Dell Data Protection | Endpoint Security Suite Enterprise

Guida all'installazione di base 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 di base di Endpoint Security Suite Enterprise

2017 - 04

Rev. A01

Sommario

1

Introduzione

Questa guida descrive in dettaglio la procedura per installare e configurare l'applicazione usando il programma di installazione principale di ESS. Questa guida fornisce un'assistenza di base per l'installazione. Consultare la *Guida all'installazione avanzata* per informazioni su installazione dei programmi di installazione figlio, configurazione di EE Server/VE Server o informazioni oltre l'assistenza di base con il programma di installazione principale di ESS .

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:

- Consultare Requisiti per i prerequisiti del client.
- Selezionare una delle seguenti operazioni:
  - 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

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

- 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 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 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.
- 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.

Prerequisito

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

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 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.

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.

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

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,

Sistemi operativi Windows (a 32 e 64 bit)

- 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.

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

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

Sistemi operativi Windows (a 32 e 64 bit)

- 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.
- 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.
- 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.

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

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
- 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 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 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 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.

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.
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.

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**.

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

- 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.

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.
- 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").

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.

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**.

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.

Interazioni tra EMS e il Sistema di controllo porte

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

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

Per crittografare dati scritti su CD/DVD

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

Usare WSScan

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

Eseguire WSScan

1 Dal supporto di installazione Dell, copiare WSScan.exe nel computer Windows che si desidera sottoporre a scansione.

2 Avviare una riga di comando dal percorso suindicato e immettere **wsscan.exe** al prompt dei comandi. WSScan si avvia.

3 Fare clic su **Avanzate**.

4 Selezionare il tipo di unità da analizzare dal menu a discesa: *Tutte le unità, Tutte le unità fisse, Unità rimovibili* o *CDROM/ DVDROM.*

5 Selezionare il Tipo di rapporto di crittografia desiderato dal menu a discesa: *file crittografati*, *file non crittografati*, *tutti i file* o *file non crittografati in violazione*:

   - *File crittografati* - per garantire che tutti i dati vengano decrittografati durante la disinstallazione del client di crittografia. Seguire il processo esistente per la decrittografia dei dati, ad esempio impostare l'aggiornamento di un criterio di decrittografia. Dopo la decrittografia dei dati, ma prima di eseguire il riavvio in preparazione per la disinstallazione, eseguire WSScan per verificare che tutti i dati siano stati decrittografati.
   - *File non crittografati* - Per individuare i file che non sono crittografati, con un'indicazione sulla necessità o meno di crittografare i file (S/N).
   - *Tutti i file* - Per visualizzare l'elenco di tutti i file crittografati e non crittografati, con un'indicazione sulla necessità o meno di crittografare i file (S/N).
   - *File non crittografati in violazione* - Per individuare i file che non sono crittografati che devono essere crittografati.

6 Fare clic su **Cerca**.

OPPURE

1 Fare clic su **Avanzate** per attivare/disattivare la visualizzazione su **Semplice** per sottoporre a scansione una cartella specifica.

2 Accedere a Impostazioni di scansione e inserire il percorso della cartella nel campo **Percorso di ricerca**. Se si utilizza questo campo, la selezione nella casella di riepilogo viene ignorata.

3 Se non si desidera scrivere i risultati della scansione di WSScan su file, disattivare la casella di controllo **Output su file**.

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

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

6 Scegliere il formato di output:

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

7 Fare clic su **Cerca**.

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

Output WSScan

I dati WSScan sui file crittografati contengono le seguenti informazioni.

Esempio di output:

