Dell Data Protection | Endpoint Security Suite Enterprise for Mac

Administrator Guide v1.1

Messaggi di N.B., Attenzione e Avvertenza

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

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

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

Administrator Guide

2017 - 05

Rev. A02

Contents

1

Introduzione

La Guida dell'amministratore di Endpoint Security Suite Enterprise per Mac fornisce le informazioni necessarie a distribuire e installare il software client.

Argomenti:

Panoramica

Endpoint Security Suite Enterprise per Mac offre una prevenzione avanzata contro le minacce al sistema operativo e ai livelli di memoria e di crittografia, il tutto gestito a livello centrale da Dell Data Protection Server. Grazie alla gestione centralizzata, alla creazione di report di conformità consolidati e agli avvisi di minaccia alla console, le aziende possono facilmente applicare e dimostrare la conformità dei propri endpoint. L'esperienza della protezione è integrata con diverse funzioni, come ad esempio criteri predefiniti e modelli di rapporto, per aiutare le aziende a ridurre i costi di gestione IT e la complessità.

- Endpoint Security Suite Enterprise per Mac - una suite di software per il client di crittografia dei dati e la prevenzione avanzata contro le minacce.
- Proxy Policy - utilizzato per distribuire i criteri
- Security Server - utilizzato per le attivazioni del software di crittografia del client
- Enterprise Server o Dell Enterprise Server - VE - fornisce l'amministrazione dei criteri di sicurezza centralizzata, integrandosi con le directory aziendali esistenti e creando rapporti. Ai fini del presente documento, entrambi i server sono indicati come "server Dell", a meno che non sia necessario indicare una versione specifica (ad esempio, se una procedura è diversa quando si utilizza Dell Enterprise Server - VE).

  Questi componenti Dell devono interagire perfettamente per fornire un ambiente mobile sicuro senza compromettere l'esperienza dell'utente.

Endpoint Security Suite Enterprise per Mac dispone di due file .dmg - uno per il client di crittografia e uno per Advanced Threat Prevention. È possibile installarli entrambi o solo uno.

Dell Encryption Client e crittografia FileVault

L'opzione di gestione della crittografia FileVault, insieme a Dell Encryption Client, è disponibile con Endpoint Security Suite Enterprise per Mac. L'opzione appropriata dipende dai requisiti di crittografia dell'azienda. Per ulteriori informazioni sui criteri di crittografia, consultare Crittografia Mac > Crittografia volume di Dell.

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.

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

2

Requisiti

In questo capitolo sono specificati i requisiti hardware e software client. Prima di continuare con le attività di distribuzione, accertarsi che l'ambiente di distribuzione soddisfi i requisiti.

Argomenti:

Encryption Client

Hardware del client di crittografia

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

N.B.: Il disco di sistema deve essere partizionato secondo lo schema di partizione della Tabella di partizione GUID (GPT, GUID Partition Table) e avere un formato Mac OS X Esteso (Journaled).

Hardware

- 30 MB di spazio libero su disco
- Scheda di interfaccia di rete 10/100/1000 o Wi-Fi

Encryption Client Software

The following table details supported software.

NOTE: If you intend to perform a major operating system upgrade when using the Dell Encryption client (not FileVault encryption), a decrypt and uninstall operation will be needed followed by regular installation of the Encryption client for Mac on the new operating system.

Operating Systems (64-bit kernels)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption Client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

NOTE: If you are using a network user account to authenticate, that account must be set up as a mobile account in order to fully configure FileVault 2 management.

The following table details the operating systems supported when accessing Dell-encrypted external media.

NOTE: External Media Shield supports FAT32, exFAT, or HFS Plus (Mac OS Extended) formatted media with Master Boot Record (MBR) or GUID Partition Table (GPT) partition schemes. See Enable HFS Plus.

NOTE: External media must have 55 MB available, plus open space on the media that is equal to the largest file to be encrypted, to host External Media Shield.

Encrypted Media

Windows Operating Systems (32- and 64-bit) Supported to Access Encrypted Media

- Microsoft Windows 7 SP0-SP1
  - Enterprise
  - Professional
  - Ultimate
  - Home Premium
- Microsoft Windows 8
  - Enterprise
  - Pro
  - Windows 8 (Consumer)
- Microsoft Windows 8.1 - Windows 8.1 Update 1
  - Enterprise
  - Pro
- Microsoft Windows 10
  - Enterprise
  - Pro

Mac Operating Systems (64-bit kernels) Supported to Access Encrypted Media

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

Advanced Threat Prevention

- Per evitare errori di installazione, disinstallare le applicazioni antivirus, antimalware e antispyware di altri fornitori prima di installare il client Advanced Threat Prevention.

Hardware di Advanced Threat Prevention

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

Hardware

- 500 MB di spazio libero su disco, a seconda del sistema operativo
- 2 GB RAM
- Scheda di interfaccia di rete 10/100/1000 o Wi-Fi

Software di Advanced Threat Protection

La tabella seguente descrive in dettaglio il software supportato.

Sistemi operativi (kernel a 64 bit)

- Mac OS X Mavericks 10.9.5

N.B.: Questa versione si applica solo per Advanced Threat Prevention e non per il client di crittografia.

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6

N.B.: Non è previsto alcun supporto per file system con distinzione tra maiuscolo/minuscolo.

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

Attività per il client di crittografia

Installare/aggiornare Encryption Client

Questa sezione guida l'utente nel processo di installazione/aggiornamento Encryption Client per Mac.

Vi sono due metodi per installare/aggiornare Encryption Client per Mac. Selezionare **una** delle seguenti operazioni:

- Installazione interattiva/Aggiornamento e attivazione - è il metodo più semplice per installare o aggiornare il pacchetto software client. Tuttavia, questo metodo non consente alcuna personalizzazione. Se si intende utilizzare il Boot Camp o una versione del sistema operativo che non ancora completamente supportata da Dell (tramite la modifica .plist), è necessario utilizzare il metodo di installazione/aggiornamento dalla riga di comando. Per ulteriori informazioni sull'utilizzo del Boot Camp, consultare Utilizzare il Boot Camp.
- Installazione/aggiornamento dalla riga di comando - Si tratta di un metodo di installazione/aggiornamento avanzato che dovrebbe essere utilizzato solo dagli amministratori esperti con la sintassi dalla riga di comando. Se si intende utilizzare il Boot Camp o una versione del sistema operativo che non ancora completamente supportata da Dell (tramite la modifica .plist), è necessario utilizzare questo metodo per installare o aggiornare dalla riga di comando il pacchetto software client. Per ulteriori informazioni sull'utilizzo del Boot Camp, consultare Utilizzare il Boot Camp.

  Per maggiori informazioni sulle opzioni di comando del programma di installazione, consultare la libreria di riferimento di Mac OS X all'indirizzo http://developer.apple.com. Dell consiglia vivamente di utilizzare strumenti di distribuzione remoti, come Apple Remote Desktop, per distribuire il pacchetto di installazione del client.

  N.B.: Apple spesso rilascia nuove versioni dei sistemi operativi tra le versioni di Endpoint Security Suite Enterprise per Mac. Per andare incontro a più clienti possibile, è consentita la modifica del file com.dell.ddp.plist per supportare questi casi. Non appena Apple rilascia una nuova versione, si inizia un test di queste versioni per assicurare che siano compatibili con Encryption Client per Mac.

