Dell Data Protection | Endpoint Security Suite Enterprise

Guida all'installazione avanzata v1.4

Messaggi di N.B., Attenzione e Avvertenza

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

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

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

Guida all'installazione avanzata di Endpoint Security Suite Enterprise

2017 - 04

Rev. A01

Sommario

1

Introduzione

Questa guida descrive in dettaglio la procedura per installare e configurare Advanced Threat Protection, , il client di crittografia, il client di SED Management, Autenticazione avanzata e BitLocker Manager.

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

Prima di iniziare

1 Prima di distribuire i client, installare EE Server/VE Server. Individuare la guida corretta come mostrato di seguito, seguire le istruzioni, quindi tornare a questa guida.

   - *Guida alla migrazione e all'installazione di DDP Enterprise Server*
   - *Guida introduttiva e all'installazione di DDP Enterprise Server - Virtual Edition*

   Verificare che i criteri siano impostati come desiderato. Sfogliare la Guida dell'amministratore, disponibile da **?** nella parte 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 l'EE Server/VE Server.

2 Eseguire il provisioning del tenant di Advanced Threat Prevention. Deve essere eseguito il provisioning di un tenant nel DDP Server prima che diventi attiva l'applicazione dei criteri di Advanced Threat Protection.

3 Leggere attentamente il capitolo Requisiti del presente documento.

4 Distribuire i client agli utenti finali.

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 password monouso, 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 usando il programma di installazione principale di ESSE , consultare:
  - Eseguire l'installazione interattiva usando il programma di installazione principale di ESSE

    oppure
  - Eseguire l'installazione dalla riga di comando usando il programma di installazione principale di ESSE
- Se si installano i client usando i programmi di installazione figlio, i rispettivi file eseguibili devono essere estratti dal programma di installazione principale di ESSE . Consultare Estrarre i programmi di installazione figlio dal programma di installazione principale di ESSE , quindi tornare qui.
  - Installare i programmi di installazione figlio dalla riga di comando:
    - Installare i driver - Scaricare i driver e il firmware appropriati in base all'hardware di autenticazione.
    - Installare il client di crittografia - Usare queste istruzioni per installare il client di 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 Advanced Threat Prevention - Usare queste istruzioni per installare il client di Advanced Threat Prevention, che è la protezione antivirus di ultima generazione che utilizza la scienza algoritmica e l'apprendimento automatico per identificare e classificare le cyber-minacce note e sconosciute impedendone l'esecuzione o il conseguente danneggiamento degli endpoint.
- Installare Protezione Web e Firewall - Utilizzare queste istruzioni per installare le funzioni *opzionali* Protezione Web e Firewall. Il Firewall client è un firewall con stato che controlla tutto il traffico in entrata e in uscita a fronte del suo elenco di regole. La Protezione Web monitora la navigazione Web e i download al fine di identificare minacce e, in caso ne vengano rilevate, applicare l'azione stabilita dal criterio, in base alle valutazioni dei siti Web.
- Installare i client di SED Management e Autenticazione avanzata - Usare queste istruzioni per installare il software di crittografia per le unità autocrittografanti. Sebbene le unità autocrittografanti forniscano la propria crittografia, non dispongono di una piattaforma per la gestione di crittografia e criteri. Con SED Management, 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.

  Il client di Autenticazione avanzata gestisce più metodi di autenticazione, inclusi PBA per unità autocrittografanti, Single Sign-On (SSO) e credenziali utente come impronte e password. Fornisce, inoltre, le funzionalità di Autenticazione avanzata per accedere a siti Web ed applicazioni.
- Installare il client di BitLocker Manager - Usare queste istruzioni per installare il client di BitLocker Manager, progettato per migliorare la sicurezza delle distribuzioni 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. Tuttavia, il programma di installazione figlio del client di Advanced Threat Prevention può essere installato solo dalla riga di comando.

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

Contattare Dell ProSupport

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

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

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

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

Requisiti

Tutti i client

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

- Durante la distribuzione è opportuno seguire le procedure consigliate. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e distribuzioni scaglionate agli utenti.
- L'account utente che esegue l'installazione/l'aggiornamento/la disinstallazione deve essere un utente amministratore del dominio o locale, che può essere assegnato temporaneamente tramite uno strumento di distribuzione, ad esempio Microsoft SMS o Dell KACE. Non sono supportati gli utenti non amministratori con privilegi elevati.
- Prima di iniziare l'installazione/la disinstallazione, 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).
- Accertarsi che la porta in uscita 443 sia disponibile a comunicare con l'EE Server/VE Server se i client del programma di installazione principale di ESSE verranno autorizzati usando Dell Digital Delivery (DDD). La funzionalità di assegnazione dei diritti non funzionerà se la porta 443 è bloccata (per qualsiasi motivo). DDD non viene utilizzato se l'installazione avviene tramite i programmi di installazione figlio.
- Visitare periodicamente www.dell.com/support per la documentazione più recente e i suggerimenti tecnici.

Tutti i client - Prerequisiti

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

  In tutti i computer spediti dalla fabbrica Dell è preinstallata la versione completa di Microsoft .Net Framework 4.5.2 (o versione successiva). Tuttavia, se non si sta installando il client in un hardware Dell o si sta aggiornando il client negli hardware Dell precedenti, è necessario verificare la versione di Microsoft .Net installata e aggiornarla, **prima di installare il client**, al fine di prevenire errori di installazione/aggiornamento. Per verificare la versione di Microsoft .Net installata, seguire queste istruzioni nel computer destinato all'installazione: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Per installare Microsoft .Net Framework 4.5.2, accedere a https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Driver e firmware per ControlVault, lettori di impronte e smart card (come mostrato di seguito) non sono inclusi nei file eseguibili del programma di installazione principale di ESSE o del programma di installazione figlio. I driver e il firmware devono essere sempre aggiornati ed è possibile scaricarli dal sito http://www.dell.com/support selezionando il modello del computer desiderato. Scaricare i driver e il firmware appropriati in base all'hardware di autenticazione.

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

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

Tutti i client - Hardware

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

Hardware

- I requisiti hardware minimi devono soddisfare le specifiche minime del sistema operativo.

Tutti i client - Supporto lingue

- I client di crittografia, Advanced Threat Prevention e BitLocker Manager sono compatibili con l'interfaccia utente multilingue (MUI, Multilingual User Interface) e supportano le lingue di seguito riportate. I dati di Advanced Threat Prevention che vengono visualizzati nella Remote Management Console sono solo in lingua inglese.

Supporto lingue

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

- I client dell'unità autocrittografante e di autenticazione avanzata sono compatibili con l'interfaccia utente multilingue (MUI, Multilingual User Interface) e supportano le lingue di seguito riportate. La modalità UEFI e l'autenticazione di preavvio non sono supportate in russo, cinese tradizionale e cinese semplificato.

Supporto lingue

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

Client di crittografia

- Per essere attivato, il computer client deve essere dotato della connettività di rete.
- 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.
- Per evitare che un computer non utilizzato da un utente passi alla modalità di sospensione durante la ricerca crittografia iniziale, disattivare tale modalità. La crittografia, o la decrittografia, non può essere eseguita in un computer in modalità di sospensione.
- Il client di crittografia non supporta le configurazioni di avvio doppio poiché è possibile crittografare file di sistema dell'altro sistema operativo, il che interferirebbe con il suo funzionamento.
- Il client di crittografia ora supporta la modalità Controllo. La modalità Controllo consente agli amministratori di distribuire il client di crittografia come parte dell'immagine aziendale, piuttosto che usare soluzioni SCCM di terzi o simili per distribuire il client di crittografia. Per istruzioni su come installare il client di crittografia in un'immagine aziendale, vedere http://www.dell.com/support/article/us/en/19/SLN304039.
- Il client di crittografia è stato testato ed è compatibile con McAfee, client Symantec, Kaspersky e MalwareBytes. Le esclusioni hardcoded sono utilizzate da questi provider di antivirus per impedire le incompatibilità tra crittografia e scansione antivirus. Il client di crittografia è stato testato anche con il Microsoft Enhanced Mitigation Experience Toolkit.

Se la propria organizzazione utilizza un provider di antivirus non in elenco, consultare http://www.dell.com/support/Article/us/en/19/SLN298707 oppure Contattare Dell ProSupport per ricevere assistenza.

- Il TPM è usato per sigillare la GPK. Pertanto, se si esegue il client di crittografia, cancellare il TPM nel BIOS prima di installare un nuovo sistema operativo nel computer client.
- L'aggiornamento del sistema operativo sul posto non è supportato con il client di crittografia installato. Eseguire la disinstallazione e la decrittografia del client di crittografia, l'aggiornamento al nuovo sistema operativo, quindi reinstallare il client di crittografia.

  Inoltre, la reinstallazione del sistema operativo non è supportata. Per reinstallare il sistema operativo, eseguire un backup del computer di destinazione, cancellarne i dati, installare il sistema operativo e quindi ripristinare i dati crittografati seguendo le procedure di ripristino stabilite.

Prerequisiti del client di crittografia

- Il programma di installazione principale di ESSE installa Microsoft Visual C++ 2012 Update 4 se non è già installato nel computer. **Se si usa il programma di installazione figlio**, è necessario installare questo componente prima di installare il client di crittografia.

Prerequisito
• Visual C++ 2012 Update 4 o Redistributable Package (x86 e x64) successivo

Hardware del client di crittografia

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

Hardware integrato facoltativo
• TPM 1.2 o 2.0

Sistemi operativi dei client di crittografia

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

Sistemi operativi Windows (a 32 e 64 bit)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate • Windows Embedded Standard 7 con modello Application Compatibility (la crittografia hardware non è supportata) • Windows 8: Enterprise, Pro • Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition • Windows Embedded 8.1 Industry Enterprise (la crittografia hardware non è supportata) • Windows 10: Education, Enterprise, Pro • VMware Workstation 5.5 e versioni successive

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

Sistemi operativi di External Media Shield (EMS)

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

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

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

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

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

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

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

Client di Server Encryption

Server Encryption è destinato all'utilizzo nei computer che hanno in esecuzione la modalità server, in particolare i file server.

- Server Encryption è compatibile solo con Enterprise Edition e Endpoint Security Enterprise Suite.
- Server Encryption fornisce quanto segue:
  - Crittografia del software
  - Crittografia di dispositivi di archiviazione rimovibili
  - Controllo porte

    N.B.:
    Il server deve supportare il controllo delle porte.

    I criteri del Sistema di controllo porte server 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.

Server Encryption è per l'utilizzo in:

- 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 è stato testato ed è compatibile con i client McAfee VirusScan, Symantec, gli antivirus Kaspersky e antimalware MalwareBytes. Le esclusioni hardcoded sono utilizzate da questi provider di antivirus per impedire le incompatibilità tra crittografia e scansione antivirus. Se la propria organizzazione utilizza un provider di antivirus non in elenco, consultare l'articolo della KB SLN298707 o Contattare Dell ProSupport per assistenza.

Non supportati

Server Encryption non è per l'utilizzo in:

- Dell Data Protection Server o server che hanno in esecuzione i database per Dell Data Protection Server
- Server Encryption non è compatibile con Endpoint Security Suite, Personal Edition o Security Tools.
- Server Encryption non è supportato con SED Management o il client di BitLocker Manager.
- La migrazione verso o da Server Encryption non è supportata. Gli aggiornamenti da External Media Edition a Server Encryption richiedono che il o i prodotti precedenti vengano disinstallati completamente prima di installare Server Encryption.
- 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 archiviazione di rete SAN/NAS
  - Dispositivi connessi iSCSI
  - Software di deduplicazione
  - Deduplicazione dell'hardware
  - Split RAID (volumi multipli in un unico RAID)
  - Unità autocrittografanti (RAID e NON RAID)
  - Accesso automatico (SO Windows 7, 8/8.1) per chioschi
  - Microsoft Storage Server 2012
- Server Encryption 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.
- L'aggiornamento del sistema operativo sul posto non è supportato da Server Encryption. Per aggiornare il sistema operativo, disinstallare e decrittografare Server Encryption, aggiornare al nuovo sistema operativo, quindi installare nuovamente Server Encryption.

  Inoltre, le reinstallazioni del sistema operativo non sono supportate. Se si desidera 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*.

Prerequisiti del client di Server Encryption

- È necessario installare questo componente prima di installare il client di Server Encryption.

Prerequisito
• Visual C++ 2012 Update 4 o Redistributable Package (x86 e x64) successivo

Hardware del client di Server Encryption

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

Sistemi operativi del client di Server Encryption

La tabella seguente descrive in dettaglio i sistemi operativi supportati.

Sistemi operativi (a 32 e 64 bit)

- Windows 7 SP0-SP1: Home, Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

Sistemi operativi server supportati

- Windows Server 2008 SP2: Standard Edition, Datacenter Edition con e senza Hyper-V, Enterprise Edition con e senza Hyper-V, Foundation Server Edition
- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition con e senza Hyper-V, Enterprise Edition con e senza Hyper-V, Foundation Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition

Sistemi operativi supportati in modalità UEFI

- Windows 8: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

N.B.:

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

Sistemi operativi di External Media Shield (EMS)

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

N.B.:

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

N.B.:

Windows XP è supportato solo quando si utilizza EMS Explorer.

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

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

Sistemi operativi server supportati

- Windows Server 2008 SP1 o versione successiva
- Windows Server 2012 R2

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

- OS X Mavericks 10.9.5
- OS X Yosemite 10.10.5
- OS X El Capitan 10.11.4 e 10.11.5

Client di Advanced Threat Prevention

- Il client di Advanced Threat Protection non può essere installato se non è stato rilevato il Dell Client Security Framework (EMAgent) nel computer. e in tal caso non sarà possibile eseguire l'installazione.
- Per completare l'installazione di Advanced Threat Prevention se il Dell Enterprise Server/VE che gestisce il client è in esecuzione in modalità connessa (impostazione predefinita), il computer deve disporre di connettività di rete. Tuttavia, la connettività di rete ***non*** è richiesta per l'installazione di Advanced Threat Prevention se il Dell Server di gestione è in esecuzione in modalità disconnessa.
- Per effettuare il provisioning di un tenant per Advanced Threat Protection, il Dell Server deve disporre di connettività Internet.

  N.B.: La connettività Internet non è richiesta se il server Dell è in esecuzione in modalità disconnessa.
- Le funzioni opzionali Firewall client e Protezione Web ***non*** devono essere installate sui computer client che sono gestiti da Dell Enterprise Server/VE in esecuzione in modalità disconnessa.
- Applicazioni antivirus, antimalware e antispyware di altri fornitori potrebbero entrare in conflitto con il client di Advanced Threat Prevention. Se possibile, disinstallare queste applicazioni. Fra i software che possono entrare in conflitto non è compreso Windows Defender. Le applicazioni firewall sono consentite.

  Se la disinstallazione di applicazioni antivirus, antimalware e antispyware di altri fornitori non è possibile, è necessario aggiungere le esclusioni a Advanced Threat Protection in Dell Server e anche alle altre applicazioni. Per istruzioni su come aggiungere esclusioni a Advanced Threat Protection nel server Dell, consultare http://www.dell.com/support/article/us/en/04/SLN300970. Per un elenco delle esclusioni da aggiungere ad altre applicazioni antivirus, consultare http://www.dell.com/support/article/us/en/19/SLN301134.

Sistemi operativi per Advanced Threat Prevention

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

Sistemi operativi Windows (a 32 e 64 bit)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Porte di Advanced Threat Prevention

- Gli agenti di Advanced Threat Prevention sono gestiti da e rispondono alla piattaforma SaaS della console di gestione. La porta 443 (https) viene utilizzata per le comunicazioni e deve essere aperta sul firewall affinché gli agenti possano comunicare con la console. La console è ospitata da Amazon Web Services e non è dotata di IP fissi. Se la porta 443 è bloccata per qualsiasi motivo, è impossibile scaricare gli aggiornamenti, quindi i computer potrebbero non disporre della protezione più recente. Accertarsi che i computer client abbiano accesso agli URL della tabella seguente.