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

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

Output	Significato
	AES 128
	AES 256
	3DES

Verificare lo stato dell'Encryption Removal Agent

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

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

Risoluzione dei problemi del client di Advanced Threat Prevention

Trovare il codice prodotto con Windows PowerShell

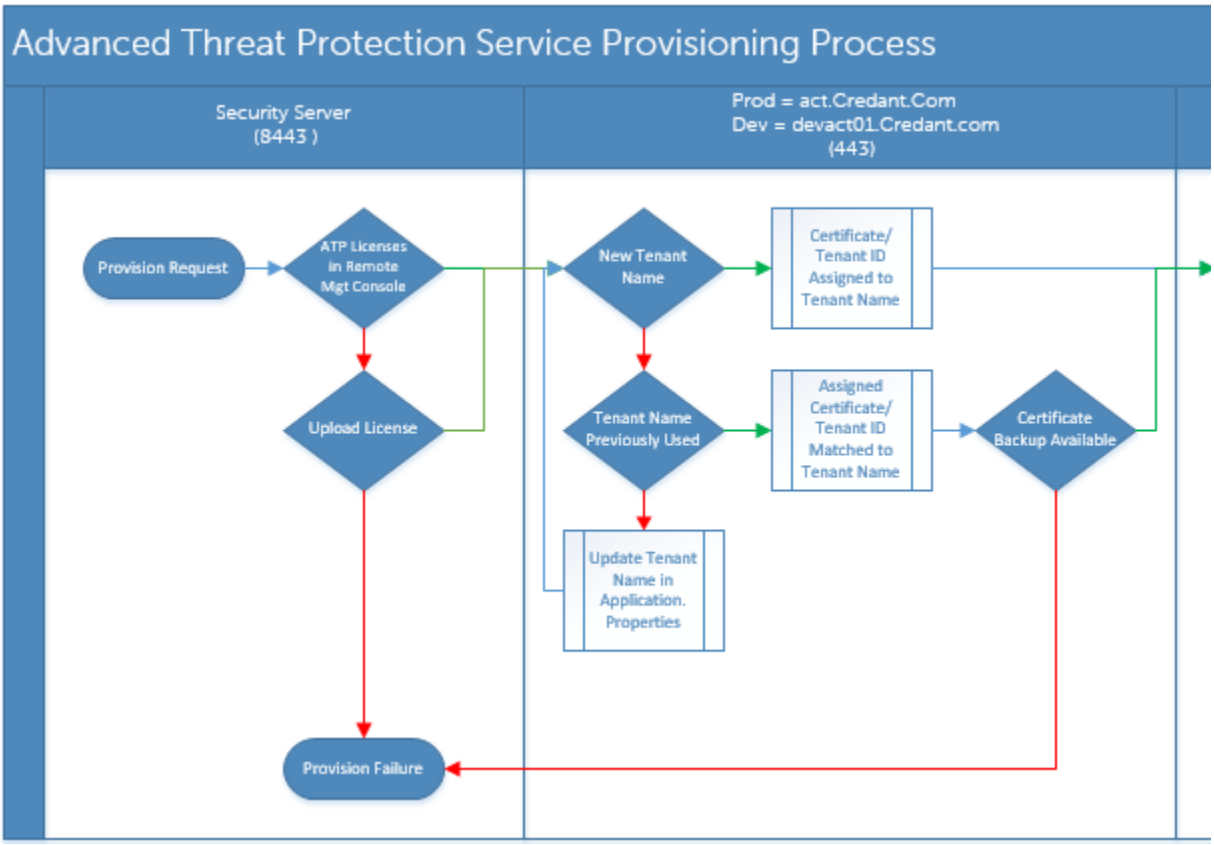
- Utilizzando questo metodo è possibile identificare facilmente il codice di prodotto, se il codice di prodotto viene modificato in futuro.

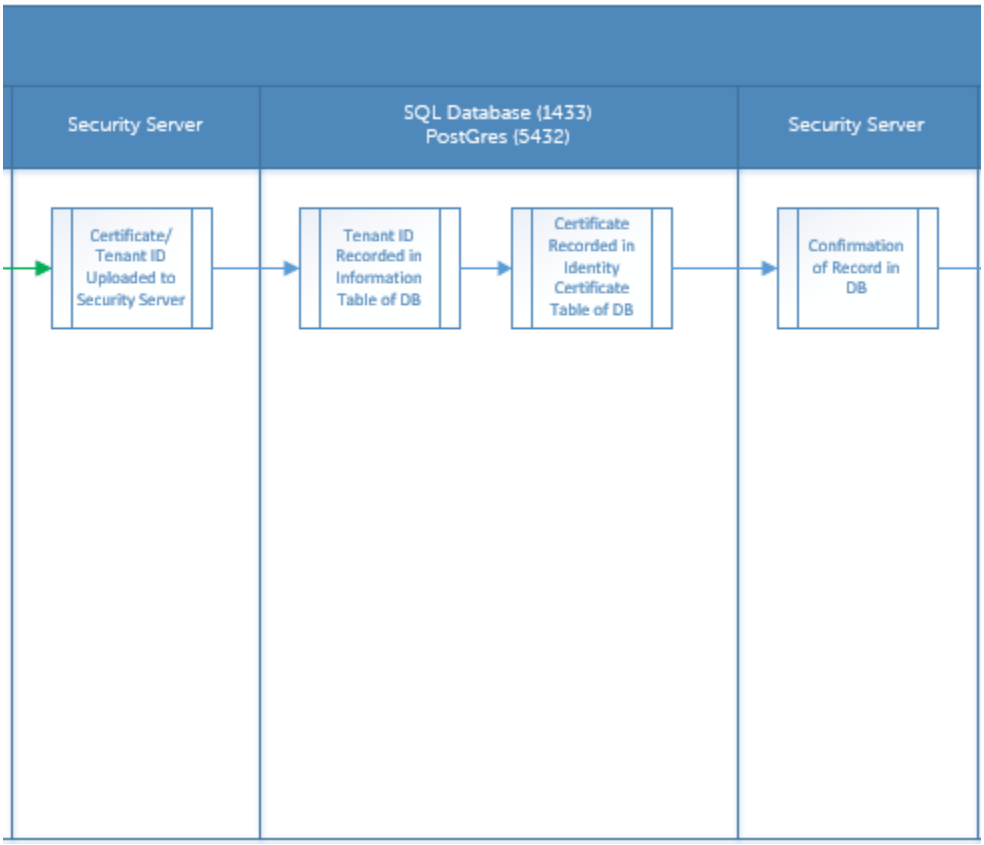
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