Prerequisiti

Dell invita a seguire le procedure consigliate durante la distribuzione del software client. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e distribuzioni scaglionate agli utenti.

Prima di iniziare questo processo, accertarsi che siano soddisfatti i seguenti prerequisiti:

- Assicurarsi che il server Dell e i suoi componenti siano già installati.

  Se non è ancora stato installato il server Dell, seguire le istruzioni nella guida appropriata di seguito.

  Guida alla migrazione e all'installazione di Enterprise Server

  Guida introduttiva e all'installazione di Enterprise Server - Virtual Edition
- Assicurarsi di avere a portata di mano l'URL del Security Server e del Policy Proxy. Saranno entrambi necessari per l'installazione e l'attivazione del software client.
- Se la distribuzione utilizza una configurazione non predefinita, assicurarsi di conoscere il numero di porta del Security Server. Sarà necessario per l'installazione e l'attivazione del software client.
- Assicurarsi che il computer di destinazione disponga di connettività di rete con Security Server e Policy Proxy.
- Accertarsi di possedere un account utente di dominio nell'installazione di Active Directory configurato per l'utilizzo con il server di Dell. L'account utente di dominio verrà utilizzato per l'attivazione del software client. Non è necessario configurare gli endpoint Mac per l'autenticazione del dominio (rete).
- Per applicare la crittografia nel computer client, selezionare prima l'opzione di crittografia appropriata per la propria organizzazione.

Dell Encryption	Crittografia tramite FileVault
Selezionare questa opzione per:	Selezionare questa opzione per:
• Crittografare tutte le partizioni nell'unità di avvio • Ignorare l'autenticazione di preavvio • Utilizzare una crittografia a 256 bit	• Crittografare le unità Fusion • Utilizzare l'autenticazione di preavvio • Utilizzare una soluzione supportata da Apple
N.B.: Se si utilizza Dell Encryption, è necessario disabilitare Protezione integrità di sistema (SIP). Consultare Installazione/aggiornamento e attivazione, passaggio 4.	**N.B.: Se un Mac ha un'unità Fusion, è necessario abilitare FileVault per crittografare tale unità.**

Le impostazioni dei criteri di crittografia devono riflettere l'opzione di crittografia selezionata. Prima di impostare i criteri di crittografia, assicurarsi di comprendere la *Crittografa tramite FileVault per Mac* e *i volumi destinati ai criteri di crittografia.* Per utilizzare sia Dell Encryption o la crittografia FileVault, il criterio di *crittografia volume di Dell* deve essere su *Acceso.*

Per ulteriori informazioni sui criteri di crittografia, consultare Crittografia Mac > Crittografia volume di Dell.

Installazione/aggiornamento e attivazione interattiva

Per installare/aggiornare e attivare il software client, seguire la procedura seguente. Per eseguire la procedura, è necessario disporre di un account amministratore.

N.B.: Prima di iniziare, salvare il lavoro dell'utente e chiudere le applicazioni; al termine dell'installazione sarà necessario riavviare immediatamente il computer.

1 Dal supporto di installazione Dell, montare il file Dell-Data-Protection-<version>.dmg.

2 Fare doppio clic sul programma di installazione del pacchetto. Viene visualizzato il seguente messaggio:

Il pacchetto eseguirà un programma per determinare se il software può essere installato.

3 Fare clic su **Continua** per proseguire.

4 Leggere il testo iniziale e fare clic su **Continua**.

5 Per verificare il contratto di licenza, fare clic su **Continua**, quindi su **Accetto** per accettare i termini del contratto di licenza.

Se si utilizza Dell Encryption con Mac OS X v10.11 o successiva, viene visualizzata una finestra di dialogo dal titolo *La protezione integrità di sistema per Mac OS è abilitata.* È necessario disabilitare Protezione integrità di sistema (SIP).

Seguire la seguente procedura:

a Consultarehttp://www.dell.com/support/Article/us/en/19/SLN299063 per disattivare la SIP.

b Nella procedura guidata, fare clic su **OK** e continuare con *Configurazione della protezione dati Dell.*

6 Nel campo `indirizzo di dominio:`, immettere il dominio completo per gli utenti di destinazione, come ad esempio *dipartimento.organizzazione.com*.

7 Nel campo **Nome visualizzato (opzionale):** considerare l'impostazione del *nome visualizzato* per il nome del dominio NetBIOS (già nel sistema operativo Windows 2000), che generalmente è in maiuscolo.

Se impostato, viene visualizzato nella finestra di dialogo *Attivazione* anziché *Indirizzo di dominio*. Questo fornisce coerenza con il nome di dominio visualizzato nelle finestre di dialogo *Autenticazione* per i computer gestiti dal dominio Windows.

8 Nel campo **Security Server**: inserire il nome host del Security Server.

Se la distribuzione utilizza una configurazione non predefinita, aggiornare i campi delle porte e la casella di controllo **Utilizza SSL**.

Una volta stabilita la connessione, l'indicatore della connettività del Security Server cambia da rosso a verde.

9 Nel campo **Policy Proxy:** il nome host del Policy Proxy viene compilato automaticamente con un host Policy Proxy corrispondente all'host del Security Server. Questo host viene utilizzato come policy proxy se non ci sono host specificati nella configurazione del criterio.

Dopo aver stabilito la connessione, l'indicatore della connettività della Policy Proxy cambia da rosso a verde.

10 Una volta che la finestra di dialogo Configurazione Dell è stata completata e la connessione è stata stabilita con il Security Server e Policy Proxy, fare clic su **Continua** per mostrare il tipo di installazione.

11 Alcune installazioni su computer specifici visualizzano una finestra di dialogo *Seleziona una destinazione* prima che venga visualizzata la finestra di dialogo *Tipo di installazione*. In questo caso, selezionare il disco di sistema corrente dall'elenco di dischi che viene visualizzato. L'icona del disco di sistema corrente mostra una freccia verde puntata verso il disco. Fare clic su **Continua.**

12 Dopo che tipo di installazione viene visualizzato, fare clic su **Installa** per continuare con l'installazione.

13 Quando richiesto, immettere le credenziali dell'account amministratore (richieste dall'applicazione del programma di installazione di Mac OS X), quindi fare clic su **OK**.

N.B.: Al termine dell'installazione sarà necessario riavviare immediatamente il computer. Se si aprono dei file in altre applicazioni e non sono pronti per il riavvio, fare clic su Annulla, salvare il lavoro e chiudere le altre applicazioni.

14 Fare clic su **Continuare l'installazione**. L'installazione viene avviata.

15 Al completamento dell'installazione, fare clic su **Riavvia**.

16 Continuare per Attivare la crittografia client per Mac.

Installazione/aggiornamento dalla riga di comando

Per installare il software client dalla riga di comando, attenersi alla procedura seguente.

N.B.: Se si utilizza Dell Encryption con Mac OS X v10.11.x, è necessario disabilitare SIP. Consultare http://www.dell.com/support/Article/us/en/19/SLN299063.

1 Dal supporto di installazione Dell, montare il file Protezione dati Dell-<version>.dmg.

2 Copiare il pacchetto **Installazione protezione dati Dell** e il file **com.dell.ddp.plist** per l'unità locale.

3 In Remote Management Console, modificare i seguenti criteri, se necessario. Le impostazioni dei criteri sovrascrivono le impostazioni del file .plist. Utilizzare le impostazioni del file .plist se in Remote Management Console non esistono criteri.

