in un intervallo di tempo.

    Per dettagli sul criterio di *Intervallo tra tentativi a seguito di un errore di rete*, fare riferimento ad AdminHelp, disponibile nella Management console.

Autenticazione e attivazione del dispositivo

Il diagramma seguente illustra l'autenticazione e l'attivazione del dispositivo corrette.

1. Una volta riavviato dopo una attivazione iniziale completata, un computer con Server Encryption si autentica automaticamente usando l'account utente virtuale del server ed esegue il client di crittografia in modalità Server.
2. Il computer controlla lo stato di attivazione del dispositivo con il Dell Server:
   - Se il computer non ha eseguito l'attivazione del dispositivo in precedenza, il Dell Server assegna al computer un MCID, un DCID e un certificato di attendibilità e memorizza tutte le informazioni nell'insieme di credenziali del Dell Server.
   - Se il computer ha eseguito l'attivazione del dispositivo in precedenza, il Dell Server verifica il certificato di attendibilità.
3. Dopo che il Dell Server ha assegnato il certificato di attendibilità al server, il server può accedere alle chiavi di cifratura.
4. L'attivazione del dispositivo è stata completata.

   N.B.:

   Quando è in esecuzione in modalità Server, per accedere alle chiavi di crittografia il client di crittografia deve avere accesso allo stesso certificato utilizzato per l'attivazione del dispositivo.

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.

Uso della riga di comando di WSScan

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r]
[-u[a][-|v]] [-d<delimeter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

Opzione	Significato
Unità	Unità da sottoporre a scansione. Se non è specificato, l'impostazione predefinita è tutte le unità fisse locali. Può essere un'unità di rete mappata.
-ta	Eseguire la scansione di tutte le unità
-tf	Eseguire la scansione delle unità fisse (predefinita)
-tr	Eseguire la scansione delle unità rimovibili
-tc	Eseguire la scansione di CDROM/DVDROM
-s	Operazione invisibile all'utente
-o	Percorso del file di output
-a	Aggiungere al file di output. Il comportamento predefinito tronca il file di output.
-f	Identificatore di formato rapporto (Rapporto, Fisso, Delimitato)
-r	Eseguire WSScan senza i privilegi di amministratore. **In questa modalità alcuni file potrebbero non essere visibili.**
-u	Includere file non crittografati nel file di output. Questa opzione è sensibile all'ordine: “u” deve essere la prima, “a” deve essere la seconda (oppure omessa), “-” o “v” deve essere l'ultima.

Opzione	Significato
-u-	Includere solo file non crittografati nel file di output.
-ua	Riportare anche i file non crittografati, ma usare tutti i criteri utente per visualizzare il campo “should” (deve).
-ua-	Riportare solo i file non crittografati, ma usare tutti i criteri utente per visualizzare il campo “should” (deve).
-uv	Riportare solo i file non crittografati che violano il criterio (Is=No / Should=Y)
-uav	Riportare solo i file non crittografati che violano il criterio (Is=No / Should=Y), usando tutti i criteri utente.
-d	Specifica cosa usare come separatore di valori per l'output delimitato
-q	Specifica i valori che devono essere racchiusi tra virgolette per l'output delimitato
-e	Includere i campi di crittografia estesi nell'output delimitato
-x	Escludere la directory dalla scansione. Sono consentite più esclusioni.
-y	Sospensione (in millisecondi) tra directory. Questa opzione dà come risultato scansioni più lente, ma potenzialmente una CPU più reattiva.

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**"

Output	Significato
	RIJNDAEL 128 RIJNDAEL 256 AES-128 AES-256 3DES

Usare WSProbe

La Probing Utility può essere usata con tutte le versioni di crittografia, ad eccezione dei criteri di Encryption External Media. Utilizzare la Probing Utility per:

- Sottoporre a scansione o pianificare la scansione di un computer crittografato. La Probing Utility rispetta il criterio di priorità scansione workstation.
- Disabilitare temporaneamente o abilitare di nuovo l'Elenco Application Data Encryption dell'utente corrente.
- Aggiungere o rimuovere nomi di processi dall'elenco privilegiato.
- Risolvere i problemi seguendo le istruzioni di Dell ProSupport.

Metodi per la crittografia dei dati

Se si specificano i criteri per crittografare i dati nei dispositivi Windows, è possibile utilizzare uno dei metodi seguenti:

- Il primo metodo consiste nell'accettare il comportamento predefinito del client. Se si specificano le cartelle in Cartelle crittografate comuni o Cartelle crittografate utente, o si seleziona Crittografa “Documenti”, Crittografa cartelle personali Outlook, Crittografa file temporanei, Crittografa file temporanei di Internet o Crittografa file di paging Windows, i file interessati vengono crittografati quando vengono creati o, se sono stati creati da un utente non gestito, quando un utente gestito effettua l'accesso. Il client esegue la scansione anche di cartelle specificate nei o correlate a questi criteri per l'eventuale crittografia/decrittografia quando una cartella viene rinominata o quando il client riceve modifiche a questi criteri.
- Inoltre, è possibile impostare Esegui scansione workstation all'accesso su Selezionato. Se Esegui scansione workstation all'accesso è impostato su Selezionato, quando un utente effettua l'accesso il client confronta il modo in cui sono crittografati i file nelle cartelle attualmente, e precedentemente, crittografate con i criteri dell'utente e apporta eventuali modifiche necessarie.
- Per crittografare i file che soddisfano i criteri di crittografia ma sono stati creati prima che venissero attivati i criteri di crittografia, e se non si desidera che le prestazioni siano influenzate da scansioni frequenti, è possibile usare questa utilità per eseguire o pianificare la scansione del computer.

Prerequisiti

- Il dispositivo Windows con il quale lavorare deve essere crittografato.
- L'utente con il quale lavorare deve aver effettuato l'accesso.

Usare la Probing Utility

WSProbe.exe si trova nel supporto di installazione.

Sintassi

```
wsprobe [path]
wsprobe [-h]
wsprobe [-f path]
wsprobe [-u n] [-x process_names] [-i process_names]
```

Parametri

Parametro	Per
path	Specificare facoltativamente un percorso specifico nel dispositivo da sottoporre a scansione per eventuale crittografia/decrittografia. Se non viene specificato un percorso, l'utilità sottopone a scansione tutte le cartelle relative ai criteri di crittografia.

Parametro	Per
-h	Visualizzare la guida della riga di comando.
-f	Risolvere i problemi seguendo le istruzioni di Dell ProSupport
-u	Disabilitare temporaneamente o abilitare di nuovo l'Elenco Application Data Encryption dell'utente. L'elenco è valido solo se Crittografia abilitata è selezionato per l'utente corrente. Specificare 0 per disabilitare o 1 per abilitare di nuovo. Il criterio corrente attivo per l'utente viene ripristinato all'accesso successivo.
-x	Aggiungere nomi di processi all'elenco privilegiato. I nomi di processi del computer e del programma di installazione in questo elenco, oltre a quelli aggiunti utilizzando questo parametro o HKLM\Software\CREDANT\CMGShield\EUWPrivilegedList, vengono ignorati se specificato nell'Elenco Application Data Encryption. Separare i nomi di processi con le virgole. Se l'elenco comprende uno o più spazi, racchiudere l'elenco tra virgolette.
-i	Rimuovere i nomi di processi aggiunti in precedenza all'elenco privilegiato (non è possibile rimuovere nomi di processi hardcoded). Separare i nomi di processi con le virgole. Se l'elenco comprende uno o più spazi, racchiudere l'elenco tra virgolette.

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. Per istruzioni, consultare Creare un file di registro dell'Encryption Removal Agent (facoltativo).
- **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.

Risoluzione dei problemi SED

Usare il Codice di accesso iniziale

- Questo criterio viene utilizzato per eseguire l'accesso a un computer se l'accesso di rete non è disponibile, Ovvero se non è possibile accedere al Dell Server e AD. Usare il criterio *Codice di accesso iniziale* solo in caso di stretta necessità. Dell sconsiglia di eseguire l'accesso con questo metodo. Il criterio *Codice di accesso iniziale* non fornisce lo stesso livello di sicurezza del tradizionale metodo di autenticazione con accesso tramite nome utente, dominio e password.

  Oltre a essere meno sicuro, questo metodo di accesso non consente di registrare nel Dell Server l'attivazione di un utente finale se tale attivazione viene eseguita mediante il *Codice di accesso iniziale*. Inoltre, se le domande per la risoluzione autonoma dei problemi e l'inserimento della password non risultano utili, non è possibile generare un codice di risposta dal Dell Server per l'utente.

- Il *Codice di accesso iniziale* può essere utilizzato **una volta** sola, subito dopo l'attivazione. Dopo l'accesso di un utente finale, il *Codice di accesso iniziale* non sarà più disponibile. Il primo accesso al dominio eseguito dopo l'immissione del *Codice di accesso iniziale* viene memorizzato nella cache e il valore del campo *Codice di accesso iniziale* non viene più visualizzato.
- Il *Codice di accesso iniziale* viene visualizzato **solo** nelle condizioni seguenti:
  - Un utente non è mai stato attivato all'interno di PBA.
  - Il client non dispone di connettività alla rete o al Dell Server.

Usare il Codice di accesso iniziale

1. Impostare un valore per il criterio **Codice di accesso iniziale** nella Management Console.
2. Salvare il criterio ed eseguire il relativo commit.
3. Avviare il computer locale.
4. Quando viene visualizzata la schermata del codice di accesso, immettere il **Codice di accesso iniziale**.
5. Fare clic sulla **freccia blu**.
6. Quando viene visualizzata la schermata Note legali, fare clic su **OK**.
7. Accedere a Windows con le credenziali dell'utente per questo computer. Queste credenziali devono far parte del dominio.
8. Dopo aver eseguito l'accesso, aprire Data Security Console e verificare che l'utente PBA sia stato creato correttamente.

   Fare clic su **Registro** nel menu principale e cercare il messaggio *Utente PBA di <DOMAIN\Username> creato*, che indica il buon esito del processo.
9. Arrestare e riavviare il sistema.
10. Nella schermata di accesso, immettere nome utente, dominio e password utilizzati in precedenza per accedere a Windows.

    Il formato del nome utente deve corrispondere a quello utilizzato durante la creazione dell'utente PBA. Pertanto, se è stato usato il formato DOMINIO/nome utente, è necessario inserire DOMINIO/nome utente come nome utente.
11. Quando viene visualizzata la schermata Note legali, fare clic su **Accedi**.

    Windows viene quindi avviato ed è possibile usare normalmente il computer.

Come creare un file di registro PBA per la risoluzione dei problemi

- Potrebbe essere necessario usare un file di registro PBA per la risoluzione di problemi relativi a PBA, ad esempio:
  - Non è possibile visualizzare l'icona della connettività di rete, sebbene sia presente una connettività di rete. Il file di registro contiene informazioni DHCP per la soluzione del problema.
  - Non è possibile visualizzare l'icona di connessione al Dell Server. Il file di registro contiene informazioni che consentono di individuare i problemi di connettività.
  - L'autenticazione non viene eseguita sebbene vengano immesse le credenziali corrette. Il file di registro usato con i registri del server del Dell Server consente di diagnosticare il problema.

Acquisire i registri all'avvio nella PBA (PBA legacy)

1. Creare una cartella all'interno di un'unità USB, quindi nominarla `\CredantSED`, nel livello radice dell'unità USB.
2. Creare un file denominato actions.txt e posizionarlo nella cartella **`\CredantSED.`**
3. In actions.txt, aggiungere la riga:

   ```
   get logs
   ```

4. Salvare e chiudere i file.

   Non inserire l'unità USB mentre il computer è spento. Se l'unità USB è già inserita durante lo stato di arresto, rimuoverla.

5. L'accensione del computer riproduce il problema. Inserire l'unità USB nel computer da cui raccogliere i registri durante questa fase.
6. Una volta inserita l'unità USB, attendere 5-10 secondi, quindi rimuovere l'unità.

   Viene creato un file credpbaenv.tgz nella cartella **\CredantSED** contenente i file di registro necessari.

Acquisire i registri all'avvio nella PBA (PBA UEFI)

1. Creare un file denominato **PBAErr.log** a livello root dell'unità USB.
2. Inserire l'unità USB **prima** di accendere il computer.
3. Rimuovere l'unità USB **dopo** aver riprodotto il problema che richiede i registri.