Utilizzo	Protocollo dell'applicazione	Protocollo di trasporto	Numero di porta	Destinazione	Direzione
Tutte le comunicazioni	HTTPS	TCP	443	Consentire tutto il traffico https per *.cylance.com	In uscita

Verifica dell'integrità dell'immagine del BIOS

Se il criterio *Abilita verifica BIOS* è selezionato nella Remote Management Console, il tenant di Cylance convalida un hash del BIOS su sistemi utente finale al fine di garantire che il BIOS non sia stato modificato dalla versione di fabbrica Dell, che è un possibile vettore di attacco. Se viene rilevata una minaccia, viene passata una notifica al DDP Server e l'amministratore IT viene avvisato nella Remote Management Console. Per una panoramica del processo, consultare Processo di verifica dell'integrità dell'immagine del BIOS.

N.B.: Con questa funzione non è possibile utilizzare un'immagine di fabbrica personalizzata in quanto il BIOS è stato modificato.

Modelli di computer Dell che supportano la verifica dell'integrità dell'immagine del BIOS

- Latitude 3470
- Latitude 3570
- Latitude 7275
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision Mobile Workstation 3510
- Precision Mobile Workstation 5510
- Precision Workstation 3620
- Precision Workstation 7510
- Precision Workstation 7710
- Precision Workstation T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

Client dell'unità autocrittografante

- Per installare correttamente SED Management il computer deve disporre di una connessione di rete cablata.
- IPv6 non è supportato.
- Arrestare e riavviare il sistema dopo aver applicato i criteri per renderli effettivi.
- I computer dotati di unità autocrittografanti non possono essere utilizzati con le schede HCA. Sono presenti incompatibilità che impediscono il provisioning dell'HCA. Dell non vende computer con unità autocrittografanti che supportano il modulo HCA. Questa configurazione non supportata potrebbe essere una configurazione post vendita.
- Se il computer destinato alla crittografia è dotato di un'unità autocrittografante, 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.

IMPORTANTE:

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

- SED Management non è supportato da Server Encryption o Advanced Threat Prevention nel sistema operativo di un server.

Driver OPAL

- Le unità autocrittografanti compatibili con OPAL richiedono driver Intel Rapid Storage Technology aggiornati, che si trovano all'indirizzo http://www.dell.com/support.

Prerequisiti del client di crittografia

- Il programma di installazione principale di ESSE installa Microsoft Visual C++2010 SP1 **e** Microsoft Visual C++ 2012 Update 4 se non sono già installati nel computer. **Se si usa il programma di installazione figlio**, è necessario installare questi componenti prima di installare SED management.

Prerequisiti

- Visual C++ 2010 SP1 o Redistributable Package (x86 e x64) successivo
- Visual C++ 2012 Update 4 o Redistributable Package (x86 e x64) successivo

Hardware client dell'unità autocrittografante

Unità autocrittografanti compatibili con OPAL

- Per l'elenco più aggiornato di unità autocrittografanti compatibili con Opal supportate da SED Management, fare riferimento a questo articolo KB: http://www.dell.com/support/article/us/en/19/SLN296720.

Modelli di computer Dell supportati con UEFI

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

Modelli di computer Dell - Supporto UEFI

- Latitude 5280
- Latitude 5480
- Latitude 5580
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7270
- Latitude E7275
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M5520
- Precision M6800
- Precision M7510
- Precision M7520
- Precision M7710
- Precision M7720
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- OptiPlex 3050 All-In-One
- OptiPlex 3050 Tower, Small Form Factor, Micro
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 5050 Tower, Small Form Factor, Micro
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- OptiPlex 7050 Tower, Small Form Factor, Micro
- Venue Pro 11 (modelli 5175/5179)
- Venue Pro 11 (modello 7139)

Modelli di computer Dell - Supporto UEFI

- Latitude E7280
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude E7470
- Latitude E7480
- Latitude 12 Rugged Extreme
- Tablet Latitude 12 Rugged (modello 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Optiplex 3240 All-In-One
- OptiPlex 5250 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 7450 All-In-One
- OptiPlex 9020 Micro

N.B.:
Le funzionalità di autenticazione sono supportate in modalità UEFI in questi computer in cui sono in esecuzione Windows 8, Windows 8.1 e Windows 10 e dispongono di Unità autocrittografanti compatibili con OPAL qualificate. Altri computer in cui sono in esecuzione Windows 7, Windows 8, Windows 8.1 e Windows 10 supportano la modalità di avvio Legacy.

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-CH - Tedesco svizzero
- DE-FR - Francese svizzero

Supporto tastiere internazionali - Non-UEFI

- AR - Arabo (utilizza l'alfabeto latino)
- DE-CH - Tedesco svizzero
- DE-FR - Francese svizzero

Sistemi operativi dei client dell'unità autocrittografante

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

Sistemi operativi Windows (a 32 e 64 bit)

- Windows 7 SP0-SP1: Enterprise, Professional (supportato con modalità di avvio Legacy ma non UEFI)

  N.B.:
  La modalità di avvio Legacy è supportata in Windows 7. UEFI non è supportato in Windows 7.

- Windows 8: Enterprise, Pro,
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Client di autenticazione avanzata

- Se si usa Autenticazione avanzata, l'accesso degli utenti al computer verrà protetto utilizzando credenziali di autenticazione avanzata gestite e registrate tramite Security Tools. Security Tools sarà il gestore primario delle credenziali di autenticazione per l'accesso a Windows, incluse password, impronte digitali e smart card di Windows. Le credenziali per la password grafica, per il PIN e per le impronte digitali registrate tramite sistema operativo Microsoft non verranno riconosciute durante l'accesso a Windows.

  Per continuare a usare il sistema operativo Microsoft per la gestione delle credenziali, non installare o disinstallare Security Tools.
- Per la funzionalità Password monouso (OTP) di Security Tools è necessario che il computer sia dotato di TPM abilitato e di proprietà. L'OTP non è supportata con TPM 2.0. Per cancellare e impostare la proprietà del TPM, consultare https://technet.microsoft.com.
- Per un'unità autocrittografante non è necessario che il TPM fornisca l'Autenticazione avanzata o la crittografia.

Hardware del client di autenticazione avanzata

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

Lettori di impronte digitali e di smart card

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

Schede senza contatto

- Schede senza contatti che utilizzano lettori per schede senza contatti integrati nei portatili Dell specificati

Smart card

- Smart card PKCS #11 che utilizzano il client ActivIdentity

  N.B.:
  Il client ActivIdentity non è precaricato e deve essere installato separatamente.
- Schede per provider del servizio di crittografia (CSP, Cryptographic Service Provider)
- Schede di accesso comune (CAC, Common Access Card)
- Schede classe B/SIPR Net

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

Modelli di computer Dell - Supporto schede Classe B/SIPR Net

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Sistemi operativi del client di autenticazione avanzata

Sistemi operativi Windows

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

Sistemi operativi Windows (a 32 e 64 bit)

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

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

Sistemi operativi dei dispositivi mobili

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

Sistemi operativi Android

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

Sistemi operativi iOS

- iOS 7.x
- iOS 8.x

Sistemi operativi Windows Phone

- Windows Phone 8.1
- Windows 10 Mobile

Client di 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.
- 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 assumerà la proprietà del dispositivo TPM senza richiedere il riavvio. Tuttavia, se esiste già una proprietà TPM, BitLocker Manager inizierà il processo di configurazione della crittografia (senza richiedere il riavvio). È necessario che il TPM sia "di proprietà" e venga attivato.
- Il client di BitLocker Manager userà gli algoritmi convalidati AES FIPS approvati se è abilitata la modalità FIPS per l'impostazione di sicurezza del GPO per la “Crittografia del sistema: usando gli algoritmi conformi al FIPS per crittografia, hash e firma” nel dispositivo, sarà possibile gestire tale dispositivo attraverso il nostro prodotto. Questa modalità non viene impostata come predefinita 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 Server Encryption o Advanced Threat Prevention nel SO di un server.

Prerequisiti del client di BitLocker Manager

- Il programma di installazione principale di ESSE installa Microsoft Visual C++2010 SP1 **e** Microsoft Visual C++ 2012 Update 4 se non sono già installati nel computer. **Se si usa il programma di installazione figlio**, è necessario installare questi componenti prima di installare BitLocker Manager.

Prerequisiti

- Visual C++ 2010 SP1 o Redistributable Package (x86 e x64) successivo
- Visual C++ 2012 Update 4 o Redistributable Package (x86 e x64) successivo

Sistemi operativi del client di BitLocker Manager

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

Sistemi operativi Windows

- Windows 7 SP0-SP1: Enterprise, Ultimate (a 32 e 64 bit)
- Windows 8: Enterprise (a 64 bit)
- Windows 8.1: Enterprise Edition, Pro Edition (a 64 bit)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (a 64 bit)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (a 64 bit)
- Windows Server 2016

Opzioni di autenticazione

- Le seguenti opzioni di autenticazione richiedono hardware specifico: impronte digitali, smart card, schede senza contatto, schede classe B/SIPR Net e autenticazione su computer UEFI. Le opzioni seguenti richiedono le configurazioni di: smart card con Autenticazione di Windows, smart card con Autenticazione di preavvio e Password monouso. Le seguenti tabelle mostrano le opzioni di autenticazione disponibili a seconda del sistema operativo, quando i requisiti hardware e di configurazione vengono soddisfatti.

Client di crittografia

Non UEFI

	PBA					Autenticazione di Windows				
	Password	Impronta	Smart card con contatti	La sicurezza della OTP	Scheda SIPR	Password	Impronta	Smart card	La sicurezza della OTP	Scheda SIPR
Windows 7 SP0-SP1						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1 Update 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

1. Disponibile quando installato con il programma di installazione principale o con il pacchetto di Autenticazione avanzata quando vengono usati i programmi di installazione figlio.

2. Disponibile quando i driver di autenticazione vengono scaricati dal sito support.dell.com.

UEFI

	PBA - su computer Dell supportati					Autenticazione di Windows				
	Password	Impronta	Smart card con contatti	La sicurezza della OTP	Scheda SIPR	Password	Impronta	Smart card	La sicurezza della OTP	Scheda SIPR
Windows 7 SP0-SP1										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1 Update 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

1. Disponibile quando installato con il programma di installazione principale o con il pacchetto di Autenticazione avanzata quando vengono usati i programmi di installazione figlio.

2. Disponibile quando i driver di autenticazione vengono scaricati dal sito support.dell.com.

Client dell'unità autocrittografante

Non UEFI

	PBA					Autenticazione di Windows				
	Password	Impronta	Smart card con contatti	La sicurezza della OTP	Scheda SIPR	Password	Impronta	Smart card	La sicurezza della OTP	Scheda SIPR
Windows 7 SP0-SP1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8.1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 10	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]

1. Disponibile quando installato con il programma di installazione principale o con il pacchetto di Autenticazione avanzata quando vengono usati i programmi di installazione figlio.

2. Disponibile quando i driver di autenticazione vengono scaricati dal sito support.dell.com.

3. Disponibile con una SED OPAL supportata.

UEFI

	PBA - su computer Dell supportati					Autenticazione di Windows				
	Password	Impronta	Smart card con contatti	La sicurezza della OTP	Scheda SIPR	Password	Impronta	Smart card	La sicurezza della OTP	Scheda SIPR
Windows 7										
Windows 8	X[4]					X	X[2]	X[2]	X[1]	X[2]
Windows 8.1	X[4]					X	X[2]	X[2]	X[1]	X[2]

UEFI

	PBA - su computer Dell supportati					Autenticazione di Windows				
	Password	**Impronta**	**Smart card con contatti**	**La sicurezza della OTP**	**Scheda SIPR**	**Password**	**Impronta**	**Smart card**	**La sicurezza della OTP**	**Scheda SIPR**
Windows 10	X[4]					X	X[2]	X[2]	X[1]	X[2]

1. Disponibile quando installato con il programma di installazione principale o con il pacchetto di Autenticazione avanzata quando vengono usati i programmi di installazione figlio.

2. Disponibile quando i driver di autenticazione vengono scaricati dal sito support.dell.com.

4. Disponibile con una SED OPAL supportata in computer UEFI supportati.

BitLocker Manager

Non UEFI

	PBA [5]					Autenticazione di Windows				
	Password	**Impronta**	**Smart card con contatti**	**La sicurezza della OTP**	**Scheda SIPR**	**Password**	**Impronta**	**Smart card**	**La sicurezza della OTP**	**Scheda SIPR**
Windows 7						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]
Windows Server 2008 R2 (a 64 bit)						X		X[2]		

1. Disponibile quando installato con il programma di installazione principale o con il pacchetto di Autenticazione avanzata quando vengono usati i programmi di installazione figlio.

2. Disponibile quando i driver di autenticazione vengono scaricati dal sito support.dell.com.

5. Il PIN di preavvio di BitLocker è gestito tramite la funzionalità Microsoft.

UEFI

	PBA[5] - in computer Dell supportati					Autenticazione di Windows				
	Password	**Impronta**	**Smart card con contatti**	**La sicurezza della OTP**	**Scheda SIPR**	**Password**	**Impronta**	**Smart card**	**La sicurezza della OTP**	**Scheda SIPR**
Windows 7										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

UEFI

	PBA[5] - in computer Dell supportati					Autenticazione di Windows				
	Password	**Impronta**	**Smart card con contatti**	**La sicurezza della OTP**	**Scheda SIPR**	**Password**	**Impronta**	**Smart card**	**La sicurezza della OTP**	**Scheda SIPR**
Windows Server 2008 R2 (a 64 bit)						X		X[2]		

1. Disponibile quando installato con il programma di installazione principale o con il pacchetto di Autenticazione avanzata quando vengono usati i programmi di installazione figlio.

2. Disponibile quando i driver di autenticazione vengono scaricati dal sito support.dell.com.

5. Il PIN di preavvio di BitLocker è gestito tramite la funzionalità Microsoft.

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, verrà 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.

Impostazioni di registro del client di crittografia

- Se viene usato un certificato autofirmato nel server Dell per Enterprise Edition per Windows, la convalida dell'attendibilità del certificato deve rimanere disabilitata nel computer client (la convalida dell'attendibilità è *disabilitata* per impostazione predefinita in Enterprise Edition per Windows). 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 in EE Server/VE Server.
  - La catena di attendibilità completa del certificato deve essere archiviata nell'archivio chiavi Microsoft nel computer client.
  - Per *abilitare* la convalida dell'attendibilità per EE per Windows, modificare il valore della seguente voce di registro su 0 nel computer client.

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

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

  "MSSmartcardSupport"=dword:1
- 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 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 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 del registro nel modo seguente:

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

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

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

  "SnoozeBeforeSweep"=DWORD:1

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

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

  (NUMERO DI RITARDI DI AGGIORNAMENTO CRITERI CONSENTITI x DURATA DI CIASCUN RITARDO DI AGGIORNAMENTO CRITERI) + (5 MINUTI [NUMERO DI RITARDI DI AGGIORNAMENTO CRITERI CONSENTITI - 1])
- Usare la seguente impostazione di registro per fare eseguire al client di crittografia il polling dell'EE Server/VE Server per un aggiornamento forzato dei criteri. Creare o modificare l'impostazione del registro nel modo seguente:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  L'impostazione di registro scomparirà automaticamente al termine dell'operazione.
- Usare le seguenti impostazioni di registro per consentire al client di crittografia di inviare un inventario ottimizzato all'EE Server/VE Server, inviare un inventario completo all'EE Server/VE Server, o inviare un inventario completo all'EE Server/VE Server per tutti gli utenti attivati.