- **Modalità password firmware**: se si intende utilizzare Boot Camp su computer Mac crittografati o una versione di sistema operativo non ancora completamente supportata da Dell, è **obbligatorio** impostare questo criterio su *Facoltativo* per **non** utilizzare la protezione della password del firmware. Per ulteriori informazioni, consultare la sezione Informazioni sulla protezione della password del firmware opzionale.

  N.B.:
  Quando il criterio Modalità password firmware è impostato su **Facoltativo**, disabilita solo l'applicazione della protezione della password del firmware del software client. **Non** rimuovere un'eventuale protezione della password del firmware esistente. Al termine di questa procedura, l'installazione è completata e il computer si riavvia, è possibile rimuovere eventuali protezioni con password del firmware esistenti utilizzando l'Utility Password Firmware di Mac OS X.

- **Elenco utenti senza autenticazione**: in alcuni casi, è possibile modificare questo criterio in modo che gli utenti o le classi di utenti specificati non debbano eseguire l'attivazione sul server Dell. Ad esempio, in una struttura educativa può essere richiesto agli insegnati di attivare il proprio computer contro il server Dell, ma singoli studenti utilizzando i computer del laboratorio non lo fanno. L'amministratore di laboratorio potrebbe utilizzare questo criterio e l'account su cui è in esecuzione lo strumento client, in modo che gli utenti studenti possano effettuare l'accesso senza che gli venga chiesto di eseguire l'attivazione. Per informazioni su Client Tool, consultare Strumento client. Se un'azienda ha bisogno di sapere quale account utente è associato a ciascun computer Mac, tutti gli utenti devono attivarsi contro il server Dell, in modo che l'azienda non modifichi questa proprietà. Tuttavia, se un utente desidera effettuare il provisioning del supporto EMS, deve essere autenticato sul server Dell.

4 Aprire il file .plist e modificare i valori variabile aggiuntivi:

N.B.:
Apple spesso rilascia nuove versioni dei sistemi operativi tra le versioni di Endpoint Security Suite Enterprise per Mac. Per andare incontro a più clienti possibile, Dell consente la modifica del file .plist per supportare questi casi. Non appena Apple rilascia una nuova versione, Dell inizia un test di queste versioni per assicurare che siano compatibili con client di crittografia per Mac.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
```

```
  <key>NoAuthenticateUsers</key> [In this sample code, after one user activates the computer
against the Dell Server, other users can log in without being prompted to activate.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, users from a specific domain name can
log in without being prompted to activate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;*@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, specific users can log in without
being prompted to authenticate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string>
  <string>;Kerberosv5;;username2@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the default .plist
file, it must be added to the file. Add from <key> through </array> to allow a newer version
of operating system to be used. See Note above.]
  <array>
   <string>10.<x.x></string> [Operating system version]
  </array>
  <key>UseRecoveryKey</key>
  <false/> [This value is obsolete since current versions can use both personal and
institutional recovery keys for FileVault encryption.]
  <key>SecurityServers</key>
  <array>
   <dict>
      <key>Host</key>
      <string>securityserver.organization.com</string> [Replace this value with your
Security Server URL]
      <key>Port</key>
     <integer>8443</integer> [Beginning in v8.0, the default port number is 8443. However,
port number 8081 will still allow activations. In general, if your Dell Server is v8.0 or
later, use port 8443. If your Dell Server is pre-v8.0, use port 8081.]
      <key>UseSSL</key>
      <true/> [We recommend a true value]
   </dict>
  </array>
  <key>ReuseUniqueIdentifier</key>
  <false/> [When this value is set to true, the computer identifies itself to the Dell
Server by the same hostname it was activated with, regardless of changes to the computer
hostname.]
  <key>Domains</key>
  <array>
   <dict>
      <key>DisplayName</key>
      <string>COMPANY</string>
      <key>Domain</key>
      <string>department.organization.com</string> [Replace this value with the Domain URL
that users will activate against]
   </dict>
  </array>
  <key>FirmwarePasswordMode</key>
  <string>Required</string> [If using Boot Camp, this value must be Optional. For more
information, see About Optional Firmware Password Protection.]
  <key>PolicyProxies</key>
  <array>
   <dict>
      <key>Host</key>
```

```
      <string>policyproxy.organization.com</string> [Replace this value with your Policy
Proxy URL]
      <key>Port</key>
      <integer>8000</integer> [Leave as-is unless there is a conflict with an existing port]
   </dict>
  </array>
  <key>Version</key>
  <integer>2</integer> [Do not modify]
  <key>MaxPasswordDelay</key>
  <integer>xxxx</integer> [Number of seconds to apply to the security policy, "Require
password XXXX after sleep or screen saver begins." The acceptable range is 0-32400.]
  <key>EMSTreatsUnsupportedFileSystemAs</key>
  <string>ignore</string> [For handling Mac OS Extended media. Possible values are ignore,
provisioningRejected, or unshieldable. ignore - the media is usable (default).
provisioningRejected - retains the value in the Dell Server policy, EMS Access to unShielded
Media. unshieldable - If the EMS Access to unShielded Media policy is set to Block, the
media is ejected. If the EMS Access to unShielded Media policy is not set to Block, it is
usable as provisioningRejected. The key and value are case sensitive.]
  <key>ClientActivationTimeout</key>
  <integer>120</integer> [Range: 5 to 300, inclusive. The default value is 30. The time in
seconds to give the Security Server time to respond to an activation attempt before giving
up. This plist value is valid for clients running v8.6.0.6627 or later.]
</dict>
</plist>
```

5 Salvare e chiudere i file .plist.

6 Per ogni computer di destinazione, copiare il pacchetto in una cartella temporanea e il file **com.dell.ddp.plist file in /Library/ Preferences.**

7 Eseguire un'installazione del pacchetto dalla riga di comando utilizzando il comando del **programma di installazione**:

```
sudo installer -pkg "Install Dell Data Protection.pkg" -target /
```

8 Riavviare il computer utilizzando la seguente riga di comando: `sudo shutdown -r now`

9 Continuare per Attivare la crittografia client per Mac.

Attivare Encryption Client

Il processo di attivazione associa gli account utente di rete nel server Dell al computer Mac e recupera ciascun criterio della protezione degli account, invia l'inventario e gli aggiornamenti di stato, consente il ripristino dei flussi di lavoro e fornisce un report di conformità completo. Il software client esegue il processo di attivazione per ogni account utente che trova nel computer quando ogni utente effettua l'accesso al proprio account utente.

N.B.: Per istruzioni sull'attivazione di un Mac non di dominio, consultare l'articolo della Knowledge Base SLN302497.

Al termine dell'installazione del software client e quando il Mac è stato riavviato, l'utente effettua l'accesso:

1 Immettere il nome utente e la password gestiti da Active Directory.

Se la finestra di dialogo della password va in timeout, premere **Aggiorna** sulla scheda dei criteri. In Visualizzare il criterio e lo stato nel computer locale, consultare il passaggio 1.

2 Selezionare il dominio al quale accedere.

Se il server Dell è configurato per il supporto multidominio e un dominio diverso deve essere utilizzato per l'attivazione, utilizzare il nome dell'entità utente (UPN), che è nel formato *<username>@<domain>*.

3 Le opzioni sono:

- Fare clic su **Attiva**.
  - Se l'attivazione viene completata, viene visualizzato un messaggio che lo conferma. Encryption Client per Mac ora è pienamente operativo e gestito dal server Dell.
  - Se l'attivazione non ha luogo, il software client consente tre tentativi per immettere le credenziali di dominio corrette. Se non riesce nessuno dei tre tentativi, la richiesta delle credenziali di dominio viene visualizzata di nuovo al successivo accesso dell'utente.
- Fare clic su **Non ora** per ignorare la finestra di dialogo, che viene nuovamente visualizzata all'accesso successivo dell'utente.

N.B.: Quando è necessario che l'amministratore decrittografi un'unità in un computer Mac, che sia da una postazione remota, eseguendo uno script o di persona, il software client chiederà all'utente di consentire l'accesso all'amministratore e richiederà all'utente di immettere la propria password.

N.B.: Se il computer viene impostato per la crittografia tramite FileVault e i file vengono crittografati, accertarsi di effettuare l'accesso a un account da cui è possibile poi avviare il sistema.

4 Eseguire una delle azioni seguenti:

- Se la crittografia **non** è stata abilitata prima dell'attivazione, continuare con il processo di crittografia.
- Se la crittografia **è stata** abilitato prima dell'attivazione, continuare con visualizzare i criteri di crittografia e lo stato.

Visualizzare il criterio e lo stato della crittografia

È possibile visualizzare il criterio e lo stato di crittografia nel computer crittografato o nella Remote Management Console.

Visualizzare il criterio e lo stato nel computer locale

Per visualizzare il criterio di crittografia e lo stato di crittografia nel computer locale, seguire la procedura seguente.

1 Avviare *preferenze di sistema* e fare clic su **Dell Data Protection**.

2 Fare clic sulla scheda **Criteri** per visualizzare il criterio attuale impostato per questo computer. Utilizzare questa schermata per confermare i criteri di crittografia specifici applicati per il computer.

SUGGERIMENTO: Fare clic su Aggiorna per verificare gli aggiornamenti del criterio.

La Remote Management Console elenca i criteri Mac nei seguenti gruppi di tecnologia:

- **Crittografia Mac**
- **Crittografia dei supporti rimovibili**

In base ai requisiti di crittografia dell'azienda, è possibile impostare i criteri per Dell o crittografia tramite FileVault. La tabella seguente elenca le opzioni per i criteri di ognuna.

Crittografia Mac > Crittografia dei volumi Dell

Crittografia dei volumi Dell	*Attivato* o *Disattivato* È il "criterio principale" per tutti gli altri criteri di Crittografia dei volumi Dell. Questo criterio deve essere impostato su *Attivato* per poter applicare qualsiasi altro criterio della crittografia del volume Dell. *Attivato* abilita la crittografia e avvia la crittografia dei volumi non crittografati, per il criterio Volumi destinati alla crittografia o Crittografa tramite FileVault per Mac. L'impostazione predefinita è *attivata.* Disattivato disabilita la crittografia e avvia una ricerca della decrittografia per tutti i volumi completamente o parzialmente crittografati.
Crittografa tramite FileVault per Mac	Se si desidera usare Crittografia tramite FileVault, impostare prima la crittografia del volume Dell su *attivato*. "Verificare che il criterio Crittografa tramite FileVault per Mac sia impostato attivato nel Server Dell. Quando è attivato, FileVault viene utilizzato per crittografare il volume di sistema incluse le unità Fusion, in base all'impostazione del criterio Volumi destinati alla crittografia. **N.B.: Se si utilizza Dell Encryption (non FileVault) e questo criterio è abilitato, ne consegue un conflitto di criteri.**

N.B.:
Se si pianifica di eseguire la migrazione dalla crittografia Dell alla crittografia tramite FileVault, vedere la sezione Migrazione dalla crittografia dei volumi Dell alla crittografia tramite FileVault.

Crittografia Mac > Impostazioni globali Mac

Volumi destinati alla crittografia	*Solo il volume di sistema* oppure *Tutti i volumi fissi* Solo il volume di sistema protegge solo il volume di sistema attualmente in esecuzione. L'impostazione **Tutti i volumi fissi** protegge tutti i volumi estesi Mac OS su tutti i dischi fissi, insieme al volume di sistema attualmente in esecuzione.

3 Per le descrizioni di tutti i criteri, consultare *AdminHelp* disponibile nella Remote Management Console. Per individuare un criterio specifico in *AdminHelp:*

a Fare clic sull'icona Cerca.

b Nel campo Cerca, immettere il nome del criterio compreso tra virgolette.

c Fare clic sul collegamento all'argomento che viene visualizzato. Il nome del criterio immesso tra virgolette è evidenziato nell'argomento.

4 Fare clic sulla scheda **Volumi di sistema** per visualizzare lo stato dei volumi assegnati per la crittografia.

Stato	Descrizione
Escluso	Il volume è escluso dalla crittografia. Questo stato si applica ai volumi non crittografati quando la crittografia è disattivata, ai volumi esterni, ai volumi con formati diversi da Mac OS X Esteso (Journaled) e a volumi non di sistema quando il criterio *Volumi assegnati per la crittografia* è impostato solo su *volume di sistema*.
Preparazione del volume per la crittografia in corso...	Il software client sta attualmente avviando il processo di crittografia per il volume, ma non ha iniziato la ricerca della crittografia.
Impossibile ridimensionare il volume	Il software client non può avviare la crittografia perché è impossibile ridimensionare appropriatamente il volume. Dopo aver ricevuto questo messaggio, contattare Dell ProSupport e fornire i file di registro.
Ripristino necessario prima dell'inizio della crittografia	Il volume non ha superato la verifica di Utility Disco. Per ripristinare un volume, seguire le istruzioni nell'articolo HT1782 del supporto Apple (http://support.apple.com/kb/HT1782).