Il file PBAErr.log viene aggiornato e scritto in tempo reale.

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.

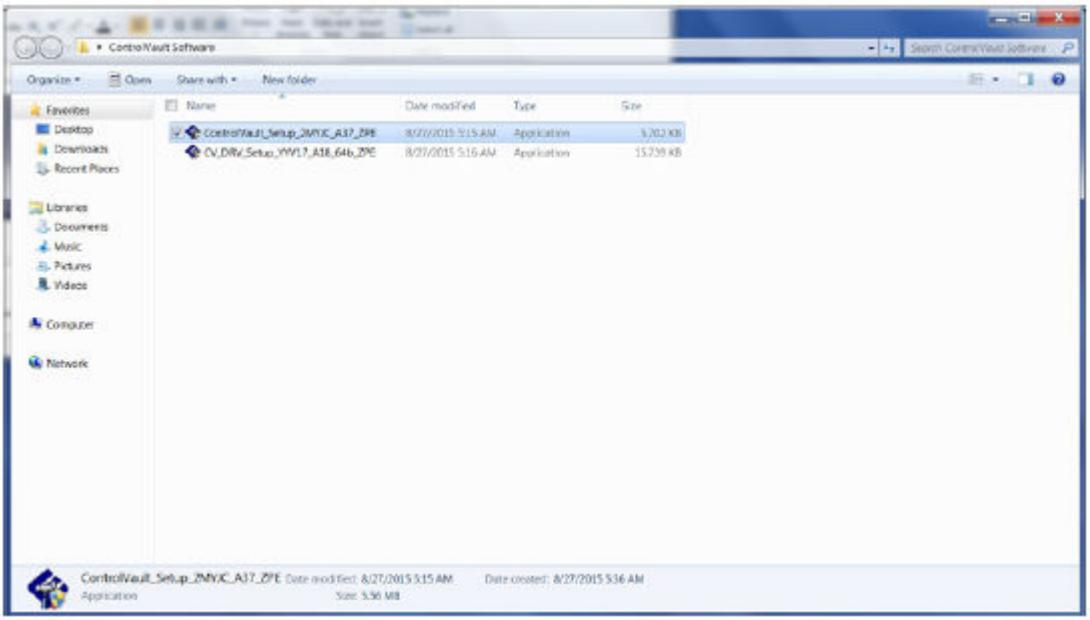
10. Cliccare su **Avanti** per l'installazione dei driver nel percorso predefinito `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Selezionare l'opzione **Completata** e cliccare su **Avanti**.
12. Cliccare su **Installa** per avviare l'installazione dei driver.
13. È possibile, 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

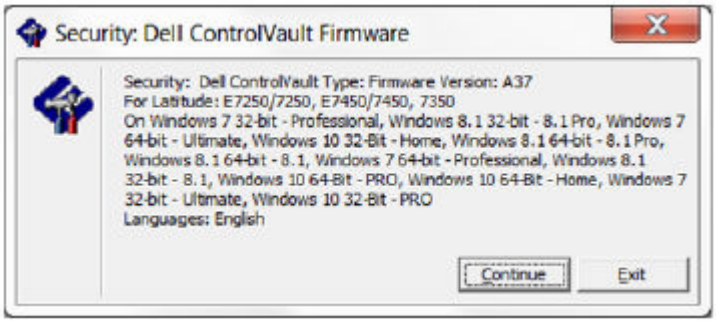
- Device Manager avrà un dispositivo Dell ControlVault (e altri dispositivi) a seconda del sistema operativo e della configurazione dell'hardware.

Installare il firmware di Dell ControlVault

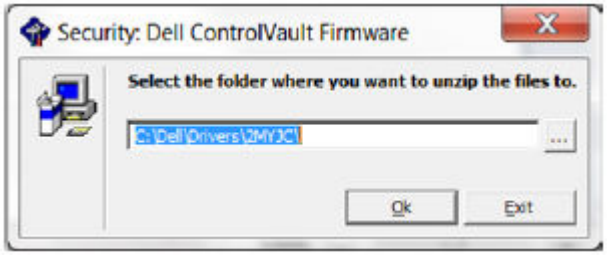
1. Passare alla cartella in cui è stato scaricato il file di installazione del firmware.



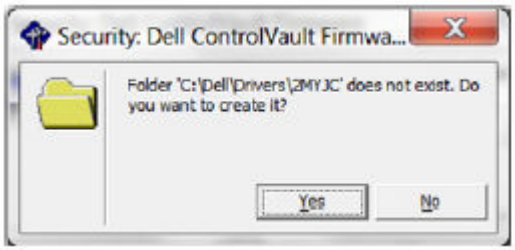
2. Cliccare due volte sul firmware di Dell ControlVault per avviare il file eseguibile autoestraente.
3. Cliccare su **Continua** per iniziare.



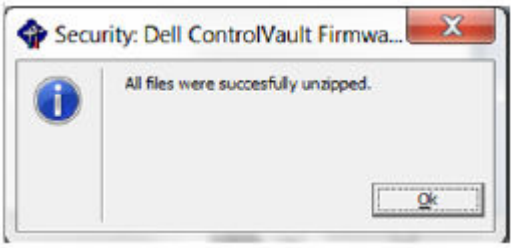
4. Cliccare su **OK** per decomprimere i file del driver nel percorso predefinito `C:\Dell\Drivers\<New Folder>`.



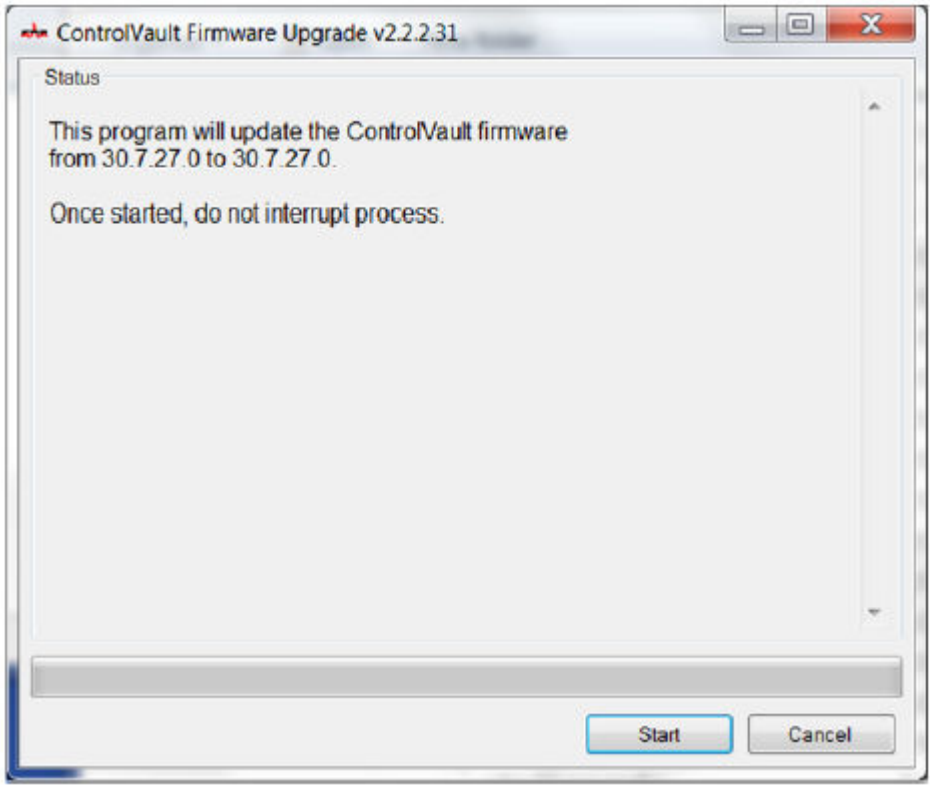
5. Cliccare su **Sì** per consentire la creazione di una nuova cartella.



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.

Computer UEFI

Risoluzione dei problemi di connessione di rete

- Per eseguire l'autenticazione di preavvio in un computer con firmware UEFI, la modalità PBA deve disporre della connettività di rete. Per impostazione predefinita, i computer con firmware UEFI non dispongono di connettività di rete fino al caricamento del sistema operativo, che avviene dopo la modalità PBA. Se la procedura per computer delineata in Configurazione di preinstallazione per computer UEFI ha esito positivo e la configurazione avviene correttamente, l'icona della connessione di rete viene visualizzata nella schermata dell'autenticazione di preavvio quando il computer è connesso alla rete.

- Se l'icona della connessione di rete non viene ancora visualizzata durante l'autenticazione di preavvio, verificare che il cavo di rete sia collegato al computer. Riavviare il sistema per riavviare la modalità PBA nel caso in cui il cavo non sia collegato o sia allentato.

TPM e BitLocker

Codici di errore di TPM e BitLocker

Costante/valore	Descrizione
TPM_E_ERROR_MASK 0x80280000	Maschera per la conversione di errori hardware TPM in errori di Windows.
TPM_E_AUTHFAIL 0x80280001	Autenticazione non riuscita.
TPM_E_BADINDEX 0x80280002	Indice PCR, DIR o di altre registrazioni non corretto.
TPM_E_BAD_PARAMETER 0x80280003	Uno o più parametri sono errati.
TPM_E_AUDITFAILURE 0x80280004	L'operazione è stata completata ma il relativo controllo non è riuscito.
TPM_E_CLEAR_DISABLED 0x80280005	Il flag di disattivazione della cancellazione è impostato. Per le operazioni di cancellazione è necessario l'accesso fisico.
TPM_E_DEACTIVATED 0x80280006	Attivare il TPM.
TPM_E_DISABLED 0x80280007	Abilitare il TPM.
TPM_E_DISABLED_CMD 0x80280008	Comando di destinazione disabilitato.

Costante/valore	Descrizione
TPM_E_FAIL 0x80280009	Operazione non riuscita.
TPM_E_BAD_ORDINAL 0x8028000A	Ordinale sconosciuto o incoerente.
TPM_E_INSTALL_DISABLED 0x8028000B	Installazione del proprietario disabilitata.
TPM_E_INVALID_KEYHANDLE 0x8028000C	Impossibile interpretare l'handle della chiave.
TPM_E_KEYNOTFOUND 0x8028000D	L'handle della chiave punta a una chiave non valida.
TPM_E_INAPPROPRIATE_ENC 0x8028000E	Schema di crittografia non accettabile.
TPM_E_MIGRATEFAIL 0x8028000F	Autorizzazione della migrazione non riuscita.
TPM_E_INVALID_PCR_INFO 0x80280010	Impossibile interpretare le informazioni PCR.
TPM_E_NOSPACE 0x80280011	Spazio insufficiente per caricare la chiave.
TPM_E_NOSRK 0x80280012	Nessuna chiave radice di archiviazione (SRK) impostata.
TPM_E_NOTSEALED_BLOB 0x80280013	BLOB crittografato non valido o non creato da questo TPM.
TPM_E_OWNER_SET 0x80280014	Un proprietario del TPM (Trusted Platform Module) esiste già.
TPM_E_RESOURCES 0x80280015	TPM: risorse interne insufficienti per eseguire l'azione richiesta.
TPM_E_SHORTRANDOM 0x80280016	Stringa casuale troppo breve.
TPM_E_SIZE 0x80280017	TPM: spazio insufficiente per eseguire l'operazione.
TPM_E_WRONGPCRVAL 0x80280018	Il valore PCR denominato non corrisponde al valore PCR corrente.
TPM_E_BAD_PARAM_SIZE 0x80280019	Valore non corretto dell'argomento paramSize del comando.