  - Inviare l'inventario ottimizzato all'EE Server/VE Server:

    Creare o modificare l'impostazione del registro nel modo seguente:

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

    "OnlySendInvChanges"=REG_DWORD:1

    Se non è presente alcuna voce, l'inventario ottimizzato viene inviato all'EE Server/VE Server.
  - Inviare l'inventario completo all'EE Server/VE Server:

Creare o modificare l'impostazione del registro nel modo seguente:

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

"OnlySendInvChanges"=REG_DWORD:0

Se non è presente alcuna voce, l'inventario ottimizzato viene inviato all'EE Server/VE 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 nell'insieme di credenziali in modo che, anche se il computer viene riavviato prima del caricamento dell'inventario, il client di 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 dell'EE Server/VE Server durante una distribuzione 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.

  IMPORTANTE:
  Configurare l'Attivazione in slot solo con l'assistenza di Dell ProSupport. Una configurazione impropria degli slot di tempo potrebbe comportare un tentativo, da parte di un gran numero di client, di attivazione per un EE Server/VE Server contemporaneamente, creando problemi potenzialmente gravi relativi alle prestazioni.

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

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

    Abilita o disabilita l'Attivazione in slot

    Disabilitata=0 (predefinito)

    Abilitata=1
  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat]

    Il periodo di tempo in secondi in cui ha luogo l'intervallo di slot di attivazione. Usare questa impostazione per modificare 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.
  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\SlotIntervals]

    L'intervallo nella ripetizione, ACTIVATION_SLOT_CALREPEAT, quando hanno luogo tutti gli slot di tempi di attivazione. È consentito solo un intervallo. L'impostazione deve essere 0,<CalRepeat>. Una variazione da 0 potrebbe causare risultati imprevisti. L'impostazione predefinita è 0,86400. Per impostare una ripetizione ogni sette ore, usare l'impostazione 0,25200. CALREPEAT viene attivato all'accesso di un utente.
  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\MissThreshold]

    Il numero di slot di attivazione che può essere perso prima che il computer tenti l'attivazione all'accesso successivo dell'utente la cui attivazione è stata suddivisa in slot. Se l'attivazione non ha luogo durante questo tentativo immediato, il client riprende i tentativi di attivazione in slot. Se l'attivazione non ha luogo a causa di un errore di rete, l'attivazione viene tentata alla riconnessione alla rete, anche se il valore in MISSTHRESHOLD non è stato superato. Se un utente si disconnette prima del raggiungimento del tempo dello slot di attivazione, verrà assegnato un nuovo slot all'accesso successivo.

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

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=dword:00000001

  0 =Disabled (Disabilitata; impostazione predefinita)

  1=Enabled (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 il client di crittografia sta elaborando un aggiornamento del criterio che include un criterio SDE attivo, la directory del profilo utente in uso viene crittografata per impostazione predefinita con la chiave SDUser (una chiave utente) piuttosto che con la chiave SDE (una chiave dispositivo). La chiave SDUser viene anche usata per crittografare file o cartelle che vengono copiate (non spostate) in una directory dell'utente che non è crittografata con SDE.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=dword:00000000

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

  Per ulteriori informazioni su SDUser, vedere www.dell.com/support/article/us/en/19/SLN304916
- 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 =Disabled (Disabilitata; impostazione predefinita)

  1=Enabled (Abilitata)

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

Impostazioni di registro del client di Advanced Threat Prevention

- Per far monitorare HKLM\SOFTWARE\Dell\Dell Data Protection al plug-in Advanced Threat Prevention per modifiche al valore LogVerbosity, e aggiornare il livello di registro del client di conseguenza, impostare il seguente valore.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=dword:<vedere di seguito>

  Dump: 0

  Errore irreversibile: 1

  Errore 3

  Avviso 5

  Info 10

  Dettagliata 12

  Traccia 14

  Debug 15

  Il valore del registro viene selezionato all'avvio del servizio ATP o quando cambia il valore. Se il valore del registro non esiste, non vi sarà alcun cambiamento a livello di registrazione.

  Usare questa impostazione di registro solo per esecuzione di test/debug, in quanto questa impostazione di registro controlla i dettagli di registro per altri componenti, inclusi client di crittografia e Client Security Framework.

- La Modalità di compatibilità consente l'esecuzione delle applicazioni nel computer client mentre i criteri Protezione della memoria oppure Protezione della memoria e Controllo script sono abilitati. L'abilitazione della modalità di compatibilità richiede l'aggiunta di un valore di registro nel computer client.

  Per abilitare la modalità di compatibilità, attenersi alla seguente procedura:

  a Nella Remote Management Console, disabilitare il criterio Protezione della memoria abilitata. Se il criterio Controllo script è abilitato, disabilitarlo.

  b Aggiungere il valore di registro CompatibilityMode.

  1 Usando l'editor del Registro di sistema nel computer client, andare a HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.

  2 Fare clic con il pulsante destro del mouse su **Desktop**, fare clic su **Autorizzazioni**, quindi assumere la proprietà e assicurarsi il pieno controllo.

  3 Fare clic con il pulsante destro del mouse su **Desktop**, quindi selezionare **Nuovo** > **Valore binario**.

  4 Per il nome, digitare `CompatibilityMode`.

  5 Aprire le impostazioni di registro e modificare il valore in `01`.

  6 Fare clic su **OK**, quindi chiudere l'editor del Registro di sistema.

  Per aggiungere il valore di registro con un comando, è possibile usare una delle seguenti opzioni della riga di comando da eseguire nel computer client:

  - Per un computer - Psexec:

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v CompatibilityMode /t
REG_BINARY /d 01
```

- (Per più computer) Invoke-Command cmdlet:

```
$servers = "testComp1","testComp2","textComp3"

$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item -
Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value 01}
```

c Nella Remote Management Console, abilitare nuovamente il criterio Protezione della memoria abilitata. Se il criterio Controllo script era abilitato in precedenza, abilitarlo nuovamente.

Impostazioni di registro del client dell'unità autocrittografante

- Per impostare l'intervallo tra tentativi quando l'EE Server/VE Server non è disponibile a comunicare con il client dell'unità autocrittografante, aggiungere il seguente valore di registro:

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

  "CommErrorSleepSecs"=dword:300

  Questo valore è il numero di secondi che il client dell'unità autocrittografante attende prima di provare a contattare l'EE Server/VE Server se questo non è disponibile a comunicare con tale client. Il valore predefinito è 300 secondi (5 minuti).
- Se viene usato un certificato autofirmato nell'EE Server/VE Server per SED Management, 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 Management). 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 in EE Server/VE 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 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 usare le smart card con l'Autenticazione di Windows, è necessario impostare il seguente valore di registro nel computer client:

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

  "MSSmartcardSupport"=dword:1
- Per usare smart card con l'autenticazione di preavvio, è necessario impostare il seguente valore di registro nel computer client. Impostare anche il criterio Metodo di autenticazione su Smart card nella Remote Management Console ed eseguire il commit della modifica.

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

  "MSSmartcardSupport"=dword:1
- 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 impostare l'intervallo in cui il client dell'unità autocrittografante proverà a contattare l'EE Server/VE Server quando non è disponibile a comunicare con tale client, impostare il valore seguente nel computer client:

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

  "CommErrorSleepSecs"=DWORD Value:300

  Questo valore è il numero di secondi che il client dell'unità autocrittografante attende prima di provare a contattare l'EE Server/VE Server se questo non è disponibile a comunicare con tale client. Il valore predefinito è 300 secondi (5 minuti).
- 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:<nuovo nome>.<organizzazione>.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
- 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://<nuovo nome>.<organizzazione>.com:8888/agent

Impostazioni di registro del client di Autenticazione avanzata

- Se **non** si desidera che il client di Autenticazione avanzata (Security Tools) 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**, Security Tools non tenterà di avviare i seguenti tre servizi:

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

    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 l'Autenticazione di Windows, è necessario impostare il seguente valore di registro nel computer client:

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

  "MSSmartcardSupport"=dword:1
- Per usare le smart card con autenticazione di preavvio dell'unità crittografante, è necessario impostare il seguente valore di registro nel computer client dotato di unità autocrittografante.

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

  "MSSmartcardSupport"=dword:1

  Impostare il criterio Metodo di autenticazione su Smart card nella Remote Management Console ed eseguire il commit della modifica.

Impostazioni di registro del client di BitLocker Manager

- Se viene usato un certificato autofirmato nell'EE Server/VE 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 in EE Server/VE 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

Eseguire l'installazione usando il programma di installazione principale di ESS

- 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 di ESS.
- I file di registro del programma di installazione principale diESS m si trovano in **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- 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 del client di crittografia. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consultare la *Guida a EMS* per istruzioni sulle funzioni dell'External Media Shield. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consultare *Security Tools, Guida a Endpoint Security Suite e Guida a Endpoint Security Suite Enterprise* per istruzioni sull'utilizzo delle funzioni di Autenticazione avanzata e Advanced Threat Prevention. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.
- Al completamento dell'installazione, gli utenti devono aggiornare i propri criteri facendo clic con il pulsante destro del mouse sull'icona di Dell Data Protection nell'area di notifica e selezionando **Verificare la disponibilità di aggiornamenti ai criteri**.
- Il programma di installazione principale di ESS installa l'intera suite di prodotti. Vi sono due metodi per eseguire l'installazione usando il programma di installazione principale di ESS. Scegliere uno dei seguenti:
  - Eseguire l'installazione interattiva usando il programma di installazione principale di ESSE

  oppure

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

Eseguire l'installazione interattiva usando il programma di installazione principale di ESS

- Il programma di installazione di ESS è disponibile:
  - **Dall'account Dell FTP** - Individuare il bundle di installazione in DDP-Endpoint-Security-Suite-1.x.x.xxx.zip.
- Usare queste istruzioni per installare Dell Endpoint Security Suite Enterprise interattivamente usando il programma di installazione principale di ESSE. Il presente metodo può essere utilizzato per installare la suite di prodotti in un computer alla volta.

1. Individuare **DDPSuite.exe** nel supporto di installazione Dell. Copiarlo nel computer locale.
2. Fare doppio clic su **DDPSuite.exe** per avviare il programma di installazione. L'operazione potrebbe richiedere alcuni minuti.
3. Fare clic su **Avanti** nella finestra di dialogo Introduzione.
4. Leggere il contratto di licenza, accettare i termini, e fare clic su **Avanti**.
5. Nel campo **Nome Enterprise Server**, immettere il nome host completo dell'EE Server/VE Server che gestirà l'utente di destinazione, ad esempio server.organizzazione.com.

   Nel campo **URL Device Server**, immettere l'URL del Device Server (Security Server) con cui comunicherà il client.

   , il formato è https://server.organization.com:**8443**/xapi**/** (inclusa la barra finale).

Fare clic su **Avanti.**

6 Fare clic su **Avanti** per installare il prodotto nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection\. Dell consiglia di eseguire l'installazione solo nel percorso predefinito**, in quanto potrebbero verificarsi problemi con l'installazione in altri percorsi.

7 Selezionare i componenti da installare.

Security Framework installa il framework di sicurezza di base e Security Tools, il client di autenticazione avanzata che gestisce più metodi di autenticazione, inclusi PBA e credenziali come impronte e password.

L'autenticazione avanzata consente di installare i file e i servizi necessari per l'autenticazione avanzata.

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

Threat Protection installa i client di Threat Protection, che sono la protezione da malware e antivirus per la ricerca di virus, spyware e programmi indesiderati, il firewall client per monitorare la comunicazione tra il computer e le risorse in rete/Internet, e il filtro Web per visualizzare le valutazioni di sicurezza o per bloccare l'accesso ai siti Web durante la navigazione online.

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.

Advanced Threat Protection installa il client di Advanced Threat Prevention, che è la protezione antivirus di ultima generazione che utilizza la scienza algoritmica e l'apprendimento automatico per identificare e classificare le cyber-minacce note e sconosciute e impedirne l'esecuzione o il danneggiamento degli endpoint.

Protezione *Web e Firewall* consente di installare le funzioni opzionali Protezione Web e Firewall. Il Firewall client controlla tutto il traffico in entrata e in uscita a fronte del suo elenco di regole. La Protezione Web monitora la navigazione Web e i download al fine di identificare minacce e, in caso ne vengano rilevate, applicare l'azione stabilita dal criterio, in base alle valutazioni dei siti Web.

> **N.B.: Threat Protection e Advanced Threat Prevention non possono coesistere nello stesso computer. Il programma di installazione impedisce automaticamente la selezione di entrambi i componenti. Se si desidera installare Threat Protection, per istruzioni scaricare la Guida all'installazione avanzata di Endpoint Security Suite.**

Fare clic su **Avanti** al termine delle selezioni.

8 Fare clic su **Installa** per avviare l'installazione. L'installazione potrebbe richiedere alcuni minuti.

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

L'installazione è completata.

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

- Nell'installazione dalla riga di comando le opzioni devono essere specificate per prime. Gli altri parametri devono essere inseriti nell'argomento che viene passato all'opzione /v.

Opzioni

- Nella tabella seguente sono illustrate le opzioni utilizzabili con il programma di installazione principale di ESSE.

Opzione	Descrizione
-y -gm2	Pre-estrazione del programma di installazione principale di ESS. Le opzioni -y e -gm2 devono essere utilizzate contemporaneamente. Non separare le opzioni.
/S	Installazione invisibile all'utente
/z	Consente di passare variabili al file .msi all'interno di DDPSuite.exe

Parametri

- Nella tabella seguente sono illustrati i parametri utilizzabili con il programma di installazione principale di ESS. Il programma di installazione principale di ESSE non può escludere singoli componenti ma può ricevere comandi per specificare quali componenti devono essere installati.

Parametro	Descrizione
SUPPRESSREBOOT	Sopprime il riavvio automatico al termine dell'installazione. Può essere usato in MODALITÀ NON INTERATTIVA.
SERVER	Specifica l'URL dell'EE Server/VE 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. ATP = Advanced Threat Prevention ***solo*** nel SO di un server; Advanced Threat Prevention ***ed*** Encryption nel SO di una workstation DE-ATP = Advanced Threat Prevention ed Encryption nel SO di un server. Utilizzare ***solo*** per l'installazione nel SO di un server. Questa è l'installazione predefinita nel SO di un server se il parametro FEATURES non è specificato. DE = Crittografia unità (client di crittografia) utilizzare ***solo*** per l'installazione nel SO di un server. BLM = BitLocker Manager SED = Gestione unità autocrittografanti (EMAgent/Manager, driver PBA/GPE)(disponibile solo quando vengono installate sul SO di una workstation) ATP-WEBFIREWALL = Firewall client e Protezione Web sul SO di una workstation DE-ATP-WEBFIREWALL = Firewall client e Protezione Web sul SO di un server **N.B.: Per gli aggiornamenti da Enterprise Edition o pre-v1.4 Endpoint Security Suite Enterprise, ATP-WEBFIREWALL o DE-ATP-WEBFIREWALL *deve* essere specificato al fine di installare Firewall client e Protezione Web. Non specificare ATP-WEBFIREWALL o DE-ATP-WEBFIREWALL quando si installa un client che sarà gestito da Dell Enterprise Server/VE in esecuzione in modalità Disconnesso.**
BLM_ONLY=1	Deve essere usato con FEATURES=BLM nella riga di comando per escludere il plug-in SED Management.

Esempio di riga di comando

- I parametri della riga di comando fanno distinzione tra maiuscole e minuscole.
- (nel SO di una workstation) In questo esempio vengono installati tutti i componenti usando il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente, nel percorso predefinito C:\Program Files\Dell\Dell Data Protection\e configurati per usare l'EE Server/VE Server specificato:

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- (nel SO di una workstation) In questo esempio viene installato Advanced Threat Prevention ed Encryption usando ***solo*** il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente, nel percorso predefinito C:\Program Files\Dell\Dell Data Protection\ e configurato per usare l'EE Server/VE Server specificato.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (nel SO di una workstation) In questo esempio viene installato Advanced Threat Prevention, Encryption e SED Management usando il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente e nessun riavvio, nel percorso predefinito C:\Program Files\Dell\Dell Data Protection\ e configurato per usare l'EE Server/VE Server specificato.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-SED,
SUPPRESSREBOOT=1\""
```

- (nel SO di una workstation) In questo esempio viene installato Advanced Threat Prevention, Encryption, Protezione Web e Firewall client usando il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente, nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection** e configurato per usare l'EE Server/VE Server specificato.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL\""
  ```

- (nel SO di un server) In questo esempio viene installato Advanced Threat Prevention ed Encryption usando ***solo*** il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente, nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection** e configurato per usare l'EE Server/VE Server specificato.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
  ```

- (nel SO di un server) In questo esempio viene installato Advanced Threat Prevention, Encryption, Protezione Web e Firewall client usando il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente, nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection**

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREWALL\""
  ```

- (nel SO di un server) In questo esempio viene installato Advanced Threat Prevention usando ***solo*** il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente, nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection** e configurato per usare l'EE Server/VE Server specificato.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
  ```

- (nel SO di un server) In questo esempio viene installato Encryption usando ***solo*** il programma di installazione principale di ESSE tramite porte standard, installazione invisibile all'utente, nel percorso predefinito **C:\Program Files\Dell\Dell Data Protection** e configurato per usare l'EE Server/VE Server specificato.

  ```
  "DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE\""
  ```

Eseguire la disinstallazione usando il programma di installazione principale di ESS

- Ciascun componente deve essere disinstallato separatamente, seguito dalla disinstallazione del programma di installazione principale di ESS. 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 di ESSE per ottenere i programmi di installazione figlio.
- Per la disinstallazione accertarsi di usare la stessa versione del programma di installazione principale di ESSE (e quindi dei client) usata 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 di ESS.
- Disinstallare i client nell'ordine seguente:

  a Disinstallare il client di crittografia.

  b Disinstallare Advanced Threat Prevention.

  c Disinstallare i client delle unità autocrittografanti e di Autenticazione avanzata (in questo modo si disinstalla il Client Security Framework di Dell, che non può essere disinstallato fino a quando non viene disinstallato Advanced Threat Prevention).

  d Disinstallare il client di BitLocker Manager

  Non è necessario disinstallare il pacchetto di driver.
- Passare a Disinstallare il programma di installazione principale di ESSE .