Preparazione della crittografia completata. Riavvio in sospeso...	La crittografia verrà avviata dopo il riavvio.
Conflitto criteri di crittografia	È impossibile inglobare il disco nel criterio perché è crittografato con un'impostazione errata. Consultare Crittografa tramite FileVault per Mac.
In attesa di depositare le chiavi nel server Dell...	Per far sì che tutti i dati crittografati siano ripristinabili, il software client non avvierà il processo di crittografia fino a quando tutte le chiavi di crittografia non saranno depositate nel Server Dell. Il software client eseguirà il polling per la connettività del Security Server in questo stato, finché le chiavi non saranno depositate.
Crittografia in corso...	È in corso una ricerca della crittografia.
Crittografato	La ricerca della crittografia è stata completata.
Decrittografia in corso...	È in corso una ricerca della decrittografia.

Stato	Descrizione
Ripristino allo stato originale in corso...	Il software client sta ripristinando lo schema di partizione allo stato originale al termine del processo "Decrittografia in corso...". È la ricerca della decrittografia equivalente allo stato "Preparazione del volume per la crittografia in corso".
Decrittografato	La ricerca della decrittografia è stata completata.

Colore	Descrizione
Verde	Porzione crittografata
Rosso	Porzione non crittografata
Giallo	Porzione con nuova crittografia in corso Per esempio, da una modifica negli algoritmi di crittografia. I dati sono ancora protetti, è semplicemente in corso una transizione verso un tipo di crittografia differente.

La scheda Volumi di sistema mostra tutti i volumi collegati al computer che si trovano nei dischi formattati della Tabella di partizione GUID (GPT). La tabella seguente elenca degli esempi di configurazioni di volumi per unità interne.

N.B.: I badge e le icone possono cambiare lievemente a seconda del sistema operativo.

Badge	Tipo e stato del volume
	Il volume del sistema Mac OS X attualmente avviato. Il badge della cartella con X indica la partizione di avvio corrente. Dell Encryption non è supportato con Protezione integrità di sistema (SIP). Se questa condizione di incompatibilità viene specificata dal criterio e SIP viene abilitata, viene visualizzato un errore accanto all'unità nella scheda Volumi di sistema. Consultare Installazione/aggiornamento e attivazione interattiva, passaggio 4 per disattivare la SIP.
	Un volume configurato per la crittografia. Il badge indica una partizione crittografata di Dell.
	Un volume configurato per la crittografia. Il badge Sicurezza e Privacy indica una partizione protetta tramite FileVault.
	Un volume non di avvio configurato per la crittografia. Il badge Sicurezza e Privacy indica una partizione protetta tramite FileVault.
 	Unità multiple e nessuna crittografia. **N.B.: L'icona del volume senza un badge indica che al disco non è stato fatto nulla. Non è un disco di avvio.**

Badge	Tipo e stato del volume
	Unità multiple in cui solo il volume di sistema è crittografato. Questo è un esempio della partizione crittografata di Dell.

5 Fare clic sulla scheda **Supporti rimovibili** per visualizzare lo stato dei volumi assegnati per la crittografia. La tabella seguente elenca degli esempi di configurazioni di volumi per supporti rimovibili.

I badge e le icone possono cambiare lievemente a seconda del sistema operativo.

Badge	Stato
	L'icona di un volume in grigio indica un dispositivo non montato. Tra i motivi possibili: · È possibile che l'utente abbia scelto di non sottoporlo a provisioning. · Il supporto potrebbe essere bloccato. **N.B.: Il badge di un cerchio/barra rossa su questa icona indica una partizione esclusa dalla protezione perché non è supportata. Sono inclusi i volumi formattati con FAT32.**
	L'icona saturata di un volume indica un dispositivo montato. Il badge di scrittura vietata indica che è di sola lettura. La crittografia è attivata, ma non è stato eseguito il provisioning del supporto e l'accesso EMS ai supporti non schermato è impostato su Sola Lettura.
	Supporto crittografato tramite EMS, indicato da un badge di Dell.

Visualizzare lo stato e il criterio nella Remote Management Console

Per visualizzare il criterio di crittografia e lo stato di crittografia nella Remote Management Console, seguire la procedura seguente.

1 Eseguire l'accesso alla Remote Management Console come amministratore Dell.

2 Nel riquadro sinistro, fare clic su **Popolamenti > Endpoint**.

3 Per workstation, fare clic su un'opzione nel campo Nome host o, se si conosce il nome host dell'endpoint, immetterlo nel campo Cerca. È anche possibile immettere un filtro per eseguire la ricerca dell'endpoint.

N.B.: Il carattere jolly (*) può essere utilizzato ma non necessariamente all'inizio o alla fine del testo. È possibile immettere un Nome comune, un Nome principale utente oppure un SamAccountName.

4 Fare clic sull'endpoint appropriato.

5 Fare clic sulla scheda **Dettagli e azioni**.

L'area Dettagli endpoint mostra informazioni sul computer Mac.

Lo schermo area dettagli visualizza le informazioni sul software client, inclusa l'ora di fine e di avvio di una ricerca di crittografia per questo computer.

Per visualizzare i criteri validi, nell'area Azioni, fare clic su **Visualizza criteri effettivi.**

6 Fare clic sulla scheda **Criteri di protezione**. Da questa scheda è possibile espandere i tipi di criteri e modificare i singoli criteri.

a Al termine, fare clic su **Salva**.

b Nel riquadro sinistro fare clic su **Gestione** > **Esegui commit**.

N.B.: Il numero che appare accanto a Modifiche dei criteri in sospeso è cumulativo. Può includere le modifiche eseguite in altri endpoint o eseguite da altri amministratori che usano lo stesso account.

c Immettere una descrizione delle modifiche nella casella Commenti e fare clic su **Eseguire il commit dei criteri**.

7 Fare clic sulla scheda **Utenti**. Questa scheda mostra un elenco di utenti attivati nel computer Mac. Fare clic sul nome dell'utente per visualizzare le informazioni su tutti i computer per i quali tale utente è attivato.

8 Fare clic sulla scheda **Gruppi di endpoint**. Quest'area mostra tutti i gruppi di endpoint dei quali fa parte il computer Mac.

Volumi di sistema

Abilitare la crittografia

N.B.: La crittografia è supportata solo dai volumi di Mac OS X Esteso (Journaled) e dai dischi di sistema partizionati secondo lo schema di partizione della Tabella di partizione GUID (GPT).

Utilizzare questo processo per abilitare la crittografia in un computer client se la crittografia **non** è abilitata prima dell'attivazione. Questo processo abilita la crittografia solo per un unico computer. Se lo si desidera, è possibile scegliere di abilitare la crittografia per tutti i computer Mac al livello di criterio Aziendale. Per ulteriori istruzioni su come abilitare la crittografia a *livello del criterio Enterprise,* consultare *AdminHelp*.

1 Eseguire l'accesso alla Remote Management Console come amministratore Dell.

2 Nel riquadro sinistro, fare clic su **Popolamenti** > **Endpoint**.

3 Per workstation, fare clic su un'opzione nella colonna Nome host o, se si conosce il nome host dell'endpoint, immetterlo nel campo Cerca. È anche possibile immettere un filtro per eseguire la ricerca dell'endpoint.