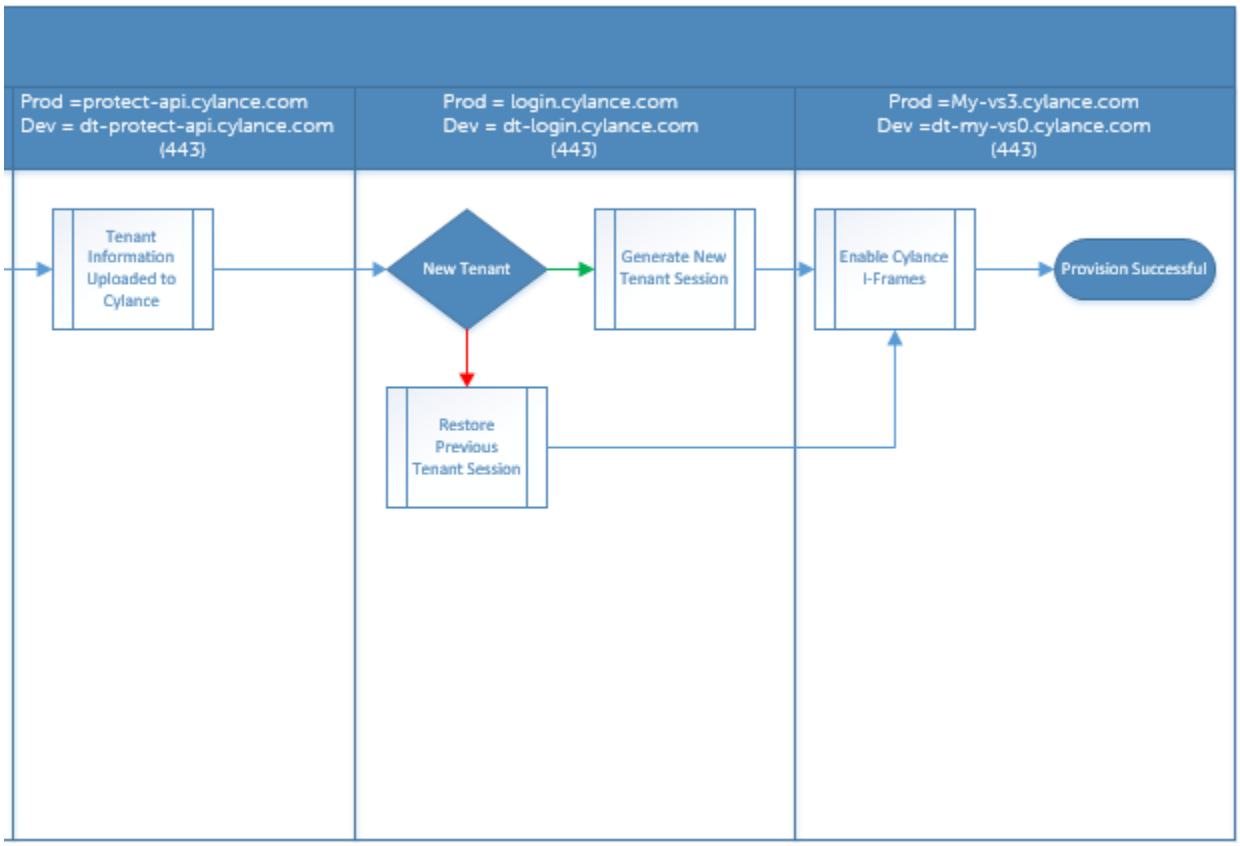
  L'output risulterà con il percorso completo e il nome del file .msi (il nome esadecimale del file convertito).