Costante/valore	Descrizione
TPM_E_SHA_THREAD 0x8028001A	Nessun thread SHA-1 esistente.
TPM_E_SHA_ERROR 0x8028001B	Impossibile continuare il calcolo. Errore rilevato dal thread SHA-1 esistente.
TPM_E_FAILEDSELFTEST 0x8028001C	Errore segnalato dal dispositivo hardware TPM durante il test automatico interno. Provare a riavviare il computer per risolvere il problema. Se il problema persiste, potrebbe essere necessario sostituire l'hardware TPM o la scheda madre.
TPM_E_AUTH2FAIL 0x8028001D	Impossibile eseguire l'autorizzazione. Autorizzazione per la seconda chiave della funzione a due chiavi non riuscita.
TPM_E_BADTAG 0x8028001E	Il valore del tag inviato al comando non è valido.
TPM_E_IOERROR 0x8028001F	Errore I/O durante la trasmissione delle informazioni al TPM.
TPM_E_ENCRYPT_ERROR 0x80280020	Errore durante il processo di crittografia.
TPM_E_DECRYPT_ERROR 0x80280021	Impossibile completare il processo di decrittografia.
TPM_E_INVALID_AUTHHANDLE 0x80280022	Handle non valido.
TPM_E_NO_ENDORSEMENT 0x80280023	Per il TPM non è installata alcuna chiave di verifica dell'autenticità.
TPM_E_INVALID_KEYUSAGE 0x80280024	Utilizzo di una chiave non consentito.
TPM_E_WRONG_ENTITYTYPE 0x80280025	Il tipo dell'entità inviata non è consentito.
TPM_E_INVALID_POSTINIT 0x80280026	Sequenza del comando non corretta. La sequenza corretta è TPM_Init e successivamente TPM_Startup.
TPM_E_INAPPROPRIATE_SIG 0x80280027	Impossibile inserire informazioni DER aggiuntive nei dati firmati.
TPM_E_BAD_KEY_PROPERTY 0x80280028	Le proprietà della chiave nei TPM_KEY_PARM non sono supportate dal TPM.
TPM_E_BAD_MIGRATION 0x80280029	Proprietà di migrazione della chiave non corrette.
TPM_E_BAD_SCHEME	Firma o schema di crittografia per la chiave non corretto o non consentito in questa situazione.

Costante/valore	Descrizione
0x8028002A	
TPM_E_BAD_DATASIZE 0x8028002B	Dimensioni del parametro relativo ai dati o al BLOB non valide o incoerenti con la chiave a cui si fa riferimento.
TPM_E_BAD_MODE 0x8028002C	Parametro relativo alla modalità non valido, ad esempio capArea o subCapArea per TPM_GetCapability, phsicalPresence per TPM_PhysicalPresence o migrationType per TPM_CreateMigrationBlob.
TPM_E_BAD_PRESENCE 0x8028002D	Valore errato dei bit physicalPresence o physicalPresenceLock.
TPM_E_BAD_VERSION 0x8028002E	TPM: impossibile eseguire questa versione della caratteristica.
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	TPM: sessioni di trasporto incapsulate non consentite.
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	TPM: costruzione del controllo non riuscita. Il comando sottostante ha restituito un errore.
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	TPM: costruzione del controllo non riuscita. Il comando sottostante è stato eseguito correttamente.
TPM_E_NOTRESETABLE 0x80280032	Tentativo di reimpostazione di una registrazione PCR priva dell'attributo necessario per questa operazione.
TPM_E_NOTLOCAL 0x80280033	Tentativo di reimpostazione di una registrazione PCR per la quale la località e il modificatore di località non devono far parte del trasporto del comando.
TPM_E_BAD_TYPE 0x80280034	BLOB di creazione dell'identità digitato non correttamente.
TPM_E_INVALID_RESOURCE 0x80280035	Il tipo di risorsa identificato durante il salvataggio del contesto non corrisponde al tipo della risorsa effettiva.
TPM_E_NOTFIPS 0x80280036	TPM: tentativo di esecuzione di un comando disponibile solo in modalità FIPS.
TPM_E_INVALID_FAMILY 0x80280037	Tentativo di utilizzare un ID famiglia non valido da parte del comando.
TPM_E_NO_NV_PERMISSION 0x80280038	L'autorizzazione per la modifica dell'archivio non volatile non è disponibile.
TPM_E_REQUIRES_SIGN 0x80280039	Per l'operazione è necessario un comando firmato.
TPM_E_KEY_NOTSUPPORTED 0x8028003A	Operazione errata per il caricamento di una chiave non volatile.

Costante/valore	Descrizione
TPM_E_AUTH_CONFLICT 0x8028003B	Per il BLOB NV_LoadKey è necessaria l'autorizzazione del proprietario e del BLOB.
TPM_E_AREA_LOCKED 0x8028003C	Area non volatile bloccata e di sola lettura.
TPM_E_BAD_LOCALITY 0x8028003D	Località non corretta per l'operazione desiderata.
TPM_E_READ_ONLY 0x8028003E	L'area non volatile è di sola lettura e non può essere scritta.
TPM_E_PER_NOWRITE 0x8028003F	Nessuna protezione da scrittura per l'area non volatile.
TPM_E_FAMILYCOUNT 0x80280040	Valore del conteggio delle famiglie non corrispondente.
TPM_E_WRITE_LOCKED 0x80280041	Scrittura già eseguita nell'area non volatile.
TPM_E_BAD_ATTRIBUTES 0x80280042	Conflitto tra attributi dell'area non volatile.
TPM_E_INVALID_STRUCTURE 0x80280043	Tag e versione della struttura non validi o incoerenti.
TPM_E_KEY_OWNER_CONTROL 0x80280044	La chiave è sotto il controllo del proprietario del TPM e può essere rimossa solo da quest'ultimo.
TPM_E_BAD_COUNTER 0x80280045	Handle del contatore non corretto.
TPM_E_NOT_FULLWRITE 0x80280046	La scrittura non rappresenta una scrittura completa dell'area.
TPM_E_CONTEXT_GAP 0x80280047	L'interruzione tra conteggi di contesti salvati è troppo ampia.
TPM_E_MAXNVWRITES 0x80280048	È stato superato il numero massimo di scritture non volatili senza proprietario.
TPM_E_NOOPERATOR 0x80280049	Nessun valore impostato per AuthData dell'operatore.
TPM_E_RESOURCEMISSING 0x8028004A	La risorsa a cui il contesto fa riferimento non è caricata.
TPM_E_DELEGATE_LOCK 0x8028004B	Amministrazione delegata bloccata.

Costante/valore	Descrizione
TPM_E_DELEGATE_FAMILY 0x8028004C	Tentativo di gestione di una famiglia diversa da quella delegata.
TPM_E_DELEGATE_ADMIN 0x8028004D	La gestione della tabella delle deleghe non è abilitata.
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	Comando eseguito al di fuori di una sessione di trasporto esclusiva.
TPM_E_OWNER_CONTROL 0x8028004F	Tentativo di salvataggio di una chiave la cui rimozione è controllata dal proprietario.
TPM_E_DAA_RESOURCES 0x80280050	Nessuna risorsa disponibile per il comando DAA per l'esecuzione del comando.
TPM_E_DAA_INPUT_DATA0 0x80280051	Verifica di coerenza per il parametro DAA inputData0 non riuscita.
TPM_E_DAA_INPUT_DATA1 0x80280052	Verifica di coerenza per il parametro DAA inputData1 non riuscita.
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	Verifica di coerenza per DAA_issuerSettings non riuscita.
TPM_E_DAA_TPM_SETTINGS 0x80280054	Verifica di coerenza per DAA_tpmSpecific non riuscita.
TPM_E_DAA_STAGE 0x80280055	Processo imprevisto indicato dal comando DAA inviato.
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	Incoerenza rilevata dalla verifica di validità dell'autorità.
TPM_E_DAA_WRONG_W 0x80280057	Verifica di coerenza per w non riuscita.
TPM_E_BAD_HANDLE 0x80280058	Handle non corretto.
TPM_E_BAD_DELEGATE 0x80280059	Delega non corretta.
TPM_E_BADCONTEXT 0x8028005A	BLOB di contesto non valido.
TPM_E_TOOMANYCONTEXTS 0x8028005B	Troppi contesti per il TPM.
TPM_E_MA_TICKET_SIGNATURE 0x8028005C	Errore di convalida della firma dell'autorità di migrazione.

Costante/valore	Descrizione
TPM_E_MA_DESTINATION 0x8028005D	Destinazione della migrazione non autenticata.
TPM_E_MA_SOURCE 0x8028005E	Origine della migrazione non corretta.
TPM_E_MA_AUTHORITY 0x8028005F	Autorità di migrazione non corretta.
TPM_E_PERMANENTEK 0x80280061	Tentativo di revocare la chiave di crittografia. Impossibile revocare tale chiave.
TPM_E_BAD_SIGNATURE 0x80280062	Firma del ticket CMK non valida.
TPM_E_NOCONTEXTSPACE 0x80280063	Spazio insufficiente per ulteriori contesti nell'elenco dei contesti.
TPM_E_COMMAND_BLOCKED 0x80280400	Comando bloccato.
TPM_E_INVALID_HANDLE 0x80280401	Impossibile trovare l'handle specificato.
TPM_E_DUPLICATE_VHANDLE 0x80280402	Handle duplicato restituito dal TPM. Inviare di nuovo il comando.
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	Il comando all'interno del trasporto è bloccato.
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	Il comando all'interno del trasporto non è supportato.
TPM_E_RETRY 0x80280800	Impossibile ottenere una risposta immediata al comando. TPM occupato. Inviare di nuovo il comando in seguito.
TPM_E_NEEDS_SELFTEST 0x80280801	Comando SelfTestFull non eseguito.
TPM_E_DOING_SELFTEST 0x80280802	TPM: test automatico in corso.
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	TPM: è in corso un periodo di timeout durante la difesa da attacchi con dizionario.
TBS_E_INTERNAL_ERROR 0x80284001	Errore software interno.
TBS_E_BAD_PARAMETER 0x80284002	Uno o più parametri di input non sono validi.

Costante/valore	Descrizione
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	Il puntatore di output specificato non è valido.
TBS_E_INVALID_CONTEXT 0x80284004	L'handle di contesto fa riferimento a un contesto non valido.
TBS_E_INSUFFICIENT_BUFFER 0x80284005	Buffer di output specificato insufficiente.
TBS_E_IOERROR 0x80284006	Errore durante la comunicazione con il TPM.
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	Uno o più parametri di contesto non validi.
TBS_E_SERVICE_NOT_RUNNING 0x80284008	Il servizio TBS non è in esecuzione. Impossibile avviarlo.
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	Impossibile creare un nuovo contesto. Troppi contesti aperti.
TBS_E_TOO_MANY_RESOURCES 0x8028400A	Non è stato possibile creare una nuova risorsa virtuale perché ci sono troppe risorse virtuali aperte.
TBS_E_SERVICE_START_PENDING 0x8028400B	Servizio TBS avviato ma non ancora in esecuzione.
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	L'interfaccia di presenza fisica non è supportata.
TBS_E_COMMAND_CANCELED 0x8028400D	Il comando è stato annullato.
TBS_E_BUFFER_TOO_LARGE 0x8028400E	Buffer di input o output troppo grande.
TBS_E_TPM_NOT_FOUND 0x8028400F	Impossibile trovare un dispositivo di protezione TPM (Trusted Platform Module) compatibile nel computer in uso.
TBS_E_SERVICE_DISABLED 0x80284010	Il servizio TBS è stato disattivato.
TBS_E_NO_EVENT_LOG 0x80284011	Non è disponibile nessun registro eventi TCG.
TBS_E_ACCESS_DENIED 0x80284012	Il chiamante non dispone dei diritti appropriati per eseguire l'operazione richiesta.
TBS_E_PROVISIONING_NOT_ALLOWED 0x80284013	L'azione di provisioning del TPM non è consentita dai contrassegni specificati. Per eseguire il provisioning, potrebbe essere necessaria una delle azioni riportate di seguito. Può essere utile l'azione della console di

Costante/valore	Descrizione
	gestione TPM (tpm.msc) per preparare il TPM. Per ulteriori informazioni, vedere la documentazione per il metodo WMI Win32_Tpm "Provision". Le azioni che potrebbero essere necessarie includono l'importazione del valore di autorizzazione del proprietario del TPM nel sistema, la chiamata del metodo WMI Win32_Tpm per il provisioning del TPM e l'impostazione di "ForceClear_Allowed" o "PhysicalPresencePrompts_Allowed" su TRUE, come indicato dal valore restituito nelle informazioni aggiuntive, oppure l'abilitazione del TPM nel BIOS di sistema.
TBS_E_PPI_FUNCTION_UNSUPPORTED 0x80284014	L'interfaccia di presenza fisica del firmware non supporta il metodo richiesto.
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	Impossibile trovare il valore OwnerAuth del TPM richiesto.
TBS_E_PROVISIONING_INCOMPLETE 0x80284016	Provisioning del TPM non completato. Per ulteriori informazioni sul completamento del provisioning, chiamare il metodo WMI Win32_Tpm per il provisioning del TPM ("Provision") e leggere le informazioni restituite.
TPMAPI_E_INVALID_STATE 0x80290100	Stato del buffer dei comandi non corretto.
TPMAPI_E_NOT_ENOUGH_DATA 0x80290101	I dati nel buffer dei comandi non sono sufficienti per soddisfare la richiesta.
TPMAPI_E_TOO_MUCH_DATA 0x80290102	Impossibile inserire altri dati nel buffer dei comandi.
TPMAPI_E_INVALID_OUTPUT_POINTER 0x80290103	Uno o più parametri NULL o non validi.
TPMAPI_E_INVALID_PARAMETER 0x80290104	Uno o più parametri non sono validi.
TPMAPI_E_OUT_OF_MEMORY 0x80290105	Memoria insufficiente per soddisfare la richiesta.
TPMAPI_E_BUFFER_TOO_SMALL 0x80290106	Il buffer specificato era insufficiente.
TPMAPI_E_INTERNAL_ERROR 0x80290107	Errore interno.
TPMAPI_E_ACCESS_DENIED 0x80290108	Il chiamante non dispone dei diritti appropriati per eseguire l'operazione richiesta.
TPMAPI_E_AUTHORIZATION_FAILED 0x80290109	Informazioni di autorizzazione specificate non valide.
TPMAPI_E_INVALID_CONTEXT_HANDLE 0x8029010A	Handle di contesto specificato non valido.

