Encryption

Requisiti di sistema v10.1

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.

2018 - 11

Rev. A01

Sommario

1

Introduzione

Questo documento elenca i requisiti di Dell Encryption.

Per accedere alla documentazione di Dell Encryption, consultare www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.

Contattare Dell ProSupport

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

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

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

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

2

Requisiti

Tutti i client

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

- Durante 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 Security Management Server/Security Management Server Virtual se i client del programma di installazione principale verranno autorizzati tramite 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 i client del programma di installazione principale e del programma di installazione figlio di . 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 digitali e smart card (come mostrato di seguito) non sono inclusi nei file eseguibili del programma di installazione principale o figlio di . I driver e il firmware devono essere sempre aggiornati ed è possibile scaricarli dal sito http://www.dell.com/support selezionando il modello del computer desiderato. Scaricare i driver e il firmware appropriati in base all'hardware di autenticazione.
  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity Fingerprint Reader 495 Driver
  - O2Micro Smart Card Driver

Tutti i client - Hardware

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

Hardware
– Processore Intel Pentium o AMD

Hardware

- 110 MB di spazio disponibile su disco
- 512 MB di RAM

N.B.: È richiesto spazio aggiuntivo sul disco per crittografare i file sull'endpoint. La quantità di spazio varia in base ai criteri e alle dimensioni dell'unità.

Tutti i client - Localizzazione

- I client di crittografia e BitLocker Manager sono compatibili con l'interfaccia utente multilingue (MUI, Multilingual User Interface) e sono localizzati nelle lingue di seguito riportate.

Supporto lingue

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

Client di 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 programma di installazione principale non supporta aggiornamenti da componenti di una versione precedente alla v8.0. Estrarre i programmi di installazione figlio dal programma di installazione principale e aggiornare singolarmente i componenti.
- 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, vedere http://www.dell.com/support/article/us/en/19/SLN288353 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 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 – Visual C++ 2015 Update 3 o Redistributable Package (x86 e x64) versione successiva

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 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 dalla versione 1607 (Anniversary Update/Redstone 1) alla versione 1803 (aggiornamento di aprile 2018/Redstone 4) – VMware Workstation 12.5 e versioni successive

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

Sistemi operativi per Encryption External Media

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

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

Sistemi operativi Windows supportati per l'accesso a supporti protetti da Encryption External Media (a 32 e 64 bit)
– Windows 7 SP1: Enterprise, Professional, Ultimate

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

- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro dalla versione 1607 (Anniversary Update/Redstone 1) alla versione 1803 (aggiornamento di aprile 2018/Redstone 4)

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

- macOS Sierra 10.12.4 e 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

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 Encryption Enterprise e Endpoint Security Suite Enterprise.
- Server Encryption fornisce quanto segue:
  - Crittografia del software
  - Crittografia dei supporti rimovibili
  - Controllo porte

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

    I criteri del sistema di controllo delle porte del 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 viene convalidato per soluzioni antivirus leader del settore. Le esclusioni hardcoded sono utilizzate da questi provider di antivirus per impedire le incompatibilità tra crittografia e scansione antivirus. Se 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:

- Security Management Server Security Management Server Virtual o i server che eseguono i database per Security Management Server Security Management Server Virtual.
- Server Encryption non è compatibile con Encryption Personal.
- Server Encryption non è supportato con SED Management o il client di BitLocker Manager.
- Server Encryption non è supportato sui server che fanno parte di sistemi di file system distribuiti (DFS).

- La migrazione verso o da Server Encryption non è supportata. Gli aggiornamenti da Encryption External Media 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 (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.
- Le reinstallazioni del sistema operativo sul posto non sono supportate. Per reinstallare il sistema operativo, eseguire un backup del computer di destinazione, cancellarne i dati, installare il sistema operativo e quindi ripristinare i dati crittografati seguendo le procedure di ripristino. Per maggiori informazioni sul ripristino dei dati crittografati, fare riferimento alla *Recovery Guide* (Guida al ripristino).

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 SP1: Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro dalla versione 1607 (Anniversary Update/Redstone 1) alla versione 1803 (aggiornamento di aprile 2018/Redstone 4)

Sistemi operativi server supportati

- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Datacenter Edition (Server Core non supportato)
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition (Server Core non supportato)
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition (Server Core non supportato)

Sistemi operativi supportati in modalità UEFI

- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro dalla versione 1607 (Anniversary Update/Redstone 1) alla versione 1803 (aggiornamento di aprile 2018/Redstone 4)

N.B.:

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

Sistemi operativi per Encryption External Media

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

N.B.:

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

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

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Enterprise, Pro
- Windows 10: Education, Enterprise, Pro dalla versione 1607 (Anniversary Update/Redstone 1) alla versione 1803 (aggiornamento di aprile 2018/Redstone 4)

Sistemi operativi server supportati

- Windows Server 2012 R2

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

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14