Disinstallare il programma di installazione principale di ESS

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

Disinstallazione dalla riga di comando

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

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

  Al termine, riavviare il sistema.

Eseguire l'installazione usando i programmi di installazione figlio

- Per installare ciascun client singolarmente, i file eseguibili figlio devono essere prima estratti dal programma di installazione principale di ESSE, come mostrato in Estrarre i programmi di installazione figlio dal programma di installazione principale di ESS .
- 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 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 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 verranno 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
/norestart	Viene eliminato il riavvio

- 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 del client di crittografia. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consultare la *Guida a EMS* per istruzioni sulle funzioni dell'External Media Shield. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consultare la per istruzioni sull'utilizzo delle funzioni di Autenticazione avanzata e Advanced Threat Prevention. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\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 ESSE. 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 il client di crittografia

- Se la propria organizzazione sta usando un certificato firmato da un'autorità radice, come EnTrust o Verisign, consultare i Requisiti del client di crittografia. Per abilitare la convalida del certificato, è necessario modificare le impostazioni di registro nel computer client.
- Al completamento dell'installazione, gli utenti devono aggiornare i propri criteri facendo clic con il pulsante destro del mouse sull'icona di Dell Data Protection nell'area di notifica e selezionando **Verificare la disponibilità di aggiornamenti ai criteri**.
- Il programma di installazione del client di crittografia è disponibile:
  - **Dall'account Dell FTP** - Individuare il bundle di installazione in DDP-Endpoint-Security-Suite-1.x.x.xxx.zip quindi Estrarre i programmi di installazione figlio dal programma di installazione principale di ESSE . Dopo l'estrazione, il file si trova in **C:\extracted\Encryption**.

Installazione dalla riga di comando

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

Parametri
SERVERHOSTNAME=<ServerName> (FQDN del server Dell 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 le icone dell'area di notifica, 1 le disabilita)

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=30,300 (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=300 (DEVE essere uguale o maggiore del limite superiore impostato in SLOTINTERVAL. Il tempo in secondi che il client di crittografia attende prima di generare un tentativo di attivazione in base a SLOTINTERVAL.)

Esempio di riga di comando

- 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"
```

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 il client di crittografia ed Encrypt for Sharing, vengono nascoste l'icona dell'area di notifica DDP e le icone sovrapposte, senza finestra di dialogo e barra di avanzamento, il riavvio viene eliminato e l'installazione avviene 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/ 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"
```

N.B.:

Alcuni client meno recenti potrebbero richiedere caratteri di escape \" 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 il client di Server Encryption

Sono disponibili due metodi per installare Server Encryption. Scegliere uno dei seguenti metodi:

- Installare il client di Server Encryption in maniera interattiva

  N.B.:

  Server Encryption può essere installato in maniera interattiva solo nei computer in cui sono in esecuzione i sistemi operativi dei 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 Server Encryption dalla riga di comando

Account utente virtuale

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

Prima di iniziare

- L'account utente che esegue l'installazione deve essere un utente locale o di dominio con autorizzazioni di livello amministratore.
- Per sostituire il requisito che un amministratore di dominio attivi Server Encryption, o per eseguire Server Encryption in server non di dominio o multi dominio, impostare la proprietà ssos.domainadmin.verify su falso nel file application.properties. Il file viene archiviato nei seguenti percorsi di file, in base al DDP Server che si sta utilizzando:

  Dell Enterprise Server - <cartella installazione>/Security Server/conf/application.properties

  Virtual Edition - /opt/dell/server/security-server/conf/application.properties
- Il server deve supportare il controllo delle porte.

  I criteri del Sistema di controllo porte server 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.
- Per attivare correttamente Server Encryption, 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, Server Encryption usa l'API di protezione dati (DPAPI) di Microsoft per proteggere la General Purpose Key.

  N.B.:

  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. Per istruzioni, consultare https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Estrarre il programma di installazione figlio

- Server Encryption richiede solo uno dei programmi di installazione nel programma di installazione principale. Per installare Server Encryption, è prima necessario estrarre il programma di installazione figlio del client di crittografia,**DDPE_xxbit_setup.exe**, dal programma di installazione principale. Consultare Estrarre i programmi di installazione figlio dal programma di installazione principale

Installare il client di Server Encryption in maniera interattiva

- Usare queste istruzioni per installare Server Encryption in modo interattivo. Il presente 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 Server Encryption in un server, fare doppio clic sul file **DDPE_XXbit_setup.exe** per avviare il programma di installazione.

> **N.B.:**
> Quando Server Encryption è installato in un computer che ha in esecuzione un sistema operativo del server come Windows Server 2012 R2, il programma di installazione installa la crittografia in modalità server per impostazione predefinita.

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 Fare clic su **Avanti** per installare Server Encryption nel percorso predefinito.

> **N.B.:**
> Dell consiglia di effettuare l'installazione nel percorso predefinito. È sconsigliata l'installazione in un percorso diverso da quello predefinito, che sia in una directory diversa, nell'unità D o in un'unità USB.

6 Fare clic su **Avanti** per ignorare la finestra di dialogo **Tipo di gestione**.

7 Nel campo Nome Dell Enterprise Server, immettere il nome host completo di Dell Enterprise Server o Virtual Edition che gestirà l'utente di destinazione (ad esempio *server.organizzazione.com*).

8 Immettere il nome di dominio nel campo **Dominio gestito** (ad esempio, organizzazione) e fare clic su **Avanti**.

9 Fare clic su **Avanti** per ignorare la finestra di dialogo **Informazioni su Dell proxy policy** popolata automaticamente.

10 Fare clic su **Avanti** per ignorare la finestra di dialogo **Informazioni su Dell Device Server** popolata automaticamente.

11 Fare clic su **Installa** per avviare l'installazione.
L'installazione potrebbe richiedere alcuni minuti.

12 Nella finestra di dialogo **Configurazione completata**, fare clic su Fine.
L'installazione è completata.

> **N.B.:**
> Il file di registro per l'installazione si trova nella directory %temp% dell'account, disponibile al percorso C:\Users\<nome utente>\AppData\Local\Temp. Per individuare il file di registro del programma di installazione, cercare un nome di file che inizi con MSI e termini con un'estensione .log. Il file deve avere un indicatore di data/ora corrispondente a quando è stato eseguito il programma di installazione.

> **N.B.:**
> Come parte dell'installazione, viene creato un **account utente virtuale del server** per l'uso esclusivo di Server Encryption. La password e l'autenticazione DPAPI sono disabilitate in modo che solo l'utente virtuale del server possa accedere alle chiavi di crittografia nel computer.

13 Riavviare il sistema.

> **IMPORTANTE: Selezionare Posporre riavvio solo se è necessario del tempo per salvare il lavoro e chiudere eventuali applicazioni aperte.**

Installare Server Encryption dalla riga di comando

Client di Server Encryption: individuare il programma di installazione 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=<Nome server di gestione> SERVERMODE=1 POLICYPROXYHOSTNAME=<Nome RGK> MANAGEDDOMAIN=<Proprio dominio> DEVICESERVERURL=<Nome server di attivazione> GKPORT=<Nuova porta GK> MACHINEID=<Nome computer> RECOVERYID=<ID ripristino> REBOOT=ReallySuppress HIDEOVERLAYICONS=1 HIDESYSTRAYICON=1 EME=1

N.B.:
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.
- È sconsigliata l'installazione in un percorso diverso da quello predefinito, che sia in una directory diversa, in un'unità diversa da C: o in un'unità USB. Dell consiglia di effettuare l'installazione nel percorso predefinito.
- Racchiudere un valore contenente uno o più caratteri speciali, ad esempio uno spazio, tra virgolette con escape.
- L'URL di Dell Activation Server (DEVICESERVERURL) rileva la distinzione tra maiuscole e minuscole.

Esempio di installazione dalla riga di comando

- Nell'esempio seguente viene installato il client di Server Encryption con i parametri predefiniti (client di Server Encryption, installazione invisibile all'utente, Encrypt for Sharing, senza finestra di dialogo, senza indicatore di stato, 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 il client di Server Encryption con un file di registro e parametri predefiniti (client di Server Encryption, installazione invisibile all'utente, Encrypt for Sharing, senza finestra di dialogo, senza barra di stato, 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.

  ```
  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"
```

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**.

Riavviare il sistema

Dopo l'installazione, riavviare il sistema. Il computer deve essere riavviato il prima possibile.

IMPORTANTE:

Selezionare **Posporre riavvio** solo se è necessario del tempo per salvare il lavoro e chiudere eventuali applicazioni aperte.

Attivare Server Encryption

- Il server deve essere connesso alla rete della propria organizzazione.
- Assicurarsi che il nome del computer del server sia il nome endpoint che si desidera visualizzare nella Remote Management Console.
- Un utente attivo e 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). Il client di Server Encryption non si attiva automaticamente.
- Durante l'attivazione iniziale, viene creato un account utente virtuale del server. 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 virtuale del server. Il pacchetto chiavi di crittografia associa le chiavi di crittografia e i criteri al nuovo utente virtuale del server per creare una relazione indissolubile tra i dati crittografati, il computer specifico e l'utente virtuale del server. Dopo l'attivazione del dispositivo, l'utente virtuale del server appare nella Remote Management Console come UTENTE-SERVER@*<nome server completo>*. 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 Remote Management Console. Tuttavia, se il client di Server Encryption si attiva nuovamente dopo che il nome del server viene modificato, il nuovo nome del server viene visualizzato nella Remote Management Console.

Una finestra di dialogo Attivazione viene visualizzata una volta dopo ogni riavvio per richiedere all'utente di attivare Server Encryption. Se l'attivazione non viene completata, seguire questa procedura:

1 Effettuare l'accesso al server o al server oppure usando la Connessione desktop remoto.

2 Fare clic con il pulsante destro del mouse sull'icona di Encryption  nell'area di notifica, e fare clic su **Informazioni**.

3 Verificare che Encryption sia in esecuzione in modalità server.

4 Selezionare **Attiva crittografia** dal menu.

5 Immettere il nome utente di un amministratore di dominio in formato UPN e la password, quindi fare clic su **Attiva**. È la stessa finestra di dialogo di attivazione che appare ogni volta che viene riavviato un sistema non attivato.

Il DDP Server emette una chiave di crittografia per l'ID della macchina, crea l'**account utente virtuale del server**, 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 virtuale del server.

6 Fare clic su **Chiudi**.

Al termine dell'attivazione, viene avviata la crittografia.

7 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 impostato su Vero, Server Encryption crittografa i file **\Windows \system32\config**, che includono le credenziali di Windows. I file in **\Windows\system32\config** vengono crittografati anche se il criterio *Crittografia SDE abilitata* è **Non selezionato**. Per impostazione predefinita, il criterio *Credenziali Windows di protezione* è **Selezionato**.

N.B.:
Dopo il riavvio del computer, l'autenticazione per il materiale della chiave comune richiede *sempre* la Chiave di macchina del server protetto. Il DDP Server restituisce una chiave di sblocco per accedere alle chiavi di crittografia e ai criteri nell'insieme di credenziali (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 Server Encryption è installato, autenticato e in modalità server. Se l'ID Shield è **rosso**, la crittografia non è stata ancora attivata.

L'utente virtuale del server

- Nella Remote Management Console, è possibile trovare un server protetto con il suo nome della macchina. Inoltre, ogni server protetto ha il proprio account utente virtuale del server. Ogni account ha un nome utente statico e un nome della macchina univoci.
- L'account utente virtuale del server viene usato solo da Server Encryption ed è altrimenti trasparente per il funzionamento del server protetto. L'utente virtuale del server è associato al pacchetto chiavi di crittografia e al policy proxy.
- Dopo l'attivazione, l'account utente virtuale del server è l'account utente che viene attivato e associato al server.
- Dopo che l'account utente virtuale del server ha effettuato l'attivazione, 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 virtuale del server, quindi scarica la chiave di macchina dal Dell Data Protection Server.

Installare il client di Advanced Threat Prevention

- Threat Protection e Advanced Threat Prevention **non possono coesistere nello stesso computer**. Non installare entrambi i componenti nello stesso computer perché si verificherebbero problemi di compatibilità. Se si desidera installare Threat Protection, per istruzioni scaricare la Guida all'installazione avanzata di Endpoint Security Suite.
- I programmi di installazione devono essere eseguiti seguendo un ordine specifico, altrimenti si verificherà un errore durante l'installazione. Eseguire i programmi di installazione nell'ordine seguente:

1 **(solo nel sistema operativo di una workstation)** \Security Tools - Advanced Threat Prevention necessita del componente Dell Client Security Framework.

(solo nel SO di un server) componente Dell Client Security Framework, come mostrato in Installazione dalla riga di comando.

2 **(solo nel SO di una workstation)** \Security Tools\Authentication - nel SO di una workstation, Security Tools e Authentication devono essere installati insieme; Authentication non è disponibile nel SO di un server e non deve essere installato.

3 Client di Advanced Threat Prevention, come mostrato in Installazione dalla riga di comando.

- Il programma di installazione del client di Advanced Threat Prevention è disponibile:
  - **Dall'account Dell FTP** - Individuare il pacchetto di installazione in DDP-Endpoint-Security-Suite-1.x.x.xxx.zip quindi Estrarre i programmi di installazione figlio dal programma di installazione principale di ESSE . Dopo l'estrazione, il file si trova in **C:\extracted \Advanced Threat Protection**.
- I programmi di installazione dei client dell'unità autocrittografante e Autenticazione avanzata si trovano in:
  - **Dall'account Dell FTP** - Individuare il pacchetto di installazione in DDP-Endpoint-Security-Suite-1.x.x.xxx.zip quindi Estrarre i programmi di installazione figlio dal programma di installazione principale di ESSE . Dopo l'estrazione, il file si trova in **C:\extracted \Security Tools** e **C:\extracted\Security Tools\Authentication**.