Costante/valore	Descrizione
TPMAPI_E_TBS_COMMUNICATION_ERROR 0x8029010B	Errore durante la comunicazione con il servizio TBS.
TPMAPI_E_TPM_COMMAND_ERROR 0x8029010C	Risultato imprevisto restituito dal TPM.
TPMAPI_E_MESSAGE_TOO_LARGE 0x8029010D	Messaggio troppo grande per lo schema di codifica.
TPMAPI_E_INVALID_ENCODING 0x8029010E	Codifica nel BLOB non riconosciuta.
TPMAPI_E_INVALID_KEY_SIZE 0x8029010F	Dimensioni della chiave non valide.
TPMAPI_E_ENCRYPTION_FAILED 0x80290110	Crittografia non riuscita.
TPMAPI_E_INVALID_KEY_PARAMS 0x80290111	Struttura dei parametri della chiave non valida.
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB 0x80290112	I dati obbligatori forniti non costituiscono un BLOB di autorizzazione di migrazione valido.
TPMAPI_E_INVALID_PCR_INDEX 0x80290113	Indice PCR specificato non valido
TPMAPI_E_INVALID_DELEGATE_BLOB 0x80290114	I dati specificati non costituiscono un BLOB delegato valido.
TPMAPI_E_INVALID_CONTEXT_PARAMS 0x80290115	Uno o più parametri di contesto specificati non validi.
TPMAPI_E_INVALID_KEY_BLOB 0x80290116	I dati forniti non costituiscono un BLOB di chiave valido
TPMAPI_E_INVALID_PCR_DATA 0x80290117	Dati PCR specificati non validi.
TPMAPI_E_INVALID_OWNER_AUTH 0x80290118	Il formato dei dati di autorizzazione del proprietario non è valido.
TPMAPI_E_FIPS_RNG_CHECK_FAILED 0x80290119	Il numero casuale generato non ha superato il controllo FIPS RNG.
TPMAPI_E_EMPTY_TCG_LOG 0x8029011A	Il registro eventi TCG non contiene dati.
TPMAPI_E_INVALID_TCG_LOG_ENTRY 0x8029011B	Voce nel registro eventi TCG non valida.

Costante/valore	Descrizione
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	Impossibile trovare un separatore TCG.
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY 0x8029011D	Un valore digest in una voce del registro TCG non corrisponde ai dati con hash.
TPMAPI_E_POLICY_DENIES_OPERATION 0x8029011E	L'operazione richiesta è stata bloccata dai criteri del TPM correnti. Per ottenere assistenza, contattare l'amministratore di sistema.
TBSIMP_E_BUFFER_TOO_SMALL 0x80290200	Il buffer specificato era insufficiente.
TBSIMP_E_CLEANUP_FAILED 0x80290201	Impossibile eseguire la pulizia del contesto.
TBSIMP_E_INVALID_CONTEXT_HANDLE 0x80290202	L'handle di contesto specificato non è valido.
TBSIMP_E_INVALID_CONTEXT_PARAM 0x80290203	Specificato un parametro di contesto non valido.
TBSIMP_E_TPM_ERROR 0x80290204	Errore durante la comunicazione con il TPM
TBSIMP_E_HASH_BAD_KEY 0x80290205	Impossibile trovare una voce con la chiave specificata.
TBSIMP_E_DUPLICATE_VHANDLE 0x80290206	L'handle virtuale specificato corrisponde a un handle virtuale già in uso.
TBSIMP_E_INVALID_OUTPUT_POINTER 0x80290207	Il puntatore alla posizione dell'handle restituita è NULL o non valido
TBSIMP_E_INVALID_PARAMETER 0x80290208	Uno o più parametri non validi
TBSIMP_E_RPC_INIT_FAILED 0x80290209	Impossibile inizializzare il sottosistema RPC.
TBSIMP_E_SCHEDULER_NOT_RUNNING 0x8029020A	Utilità di pianificazione TBS non in esecuzione.
TBSIMP_E_COMMAND_CANCELED 0x8029020B	Il comando è stato annullato.
TBSIMP_E_OUT_OF_MEMORY 0x8029020C	Memoria insufficiente per soddisfare la richiesta
TBSIMP_E_LIST_NO_MORE_ITEMS 0x8029020D	L'elenco specificato è vuoto o l'iterazione ha raggiunto la fine dell'elenco.

Costante/valore	Descrizione
TBSIMP_E_LIST_NOT_FOUND 0x8029020E	Impossibile trovare l'elemento specificato nell'elenco.
TBSIMP_E_NOT_ENOUGH_SPACE 0x8029020F	TPM: spazio insufficiente per caricare la risorsa richiesta.
TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS 0x80290210	TPM: troppi contesti in uso.
TBSIMP_E_COMMAND_FAILED 0x80290211	Comando TPM non riuscito.
TBSIMP_E_UNKNOWN_ORDINAL 0x80290212	TBS: impossibile riconoscere l'ordinale specificato.
TBSIMP_E_RESOURCE_EXPIRED 0x80290213	La risorsa richiesta non è più disponibile.
TBSIMP_E_INVALID_RESOURCE 0x80290214	Tipo di risorsa non corrispondente.
TBSIMP_E_NOTHING_TO_UNLOAD 0x80290215	Nessuna risorsa scaricabile.
TBSIMP_E_HASH_TABLE_FULL 0x80290216	Impossibile aggiungere nuove voci alla tabella hash.
TBSIMP_E_TOO_MANY_TBS_CONTEXTS 0x80290217	Impossibile creare un nuovo contesto TBS. Troppi contesti aperti.
TBSIMP_E_TOO_MANY_RESOURCES 0x80290218	Non è stato possibile creare una nuova risorsa virtuale perché ci sono troppe risorse virtuali aperte.
TBSIMP_E_PPI_NOT_SUPPORTED 0x80290219	L'interfaccia di presenza fisica non è supportata.
TBSIMP_E_TPM_INCOMPATIBLE 0x8029021A	Servizio TBS incompatibile con la versione del TPM trovata.
TBSIMP_E_NO_EVENT_LOG 0x8029021B	Non è disponibile nessun registro eventi TCG.
TPM_E_PPI_ACPI_FAILURE 0x80290300	Errore generale durante l'acquisizione della risposta del BIOS a un comando per il rilevamento della presenza fisica.
TPM_E_PPI_USER_ABORT 0x80290301	Impossibile confermare la richiesta dell'operazione TPM.
TPM_E_PPI_BIOS_FAILURE 0x80290302	Impossibile eseguire l'operazione TPM richiesta. Errore del BIOS, ad esempio richiesta di operazione TPM non valida o errore di comunicazione tra BIOS e TPM.

Costante/valore	Descrizione
TPM_E_PPI_NOT_SUPPORTED 0x80290303	Interfaccia di presenza fisica non supportata dal BIOS.
TPM_E_PPI_BLOCKED_IN_BIOS 0x80290304	Il comando per il rilevamento della presenza fisica è stato bloccato dalle impostazioni correnti del BIOS. Il proprietario del sistema può essere in grado di riconfigurare le impostazioni del BIOS per consentire il comando.
TPM_E_PCP_ERROR_MASK 0x80290400	Maschera per la conversione degli errori del provider di crittografia della piattaforma in errori di Windows.
TPM_E_PCP_DEVICE_NOT_READY 0x80290401	Dispositivo di crittografia della piattaforma non pronto. Per funzionare richiede il provisioning completo.
TPM_E_PCP_INVALID_HANDLE 0x80290402	L'handle fornito dal provider di crittografia della piattaforma non è valido.
TPM_E_PCP_INVALID_PARAMETER 0x80290403	Un parametro fornito dal provider di crittografia della piattaforma non è valido.
TPM_E_PCP_FLAG_NOT_SUPPORTED 0x80290404	Un contrassegno fornito al provider di crittografia della piattaforma non è supportato.
TPM_E_PCP_NOT_SUPPORTED 0x80290405	L'operazione richiesta non è supportata dal provider di crittografia della piattaforma.
TPM_E_PCP_BUFFER_TOO_SMALL 0x80290406	Buffer troppo piccolo per contenere tutti i dati. Nessuna informazione scritta nel buffer.
TPM_E_PCP_INTERNAL_ERROR 0x80290407	Errore interno non previsto nel provider di crittografia della piattaforma.
TPM_E_PCP_AUTHENTICATION_FAILED 0x80290408	Autorizzazione di utilizzo di un oggetto del provider non riuscita.
TPM_E_PCP_AUTHENTICATION_IGNORED 0x80290409	Il dispositivo di crittografia della piattaforma ha ignorato l'autorizzazione per l'oggetto del provider per contrastare un attacco con dizionario.
TPM_E_PCP_POLICY_NOT_FOUND 0x8029040A	Criterio di riferimento non trovato.
TPM_E_PCP_PROFILE_NOT_FOUND 0x8029040B	Profilo di riferimento non trovato.
TPM_E_PCP_VALIDATION_FAILED 0x8029040C	La convalida non è stata eseguita correttamente.
PLA_E_DCS_NOT_FOUND 0x80300002	Impossibile trovare l'Insieme agenti di raccolta dati.
PLA_E_DCS_IN_USE 0x803000AA	L'Insieme agenti di raccolta dati o una delle relative dipendenze è già in uso.