N.B.: Il carattere jolly (*) può essere utilizzato ma non necessariamente all'inizio o alla fine del testo. È possibile immettere un Nome comune, un Nome principale utente oppure un SamAccountName.

4 Fare clic sull'endpoint appropriato.

5 Sulla pagina Criteri di protezione, fare clic sul gruppo della tecnologia di *Crittografia Mac.*

Per impostazione predefinita, il criterio principale della *crittografia del volume Dell* è *attivato.*

6 Se un Mac dispone di un'unità Fusion, selezionare la casella di controllo per la *crittografia tramite FileVault* per criterio Mac.

N.B.: Questo criterio richiede che anche il criterio *Crittografia del volume Dell* sia attivato. Tuttavia, quando è abilitata la crittografia tramite FileVault, non sarà applicato nessuno degli altri criteri nel gruppo. Consultare Crittografia Mac > Crittografia dei volumi Dell.

7 Se FileVault non è selezionato, modificare gli altri criteri come desiderato.

Per le descrizioni di tutti i criteri, consultare *AdminHelp* disponibile nella Remote Management Console.

8 Al termine, fare clic su **Salva**.

9 Nel riquadro sinistro fare clic su **Gestione** > **Esegui commit**.

Il numero che appare accanto a Modifiche dei criteri in sospeso è cumulativo. Può includere le modifiche eseguite in altri endpoint o eseguite da altri amministratori che usano lo stesso account.

10 Immettere una descrizione delle modifiche nella casella Commenti e fare clic su **Eseguire il commit dei criteri**.

11 Per vedere le impostazioni dei criteri nel computer locale dopo che Dell Enterprise Server ha inviato il criterio, nel riquadro Criteri di Preferenze di Dell Data Protection, fare clic su **Aggiorna.**

Processo di crittografia

Il processo di crittografia varia in base a questi fattori:

- L'avvio del volume di avvio quando la crittografia è abilitata.
- Se è stata selezionata la crittografia tramite Dell Encryption o FileVault.

> **N.B.: Per mantenere l'integrità dei dati dell'utente, il software client non inizia a crittografare un volume fino a quando non è stato completato il processo di verifica in quel volume. Se la verifica di un volume non riesce, il software client informa l'utente e riporta l'errore nelle Preferenze di Dell Data Protection. Se è necessario ripristinare un volume, seguire le istruzioni nell'articolo HT1782 del supporto Apple (http://support.apple.com/kb/HT1782). Il software client tenta nuovamente di eseguire una verifica al successivo riavvio del computer.**

Selezionare una delle seguenti azioni:

- Crittografia Dell di un'unità non crittografata
- Crittografia FileVault di un volume non crittografato
- Assumere la gestione di un volume crittografato di FileVault esistente

Crittografia Dell di un'unità non crittografata

Quando il software client riceve il criterio di crittografia, esegue una convalida di Utility Disco dei volumi destinati alla crittografia e quindi li configura per la crittografia.

1 La barra di avanzamento indica lo stato della verifica. Al termine della verifica, i volumi di destinazione sono configurati per la crittografia.

   Questo processo può rallentare la risposta del computer per alcuni minuti. Per ogni volume con crittografia in sospeso, viene visualizzata una finestra di dialogo che informa l'utente che l'operazione è in corso.

2 Al termine della preparazione della crittografia, riavviare il sistema.

> **N.B.: A seconda dei criteri dell'esperienza utente impostati nella Remote Management Console, il software del client potrebbe richiedere all'utente di riavviare il computer.**

3 Al termine del riavvio, è necessario che il computer sia connesso alla rete affinché il software client depositi le informazioni di ripristino nel Server Dell.

Il software client può avviare e completare il processo di crittografia, e riportare lo stato di crittografia alla Remote Management Console, il tutto prima dell'accesso dell'utente. Questo consente di applicare la conformità a tutti i computer Mac senza che sia necessaria l'interazione dell'utente.

Crittografia FileVault di un volume non crittografato

1 Al termine dell'installazione e dell'attivazione, è necessario eseguire l'accesso all'account dal quale si desidera avviare una volta attivata la crittografia tramite FileVault.

2 Attendere il completamento della convalida dell'unità e della verifica del volume.

3 Immettere la password per l'account.

> **N.B.: Se la finestra di dialogo scade, è necessario riavviare o eseguire l'accesso per visualizzare di nuovo la finestra di dialogo della password.**

4 Fare clic su **OK**.

Se l'account con il quale l'utente ha eseguito l'accesso è un account di rete non mobile, viene visualizzata una finestra di dialogo. Al termine della crittografia dell'unità di avvio, l'unità può essere avviata solo dall'utente che era connesso durante l'inizializzazione di FileVault.

Questo account deve essere un account locale o un account mobile di rete. Per modificare gli account di rete non mobile, andare a **Preferenze di sistema > utenti e gruppi**. Effettuare una delle seguenti operazioni:

- Rendere l'account un account mobile.
  OPPURE
- Eseguire l'accesso ad un account locale e inizializzare FileVault da quella posizione.

5 Fare clic su **OK**.

6 Al termine della preparazione della crittografia, riavviare il sistema.

N.B.: A seconda dei criteri dell'esperienza utente impostati nella Remote Management Console, il software del client potrebbe richiedere all'utente di riavviare il computer.

7 Al termine del riavvio, è necessario che il computer sia connesso alla rete affinché il software client depositi le informazioni di ripristino nel Server Dell.

Il software client può avviare e completare il processo di crittografia, e riportare lo stato di crittografia alla Dell Remote Management Console, il tutto prima dell'accesso dell'utente. Questo consente di applicare la conformità a tutti i computer Mac senza che sia necessaria l'interazione dell'utente.

Modificare il criterio per aggiungere utenti FileVault

FileVault protegge i dati presenti sul disco mediante la crittografia automatica. In un volume di avvio FileVault gestito, per consentire a più utenti di sbloccare il disco, è possibile modificare un criterio in Remote Management Console e utilizzare il dizionario di nomi e valori OpenDirectory, affinché gli utenti possano aggiungersi al disco FileVault.

1 Nei criteri *Impostazioni globali Mac* avanzati di Remote Management Console, scorrere fino al criterio *Elenco utenti FileVault 2 PBA*.

2 Nel campo del criterio *Elenco utenti FileVault 2 PBA*, inserire una regola che corrisponda agli utenti da specificare. Ad esempio, l'impostazione `<string>*</string>` per qualsiasi chiave corrisponde a tutti gli utenti del server OpenDirectory vincolato.

I codici fanno distinzione tra maiuscole e minuscole ed è necessario che l'intero valore abbia il formato corretto di un dizionario e che gli elementi di matrice siano contenuti in un elenco di proprietà. Le chiavi di dizionario sono combinate con l'operatore AND. I valori di matrice sono combinati con l'operatore OR, pertanto la corrispondenza di un elemento qualsiasi nella matrice genera una corrispondenza per l'intera matrice.

N.B.:
Se una regola non ha il formato corretto, viene visualizzato un errore in *Dell Data Protection > Preferenze*.

Il seguente <dict> riporta gli esempi per due chiavi:

```
<dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
     <string>;Kerberosv5;;user1@LKDC:*</string>
     <string>;Kerberosv5;;user2@LKDC:*</string>
     <string>;Kerberosv5;;user3@LKDC:*</string>
     <string>;Kerberosv5;;z*@LKDC:*</string>
    </array>
    <key>dsAttrTypeStandard:NFSHomeDirectory</key>
    <string>/Users/*</string>
</dict>
```

- Le voci della chiave di esempio *AuthenticationAuthority* specificano un modello di *user1*, *user2* e *user3* o qualsiasi ID utente che inizi con *z*. Per visualizzare la finestra di dialogo che fornisce la sintassi esatta per ciascun utente, premere i tasti **Control-Opzione-Comando** sul client. Copiare la sintassi per l'utente e incollarla nel server.

N.B.:
In questo esempio, gli asterischi finali rappresentano l'ultima parte dei record dell'autorità di autenticazione. In genere, per evitare una specifica inappropriata, includere il record completo invece di un asterisco finale, perché l'asterisco corrisponde a qualsiasi informazione dopo i due punti nel record OpenDirectory.

- La chiave NFSHomeDirectory richiede che tutti gli utenti che passano la prima chiave abbiano anche una directory principale in */Users/*.

N.B.:
È necessario creare la home directory se non ne esiste una per un utente.

3 Riavviare i computer.

4 Richiedere agli utenti finali di attivare l'avvio di FileVault per il proprio account utente. L'utente deve disporre di un account locale o mobile. Gli account di rete vengono automaticamente convertiti in account mobili.

Per attivare il proprio account FileVault:

1 Avviare **Preferenze di sistema** e fare clic su **Dell Data Protection**.

2 Fare clic sulla scheda **Volumi di sistema**.

3 Premere il tasto Option e fare clic sull'unità Volume di sistema e selezionare **Aggiungi utenti FileVault ad avvio FileVault**.

4 Nel campo Cerca, immettere il nome dell'utente o scorrere verso il basso. Gli account utente vengono visualizzati solo se soddisfano i criteri impostati dal criterio.

Per gli utenti locali e mobili viene visualizzato il pulsante *Abilita utente*.

Per gli utenti di rete viene visualizzato il pulsante *Converti e abilita utente*.

N.B.:
Un indicatore verde viene visualizzato accanto agli account utente che possono avviare FileVault.

5 Fare clic su **Abilita utente** o **Converti e abilita utente**.

6 Immettere la password per l'account selezionato e fare clic su **OK**. Viene visualizzato un indicatore di avanzamento.

7 Una volta visualizzata la finestra di dialogo Operazione completata, fare clic su **Fine**.

Assumere la gestione di un volume crittografato di FileVault esistente

Se il computer ha già un volume crittografato tramite FileVault e la crittografia tramite FileVault è abilitata nella Remote Management Console, la crittografia Dell può assumere la gestione del volume.

Se la crittografia Dell rileva che il volume di avvio è già crittografato, viene visualizzata la finestra di dialogo di Dell Data Protection. Per consentire alla crittografia Dell di assumere la gestione del volume, seguire la seguente procedura.

1 Selezionare **Chiave di ripristino personale o credenziali account avviabile.**

- **Chiave di ripristino personale - se si dispone della chiave di ripristino personale ricevuta quando l'unità è stata crittografata tramite FileVault.**

  1 Immettere la chiave.

  Se l'utente non dispone della chiave esistente, è possibile richiederla all'amministratore.

  2 Fare clic su **OK**.

  N.B.: Al termine del processo di assunzione, viene generata e depositata una nuova chiave di ripristino personale. La chiave di ripristino precedente viene invalidata e rimossa.

- **Credenziali account avviabile - se si dispone di nome utente e password di un account attualmente autorizzato ad avviarsi dal volume.**

1. Immettere nome utente e password.
2. Fare clic su **OK**.

2. Quando viene visualizzata una finestra di dialogo che informa che Dell ora gestisce la crittografia del volume, fare clic su **OK**.

   Se la crittografia Dell rileva che un volume non di avvio è già crittografato, viene visualizzata una richiesta di passphrase.

3. Per consentire alla crittografia Dell di assumere la gestione del volume, immettere la passphrase per accedere al volume (solo per volumi non di avvio crittografati tramite FileVault). Si tratta della password che è stata assegnata al volume quando è stato originariamente crittografato tramite FileVault.

   Una volta che Dell gestisce la crittografia del volume, la vecchia password non è più valida. Nel caso in cui l'utente abbia bisogno di assistenza per il ripristino, l'amministratore Dell può recuperare la chiave di ripristino per il volume.

   Se si sceglie di non immettere la password, il contenuto del volume sarà accessibile e crittografato tramite FileVault ma la crittografia non sarà gestita da Dell.

N.B.: Nella Remote Management Console, l'amministratore può verificare che ora il Server Dell gestisce l'endpoint.

Riciclo delle chiavi di ripristino di FileVault

Se si riscontrano problemi di sicurezza con un pacchetto di ripristino o se un volume o le chiavi sono compromesse, è possibile riciclare il materiale delle chiavi per quel volume.

È possibile riciclare le chiavi per unità di avvio e non di avvio in Mac OS X.

Per riciclare il materiale delle chiavi:

1. Scaricare un pacchetto di ripristino dalla Remote Management Console e copiarlo nel desktop del computer.
2. Avviare *preferenze di sistema* e fare clic su **Dell Data Protection**.
3. Fare clic sulla scheda **Volumi di sistema**.
4. Trascinare il pacchetto di ripristino dal passaggio 1 alla partizione appropriata.
   Una finestra di dialogo chiede di ripetere in sequenza le chiavi di FileVault.
5. Fare clic su **OK**.
   Una finestra di dialogo conferma il completamento della ripetizione in sequenza delle chiavi.
6. Fare clic su **OK**.

N.B.: Le chiavi nel pacchetto di ripristino per questa unità ora sono obsolete. È necessario scaricare un nuovo pacchetto di ripristino dalla Remote Management Console.

Esperienza utente

Per ottenere la massima sicurezza, il software client disabilita la funzione di accesso automatico ai computer Mac OS X.

Inoltre, il software client applica automaticamente la funzione per MAC OS X *richiedi password dopo che viene avviata la modalità stop/salvaschermo*. Nella modalità stop/salvaschermo è inoltre consentita una quantità di tempo configurabile prima di applicare l'autenticazione. Il software client consente ad un utente di impostare un valore fino a cinque minuti prima che l'autenticazione venga applicata.

Gli utenti possono utilizzare normalmente il computer mentre è in corso la ricerca della crittografia. È in corso la crittografia di tutti i dati nel volume di sistema attualmente avviato, incluso il sistema operativo, mentre il sistema operativo continua a funzionare.

Se il computer viene riavviato o si attiva lo stop del sistema, la ricerca della crittografia viene sospesa e riprende automaticamente dopo il riavvio o la riattivazione.

Il software client non supporta l'uso dell'ibernazione delle immagini, che la funzione di Mac OS X *sospensione sicura* utilizza per riattivare il computer se la batteria è completamente scarica durante la sospensione.

Per ridurre l'impatto sull'utente, il software client aggiorna automaticamente la modalità di stop del sistema per disabilitare l'ibernazione e applica questa impostazione. Il computer entra comunque nello stato di stop, ma lo stato attuale del sistema viene mantenuto solo in memoria. Pertanto, il computer si riavvia completamente se durante lo stop si è spento del tutto, cosa che potrebbe accadere se la batteria si scarica o viene sostituita.

Copiare la regola dell'elenco dei dispositivi consentiti

Una voce di menu nascosta consente all'utente di copiare una regola dell'elenco dispositivi consentiti per i supporti esterni.

1 Avviare **preferenze di sistema** e fare clic su **Dell Data Protection**.

2 Selezionare la scheda **Supporti rimovibili**.

3 Fare clic con il pulsante destro del mouse sulla riga di un'unità e premere contemporaneamente il tasto comando.

Viene visualizzata una voce di menu nascosta.

4 Fare clic su **Copiare la regola dell'elenco dei dispositivi consentiti** per i supporti esterni correnti. La regola dei dispositivi consentiti viene copiata negli appunti.

5 Accedere agli appunti, copiare la regola dei dispositivi consentiti e inviarla all'amministratore.