N.B.: I client dell'unità autocrittografante e di Autenticazione avanzata possono essere installati solo nel SO di una workstation e non nel SO di un server.

Installazione dalla riga di comando

- Per l'installazione sono disponibili i comandi .msi di base.
- La tabella seguente descrive in dettaglio i parametri disponibili per l'installazione.

Parametri
CM_EDITION=1 <gestione remota>
INSTALLDIR=<modificare la destinazione dell'installazione>
SERVERHOST=<securityserver.organizzazione.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organizzazione.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <nessuna voce nell'elenco Programmi nel Pannello di controllo>
REBOOT=ReallySuppress <elimina il riavvio>
FEATURE=BASIC <***richiesto*** nel SO di un server; può anche essere usato (facoltativamente) nel SO di una workstation; impedisce l'installazione di client SED Management e BitLocker Manager>

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 righe di comando

- Nell'esempio seguente viene installato il componente base di Dell Client Security Framework, senza il client di SED Management o 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"FEATURE=BASIC CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

- Nell'esempio seguente, viene installato Advanced Threat Protection (installazione invisibile all'utente, nessun riavvio, file di registro di installazione e cartella di installazione nei percorsi specificati)

```
MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress"
APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins"
ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs
\AdvancedThreatProtectionPlugins.msi.log"
```

e

```
AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:
\Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /l
"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
```

N.B.: Questi componenti devono essere installati solo dalla riga di comando. Facendo doppio clic per installare questo componente si installa una versione non Dell non gestita del prodotto, che non è supportato. In tal caso, andare a Installazione applicazioni e disinstallare tale versione.

Installare Protezione Web e Firewall

- Advanced Threat Prevention e Threat Protection **non possono coesistere sullo stesso computer**. Non installare entrambi i componenti nello stesso computer perché si verificherebbero problemi di compatibilità. Tuttavia, è possibile installare Advanced Threat Prevention con i componenti di Protezione Web e Firewall.
- I programmi di installazione devono essere eseguiti seguendo un ordine specifico, altrimenti si verificherà un errore durante l'installazione. Eseguire i programmi di installazione nell'ordine seguente:

1 Il client di crittografia è richiesto con i componenti di Protezione Web e Firewall. Per un esempio di installazione, andare a Esempio di riga di comando.

2 Protezione Web e Firewall, come mostrato in Installazione dalla riga di comando.

Installazione dalla riga di comando

- La tabella seguente descrive in dettaglio i parametri disponibili per il file **EnsMgmtSdkInstaller.exe**.

Parametri	Descrizione
LoadCert	Carica il certificato nella directory specificata.

- La tabella seguente descrive in dettaglio i parametri disponibili per il file **setupEP.exe**.

Parametri	Descrizione
ADDLOCAL="fw,wc"	Identifica i moduli da installare: fw= Firewall client wc=Protezione Web
override "hips"	Non installa Host Intrusion Prevention
INSTALLDIR	Percorso di installazione non predefinito
nocontentupdate	Indica al programma di installazione di non aggiornare automaticamente i file di dati nel quadro del processo di installazione. Dell consiglia la pianificazione di un aggiornamento non appena completato il processo di installazione.
nopreservesettings	Non salva le impostazioni.

- La tabella seguente descrive in dettaglio i parametri disponibili per il file **DellThreatProtection.msi**.

Parametri	Descrizione
Reboot=ReallySuppress	Elimina il riavvio.
ARP	0=Nessuna voce in Installazione applicazioni 1=Voce in Installazione applicazioni

- La tabella seguente descrive in dettaglio i parametri disponibili per il file **EnsMgmtSdkInstaller.exe**.

Parametri	Descrizione
ProtectProcesses	Specifica il nome del file e il percorso dei processi da proteggere.
InstallSDK	Installa SDK nel percorso specificato.

Parametri	Descrizione
RemoveRightClick	Rimuove l'opzione del menu tasto destro del mouse per gli utenti finali.
RemoveMcTray	Rimuove l'area di notifica.

Esempio di riga di comando

\Dell Threat Protection\SDK

- La seguente riga di comando carica i parametri predefiniti del certificato.

```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
```

> **N.B.:**
> Se si sta effettuando l'aggiornamento, questo programma di installazione può essere ignorato.

Quindi:

\Dell Threat Protection\EndPointSecurity

- Nel seguente esempio viene illustrata l'installazione di Protezione Web e Firewall client con i parametri predefiniti (modalità non interattiva, installazione di Firewall client e Protezione Web, sostituzione di Host Intrusion Prevention, nessun aggiornamento dei contenuti, nessuna impostazione salvata).

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /nocontentupdate /nopreservesettings /qn
```

Quindi:

\Dell Threat Protection\ThreatProtection\WinXXR

- Nell'esempio seguente viene installato il client con i parametri predefiniti (eliminazione del riavvio, nessuna finestra di dialogo, nessuna barra di avanzamento, nessuna voce nell'elenco Programmi nel Pannello di controllo).

```
"Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- L'esempio seguente installa SDK di Threat Protection.

```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

Installare i client di SED Management e Autenticazione avanzata

- Per l'autenticazione avanzata in v8.x è necessario il client dell'unità autocrittografante.
- Se la propria organizzazione sta usando un certificato firmato da un'autorità radice, come EnTrust o Verisign, consultare i Requisiti del Client dell'unità autocrittografante. 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 dei client dell'unità autocrittografante e Autenticazione avanzata si trovano in:
  - **Dall'account Dell FTP** - Individuare il bundle di installazione in DDP-Endpoint-Security-Suite-1.x.x.xxx.zip quindi Estrarre i programmi di installazione figlio dal programma di installazione principale di ESSE . Dopo l'estrazione, il file si trova in **C:\extracted\Security Tools** e **C:\extracted\Security Tools\Authentication.**

Installazione dalla riga di comando

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

Parametri
CM_EDITION=1 <gestione remota>
INSTALLDIR=<modificare la destinazione dell'installazione>
SERVERHOST=<securityserver.organizzazione.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organizzazione.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <nessuna voce nell'elenco Programmi nel Pannello di controllo>

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

\Security Tools

- Nell'esempio seguente viene installata un'unità autocrittografante gestita 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:

\Security Tools\Authentication

- Nell'esempio seguente viene installata l'Autenticazione avanzata (installazione invisibile all'utente, nessun riavvio)

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

Installare il client di BitLocker Manager

- 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 BtLocker Manager sono disponibili:
  - **Dall'account Dell FTP** - Individuare il bundle di installazione in DDP-Endpoint-Security-Suite-1.x.x.xxx.zip quindi Estrarre i programmi di installazione figlio dal programma di installazione principale di ESSE . Dopo l'estrazione, il file si trova in **C:\extracted\Security Tools**.

Installazione dalla riga di comando

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

Parametri
CM_EDITION=1 <gestione remota>
INSTALLDIR=<modificare la destinazione dell'installazione>
SERVERHOST=<securityserver.organizzazione.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organizzazione.com>
SECURITYSERVERPORT=8443
FEATURE=BLM <installare solo BitLocker Manager>
FEATURE=BLM,SED <installare BitLocker Manager con unità autocrittografante>
ARPSYSTEMCOMPONENT=1 <nessuna voce nell'elenco Programmi nel Pannello di controllo>

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"
```

Eseguire la disinstallazione usando i programmi di installazione figlio

- Per disinstallare ciascun client singolarmente, i file eseguibili figlio devono essere prima estratti dal programma di installazione principale di ESSE, come mostrato in Estrarre i programmi di installazione figlio dal programma di installazione principale di ESSE 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:\<qualsiasi directory>\<qualsiasi nome file di registro>.log**. Dell sconsiglia di usare "/l*v" (registrazione dettagliata) durante la disinstallazione da una riga di comando, poiché nome utente/password sono registrati nel file di registro.
- Per le disinstallazioni dalla riga di comando, tutti i programmi di installazione figlio usano le stesse opzioni di visualizzazione e .msi di base, tranne dove indicato diversamente. È necessario specificare prima le opzioni. L'opzione /v è obbligatoria e richiede un argomento. Gli altri parametri devono essere inseriti nell'argomento che viene passato all'opzione /v.

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

Opzione	Significato
/v	Consente di passare variabili al file .msi all'interno di setup.exe. 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 verranno copiati)

N.B.:
Con /v, sono disponibili le opzioni predefinite di Microsoft. Per un elenco di opzioni, consultare 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
/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 Protezione Web e Firewall

Se le funzioni Protezione Web e Firewall non sono installate, procedere alla sezione Disinstallare il client di crittografia.

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale di ESS, il programma di installazione del client Protezione Web e Firewall può essere trovato in **C:\extracted\Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi.**
- Nel Pannello di controllo, andare a Installazione applicazioni e disinstallare i seguenti componenti nell'ordine di seguito indicato:
  - McAfee Endpoint Security Firewall
  - McAfee Endpoint Security Web Control
  - McAfee Agent
- Quindi:
- Nel seguente esempio viene illustrata la disinstallazione di Protezione Web e Firewall.

```
MSIEXEC.EXE /x "DellThreatProtection.msi"
```

Disinstallare il client di crittografia e di crittografia 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.
- I Windows Shield ed Shield aggiornano l'EE Server/VE Server per modificare lo stato impostandolo su *Non protetto* all'inizio di un processo di disinstallazione Shield. Tuttavia, se il client non riesce a contattare l'EE Server/VE Server per qualsiasi motivo, non è possibile aggiornare lo stato. In questo caso sarà necessario selezionare manualmente l'opzione *Rimuovi endpoint* nella Remote

Management Console. Se l'organizzazione utilizza questo flusso di lavoro ai fini della conformità, Dell consiglia di verificare che lo stato *Non protetto* sia stato impostato come previsto nella Remote Management Console o in Compliance Reporter.

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.
- Prima della disinstallazione, se si usa l'opzione **Scarica chiavi dal server di Encryption Removal Agent** è necessario configurare Key Server (ed EE Server). Per istruzioni, consultare Configurare un Key Server per la disinstallazione del client di crittografia attivato per un EE Server. Non è necessaria alcuna azione precedente se il client da disinstallare è stato attivato per un VE Server, in quanto VE Server 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 Encryption Removal Agent è ancora presente nel pannello Servizi.

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale di ESSE, il programma di installazione del client di crittografia è disponibile al percorso **C:\extracted\Encryption\DDPE_XXbit_setup.exe**.
- La tabella seguente descrive in dettaglio i parametri disponibili per la disinstallazione.

Parametro	Selezione
CMG_DECRYPT	Proprietà che consente di selezionare il tipo di installazione di Encryption Removal Agent: 3 - Utilizzare il pacchetto LSARecovery 2 - Utilizzare il materiale della chiave Forensic scaricato in precedenza 1 - Scaricare le chiavi dal server Dell 0 - Non installare Encryption Removal Agent
CMGSILENTMODE	Proprietà che consente di eseguire la disinstallazione invisibile all'utente: 1 - Invisibile all'utente 0 - Visibile all'utente
Proprietà richieste	
DA_SERVER	FQHN per l'EE Server che ospita la sessione di negoziazione.
DA_PORT	Porta nell'EE Server per la richiesta (predefinita 8050).
SVCPN	Nome utente in formato UPN con cui il servizio Key Server ha effettuato l'accesso all'EE Server.

Parametro	Selezione
DA_RUNAS	Nome utente in formato compatibile con SAM nel cui contesto verrà effettuata la richiesta di ripristino delle chiavi. Questo utente deve essere incluso nell'elenco del Key Server nell'EE Server.
DA_RUNASPWD	Password per l'utente runas.
FORENSIC_ADMIN	L'account amministratore Forensic sul server Dell, 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 illustrata la disinstallazione automatica del client di crittografia e il download delle chiavi di crittografia dall'EE 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 illustrata la disinstallazione automatica del client di crittografia e il download delle chiavi di crittografia dal VE Server 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.

IMPORTANTE:

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 Remote 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.

N.B.:

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 Advanced Threat Prevention

Disinstallazione dalla riga di comando

- L'esempio seguente disinstalla il client di Advanced Threat Protection. ***Questo comando deve essere eseguito da un prompt dei comandi come amministratore.***

  ```
  wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
  ```

  Arrestare e riavviare il computer, quindi disinstallare il componente Dell Client Security Framework.

- **IMPORTANTE: Se sono stati installati sia i client delle unità autocrittografanti che di Autenticazione avanzata o è stata attivata l'autenticazione di preavvio, seguire le istruzioni di disinstallazione in Disinstallare i client delle unità autocrittografanti e di Autenticazione avanzata.**

  Il seguente esempio disinstalla solo il componente Dell Client Security Framework e non i client delle unità autocrittografanti e di Autenticazione avanzata.

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

Disinstallare i client delle unità autocrittografanti e di Autenticazione avanzata

- La connessione di rete all'EE Server/VE Server è necessaria per disattivare la PBA.

Procedura

- Disattivare la PBA, che rimuove tutti i dati di PBA dal computer e sblocca le chiavi delle unità autocrittografanti.
- Disinstallare il client dell'unità autocrittografante.
- Disinstallare il client di Autenticazione avanzata.

Disattivare la PBA

1. Eseguire l'accesso alla Remote Management Console come amministratore Dell.
2. Nel riquadro sinistro fare clic su **Protezione e gestione** > **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 l'icona **Dettagli** del computer desiderato.
7. Fare clic su **Criteri di protezione** dal menu principale.

8 Selezionare **Unità autocrittografanti** dal menu a discesa **Categoria criteri**.

9 Espandere l'area **Amministrazione unità autocrittografanti** e modificare i criteri **Attiva SED Management** e **Attiva PBA** da *True* a ***False***.

10 Fare clic su **Salva**.

11 Nel riquadro sinistro fare clic su **Azioni** > **Commit criteri**.

12 Fare clic su **Applica modifiche**.

Attendere la propagazione del criterio dall'EE Server/VE Server al computer destinato alla disattivazione.

In seguito alla disattivazione della PBA, disinstallare i client dell'unità autocrittografante e di Autenticazione avanzata.

Disinstallare il client dell'unità autocrittografante e i client di Autenticazione avanzata

Disinstallazione dalla riga di comando

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

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

  Al termine, arrestare e riavviare il sistema.

  Quindi:

- Nell'esempio seguente viene eseguita la disinstallazione automatica del client di Autenticazione avanzata.

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

  Al termine, arrestare e riavviare il sistema.

Disinstallare il client di BitLocker Manager

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale di ESSE, il programma di installazione del client di BitLocker è disponibile al percorso C:\extracted\Security Tools\EMAgent_XXbit_setup.exe.
- L'esempio seguente disinstalla automaticamente il client di BitLocker Manager.

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

  Al termine, riavviare il sistema.

8

Scenari di uso comune

- Per installare ciascun client singolarmente, i file eseguibili figlio devono essere prima estratti dal programma di installazione principale di ESSE, come mostrato in Estrarre i programmi di installazione figlio dal programma di installazione principale di ESS .
- Il client dell'unità autocrittografante è richiesto per l'Autenticazione avanzata nella v8.x, per questo fa parte della riga di comando negli esempi seguenti.
- Il programma di installazione figlio di Advanced Threat Prevention deve essere installato solo dalla riga di comando. Facendo doppio clic per installare questo componente si installa una versione non Dell non gestita del prodotto, che non è supportato. In tal caso, andare a Installazione applicazioni e disinstallare tale versione.
- 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

Opzione	Significato
/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 *Guida alla crittografia di Dell* per istruzioni sull'utilizzo della funzione del client di crittografia. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consultare la *Guida a EMS* per istruzioni sulle funzioni dell'External Media Shield. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**
  - Consultare *Security Tools, Guida a Endpoint Security Suite e Guida a Endpoint Security Suite Enterprise* per istruzioni sull'utilizzo delle funzioni di Autenticazione avanzata e Advanced Threat Prevention. Accedere alla guida da **<directory installazione>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.