Provisioning di Advanced Threat Prevention e comunicazione agente

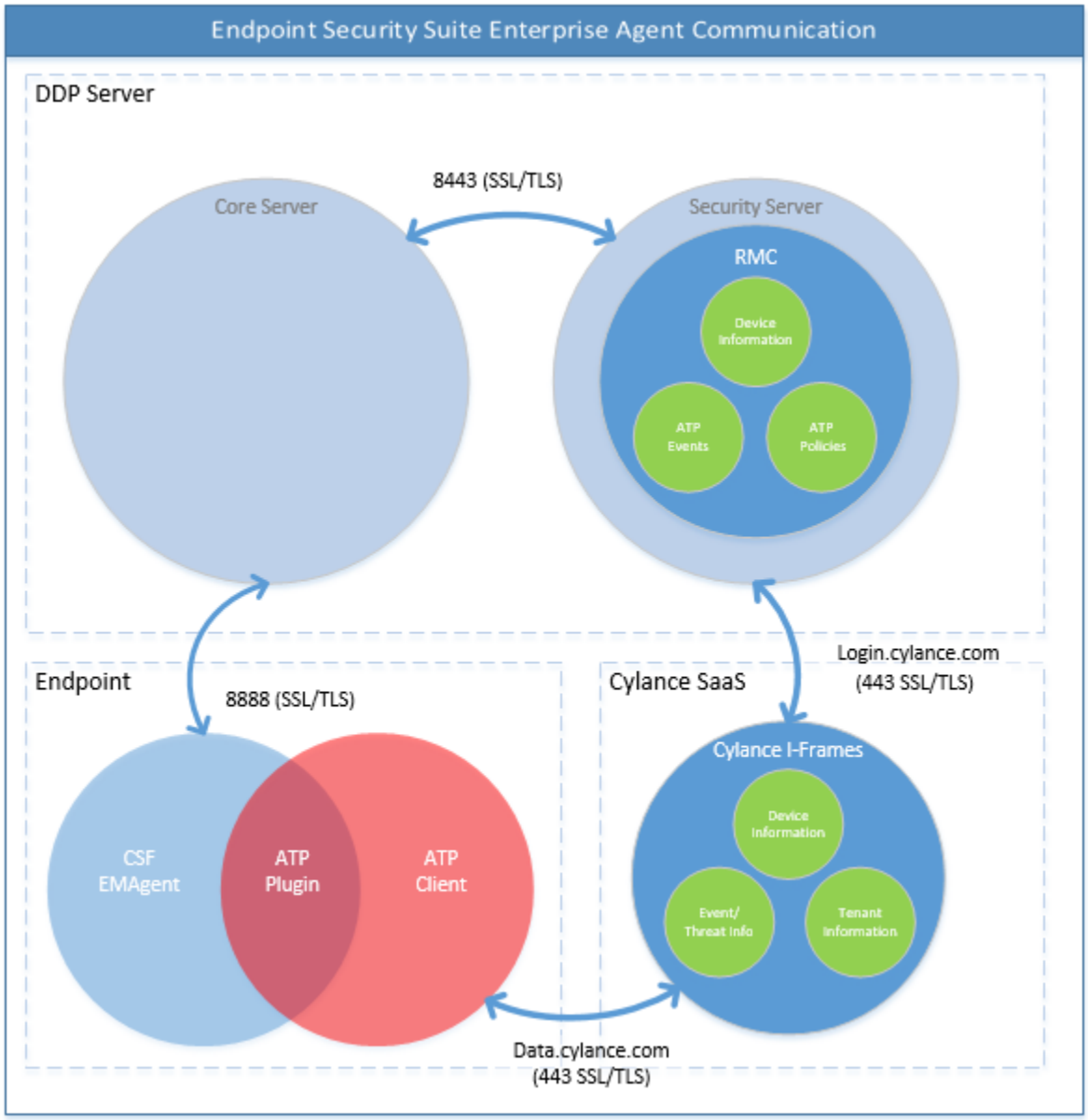
I diagrammi seguenti illustrano il processo di provisioning del servizio di Advanced Threat Prevention.