Costante/valore	Descrizione
PLA_E_TOO_MANY_FOLDERS 0x80300045	Impossibile avviare l'Insieme agenti di raccolta dati. Troppe cartelle.
PLA_E_NO_MIN_DISK 0x80300070	Spazio su disco insufficiente per l'avvio dell'Insieme agenti di raccolta dati.
PLA_E_DCS_ALREADY_EXISTS 0x803000B7	Insieme agenti di raccolta dati già esistente.
PLA_S_PROPERTY_IGNORED 0x00300100	Il valore della proprietà verrà ignorato.
PLA_E_PROPERTY_CONFLICT 0x80300101	Conflitto di valori di proprietà.
PLA_E_DCS_SINGLETON_REQUIRED 0x80300102	In base alla configurazione corrente, l'Insieme agenti di raccolta dati deve contenere un solo agente di raccolta dati.
PLA_E_CREDENTIALS_REQUIRED 0x80300103	Per il commit delle proprietà dell'Insieme agenti di raccolta dati è necessario un account utente.
PLA_E_DCS_NOT_RUNNING 0x80300104	Insieme agenti di raccolta dati non in esecuzione.
PLA_E_CONFLICT_INCL_EXCL_API 0x80300105	Conflitto nell'elenco di API di inclusione/esclusione. Non specificare la stessa API nell'elenco di inclusione e nell'elenco di esclusione.
PLA_E_NETWORK_EXE_NOT_VALID 0x80300106	Il percorso eseguibile specificato fa riferimento a una condivisione di rete o a un percorso UNC.
PLA_E_EXE_ALREADY_CONFIGURED 0x80300107	Il percorso eseguibile specificato è già configurato per la traccia delle API.
PLA_E_EXE_PATH_NOT_VALID 0x80300108	Il percorso eseguibile specificato non esiste. Verificare che sia corretto.
PLA_E_DC_ALREADY_EXISTS 0x80300109	Agente di raccolta dati già esistente.
PLA_E_DCS_START_WAIT_TIMEOUT 0x8030010A	Timeout dell'attesa della notifica dell'avvio dell'Insieme agenti di raccolta dati.
PLA_E_DC_START_WAIT_TIMEOUT 0x8030010B	Timeout dell'attesa dell'avvio dell'agente di raccolta dati.
PLA_E_REPORT_WAIT_TIMEOUT 0x8030010C	Timeout dell'attesa della fine dell'elaborazione dello strumento di generazione di rapporti.
PLA_E_NO_DUPLICATES 0x8030010D	Elementi duplicati non consentiti.

Costante/valore	Descrizione
PLA_E_EXE_FULL_PATH_REQUIRED 0x8030010E	Per specificare l'eseguibile che si desidera tracciare è necessario indicare il percorso completo dell'eseguibile. Il nome del file non è sufficiente.
PLA_E_INVALID_SESSION_NAME 0x8030010F	Nome di sessione specificato non valido.
PLA_E_PLA_CHANNEL_NOT_ENABLED 0x80300110	È possibile eseguire questa operazione solo se il canale Microsoft-Windows-Diagnosis-PLA/Operational del registro eventi è attivato.
PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED 0x80300111	È possibile eseguire questa operazione solo se il canale Microsoft-Windows-TaskScheduler del registro eventi è attivato.
PLA_E_RULES_MANAGER_FAILED 0x80300112	Impossibile eseguire Gestione regole.
PLA_E_CABAPI_FAILURE 0x80300113	Errore durante il tentativo di compressione o estrazione dei dati.
FVE_E_LOCKED_VOLUME 0x80310000	Unità bloccata da Crittografia unità BitLocker. Sbloccare l'unità dal Pannello di controllo.
FVE_E_NOT_ENCRYPTED 0x80310001	Unità non crittografata.
FVE_E_NO_TPM_BIOS 0x80310002	Il BIOS non comunica correttamente con il TPM. Per istruzioni relative all'aggiornamento del BIOS, contattare il produttore del computer.
FVE_E_NO_MBR_METRIC 0x80310003	Il BIOS non è in grado di comunicare correttamente con il record di avvio principale (MBR). Per istruzioni relative all'aggiornamento del BIOS, contattare il produttore del computer.
FVE_E_NO_BOOTSECTOR_METRIC 0x80310004	Manca una misurazione TPM obbligatoria. Se nel computer è inserito un CD o un DVD di avvio, rimuoverlo, riavviare il computer, quindi riattivare BitLocker. Se il problema persiste, verificare che il record di avvio principale sia aggiornato.
FVE_E_NO_BOOTMGR_METRIC 0x80310005	Il settore di avvio dell'unità non è compatibile con Crittografia unità BitLocker. Utilizzare lo strumento Bootrec.exe in Ambiente ripristino Windows per aggiornare o ripristinare Boot Manager (BOOTMGR).
FVE_E_WRONG_BOOTMGR 0x80310006	La versione di Boot Manager disponibile nel sistema operativo in uso non è compatibile con Crittografia unità BitLocker. Utilizzare lo strumento Bootrec.exe in Ambiente ripristino Windows per aggiornare o ripristinare Boot Manager (BOOTMGR).
FVE_E_SECURE_KEY_REQUIRED 0x80310007	Per eseguire l'operazione è necessaria almeno una protezione con chiave sicura.

Costante/valore	Descrizione
FVE_E_NOT_ACTIVATED 0x80310008	Crittografia unità BitLocker non abilitata per l'unità. Attivare BitLocker.
FVE_E_ACTION_NOT_ALLOWED 0x80310009	Crittografia unità BitLocker: impossibile eseguire l'azione richiesta. Questa condizione può verificarsi quando vengono generate due richieste contemporaneamente. Attendere alcuni istanti e riprovare.
FVE_E_AD_SCHEMA_NOT_INSTALLED 0x8031000A	La foresta di Servizi di dominio Active Directory non contiene gli attributi e le classi necessari per ospitare le informazioni di Crittografia unità BitLocker o Trusted Platform Module. Contattare l'amministratore di dominio per verificare che siano state installate tutte le estensioni dello schema di Active Directory necessarie per BitLocker.
FVE_E_AD_INVALID_DATATYPE 0x8031000B	Il tipo di dati ottenuti da Active Directory era imprevisto. Le informazioni di ripristino di BitLocker potrebbero essere mancanti o danneggiate.
FVE_E_AD_INVALID_DATASIZE 0x8031000C	Dimensioni dei dati ottenuti da Active Directory impreviste. Le informazioni di ripristino di BitLocker potrebbero essere mancanti o danneggiate.
FVE_E_AD_NO_VALUES 0x8031000D	L'attributo letto da Active Directory non contiene valori. Le informazioni di ripristino di BitLocker potrebbero essere mancanti o danneggiate.
FVE_E_AD_ATTR_NOT_SET 0x8031000E	Attributo non impostato. Verificare di essere connessi con un account di dominio autorizzato a scrivere informazioni negli oggetti di Active Directory.
FVE_E_AD_GUID_NOT_FOUND 0x8031000F	Impossibile trovare l'attributo specificato in Servizi di dominio Active Directory. Contattare l'amministratore di dominio per verificare che siano state installate tutte le estensioni dello schema di Active Directory necessarie per BitLocker.
FVE_E_BAD_INFORMATION 0x80310010	Metadati di BitLocker per l'unità crittografata non validi. È possibile tentare di riparare l'unità per ripristinare l'accesso.
FVE_E_TOO_SMALL 0x80310011	Impossibile crittografare l'unità. Spazio insufficiente. Eliminare tutti i dati non necessari dall'unità per aumentare lo spazio disponibile, quindi riprovare.
FVE_E_SYSTEM_VOLUME 0x80310012	Impossibile crittografare l'unità perché contiene le informazioni di avvio del sistema. Creare una partizione separata da utilizzare come unità di sistema contenente le informazioni di avvio e una seconda partizione da utilizzare come unità del sistema operativo, quindi crittografare l'unità del sistema operativo.
FVE_E_FAILED_WRONG_FS 0x80310013	Impossibile crittografare l'unità. File system non supportato.
FVE_E_BAD_PARTITION_SIZE 0x80310014	File system con dimensioni superiori a quelle della partizione nella tabella delle partizioni. Tale unità potrebbe essere stata danneggiata o alterata. Per utilizzarla con BitLocker, è necessario formattare la partizione.

Costante/valore	Descrizione
FVE_E_NOT_SUPPORTED 0x80310015	Impossibile crittografare l'unità.
FVE_E_BAD_DATA 0x80310016	Dati non validi.
FVE_E_VOLUME_NOT_BOUND 0x80310017	L'unità dati specificata non è impostata in modo da sbloccarsi automaticamente sul computer corrente e non può essere sbloccata automaticamente.
FVE_E_TPM_NOT_OWNED 0x80310018	È necessario inizializzare il TPM prima di poter utilizzare Crittografia unità BitLocker.
FVE_E_NOT_DATA_VOLUME 0x80310019	Impossibile eseguire l'operazione tentata sull'unità del sistema operativo.
FVE_E_AD_INSUFFICIENT_BUFFER 0x8031001A	Il buffer assegnato a una funzione non è sufficiente per contenere i dati restituiti. Aumentare le dimensioni del buffer prima di eseguire di nuovo la funzione.
FVE_E_CONV_READ 0x8031001B	Operazione di lettura non riuscita durante la conversione dell'unità. L'unità non è stata convertita. Abilitare di nuovo BitLocker.
FVE_E_CONV_WRITE 0x8031001C	Operazione di scrittura non riuscita durante la conversione dell'unità. L'unità non è stata convertita. Abilitare di nuovo BitLocker.
FVE_E_KEY_REQUIRED 0x8031001D	Sono necessarie una o più protezioni con chiave BitLocker. Impossibile eliminare l'ultima chiave per l'unità.
FVE_E_CLUSTERING_NOT_SUPPORTED 0x8031001E	Crittografia unità BitLocker non supporta le configurazioni cluster.
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	L'unità specificata è già configurata in modo da essere automaticamente sbloccata sul computer corrente.
FVE_E_OS_NOT_PROTECTED 0x80310020	L'unità del sistema operativo non è protetta da Crittografia unità BitLocker.
FVE_E_PROTECTION_DISABLED 0x80310021	La funzionalità Crittografia unità BitLocker è stata sospesa su questa unità. Tutte le protezioni con chiave BitLocker configurate per l'unità sono state disabilitate e l'unità verrà automaticamente sbloccata utilizzando una chiave non crittografata.
FVE_E_RECOVERY_KEY_REQUIRED 0x80310022	Per l'unità che si sta tentando di bloccare non sono disponibili protezioni con chiave per la crittografia, perché la protezione BitLocker è attualmente sospesa. Per bloccare l'unità, abilitare nuovamente BitLocker.
FVE_E_FOREIGN_VOLUME 0x80310023	BitLocker: impossibile utilizzare il TPM (Trusted Platform Module) per proteggere un'unità dati. La protezione basata su TPM può essere utilizzata solo con l'unità del sistema operativo.

Costante/valore	Descrizione
FVE_E_OVERLAPPED_UPDATE 0x80310024	Impossibile aggiornare i metadati di BitLocker per l'unità crittografata perché è bloccata per l'aggiornamento da parte di un altro processo. Riprovare.
FVE_E_TPM_SRK_AUTH_NOT_ZERO 0x80310025	I dati di autorizzazione per la chiave radice di archiviazione (SRK) del TPM (Trusted Platform Module) sono diversi da zero, quindi non sono compatibili con BitLocker. Inizializzare il TPM prima di tentare di utilizzarlo con BitLocker.
FVE_E_FAILED_SECTOR_SIZE 0x80310026	Impossibile utilizzare l'algoritmo di crittografia dell'unità con questa dimensione del settore.
FVE_E_FAILED_AUTHENTICATION 0x80310027	Impossibile sbloccare l'unità con la chiave fornita. Verificare che la chiave sia corretta e riprovare.
FVE_E_NOT_OS_VOLUME 0x80310028	L'unità specificata non è l'unità del sistema operativo.
FVE_E_AUTOUNLOCK_ENABLED 0x80310029	Impossibile disattivare Crittografia unità BitLocker sull'unità del sistema operativo finché la funzionalità di sblocco automatico non verrà disabilitata per le unità dati fisse e rimovibili associate al computer in uso.
FVE_E_WRONG_BOOTSECTOR 0x8031002A	Il settore di avvio della partizione di sistema non è in grado di eseguire misurazioni TPM (Trusted Platform Module). Utilizzare lo strumento Bootrec.exe in Ambiente ripristino Windows per aggiornare o ripristinare il settore di avvio.
FVE_E_WRONG_SYSTEM_FS 0x8031002B	Crittografia unità BitLocker: le unità del sistema operativo devono essere formattate con il file system NTFS per essere crittografate. Convertire l'unità a NTFS, quindi attivare BitLocker.
FVE_E_POLICY_PASSWORD_REQUIRED 0x8031002C	In base alle impostazioni dei Criteri di gruppo, prima di crittografare l'unità è necessario specificare una password di ripristino.
FVE_E_CANNOT_SET_FVEK_ENCRYPTED 0x8031002D	Impossibile impostare l'algoritmo e la chiave di crittografia per un'unità crittografata in precedenza. Per crittografare l'unità con Crittografia unità BitLocker, rimuovere la crittografia precedente e attivare BitLocker.
FVE_E_CANNOT_ENCRYPT_NO_KEY 0x8031002E	Crittografia unità BitLocker: impossibile crittografare l'unità specificata perché non è disponibile una chiave di crittografia. Per crittografare l'unità, aggiungere una protezione con chiave.
FVE_E_BOOTABLE_CDDVD 0x80310030	Crittografia unità BitLocker: rilevato supporto di avvio (CD o DVD) nel computer. Rimuovere il supporto e riavviare il computer prima di configurare BitLocker.
FVE_E_PROTECTOR_EXISTS 0x80310031	Impossibile aggiungere la protezione con chiave. Per l'unità è consentita una sola protezione con chiave di questo tipo.
FVE_E_RELATIVE_PATH 0x80310032	Impossibile trovare il file della password di ripristino perché è stato specificato un percorso relativo. Le password di ripristino devono essere salvare in un percorso completo.