Encryption Client, Advanced Threat Prevention e Autenticazione avanzata

- Nell'esempio seguente viene installata un'unità autocrittografante gestita 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**). Questo componente installa Dell Client Security Framework che è richiesto da Advanced Threat Prevention.

  ```
  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 Advanced Threat Prevention (installazione invisibile all'utente, nessun riavvio, file di registro di installazione e cartella di installazione nei percorsi specificati)

  ```
  MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress"
  APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs
  \AdvancedThreatProtectionPlugins.msi.log"
  ```

  e

  ```
  AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:
  \Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /l
  "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
  ```

- Nell'esempio seguente viene installato il client di crittografia 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"
  ```

- Nei seguenti esempi vengono installate le funzioni ***opzionali*** Protezione Web e Firewall.
- **\Dell Threat Protection\SDK**

  La seguente riga di comando carica i parametri predefiniti del certificato.

```
EnsMgmtSdkInstaller.exe -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs
\McAfeeSDKInstallerBeforeEndPoint.log"
```

N.B.:
Se si sta effettuando l'aggiornamento, questo programma di installazione può essere ignorato.

Quindi:

\Dell Threat Protection\EndPointSecurity

- Nell'esempio seguente viene illustrata l'installazione delle funzioni opzionali Protezione Web e Firewall con i parametri predefiniti (modalità non interattiva, installazione di Threat Protection, Firewall client e Protezione Web, sostituzione di Host Intrusion Prevention, nessun aggiornamento dei contenuti, nessuna impostazione salvata).

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /
nocontentupdate /nopreservesettings /qn
```

Quindi:

\Dell Threat Protection\ThreatProtection\WinXXR

- Nell'esempio seguente viene installato il client con i parametri predefiniti (eliminazione del riavvio, nessuna finestra di dialogo, nessuna barra di avanzamento, nessuna voce nell'elenco Programmi nel Pannello di controllo).

```
"DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- L'esempio seguente installa SDK di Threat Protection.

```
EnsMgmtSdkInstaller.exe -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat
Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell
\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

Client dell'unità autocrittografante (inclusa l'Autenticazione avanzata) ed External Media Shield

- Nell'esempio seguente viene installata un'unità autocrittografante gestita 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 installata solo EMS (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"
```

BitLocker Manager ed External Media Shield

- 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 installata solo EMS (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"
  ```

BitLocker Manager e Advanced Threat Prevention

- 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**). Questo componente installa Dell Client Security Framework che è richiesto da Advanced Threat 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 Advanced Threat Protection (installazione invisibile all'utente, nessun riavvio, file di registro di installazione e cartella di installazione nei percorsi specificati)

  ```
  MSIEXEC.EXE /I "AdvancedThreatProtection_xXX.msi" /qn REBOOT="ReallySuppress"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\ATP.log"
  APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection"
  ```

9

Eseguire il provisioning del tenant di Advanced Threat Prevention

Se l'organizzazione utilizza Advanced Threat Prevention, deve essere eseguito il provisioning di un tenant nel Server Dell prima che diventi attiva l'applicazione dei criteri di Advanced Threat Prevention.

Prerequisiti

- Deve essere eseguito da un amministratore con il ruolo di amministratore di sistema.
- Deve essere dotato della connettività ad Internet per eseguire il provisioning nel Server Dell.
- Deve essere dotato della connettività ad Internet nel client per visualizzare l'integrazione del servizio online di Advanced Threat Prevention nella Remote Management Console.
- Il provisioning è basato su un token generato da un certificato durante il provisioning.
- Le licenze di Advanced Threat Prevention devono essere presenti nel Server Dell.

Eseguire il provisioning di un tenant

1 Accedere alla Remote Management Console e passare a **Gestione dei servizi**.

2 Fare clic su **Imposta il servizio Advanced Threat Protection**. Se si verifica un guasto a questo punto, importare le licenze ATP.

3 La procedura guidata di installazione si avvia quando le licenze vengono importate. Fare clic su **Avanti** per iniziare.

4 Leggere e accettare l'EULA (la casella di controllo è **disattivata** per impostazione predefinita) e fare clic su **Avanti**.

5 Fornire le credenziali di identificazione al DDP server per il provisioning del tenant. Fare clic su **Avanti**. *Il provisioning di un tenant esistente che è prodotto da Cylance non è supportato.*

6 Scaricare il certificato. Questa operazione è necessaria per il ripristino in caso di emergenza con il DDP Server. Il certificato non è sottoposto a backup automatico tramite la v9.2 del "programma di aggiornamento". Eseguire il backup del certificato in una posizione sicura su un altro computer. Selezionare la casella per confermare che è stato eseguito il backup del certificato e fare clic su **Avanti**.

7 La configurazione è stata completata. Fare clic su **OK**.

Configurare l'aggiornamento automatico dell'agente di Advanced Threat Prevention

Nella Remote Management Console di Dell Server, è possibile registrarsi per ricevere gli aggiornamenti automatici dell'agente di Advanced Threat Prevention. La registrazione per ricevere gli aggiornamenti automatici dell'agente consente ai client di effettuare il download automatico e installare gli aggiornamenti dal server di Advanced Threat Prevention. Gli aggiornamenti vengono rilasciati ogni mese.

N.B.: Gli aggiornamenti automatici vengono supportati con Dell Server v9.4.1 o versione successiva.

Ricevere gli aggiornamenti automatici dell'agente

Per registrarsi per ricevere gli aggiornamenti automatici dell'agente:

1. Nel riquadro sinistro della Remote Management Console, fare clic su **Gestione** > **Gestione dei servizi**.
2. Nella scheda **Minacce avanzate**, sotto Aggiornamento automatico agente, fare clic sul pulsante **Attivato** e quindi sul pulsante **Salva preferenze**.

   L'operazione può richiedere alcuni minuti per completare le informazioni e visualizzare gli aggiornamenti automatici.

Interrompere la ricezione degli aggiornamenti automatici dell'agente

Per interrompere la ricezione degli aggiornamenti automatici dell'agente:

1. Nel riquadro sinistro della Remote Management Console, fare clic su **Gestione** > **Gestione dei servizi**.
2. Nella scheda **Minacce avanzate**, sotto Aggiornamento automatico agente, fare clic sul pulsante **Disattivato** e quindi sul pulsante **Salva preferenze**.

Configurazione di preinstallazione per Password monouso, UEFI unità autocrittografante e BitLocker

Inizializzare il TPM

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

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

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

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** (Impostazioni BIOS) e premere **Invio**.
4 Selezionare **Settings** > **General** > **Advanced Boot Options** (Impostazioni > Generali > Opzioni di avvio avanzate).
5 Deselezionare la casella di controllo **Enable Legacy Option ROMs** (Abilita ROM di opzione legacy) e fare clic su **Apply** (Applica).

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 assumerà la proprietà del TPM (non sarà necessario il riavvio). Tuttavia, se esiste già una proprietà del TPM, BitLocker Manager inizierà il processo di configurazione della crittografia. È necessario che TPM sia "di proprietà".
- 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 seguirà la stessa procedura di configurazione guidata di BitLocker.