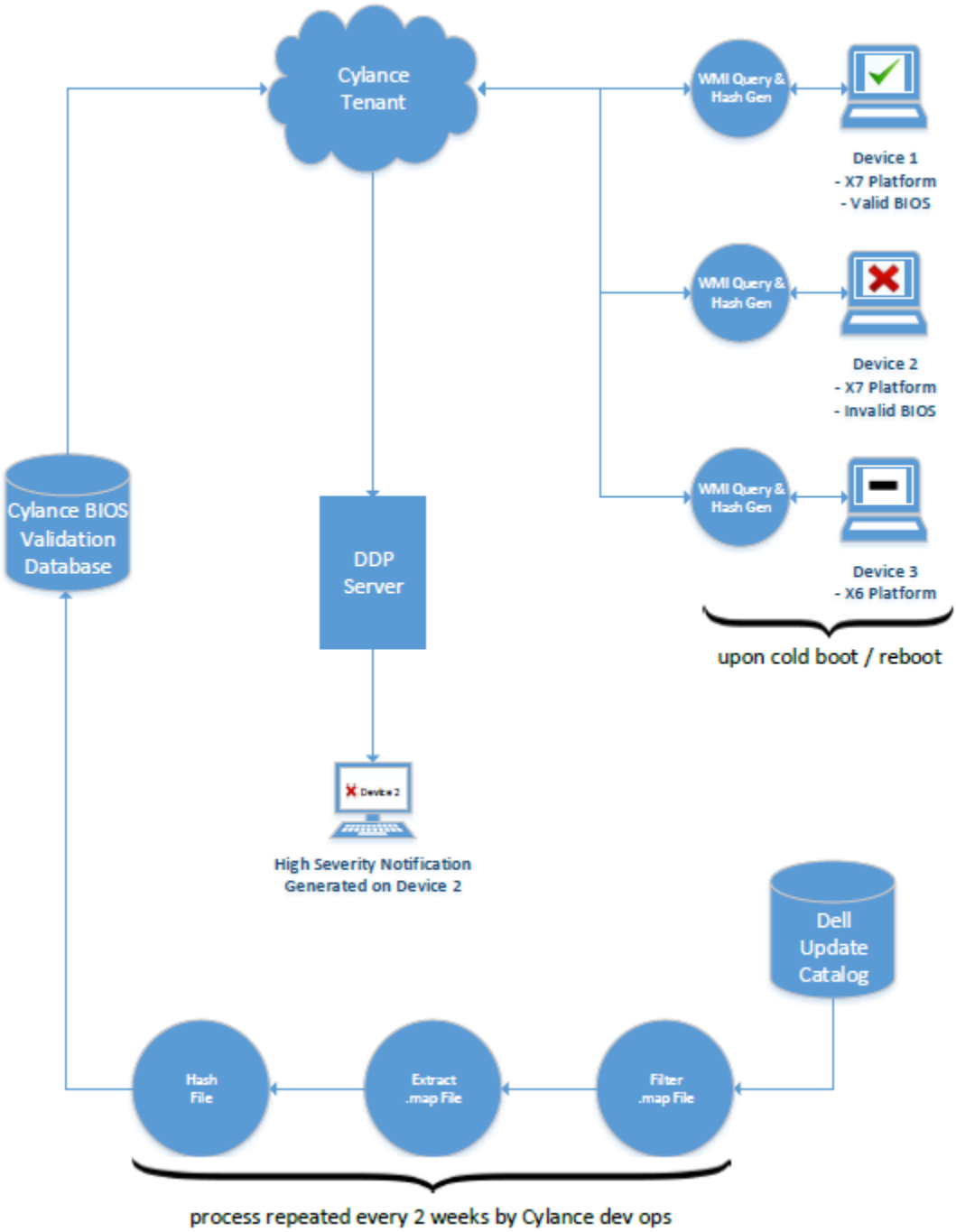


Il diagramma seguente illustra il processo di comunicazione dell'agente di Advanced Threat Prevention.



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.



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.

Glossario

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

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.

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.

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.

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.

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.