Costante/valore	Descrizione
	Nel percorso è possibile utilizzare le variabili di ambiente configurate nel computer.
FVE_E_PROTECTOR_NOT_FOUND 0x80310033	Impossibile trovare nell'unità la protezione con chiave specificata. Provare a utilizzare un'altra protezione con chiave.
FVE_E_INVALID_KEY_FORMAT 0x80310034	La chiave di ripristino fornita è danneggiata e non può essere utilizzata per accedere all'unità. Per ripristinare l'accesso all'unità è necessario utilizzare un metodo di ripristino alternativo, ad esempio una password di ripristino, un agente recupero dati o una copia di backup della chiave di ripristino.
FVE_E_INVALID_PASSWORD_FORMAT 0x80310035	Il formato di file della password di ripristino fornita non è valido. Le password di ripristino di BitLocker devono essere di 48 cifre. Verificare che il formato della password di ripristino sia corretto, quindi riprovare.
FVE_E_FIPS_RNG_CHECK_FAILED 0x80310036	Il test di controllo del generatore di numeri casuali non è stato superato.
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD 0x80310037	Le impostazioni dei Criteri di gruppo che richiedono la conformità FIPS impediscono la generazione o l'utilizzo di una password di ripristino locale da parte di Crittografia unità BitLocker. Quando si utilizza la modalità di conformità FIPS, le opzioni di ripristino di BitLocker possono essere eseguite tramite una chiave di ripristino archiviata in un'unità USB o tramite un agente recupero dati.
FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT 0x80310038	L'impostazione dei Criteri di gruppo che richiede la conformità FIPS impedisce il salvataggio della password di ripristino in Active Directory. Quando si utilizza la modalità di conformità FIPS, le opzioni di ripristino di BitLocker possono essere eseguite tramite una chiave di ripristino archiviata in un'unità USB o tramite un agente recupero dati. Controllare la configurazione delle impostazioni dei Criteri di gruppo.
FVE_E_NOT_DECRYPTED 0x80310039	Per completare l'operazione, è necessario che l'unità sia completamente decrittografata.
FVE_E_INVALID_PROTECTOR_TYPE 0x8031003A	Impossibile utilizzare la protezione con chiave specificata per questa operazione.
FVE_E_NO_PROTECTORS_TO_TEST 0x8031003B	Nell'unità non esiste alcuna protezione con chiave per l'esecuzione del test hardware.
FVE_E_KEYFILE_NOT_FOUND 0x8031003C	Impossibile trovare la chiave di avvio o la password di ripristino di BitLocker nel dispositivo USB. Verificare che il dispositivo USB sia collegato a una porta USB attiva del computer, riavviare il computer e riprovare. Se il problema persiste, contattare il produttore del computer per istruzioni sull'aggiornamento del BIOS.
FVE_E_KEYFILE_INVALID 0x8031003D	File della chiave di avvio o della password di ripristino di BitLocker danneggiato o non valido. Verificare che il file della chiave di avvio o della password di ripristino sia corretto, quindi riprovare.

Costante/valore	Descrizione
FVE_E_KEYFILE_NO_VMK 0x8031003E	Impossibile ottenere la chiave di crittografia BitLocker dalla chiave di avvio o dalla password di ripristino. Verificare che la chiave di avvio o la password di ripristino sia corretta, quindi riprovare.
FVE_E_TPM_DISABLED 0x8031003F	TPM (Trusted Platform Module) disabilitato. Prima di utilizzare il TPM con Crittografia unità BitLocker è necessario abilitarlo, inizializzarlo e impostare un proprietario valido.
FVE_E_NOT_ALLOWED_IN_SAFE_MODE 0x80310040	Impossibile gestire la configurazione di BitLocker per l'unità specificata perché il computer è attualmente in modalità provvisoria. In modalità provvisoria è possibile utilizzare Crittografia unità BitLocker solo per operazioni di ripristino.
FVE_E_TPM_INVALID_PCR 0x80310041	Impossibile sbloccare l'unità tramite il TPM (Trusted Platform Module). Le informazioni di avvio del sistema sono state modificate o è stato specificato un PIN non corretto. Verificare che l'unità non sia stata alterata e che le modifiche alle informazioni di avvio del sistema siano state apportate da una fonte attendibile. Dopo avere verificato che l'accesso all'unità è sicuro, utilizzare la Console di ripristino di emergenza di BitLocker per sbloccare l'unità, quindi sospendere e riprendere BitLocker per aggiornare le informazioni di avvio del sistema che BitLocker associa all'unità.
FVE_E_TPM_NO_VMK 0x80310042	Impossibile ottenere la chiave di crittografia BitLocker dal TPM (Trusted Platform Module).
FVE_E_PIN_INVALID 0x80310043	Impossibile ottenere la chiave di crittografia BitLocker dal TPM (Trusted Platform Module) e dal PIN.
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	Un'applicazione di avvio è cambiata dopo l'abilitazione di Crittografia unità BitLocker.
FVE_E_AUTH_INVALID_CONFIG 0x80310045	Le impostazioni dei dati di configurazione di avvio sono cambiate dopo l'abilitazione di Crittografia unità BitLocker.
FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED 0x80310046	L'impostazione dei Criteri di gruppo che richiede la conformità FIPS impedisce l'utilizzo di chiavi non crittografate e, di conseguenza, la sospensione di BitLocker su questa unità. Per ulteriori informazioni, contattare l'amministratore di dominio.
FVE_E_FS_NOT_EXTENDED 0x80310047	Crittografia unità BitLocker: impossibile decrittografare l'unità perché il file system non si estende fino alla fine dell'unità. Partizionare l'unità, quindi riprovare.
FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED 0x80310048	Impossibile abilitare Crittografia unità BitLocker sull'unità del sistema operativo. Per istruzioni relative all'aggiornamento del BIOS, contattare il produttore del computer.
FVE_E_NO_LICENSE 0x80310049	La versione di Windows in uso non include Crittografia unità BitLocker. Per utilizzare Crittografia unità BitLocker, aggiornare il sistema operativo.

Costante/valore	Descrizione
FVE_E_NOT_ON_STACK 0x8031004A	Impossibile utilizzare Crittografia unità BitLocker perché alcuni file di sistema critici per BitLocker mancano o sono danneggiati. Utilizzare lo strumento di Windows Ripristino all'avvio per ripristinare tali file nel computer in uso.
FVE_E_FS_MOUNTED 0x8031004B	Impossibile bloccare l'unità mentre è in uso.
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	Il token di accesso associato al thread corrente non è un token rappresentato.
FVE_E_DRY_RUN_FAILED 0x8031004D	Impossibile ottenere la chiave di crittografia BitLocker. Verificare che il TPM (Trusted Platform Module) sia abilitato e che la relativa proprietà sia stata acquisita. Se il computer non include un TPM, verificare che l'unità USB sia inserita e disponibile.
FVE_E_REBOOT_REQUIRED 0x8031004E	Prima di continuare con Crittografia unità BitLocker è necessario riavviare il computer.
FVE_E_DEBUGGER_ENABLED 0x8031004F	Impossibile crittografare l'unità mentre il debugger di avvio è abilitato. Per disattivare il debugger di avvio, utilizzare lo strumento da riga di comando bcdedit.
FVE_E_RAW_ACCESS 0x80310050	Nessuna operazione eseguita. Crittografia unità BitLocker in modalità di accesso in lettura/scrittura.
FVE_E_RAW_BLOCKED 0x80310051	Crittografia unità BitLocker: impossibile passare alla modalità di accesso in lettura/scrittura per l'unità specificata perché è in uso.
FVE_E_BCD_APPLICATIONS_PATH_INCORRECT 0x80310052	Il percorso specificato nei dati di configurazione di avvio per un'applicazione la cui integrità è protetta da Crittografia unità BitLocker non è corretto. Verificare e correggere le impostazioni nei dati di configurazione di avvio e riprovare.
FVE_E_NOT_ALLOWED_IN_VERSION 0x80310053	Quando il computer è in esecuzione in modalità di preinstallazione o ripristino è possibile utilizzare Crittografia unità BitLocker solo per operazioni di provisioning o di ripristino limitate.
FVE_E_NO_AUTOUNLOCK_MASTER_KEY 0x80310054	Chiave master di sblocco automatico non disponibile nell'unità del sistema operativo.
FVE_E_MOR_FAILED 0x80310055	Il firmware del sistema non è riuscito ad abilitare la cancellazione della memoria di sistema al riavvio del computer.
FVE_E_HIDDEN_VOLUME 0x80310056	Impossibile crittografare l'unità nascosta.
FVE_E_TRANSIENT_STATE 0x80310057	Le chiavi di crittografia BitLocker sono state ignorate perché l'unità è in uno stato di passaggio.
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	Protezione basata su chiave pubblica non consentita per l'unità.

Costante/valore	Descrizione
FVE_E_VOLUME_HANDLE_OPEN 0x80310059	È già in corso un'operazione di Crittografia unità BitLocker sull'unità. Completare tutte le operazioni prima di continuare.
FVE_E_NO_FEATURE_LICENSE 0x8031005A	Funzionalità di Crittografia unità BitLocker non supportata dalla versione di Windows in uso. Per utilizzare la funzionalità, aggiornare il sistema operativo.
FVE_E_INVALID_STARTUP_OPTIONS 0x8031005B	Impossibile applicare le impostazioni dei Criteri di gruppo relative alle opzioni di avvio di BitLocker perché sono in conflitto. Per ulteriori informazioni, contattare l'amministratore di sistema.
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED 0x8031005C	Creazione di una password di ripristino non consentita dai Criteri di gruppo.
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	In base alle impostazioni dei Criteri di gruppo, è necessario creare una password di ripristino.
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	Creazione di una chiave di ripristino non consentita dalle impostazioni dei Criteri di gruppo.
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	In base alle impostazioni dei Criteri di gruppo, è necessario creare una chiave di ripristino.
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 0x80310060	Utilizzo di un PIN all'avvio non consentito dalle impostazioni dei Criteri di gruppo. Scegliere un'altra opzione di avvio di BitLocker.
FVE_E_POLICY_STARTUP_PIN_REQUIRED 0x80310061	In base alle impostazioni dei Criteri di gruppo è necessario utilizzare un PIN all'avvio. Scegliere questa opzione di avvio di BitLocker.
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED 0x80310062	Utilizzo di una chiave di avvio non consentito dalle impostazioni dei Criteri di gruppo. Scegliere un'altra opzione di avvio di BitLocker.
FVE_E_POLICY_STARTUP_KEY_REQUIRED 0x80310063	In base alle impostazioni dei Criteri di gruppo è necessario utilizzare una chiave di avvio. Scegliere questa opzione di avvio di BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064	Utilizzo di una chiave di avvio e di un PIN non consentito dalle impostazioni dei Criteri di gruppo. Scegliere un'altra opzione di avvio di BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED 0x80310065	In base alle impostazioni dei Criteri di gruppo è necessario utilizzare una chiave di avvio e un PIN. Scegliere questa opzione di avvio di BitLocker.
FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED 0x80310066	Protezione solo TMP all'avvio non consentita dai Criteri di gruppo. Scegliere un'altra opzione di avvio di BitLocker.
FVE_E_POLICY_STARTUP_TPM_REQUIRED 0x80310067	In base alle impostazioni dei Criteri di gruppo è necessario utilizzare la protezione solo TMP all'avvio. Scegliere questa opzione di avvio di BitLocker.