```
BdeHdCfg -target default
```

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

Impostare l'oggetto criterio di gruppo nel controller di dominio per abilitare i diritti

- Se i client ricevono i diritti da Dell Digital Delivery (DDD), seguire queste istruzioni per impostare l'oggetto criterio di gruppo nel controller di dominio per abilitare i diritti (potrebbe non trattarsi dello stesso server in cui è in esecuzione l'EE Server/VE Server).
- La workstation deve appartenere all'unità organizzativa in cui è applicato l'oggetto criterio di gruppo.

> **N.B.:**
> Accertarsi che la porta in uscita 443 sia disponibile per la comunicazione con l'EE Server/VE Server. Se la porta 443 è bloccata (per qualsiasi motivo), la funzionalità per i diritti non sarà utilizzabile.

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: <indirizzo IP dell'EE Server/VE Server>
7. Fare clic su **OK**.
8. Effettuare la disconnessione e quindi accedere nuovamente alla workstation, oppure eseguire **gpupdate /force** per applicare il criterio di gruppo.

Estrarre i programmi di installazione figlio dal programma di installazione principale di ESS

- Per installare ciascun client individualmente, estrarre i file eseguibili figlio dal programma di installazione.
- Il programma di installazione principale di ESS non è un *programma di disinstallazione*. Ciascun client deve essere disinstallato separatamente, seguito dalla disinstallazione del programma di installazione principale di ESS. Usare questa procedura per estrarre i client dal programma di installazione principale di ESS in modo da poterli utilizzare per la disinstallazione.

1 Dal supporto di installazione Dell, copiare nel computer locale il file **DDPSuite.exe**.

2 Aprire un prompt dei comandi nello stesso percorso del file **DDPSuite.exe** e immettere:

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

Il percorso di estrazione non può superare i 63 caratteri.

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

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

Configurare un Key Server per la disinstallazione del client di crittografia attivato per un EE Server

- In questa sezione viene spiegato come configurare i componenti da usare con l'autenticazione/autorizzazione Kerberos quando si utilizza un EE Server. Il VE Server 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 accesso viene consentito nella Remote Management Console tramite singoli domini.
- Se è necessario usare l'autenticazione/autorizzazione Kerberos, il server che contiene il componente Key Server dovrà essere parte integrante del dominio coinvolto.
- Poiché il VE Server non usa il Key Server, non è possibile usare la disinstallazione tipica. Quando viene disinstallato un client di crittografia attivato per un VE Server, viene usato il recupero standard delle chiavi Forensic tramite il 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 Nell'EE 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:**.

  Nel campo *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 <directory di installazione di Key Server> per verificare che il servizio sia stato avviato.

File di configurazione di Key Server - Aggiungere un utente per la comunicazione con EE server

1 Passare a <directory di installazione di Key Server>.

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 all'EE 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 all'EE 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 "mrossi", l'operazione potrebbe avere esito negativo. L'EE Server, infatti, non sarà in grado di autenticare "mrossi" 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="<valore crittografato della password>" /> e modificare "epw" in "password". Quindi modificare "<valore crittografato della password>" con la password dell'utente al passaggio 3. Questa password viene crittografata nuovamente al riavvio dell'EE Server.

Se si utilizza "superadmin" nel passaggio 3 e la password superadmin non è "changeit", dovrà essere modificata in questo punto. Salvare e chiudere il 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 EE 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 Remote Management Console. Il formato di "superadmin" può essere qualsiasi metodo in grado di eseguire l'autenticazione all'EE 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 all'EE 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 "mrossi", l'operazione potrebbe avere esito negativo. L'EE Server, infatti, non sarà in grado di autenticare "mrossi" 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 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="valore crittografato della password" /> [password utilizzata per comunicare con il Security Server. Se la password superadmin è stata modificata, sarà necessario cambiarla in questo punto.]

</appSettings>

</configuration>

Pannello Servizi - Riavviare il 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 <directory di installazione di Key Server> per verificare che il servizio sia stato avviato.
4 Chiudere il pannello Servizi.

Remote Management Console - Aggiungere un amministratore Forensic.

1 Se necessario, accedere alla Remote Management Console.
2 Fare clic su **Popolamenti** > **Domini**.
3 Selezionare il dominio appropriato.
4 Fare clic sulla scheda **Key Server**.
5 Nel campo Account, aggiungere l'utente che eseguirà le attività di 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 nel passaggio 5. Fare clic su **Cerca**.
7 Una volta individuato l'utente corretto, fare clic sulla scheda **Amministratore**.
8 Selezionare **Amministratore Forensic** e fare clic su **Aggiorna**.
I componenti sono ora configurati per l'autenticazione/autorizzazione Kerberos.

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 ad un EE Server/VE Server.
- Questa utilità usa uno dei seguenti metodi per scaricare un bundle di 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

Usare l'Administrative Download Utility in 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/.

Amministratore Dell: nome dell'amministratore con credenziali di amministratore Forensic (abilitato nella Remote Management Console), come mrossi

Password: password dell'amministratore Forensic

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

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

> **SUGGERIMENTO:**
> Solitamente, è sufficiente specificare l'MCID *o* il DCID. Tuttavia, se sono noti, è utile immetterli entrambi. Ciascun parametro contiene informazioni diverse su client e computer client.

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 predefinito in cui salvare il file, oppure fare clic su ... 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**.

Usare l'Administrative Download Utility in modalità Amministratore

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

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

> **SUGGERIMENTO:**
> Solitamente, è sufficiente specificare l'MCID *o* il DCID. Tuttavia, se sono noti, è utile immetterli entrambi. Ciascun parametro contiene informazioni diverse su client e computer client.

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 predefinito in cui salvare il file, oppure fare clic su ... 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**.

Configurare Server Encryption

Abilitare Server Encryption

N.B.:
Server Encryption converte la crittografia dell'utente in crittografia comune.

1 Accedere come amministratore Dell alla Dell Remote Management Console.

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 Server Encryption 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 di 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 Data Protection dal menu dell'icona Encryption, che si trova nell'area di notifica.

Impostare i Criteri EMS di crittografia server

Il ***computer crittografante di origine*** è il computer che crittografa originariamente un dispositivo rimovibile. Quando il computer di origine è un ***server protetto*** (un server con Server Encryption installato e attivato) 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 EMS 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 Remote Management Console sotto il gruppo di tecnologia *Server Encryption*.

Crittografia del server e supporti esterni

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

N.B.:
Server Encryption 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 il 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 di origine 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 saranno in grado di 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.

Quando il computer crittografante di origine di un dispositivo rimovibile è un server protetto, il proprietario/utente deve sempre effettuare l'accesso al dispositivo rimovibile quando lo usa sui computer non di origine, indipendentemente dalle impostazioni di criterio EMS definite negli altri computer.

Fare riferimento alla Guida dell'amministratore per informazioni sui criteri di Controllo delle porte e EMS di Server Encryption.

Sospendere un'istanza del server crittografato

La sospensione di un server crittografato impedisce l'accesso ai suoi dati crittografati dopo un riavvio. L'utente virtuale del server non può essere sospeso. Al contrario, la Chiave di computer di Server Encryption viene 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.

IMPORTANTE:

Da utilizzare con cautela. La sospensione di un'istanza 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 Remote Management Console.
- L'amministratore deve aver effettuato l'accesso alla Remote Management Console.

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

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

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

N.B.:

Fare clic sul pulsante **Ripristina** per permettere a Server Encryption di accedere ai dati crittografati nel server dopo il riavvio.

Risoluzione dei problemi

Tutti i client - Risoluzione dei problemi

- I **file di registro del programma di installazione principale** di **ESSE** si trovano in 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\<UserName>\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\<UserName>\AppData\Local\Temp. For example, C:\Users\<UserName>\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=30653per scaricare la versione completa di Microsoft .Net Framework 4.5.
- Consultare Compatibilità di *Dell Data Protection | Security Tools* se nel computer destinato all'installazione è (o è stato in passato) installato Dell Access. DDP|A non è compatibile con questa suite di prodotti.

Risoluzione dei problemi del client di crittografia e di crittografia server

Eseguire l'aggiornamento a Windows 10 Anniversary Update

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

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 di attivazione immettere le credenziali di un amministratore di dominio e accertarsi che siano 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 DDP Security 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 DDP 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 di DDP Server deve essere la versione 9.1 o successiva. Se necessario, aggiornare il DDP Server alla versione 9.1 o successiva.
- Controllare l'URL del DDP 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 di Server Encryption richiede che un utente in tempo reale acceda al server. 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 Attivazione quando si verifica una delle seguenti due cose:

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

Il processo di attivazione iniziale è come segue:

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

N.B.:
La richiesta delle credenziali di amministratore di dominio è una misura di sicurezza che impedisce a Server Encryption di essere trasferito su altri ambienti di server che non lo supportano. Per disabilitare la richiesta di credenziali di amministratore di dominio, consultare Prima di iniziare.

6 DDP Server controlla le credenziali nell'insieme di credenziali aziendale (Active Directory o equivalente) per verificare che le credenziali sono credenziali di amministratore di dominio.

7 Un UPN è costruito usando le credenziali.

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

L'**account utente virtuale del server** è ad uso esclusivo del client di crittografia. Verrà 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 parte di attivazione, autenticazione e 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, Server Encryption effettua automaticamente l'accesso come utente virtuale del server e richiede la chiave di computer al DDP Enterprise Server. Questo avviene anche prima che qualsiasi utente possa effettuare l'accesso.

- Aprire la finestra di dialogo Informazioni per confermare che Server Encryption è autenticato e in modalità server.
- Se l'ID Shield è rosso, la crittografia non è stata ancora attivata.
- Nella Remote 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 *Intervallo tra tentativi a seguito di un errore di rete*, fare riferimento alla Guida dell'amministratore, disponibile nella Remote Management Console.

Autenticazione e processo di 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 DDP Server:

- Se il computer non ha eseguito l'attivazione del dispositivo in precedenza, il DDP Server assegna al computer un MCID, un DCID e un certificato di attendibilità e memorizza tutte le informazioni nell'insieme di credenziali del DDP Server.

- Se il computer ha eseguito l'attivazione del dispositivo in precedenza, il DDP Server verifica il certificato di attendibilità.

3 Dopo che il DDP Server ha assegnato il certificato di attendibilità al server, il server può accedere alle chiavi di crittografia.

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 errori che impediscono l'esecuzione del servizio

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

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

  5: registra informazioni sul debug

Trovare la versione TSS

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

Interazioni tra EMS e il Sistema di controllo porte

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

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

Per crittografare dati scritti su CD/DVD

- Impostare EMS - Crittografa il supporto esterno = Vero.

- Impostare EMS - Escludi crittografia CD/DVD = Falso.
- Sottoclasse memorizzazione: Controllo unità ottiche = Solo UDF

Usare WSScan

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

Eseguire WSScan

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

OPPURE

1 Fare clic su **Avanzate** per attivare/disattivare la visualizzazione su **Semplice** per sottoporre a scansione una cartella specifica.
2 Accedere a Impostazioni di scansione e inserire il percorso della cartella nel campo **Percorso di ricerca**. Se si utilizza questo campo, la selezione nella casella di riepilogo viene ignorata.
3 Se non si desidera scrivere i risultati della scansione di WSScan su file, disattivare la casella di controllo **Output su file**.
4 Modificare il percorso e il nome del file predefiniti in *Percorso*, se lo si desidera.
5 Selezionare **Aggiungi a file esistente** se non si desidera sovrascrivere nessun file di output WSScan esistente.
6 Scegliere il formato di output:
   - Selezionare Formato rapporto per un elenco di tipo rapporto dell'output sottoposto a scansione. Questo è il formato predefinito.
   - Selezionare File delimitato da valore per l'output che è possibile importare in un'applicazione per foglio di calcolo. Il delimitatore predefinito è "|", ma può essere sostituito da un massimo di 9 caratteri alfanumerici, spazi o segni di punteggiatura.
   - Selezionare l'opzione Valori tra virgolette per delimitare ogni valore tra virgolette.
   - Selezionare File a larghezza fissa per output non delimitati contenenti una linea continua di informazioni a lunghezza fissa per ciascun file crittografato.
7 Fare clic su **Cerca**.

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

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. **Se viene usata 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.
-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" is still AES256 encrypted

Output	Significato
Indicatore data e ora	La data e l'ora in cui il file è stato scansionato.
Tipo di crittografia	Il tipo di crittografia utilizzato per crittografare il file. **SysData**: chiave di crittografia SDE. **Utente**: chiave di crittografia utente. **Comune**: chiave di crittografia comune. WSScan non riporta i file crittografati tramite Encrypt for Sharing.
KCID	L'ID del computer principale. Come mostrato nell'esempio riportato sopra, "**7vdlxrsb**". Se si esegue la scansione di un'unità di rete mappata, il rapporto di scansione non genera un KCID.
UCID	L'ID utente. Come mostrato nell'esempio riportato sopra, "**_SDENCR_**". L'UCID è condiviso da tutti gli utenti del computer.
File	Il percorso del file crittografato. Come mostrato nell'esempio riportato sopra, "**c:\temp\Dell - test.log**".
Algoritmo	L'algoritmo di crittografia utilizzato per crittografare il file. Come mostrato nell'esempio riportato sopra, "**is still AES256 encrypted**" RIJNDAEL 128 RIJNDAEL 256 AES 128 AES 256 3DES

Usare WSProbe

La Probing Utility può essere usata con tutte le versioni del client di crittografia, ad eccezione dei criteri di EMS. Utilizzare la Probing Utility per:

- Sottoporre a scansione o pianificare la scansione di un computer crittografato. La Probing Utility rispetta il criterio 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 Vero. Se Esegui scansione workstation all'accesso è impostato su Vero, 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 si desidera lavorare deve essere crittografato.
- L'utente con il quale si desidera 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 che si desidera 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.
-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 aggiornare il relativo stato.

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

Risoluzione dei problemi del client di Advanced Threat Prevention

Trovare il codice prodotto con Windows PowerShell

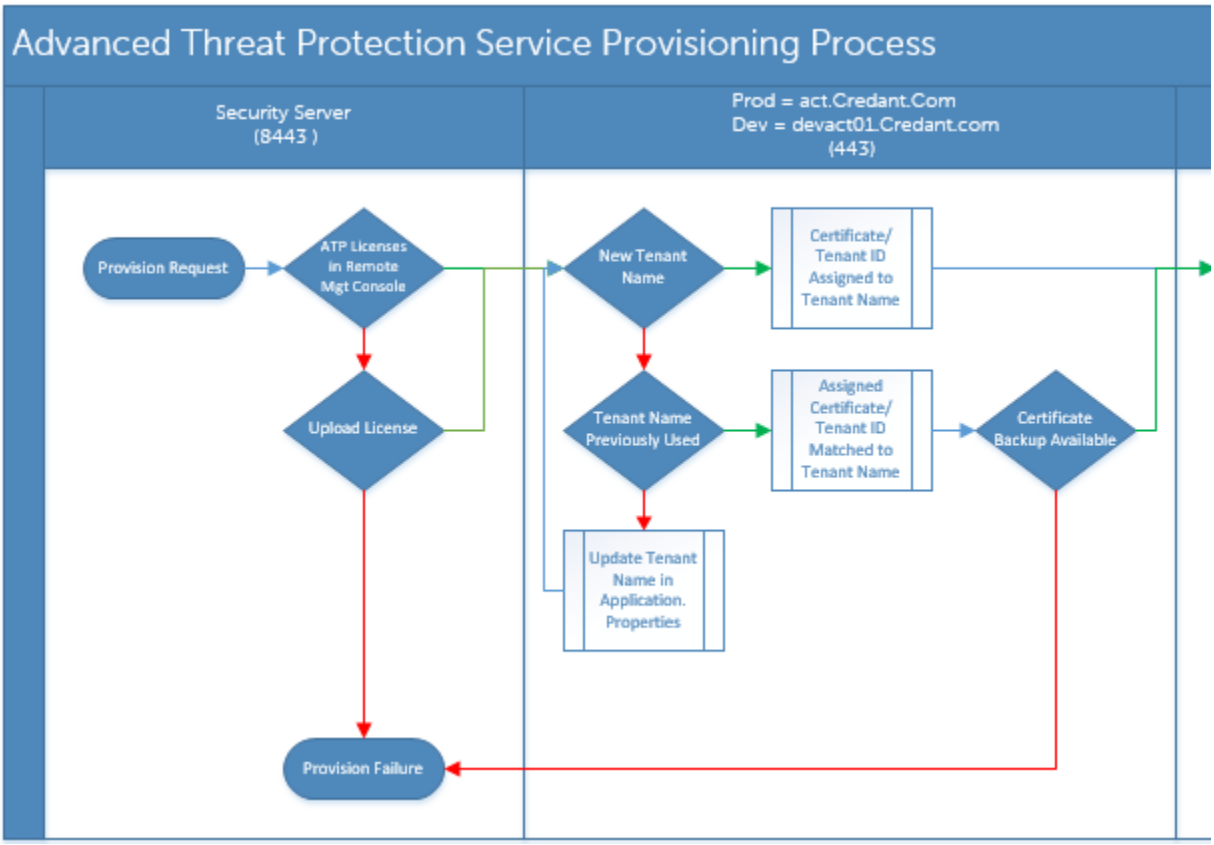
- Utilizzando questo metodo è possibile identificare facilmente il codice di prodotto, se il codice di prodotto viene modificato in futuro.

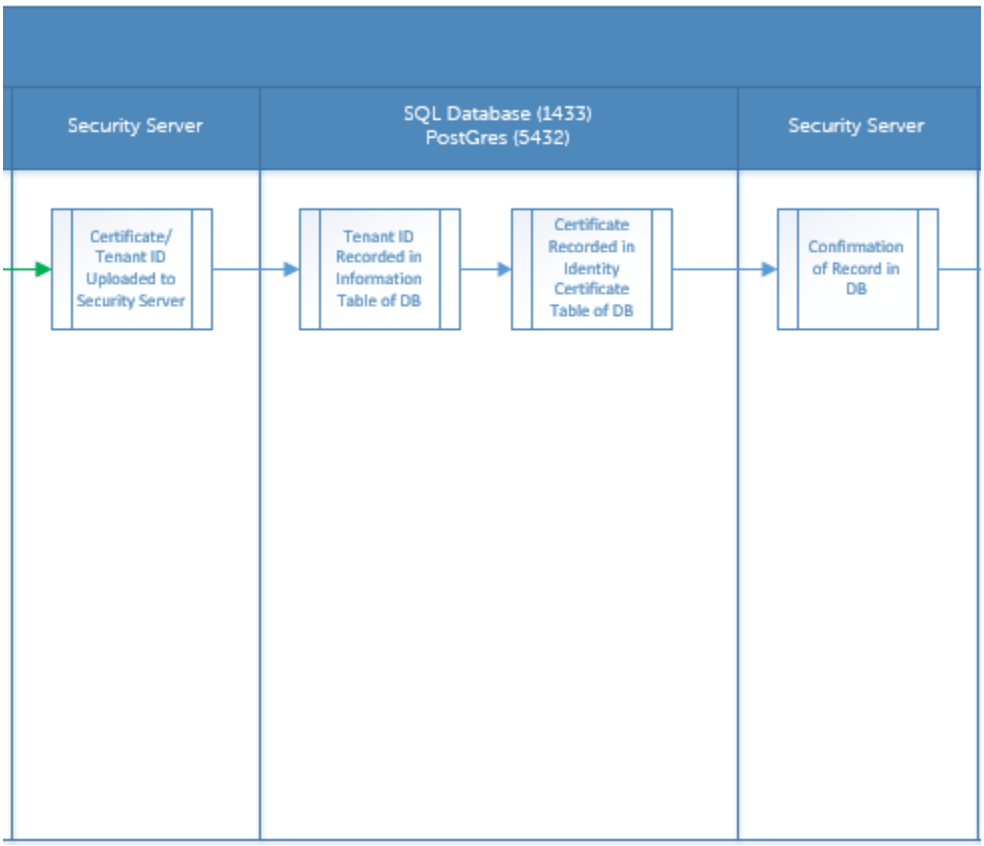
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

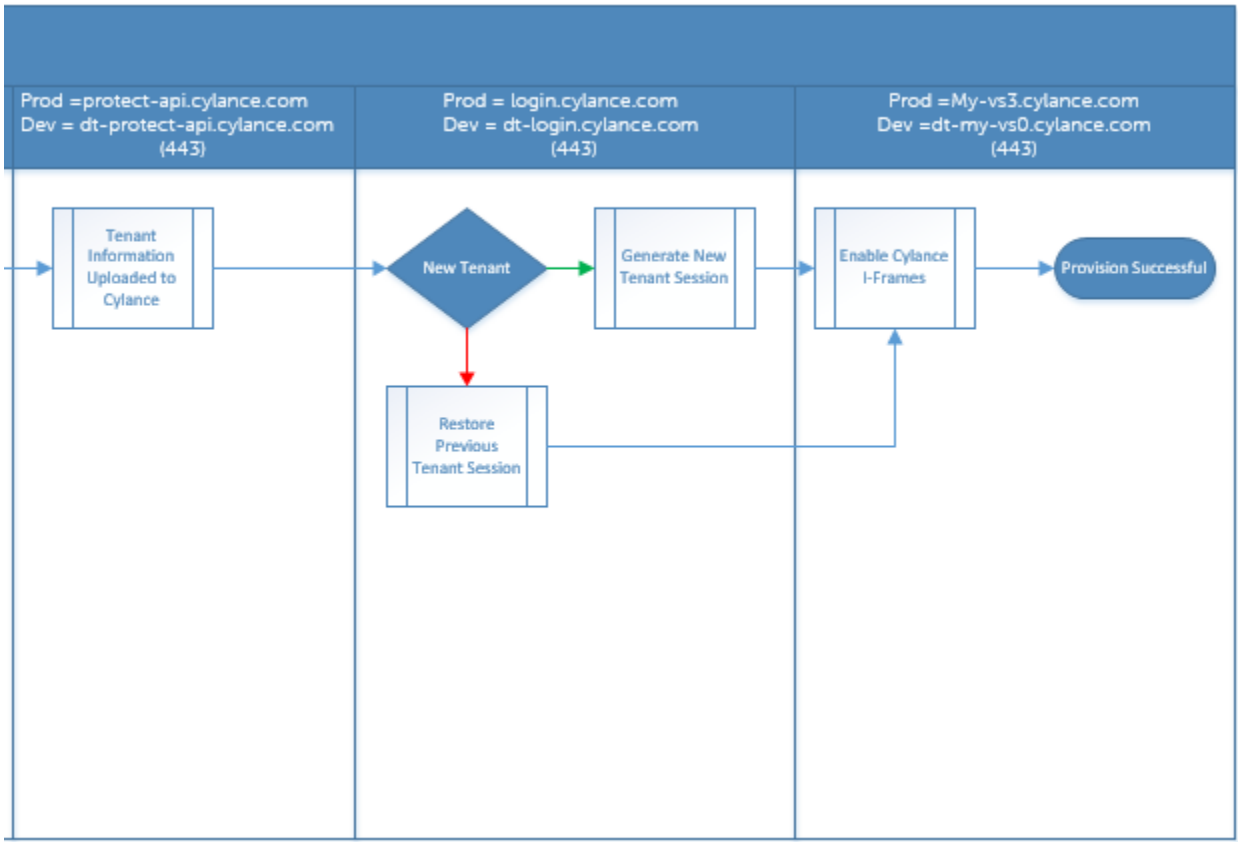
  L'output risulterà con il percorso completo e il nome del file .msi (il nome esadecimale del file convertito).

Provisioning di Advanced Threat Prevention e comunicazione agente

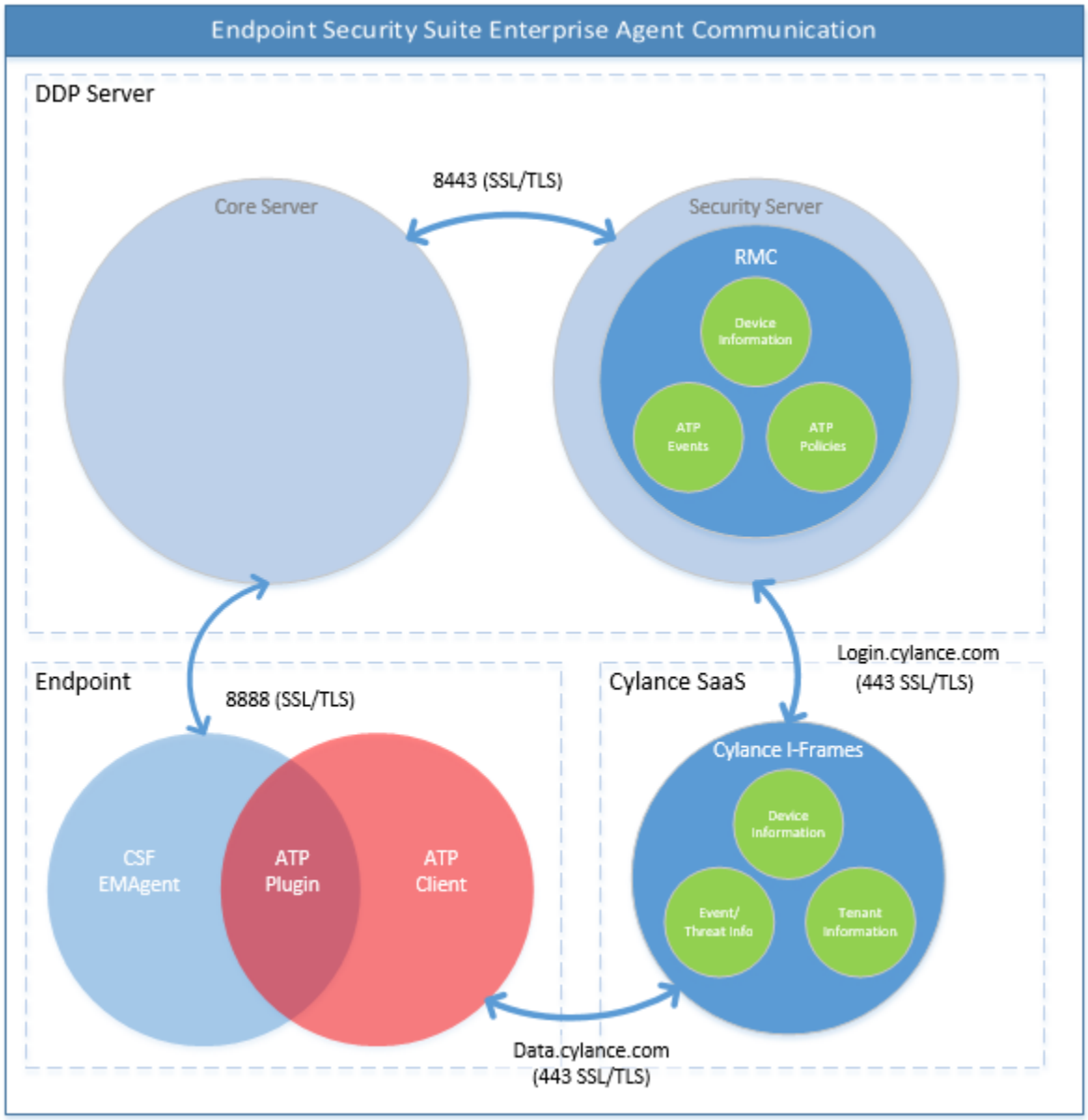
I diagrammi seguenti illustrano il processo di provisioning del servizio di Advanced Threat Prevention.


Advanced Threat Protection Service Provisioning Process
Security Server
(8443)
Prod = act.Credant.Com
Dev = devact01.Credant.com
(443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB

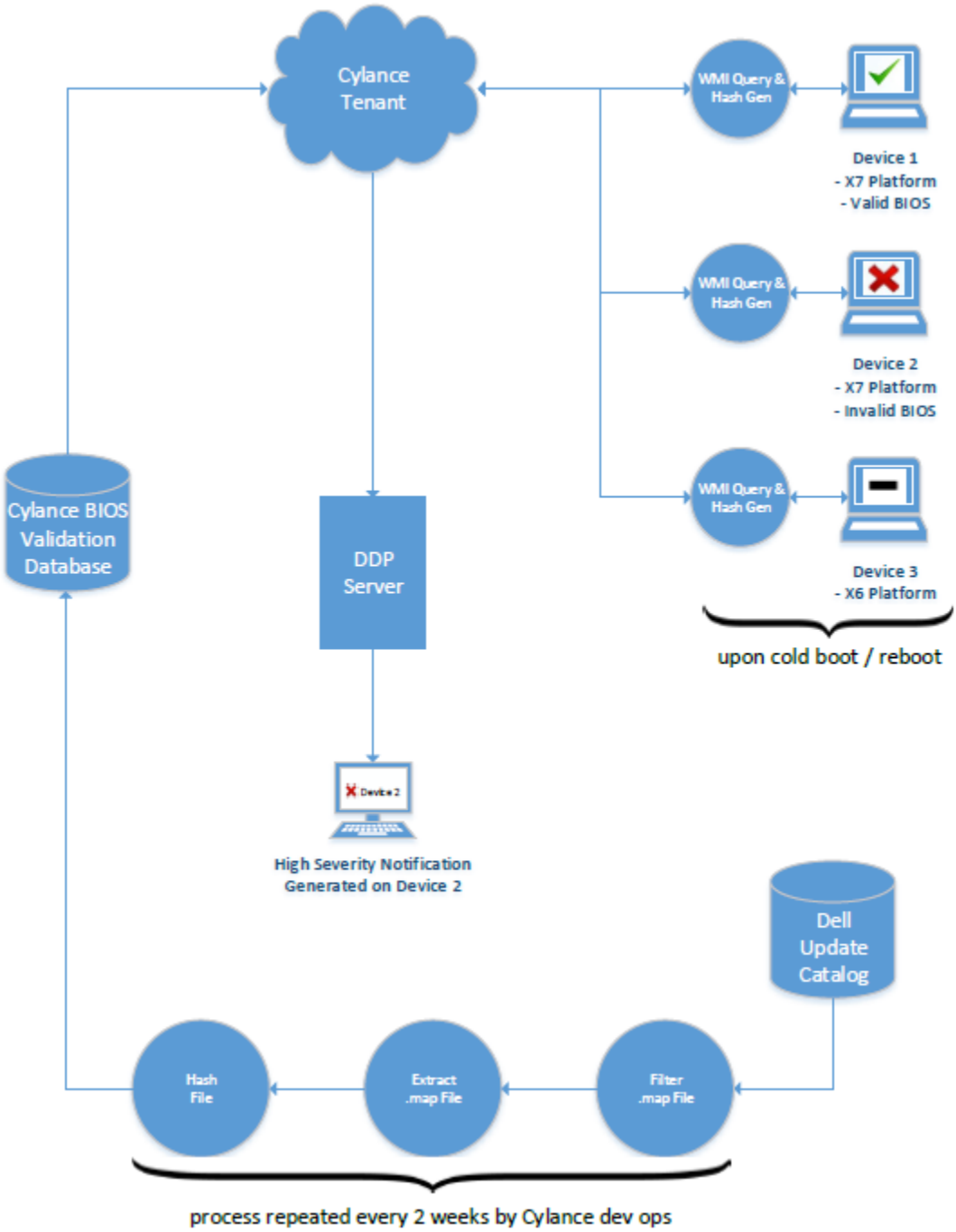


Il diagramma seguente illustra il processo di comunicazione dell'agente di Advanced Threat Prevention.



Processo di verifica dell'integrità dell'immagine del BIOS

Il diagramma seguente illustra il processo di verifica dell'integrità dell'immagine del BIOS. Per un elenco dei modelli di computer Dell che supportano la verifica dell'integrità dell'immagine del BIOS, consultare Requisiti - Verifica dell'integrità dell'immagine del BIOS.



Risoluzione dei problemi del client dell'unità autocrittografante

Usare il criterio Codice di accesso iniziale

- Questo criterio viene utilizzato per eseguire l'accesso a un computer se l'accesso di rete non è disponibile, ovvero non è possibile accedere all'EE Server/VE Server né a 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 ad essere meno sicuro, questo metodo di accesso non consente di registrare nell'EE Server/VE 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 dall'EE Server/VE Server per l'utente finale.

- 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* verrà visualizzato **solo** nelle circostanze seguenti:
  - Un utente non è mai stato attivato all'interno di PBA.
  - Il client non dispone di connettività alla rete o all'EE Server/VE Server.

Usare il Codice di accesso iniziale

1. Impostare un valore per il criterio **Codice di accesso iniziale** nella Remote 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 la 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 <dominio\nome utente> 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. (Solo gestore Credant) Rispondere ai prompt di domande e risposte.

    Fare clic sulla **freccia blu**.
12. 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 all'EE Server/VE Server. Il file di registro contiene informazioni che consentono di individuare i problemi di connettività dell'EE Server/VE server.
  - L'autenticazione non viene eseguita sebbene vengano immesse le credenziali corrette. Il file di registro usato con i registri dell'EE Server/VE 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 environment
```