Costante/valore	Descrizione
FVE_E_POLICY_INVALID_PIN_LENGTH 0x80310068	Il PIN specificato non soddisfa i requisiti relativi alla lunghezza massima o minima.
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 0x80310069	La protezione con chiave non è supportata dalla versione di Crittografia unità BitLocker attualmente applicata all'unità. Aggiornare l'unità per aggiungere la protezione con chiave.
FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED 0x8031006A	Creazione di una password non consentita dalle impostazioni dei Criteri di gruppo.
FVE_E_POLICY_PASSPHRASE_REQUIRED 0x8031006B	In base alle impostazioni dei Criteri di gruppo è necessario creare una password.
FVE_E_FIPS_PREVENTS_PASSPHRASE 0x8031006C	Le impostazioni dei Criteri di gruppo che richiedono la conformità FIPS impediscono la generazione o l'utilizzo di una password. Per ulteriori informazioni, contattare l'amministratore di dominio.
FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED 0x8031006D	Impossibile aggiungere una password all'unità del sistema operativo.
FVE_E_INVALID_BITLOCKER_OID 0x8031006E	L'identificatore di oggetto (OID) BitLocker dell'unità sembra essere non valido o danneggiato. Per reimpostare l'OID per l'unità, utilizzare manage-BDE.
FVE_E_VOLUME_TOO_SMALL 0x8031006F	Unità troppo piccola per utilizzare la protezione tramite Crittografia unità BitLocker.
FVE_E_DV_NOT_SUPPORTED_ON_FS 0x80310070	Il tipo di unità di individuazione selezionato non è compatibile con il file system nell'unità. Le unità di individuazione BitLocker To Go devono essere create su unità con formattazione FAT.
FVE_E_DV_NOT_ALLOWED_BY_GP 0x80310071	Il tipo di unità di individuazione selezionato non è consentito dalle impostazioni dei Criteri di gruppo del computer. Verificare che le impostazioni dei Criteri di gruppo consentano la creazione di unità di individuazione da utilizzare con BitLocker To Go.
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED 0x80310072	L'utilizzo di certificati utente, ad esempio smart card, con Crittografia unità Con BitLocker non è consentito dalle impostazioni dei Criteri di gruppo.
FVE_E_POLICY_USER_CERTIFICATE_REQUIRED 0x80310073	In base alle impostazioni dei Criteri di gruppo è necessario disporre di un certificato utente valido, ad esempio una smart card, da utilizzare con Crittografia unità BitLocker.
FVE_E_POLICY_USER_CERT_MUST_BE_HW 0x80310074	In base alle impostazioni dei Criteri di gruppo, con Crittografia unità BitLocker è necessario utilizzare una protezione con chiave basata su smart card.
FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED 0x80310075	Sblocco automatico delle unità dati fisse protette da BitLocker non consentito dalle impostazioni dei Criteri di gruppo.

Costante/valore	Descrizione
FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED 0x80310076	Sblocco automatico delle unità dati rimovibili protette da BitLocker non consentito dalle impostazioni dei Criteri di gruppo.
FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED 0x80310077	Configurazione di Crittografia unità BitLocker su unità dati rimovibili non consentita dalle impostazioni dei Criteri di gruppo.
FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED 0x80310078	Attivazione di Crittografia unità BitLocker su unità dati rimovibili non consentita dalle impostazioni dei Criteri di gruppo. Se è necessario attivare Crittografia unità BitLocker, contattare l'amministratore di sistema.
FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED 0x80310079	Disattivazione di Crittografia unità BitLocker su unità dati rimovibili non consentita dalle impostazioni dei Criteri di gruppo. Se è necessario disattivare Crittografia unità BitLocker, contattare l'amministratore di sistema.
FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH 0x80310080	La password in uso non soddisfa i requisiti di lunghezza minima delle password. Per impostazione predefinita, le password devono contenere almeno 8 caratteri. Per verificare i requisiti di lunghezza minima della password in vigore nell'organizzazione, contattare l'amministratore di sistema.
FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE 0x80310081	La password specificata non soddisfa i requisiti di complessità definiti dall'amministratore di sistema. Provare ad aggiungere caratteri maiuscoli e minuscoli, numeri e simboli.
FVE_E_RECOVERY_PARTITION 0x80310082	Impossibile crittografare l'unità perché è riservata per le opzioni di Ripristino di sistema di Windows.
FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON 0x80310083	Impossibile applicare Crittografia unità BitLocker all'unità a causa di conflitti nelle impostazioni dei Criteri di gruppo. Non è possibile configurare BitLocker per lo sblocco automatico delle unità dati fisse quando le opzioni di ripristino dell'utente sono disabilitate. Se si desidera sbloccare automaticamente le unità dati fisse protette da BitLocker dopo la convalida della chiave, richiedere all'amministratore di sistema di correggere le impostazioni in conflitto prima di abilitare BitLocker.
FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON 0x80310084	Impossibile applicare Crittografia unità BitLocker all'unità a causa di conflitti nelle impostazioni dei Criteri di gruppo. Non è possibile configurare BitLocker per lo sblocco automatico delle unità dati rimovibili quando le opzioni di ripristino dell'utente sono disabilitate. Se si desidera sbloccare automaticamente le unità dati rimovibili protette da BitLocker dopo la convalida della chiave, richiedere all'amministratore di sistema di correggere le impostazioni in conflitto prima di abilitare BitLocker.
FVE_E_NON_BITLOCKER_OID 0x80310085	L'attributo di utilizzo chiavi avanzato (EKU) del certificato specificato non consente di utilizzare il certificato per Crittografia unità BitLocker. BitLocker non richiede l'utilizzo di un certificato con attributo EKU. Se tuttavia tale attributo è configurato, deve essere impostato su un identificatore

Costante/valore	Descrizione
	di oggetto (OID) corrispondente a quello configurato per BitLocker.
FVE_E_POLICY_PROHIBITS_SELFSIGNED 0x80310086	Impossibile applicare Crittografia unità BitLocker all'unità con la configurazione corrente a causa delle impostazioni dei Criteri di gruppo. Il certificato fornito per la crittografia dell'unità è autofirmato. Le impostazioni correnti dei Criteri di gruppo non consentono l'utilizzo di certificati autofirmati. Prima di tentare di abilitare BitLocker, ottenere un nuovo certificato dall'Autorità di certificazione.
FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED 0x80310087	Impossibile applicare Crittografia unità BitLocker all'unità a causa di conflitti nelle impostazioni dei Criteri di gruppo. Se si nega l'accesso in scrittura a unità non protette da BitLocker, non è possibile richiedere l'utilizzo di una chiave di avvio USB. Richiedere all'amministratore di sistema di risolvere i conflitti dei criteri prima di tentare di abilitare BitLocker.
FVE_E_CONV_RECOVERY_FAILED 0x80310088	Impossibile applicare Crittografia unità BitLocker all'unità a causa di conflitti nelle impostazioni dei Criteri di gruppo per le opzioni di ripristino relative alle unità del sistema operativo. Non è possibile richiedere l'archiviazione di informazioni di ripristino in Servizi di dominio Active Directory quando non è consentita la generazione di password di ripristino. Richiedere all'amministratore di sistema di risolvere i conflitti dei criteri prima di tentare di abilitare BitLocker.
FVE_E_VIRTUALIZED_SPACE_TOO_BIG 0x80310089	La dimensione di virtualizzazione richiesta è eccessiva.
FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON 0x80310090	Impossibile applicare Crittografia unità BitLocker all'unità a causa di conflitti nelle impostazioni dei Criteri di gruppo per le opzioni di ripristino relative alle unità del sistema operativo. Non è possibile richiedere l'archiviazione di informazioni di ripristino in Servizi di dominio Active Directory quando non è consentita la generazione di password di ripristino. Richiedere all'amministratore di sistema di risolvere i conflitti dei criteri prima di tentare di abilitare BitLocker.
FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON 0x80310091	Impossibile applicare Crittografia unità BitLocker all'unità a causa di conflitti nelle impostazioni dei Criteri di gruppo per le opzioni di ripristino relative alle unità dati fisse. Non è possibile richiedere l'archiviazione di informazioni di ripristino in Servizi di dominio Active Directory quando non è consentita la generazione di password di ripristino. Richiedere all'amministratore di sistema di risolvere i conflitti dei criteri prima di tentare di abilitare BitLocker.
FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON 0x80310092	Impossibile applicare Crittografia unità BitLocker all'unità a causa di conflitti nelle impostazioni dei Criteri di gruppo per le opzioni di ripristino relative alle unità dati rimovibili. Non è possibile richiedere l'archiviazione di informazioni di ripristino in Servizi di dominio Active Directory quando non è consentita la generazione di password di ripristino. Richiedere all'amministratore di sistema di risolvere i conflitti dei criteri prima di tentare di abilitare BitLocker.

Costante/valore	Descrizione
FVE_E_NON_BITLOCKER_KU 0x80310093	L'attributo di utilizzo chiavi del certificato specificato non consente di utilizzare il certificato per Crittografia unità BitLocker. BitLocker non richiede l'utilizzo di un certificato con attributo di utilizzo chiavi. Se tuttavia tale attributo è configurato, deve essere impostato su Crittografia chiave o Chiave concordata.
FVE_E_PRIVATEKEY_AUTH_FAILED 0x80310094	Impossibile autorizzare la chiave privata associata al certificato specificato. L'autorizzazione della chiave privata non è stata fornita o l'autorizzazione fornita non è valida.
FVE_E_REMOVAL_OF_DRA_FAILED 0x80310095	Per rimuovere il certificato dell'agente recupero dati è necessario utilizzare lo snap-in Certificati.
FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME 0x80310096	Questa unità è stata crittografata utilizzando la versione di Crittografia unità BitLocker inclusa in Windows Vista e Windows Server 2008, che non supporta gli identificatori organizzativi. Per specificare identificatori organizzativi per questa unità, eseguire l'aggiornamento della crittografia unità alla versione più recente utilizzando il comando "manage-bde -upgrade".
FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME 0x80310097	Impossibile bloccare l'unità perché è sbloccata automaticamente in questo computer. Per bloccare l'unità, rimuovere la protezione di sblocco automatico.
FVE_E_FIPS_HASH_KDF_NOT_ALLOWED 0x80310098	La smart card in uso non supporta la funzione di derivazione della chiave predefinita di Bitlocker SP800-56A per le smart card ECC. L'impostazione dei Criteri di gruppo che richiede la conformità FIPS impedisce a BitLocker di utilizzare altre funzioni di derivazione della chiave per la crittografia. Negli ambienti con restrizioni FIPS è necessario utilizzare una smart card conforme agli standard FIPS.
FVE_E_ENH_PIN_INVALID 0x80310099	Impossibile ottenere la chiave di crittografia BitLocker da TPM e PIN avanzato. Provare a utilizzare un PIN contenente solo numeri.
FVE_E_INVALID_PIN_CHARS 0x8031009A	Il PIN del TPM richiesto contiene caratteri non validi.
FVE_E_INVALID_DATUM_TYPE 0x8031009B	Tipo sconosciuto nelle informazioni di gestione archiviate sull'unità. Se si utilizza una versione precedente di Windows, provare ad accedere all'unità utilizzando la versione più recente.
FVE_E_EFI_ONLY 0x8031009C	Funzionalità supportata solo su sistemi EFI.
FVE_E_MULTIPLE_NKP_CERTS 0x8031009D	Più certificati di protezione di rete con chiave trovati nel sistema.
FVE_E_REMOVAL_OF_NKP_FAILED 0x8031009E	Rimuovere il certificato di protezione di rete con chiave tramite lo snap-in Certificati.
FVE_E_INVALID_NKP_CERT 0x8031009F	Certificato non valido trovato nell'archivio certificati di protezione di rete con chiave.