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 Accendere il computer e accedere alla PBA. 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 verrà 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 Visitare il sito support.dell.com.

2 Selezionare il modello di computer.

3 Selezionare **Driver e download**.

4 Selezionare il **Sistema operativo** del computer di destinazione.

5 Espandere la categoria **Sicurezza**.

6 Scaricare e salvare i driver di Dell ControlVault.

7 Scaricare e salvare il firmware di Dell ControlVault.

8 Copiare i driver e il firmware nei computer di destinazione, se necessario.

Installare il driver di Dell ControlVault

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

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

:

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

Fare clic su **Continua** per iniziare.

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

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

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

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

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

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

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

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

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

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

Verificare l'installazione del driver

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

Installare il firmware di Dell ControlVault

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

:

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

Vengono visualizzati alcuni messaggi di stato.

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

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

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.
TPM_E_FAIL 0x80280009	Operazione non riuscita.
TPM_E_BAD_ORDINAL 0x8028000A	Ordinale sconosciuto o incoerente.
TPM_E_INSTALL_DISABLED	Installazione del proprietario disabilitata.

Costante/valore	Descrizione
0x8028000B	
TPM_E_INVALID_KEYHANDLE	Impossibile interpretare l'handle della chiave.
0x8028000C	
TPM_E_KEYNOTFOUND	L'handle della chiave punta a una chiave non valida.
0x8028000D	
TPM_E_INAPPROPRIATE_ENC	Schema di crittografia non accettabile.
0x8028000E	
TPM_E_MIGRATEFAIL	Autorizzazione della migrazione non riuscita.
0x8028000F	
TPM_E_INVALID_PCR_INFO	Impossibile interpretare le informazioni PCR.
0x80280010	
TPM_E_NOSPACE	Spazio insufficiente per caricare la chiave.
0x80280011	
TPM_E_NOSRK	Nessuna chiave radice di archiviazione (SRK) impostata.
0x80280012	
TPM_E_NOTSEALED_BLOB	BLOB crittografato non valido o non creato da questo TPM.
0x80280013	
TPM_E_OWNER_SET	Un proprietario del TPM (Trusted Platform Module) esiste già.
0x80280014	
TPM_E_RESOURCES	TPM: risorse interne insufficienti per eseguire l'azione richiesta.
0x80280015	
TPM_E_SHORTRANDOM	Stringa casuale troppo breve.
0x80280016	
TPM_E_SIZE	TPM: spazio insufficiente per eseguire l'operazione.
0x80280017	
TPM_E_WRONGPCRVAL	Il valore PCR denominato non corrisponde al valore PCR corrente.
0x80280018	
TPM_E_BAD_PARAM_SIZE	Valore non corretto dell'argomento paramSize del comando.
0x80280019	
TPM_E_SHA_THREAD	Nessun thread SHA-1 esistente.

Costante/valore	Descrizione
0x8028001A	
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	Proprietà di migrazione della chiave non corrette.

Costante/valore	Descrizione
0x80280029	
TPM_E_BAD_SCHEME 0x8028002A	Firma o schema di crittografia per la chiave non corretto o non consentito in questa situazione.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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 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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	Impossibile trovare un separatore TCG.

Costante/valore	Descrizione
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

Costante/valore	Descrizione
TBSIMP_E_LIST_NO_MORE_ITEMS 0x8029020D	L'elenco specificato è vuoto o l'iterazione ha raggiunto la fine dell'elenco.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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	Crittografia unità BitLocker non supporta le configurazioni cluster.

Costante/valore	Descrizione
0x8031001E	
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.
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	In base alle impostazioni dei Criteri di gruppo, prima di crittografare l'unità è necessario specificare una password di ripristino.

Costante/valore	Descrizione
0x8031002C	
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. 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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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	Il firmware del sistema non è riuscito ad abilitare la cancellazione della memoria di sistema al riavvio del computer.

Costante/valore	Descrizione
0x80310055	
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.
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.

Costante/valore	Descrizione
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.
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.

Costante/valore	Descrizione
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.
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

Costante/valore	Descrizione
	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 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.
FVE_E_NO_EXISTING_PIN	L'unità non è protetta da un PIN.

Costante/valore	Descrizione
0x803100A0	
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 rilevata prima dell'avvio. 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 o Ambiente ripristino Windows rilevato prima dell'avvio. 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 prima dell'avvio. 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	Le impostazioni di Criteri di gruppo richiedono la creazione di una password di ripristino, ma in questo dispositivo non è disponibile né una tastiera prima dell'avvio né 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.

Costante/valore	Descrizione
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 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.

18

Glossario

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

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

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

Advanced Threat Prevention - Il prodotto Advanced Threat Prevention è la protezione antivirus di prossima generazione che utilizza la scienza algoritmica e l'apprendimento automatico per identificare e classificare le cyber-minacce note e sconosciute, e impedirne l'esecuzione o il danneggiamento degli endpoint. La funzione opzionale Firewall client monitora la comunicazione tra il computer e le risorse in rete e Internet, intercettando le comunicazioni potenzialmente dannose. La funzione opzionale Protezione Web blocca l'accesso ai siti Web non sicuri e i download da questi siti durante la navigazione e le ricerche online in base a valutazioni di sicurezza e a rapporti relativi ai siti Web.

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

EMS - Media schermo esterno: questo servizio all'interno della crittografia Dell Client applica regole per supporti rimovibili e dispositivi di storage esterni.

Codice di accesso EMS - Questo servizio all'interno di Dell Enterprise Server/VE consente il ripristino di dispositivi protetti da External Media Shield nei casi in cui l'utente dimentica la password e non può più accedere. Il completamento di questo processo consente all'utente di ripristinare la password impostata sul supporto rimovibile o su un dispositivo di archiviazione esterno.

Client di crittografia – Il client di crittografia è il componente nel dispositivo che applica i criteri di protezione quando un endpoint è connesso alla rete, disconnesso dalla rete, perso o rubato. Creando un ambiente di elaborazione affidabile per gli endpoint, il client di

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

Endpoint - Un computer o dispositivo hardware mobile che viene gestito da Dell Enterprise Server/VE.

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

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

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

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

Controllo script - Controllo Script protegge i dispositivi bloccando l'esecuzione di script dannosi.

SED Management – SED Management 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 Management è un componente di gestione centrale e scalabile che consente di proteggere e gestire più efficacemente i propri dati. SED Management 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. 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 Remote Management Console di Dell Enterprise Server/VE.

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

Trusted Platform Module (TPM) - Il TPM è un chip di protezione che svolge tre funzioni principali: archiviazione protetta, misurazioni e attestazione. Il client di crittografia utilizza il TPM per la sua funzione di archiviazione protetta. Il TPM è inoltre in grado di fornire contenitori crittografati per l'insieme di credenziali del software. La presenza del TPM è necessaria per l'utilizzo di BitLocker Manager e funzione Password monouso (OTP).

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 esterni: quando vengono inseriti in un server con la cifratura installata, i file vengono crittografati tramite la Chiave roaming utente.