Costante/valore	Descrizione
FVE_E_NO_EXISTING_PIN 0x803100A0	L'unità non è protetta da un PIN.
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH 0x803100A1	Digitare il PIN corrente corretto.
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100A2	Per modificare il PIN o la password è necessario essere connessi con un account amministratore. Fare clic sul collegamento per reimpostare il PIN o la password come amministratore.
FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED 0x803100A3	Modifiche del PIN e della password disabilitate in BitLocker dopo un numero troppo elevato di richieste non riuscite. Fare clic sul collegamento per reimpostare il PIN o la password come amministratore.
FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII 0x803100A4	L'amministratore di sistema ha stabilito che le password devono contenere solo caratteri ASCII stampabili. Sono inclusi le lettere non accentate (A-Z, a-z), i numeri (0-9), gli spazi, i simboli aritmetici, la punteggiatura comune, i separatori e i simboli seguenti: # $ & @ ^ _ ~ .
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE 0x803100A5	Crittografia unità BitLocker supporta esclusivamente la crittografia solo dello spazio utilizzato nell'archiviazione con thin provisioning.
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE 0x803100A6	Crittografia unità BitLocker non supporta la liberazione di spazio di archiviazione per thin provisioning.
FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE 0x803100A7	L'unità non supporta la lunghezza necessaria per la chiave di autenticazione.
FVE_E_NO_EXISTING_PASSPHRASE 0x803100A8	L'unità non è protetta con una password.
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH 0x803100A9	Immettere la password corrente corretta.
FVE_E_PASSPHRASE_TOO_LONG 0x803100AA	La password non può superare i 256 caratteri.
FVE_E_NO_PASSPHRASE_WITH_TPM 0x803100AB	Impossibile aggiungere una protezione con chiave di tipo password. Protezione TPM esistente nell'unità.
FVE_E_NO_TPM_WITH_PASSPHRASE 0x803100AC	Impossibile aggiungere una protezione con chiave TPM. Protezione di tipo password esistente nell'unità.
FVE_E_NOT_ALLOWED_ON_CSV_STACK 0x803100AD	Il comando può essere eseguito solo dal nodo del coordinatore per il volume CSV specificato.
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	Impossibile eseguire il comando su un volume quando fa parte di un cluster.

Costante/valore	Descrizione
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 0x803100AF	Impossibile tornare alla crittografia software BitLocker a causa della configurazione di Criteri di gruppo.
FVE_E_EDRIVE_BAND_IN_USE 0x803100B0	Impossibile gestire l'unità in BitLocker. La funzionalità di crittografia hardware dell'unità è già in uso.
FVE_E_EDRIVE_DISALLOWED_BY_GP 0x803100B1	Le impostazioni di Criteri di gruppo non consentono l'uso della crittografia hardware.
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	L'unità specificata non supporta la crittografia hardware.
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	Impossibile aggiornare BitLocker durante la crittografia o la decrittografia del disco.
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	I volumi di individuazione non sono supportati per i volumi che utilizzano la crittografia hardware.
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	Nessuna tastiera di preavvio rilevata. L'utente potrebbe non essere in grado di fornire l'input necessario per sbloccare il volume.
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	Nessuna tastiera di preavvio o ambiente di ripristino Windows rilevato. L'utente potrebbe non essere in grado di fornire l'input necessario per sbloccare il volume.
FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE 0x803100B7	In base alle impostazioni dei Criteri di gruppo è necessario creare un PIN di avvio, ma in questo dispositivo non è disponibile una tastiera di preavvio. L'utente potrebbe non essere in grado di fornire l'input necessario per sbloccare il volume.
FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE 0x803100B8	In base alle impostazioni dei Criteri di gruppo è necessario creare una password di ripristino, ma in questo dispositivo non è disponibile né una tastiera di preavvio né un ambiente di ripristino Windows. L'utente potrebbe non essere in grado di fornire l'input necessario per sbloccare il volume.
FVE_E_WIPE_CANCEL_NOT_APPLICABLE 0x803100B9	Cancellazione dello spazio disponibile non in corso.
FVE_E_SECUREBOOT_DISABLED 0x803100BA	Impossibile utilizzare l'avvio sicuro in BitLocker per garantire l'integrità della piattaforma. L'avvio sicuro è stato disabilitato.
FVE_E_SECUREBOOT_CONFIGURATION_INVALID 0x803100BB	Impossibile utilizzare l'avvio sicuro in BitLocker per garantire l'integrità della piattaforma. La configurazione di avvio sicuro non soddisfa i requisiti di BitLocker.
FVE_E_EDRIVE_DRY_RUN_FAILED 0x803100BC	Il computer non supporta la crittografia hardware BitLocker. È consigliabile richiedere gli aggiornamenti del firmware al produttore del computer.

Costante/valore	Descrizione
FVE_E_SHADOW_COPY_PRESENT 0x803100BD	Impossibile abilitare BitLocker sul volume in quanto contiene una copia shadow del volume. Rimuovere tutte le copie shadow del volume prima di crittografarlo.
FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS 0x803100BE	Impossibile applicare Crittografia unità BitLocker all'unità. L'impostazione di Criteri di gruppo per i dati di configurazione di avvio avanzata contiene dati non validi. Richiedere all'amministratore di sistema di correggere la configurazione non valida prima di abilitare BitLocker.
FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE 0x803100BF	Il firmware del PC non supporta la crittografia hardware.
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED 0x803100C0	Modifiche della password disabilitate in BitLocker dopo un numero troppo elevato di richieste non riuscite. Fare clic sul collegamento per reimpostare la password come amministratore.
FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100C1	È necessario eseguire l'accesso con un account di amministratore per modificare la password. Fare clic sul collegamento per reimpostare la password come amministratore.
FVE_E_LIVEID_ACCOUNT_SUSPENDED 0x803100C2	BitLocker: impossibile salvare la password di ripristino perché l'account Microsoft specificato è sospeso.
FVE_E_LIVEID_ACCOUNT_BLOCKED 0x803100C3	BitLocker: impossibile salvare la password di ripristino perché l'account Microsoft specificato è bloccato.
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES 0x803100C4	Il PC non è configurato per supportare la crittografia del dispositivo. Abilitare BitLocker in tutti i volumi in modo che il PC sia conforme ai criteri di crittografia del dispositivo.
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED 0x803100C5	Il PC in uso non è in grado di supportare la crittografia del dispositivo a causa della presenza di volumi dati fissi non crittografati.
FVE_E_DE_HARDWARE_NOT_COMPLIANT 0x803100C6	Il PC in uso non soddisfa i requisiti hardware per il supporto della crittografia del dispositivo.
FVE_E_DE_WINRE_NOT_CONFIGURED 0x803100C7	Il PC in uso non è in grado di supportare la crittografia del dispositivo perché Ambiente ripristino Windows non è configurato correttamente.
FVE_E_DE_PROTECTION_SUSPENDED 0x803100C8	La protezione è abilitata nel volume ma è stata sospesa. La causa della sospensione potrebbe essere un aggiornamento applicato al sistema. Riavviare il sistema, quindi riprovare.
FVE_E_DE_OS_VOLUME_NOT_PROTECTED 0x803100C9	Il PC non è configurato per supportare la crittografia del dispositivo.
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	Blocco dispositivo attivato a causa dei troppi tentativi di accesso con password errate.
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 0x803100CB	La protezione non è abilitata nel volume. Per abilitare la protezione è necessario un account connesso. Se questo errore si verifica nonostante si disponga già di un

Costante/valore	Descrizione
	account connesso, consultare il registro eventi per ulteriori informazioni.
FVE_E_INVALID_PIN_CHARS_DETAILED 0x803100CC	Il PIN specificato contiene solo numeri da 0 a 9.
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	BitLocker: impossibile utilizzare la protezione della riproduzione hardware. Nessun contatore disponibile nel PC.
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	Convalida stato di blocco del dispositivo non riuscita. Contatore non corrispondente.
FVE_E_BUFFER_TOO_LARGE 0x803100CF	Buffer di input troppo grande.

19

Glossario

Attivare - L'attivazione avviene quando il computer è stato registrato con il Dell Server e ha ricevuto almeno un insieme iniziale di criteri.

Active Directory (AD) - Un servizio directory creato da Microsoft per reti di dominio di Windows.

Crittografia dei dati applicativi - Crittografia dei dati applicativi crittografa tutti i file scritti da un'applicazione protetta, utilizzando una Categoria 2 Sostituisci. Questo significa che qualunque directory che possiede una protezione di categoria 2 o superiore o qualunque percorso con estensioni specifiche protette da una categoria 2 o superiore fa sì che ADE non esegua la crittografia di quei file.

BitLocker Manager - Windows BitLocker è progettato per consentire la protezione dei computer Windows crittografando i file dati e del sistema operativo. Per migliorare la sicurezza delle distribuzioni BitLocker e per semplificare e ridurre il costo di proprietà, Dell fornisce una singola console di gestione centrale che affronta molti problemi relativi alla sicurezza e offre un approccio integrato alla gestione della crittografia in piattaforme non BitLocker, che siano esse fisiche, virtuali o basate su cloud. BitLocker Manager supporta la crittografia BitLocker per sistemi operativi, unità fisse e BitLocker To Go. BitLocker Manager consente di integrare facilmente BitLocker nelle proprie esigenze di crittografia e gestire BitLocker con minimo sforzo semplificando, al contempo, sicurezza e conformità. BitLocker Manager fornisce una gestione integrata del recupero delle chiavi, gestione e applicazione dei criteri, gestione automatizzata del TPM, conformità FIPS e creazione di rapporti di conformità.

Credenziali archiviate nella cache - Le credenziali archiviate nella cache vengono aggiunte al database PBA quando un utente effettua correttamente l'autenticazione con Active Directory. Queste informazioni sull'utente vengono conservate in modo tale che l'utente possa accedervi anche quando non si dispone di una connessione ad Active Directory (ad esempio, quando porta a casa il laptop).

Crittografia comune – La chiave comune rende i file crittografati accessibili a tutti gli utenti gestiti nel dispositivo in cui sono stati creati.

Disattivare - La disattivazione avviene quando SED Manager è impostato su OFF nella Management Console. In seguito alla disattivazione del computer, il database PBA viene eliminato e non esiste più alcun record di utenti archiviati nella cache.

Encryption External Media - Questo servizio all'interno della crittografia protegge i supporti rimovibili e i dispositivi di storage esterni.

Codice di accesso per Encryption External Media - Questo servizio consente il ripristino dei dispositivi protetti di Encryption External Media, per i quali l'utente dimentica la password e non riesce più ad accedere. Il completamento di questo processo consente all'utente di ripristinare la password impostata sul supporto.

Crittografia - 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, la crittografia opera come strato superiore nel sistema operativo del dispositivo e fornisce autenticazione, crittografia e autorizzazione applicate costantemente per massimizzare la protezione delle informazioni sensibili.

Endpoint - A seconda del contesto, un computer, dispositivo mobile o media esterno.

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

Ricerca crittografia - 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 attivato, 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.

Chiave di computer – Quando la crittografia è installata in un server, la Chiave di computer protegge le chiavi di crittografia dei file e dei criteri di un server. La chiave di macchina è archiviata nel Dell Server. Il nuovo server scambia certificati con il Dell Server durante l'attivazione e usa il certificato per gli eventi di autenticazione successivi.

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.

SED Manager - Fornisce una piattaforma per gestire in modo protetto le unità autocrittografanti. Sebbene le unità autocrittografanti forniscano la propria crittografia, non dispongono di una piattaforma per la gestione di tale crittografia e dei criteri disponibili. SED Manager è un componente di gestione centrale e scalabile che consente di proteggere e gestire più efficacemente i propri dati. SED Manager garantisce all'utente di amministrare la propria azienda in maniera più rapida e semplice.

Utente del server - Un account utente virtuale creato da Dell Server Encryption con lo scopo di gestire le chiavi di crittografia e gli aggiornamenti dei criteri sul sistema operativo di un server. Questo account utente non corrisponde a nessun altro account utente nel computer o all'interno del dominio, e non ha un nome utente né una password che possano essere usati fisicamente. All'account viene assegnato un valore UCID univoco nella Management Console.

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 le SDE si attiva la decrittografia automatica di tutte le directory e i file cifrati 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.

Crittografia utente – La chiave utente rende i file accessibili solo all'utente che li ha creati e solo nel dispositivo in cui sono stati creati. Quando Dell Server Encryption è in esecuzione, la crittografia utente viene convertita in crittografia comune. Viene fatta un'eccezione per i dispositivi di supporto rimovibili: quando vengono inseriti in un server con la cifratura installata, i file vengono crittografati tramite la Chiave roaming utente.