Se il *criterio di crittografia dei supporti Mac* è **attivato**, i dati vengono crittografati, inclusi le unità Thunderbolt.

Se si desidera escludere un dispositivo o un gruppo di dispositivi per impedire la scrittura di dati crittografati nell'unità Thunderbolt o nel supporto EMS, è possibile utilizzare la regola dell'elenco dei dispositivi consentiti per modificare i valori.

Usare la regola completa per specificare una particolare unità da ammettere nell'elenco dei dispositivi consentiti, per esempio:

bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101 II;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSERNUM=001CC0EC3447AA308699119F

N.B.: Accertarsi di sostituire i valori di esempio con le informazioni dell'unità.

N.B.: È necessario abilitare HFS Plus. Consultare Abilitare HFS Plus.

Per escludere i dispositivi SATA dall'applicazione del criterio EMS quando si è connessi tramite Thunderbolt:

tbolt=1;bus=SATA

È anche possibile inserire o escludere dall'elenco dei dispositivi consentiti un supporto da EMS in base a:

- **Dimensioni del supporto**

  Regola dell'elenco dei dispositivi consentiti per escludere grandi supporti dalla protezione EMS.

  size <op> <size specifier>

  <op> può essere =, <=, >=, <, >

  <size specifier> è nel formato intero decimale con un suffisso facoltativo da {K, M, G, T} allineato su 1000, non 1024. Per esempio, per escludere da EMS un supporto o un'unità più grande di 500000000 byte, usare una delle seguenti:

  size >= 500000000

  size >= 500000K

  size >= 500M
- **Tipo di file system**

Regola dell'elenco dei dispositivi consentiti:

fstype=<fstype>

<fstype> può essere ExFAT, FAT, o HFS+

Per escludere entrambi, di seguito si trova un esempio per supporti da 1 TB e HFS+ più grandi:

size>=1T;fstype=HFS+

Ripristino

Occasionalmente, potrebbe essere necessario avere accesso ai dati presenti in dischi crittografati. Come amministratore Dell, è possibile accedere ai dischi crittografati senza decodificarli, risparmiando tempo prezioso.

Possono esserci molti motivi per cui è necessario avere accesso ai dati crittografati di un utente, ma alcuni casi di utilizzo comune sono i seguenti:

- Potrebbe essere necessario spostare i dati crittografati di un utente in un altro Mac come parte di un aggiornamento dell'hardware.
- Potrebbe essere necessario avere accesso ad un disco crittografato a causa di un errore del sistema operativo che comporta il mancato avvio del volume di sistema, ed è necessario eseguire varie utilità per ripristinare il sistema operativo.
- Potrebbe essere necessario avere accesso ai dati crittografati di un utente perché l'utente ha effettuato una modifica di configurazione non autorizzata ed è necessario rimediare alla situazione.

Questa sezione guida l'utente attraverso il processo di utilizzo di **una** delle tre operazioni di ripristino disponibili.

Scegliere **un'**opzione di seguito:

- Monta volume
- Accetta nuova configurazione di sistema
- Ripristino FileVault - Utilizzare solo se si utilizza la crittografia FileVault sull'endpoint da ripristinare. FileVault può essere utilizzato con Encryption Client in esecuzione su Mac OS X 10.10.5 o versione successiva. La funzionalità di ripristino FileVault è utilizzata anche nelle unità Fusion.

Monta volume

Prerequisiti

- Un volume o computer di ripristino esterno non crittografato in cui verrà eseguita l'Utilità di ripristino
- Un cavo FireWire o Thunderbolt, in base all'hardware in dotazione
- L'ID dispositivo/ID univoco del computer destinato al ripristino: nella maggior parte dei casi, è possibile trovare il computer destinato al ripristino nella Remote Management Console cercando il nome utente del proprietario e visualizzando i dispositivi crittografati per tale utente. Il formato dell'ID univoco/ID dispositivo è "MacBook.Z4291LK58RH di Mario Rossi".
- Supporti di installazione Dell

Procedura

1 Eseguire l'accesso alla Remote Management Console come amministratore Dell.

2 Nel riquadro sinistro, fare clic su **Gestione > Ripristina endpoint**.

3 Nel campo Cerca, immettere il nome di dominio completo dell'endpoint da ripristinare e fare clic sull'icona Cerca.

4 Fare clic sul collegamento di **ripristino** del dispositivo.

5 Se l'endpoint richiede un ripristino avanzato, viene visualizzata una richiesta di password. Assegnare una nuova password al bundle di chiavi che sta per essere scaricato.

N.B.: È necessario ricordare questa password per avere accesso alle chiavi di ripristino.

6 Per salvare il pacchetto di ripristino su un volume o computer di ripristino esterno che avrà in esecuzione l'utilità di ripristino per eseguire l'operazione di ripristino, fare clic su **Download** e quindi su **Salva**.

Il file di ripristino <nome_computer.dominio>.csv viene scaricato.

> **N.B.: Se nel computer è abilitata la protezione con password del firmware, all'utente verrà richiesta la password del firmware per accedere a Startup Manager di preavvio. È possibile trovare la password del firmware di questo computer nel pacchetto di ripristino scaricato in salva pacchetto di ripristino. Consultare Come abilitare il Boot Camp per Mac OS X per ulteriori informazioni.**

7 Avviare il computer di destinazione da un volume di ripristino esterno creato in precedenza. È possibile portarlo a termine tramite l'avvio del riquadro del disco di avvio nelle Preferenze di sistema e selezionando il volume di ripristino del SO completo, o tenendo premuta la chiave **Opzione** mentre si riavvia il computer e selezionando il volume di ripristino nello Startup Manager di preavvio.

Oppure

Avviare il computer destinato al ripristino in Modalità disco di destinazione. È possibile portarlo a termine tramite l'avvio del riquadro del disco di avvio nelle Preferenze di sistema e facendo clic su **Modalità disco di destinazione**, o tenendo premuta la chiave **T** mentre si riavvia il computer.

> **N.B.: La protezione con password del firmware blocca la possibilità di utilizzare il tasto T all'avvio per entrare in Modalità disco di destinazione. Maggiori informazioni sulla Modalità disco di destinazione sono rese disponibili da Apple alla pagina all'indirizzo http://support.apple.com/kb/HT1661.**

Connettere ora il computer al computer host che eseguirà l'operazione di ripristino utilizzando un cavo FireWire o Thunderbolt, in base al proprio hardware.

8 Montare Dell-Data-Protection-<version>.dmg.

> **N.B.: La versione della Recovery Utility deve essere la stessa o più recente rispetto a quella del software client installato nel computer destinato al ripristino.**

9 Nella cartella Utilità collocata nel supporto di installazione Dell, avviare l'utilità di ripristino Dell.

Viene visualizzato un messaggio che informa: "È necessario caricare il kext [testo del kernel] di DDP per modificare i dischi crittografati. Digitare la password per consentire la modifica."

10 Immettere la password per l'amministratore o l'utente.

Viene visualizzato un messaggio che informa, "È necessario installare il ripristino."

11 Fare clic su **Installa**.

12 Selezionare il volume o l'unità che necessita di ripristino e fare clic su **Continua**.

La selezione dell'unità ripristinerà tutti i volumi nell'unità in una volta sola.

13 Selezionare il pacchetto di ripristino (salvato nel passaggio 6) e fare clic su **Apri**.

14 Selezionare l'opzione **Monta volume**.

15 Fare clic su **Continua** per confermare *Monta volume.* Viene visualizzato il messaggio di completamento dell'operazione.

16 Fare clic su **Chiudi**.

È ora possibile aprire una finestra di Finder e accedere ai dati nel volume crittografato come per un volume normale. Tutti i file vengono crittografati e decrittografati in modo trasparente quando vengono trasferiti da un volume all'altro.

Accetta nuova configurazione di sistema

Se una modifica della password del firmware o di un'altra configurazione di sistema ha invalidato la chiave di crittografia in un computer crittografato, selezionare questa opzione per accettare la configurazione di sistema aggiornata al successivo riavvio e ripristinare l'accesso al computer.

Poiché la crittografia è legata ad una configurazione specifica del dispositivo, delle modifiche alla configurazione invalidano la chiave di crittografia del software client. Quando si sceglie di accettare la nuova configurazione di sistema, si istruisce semplicemente il software client a reimpostare la propria sicurezza in base alla nuova configurazione. Per esempio, potrebbe essere necessario spostare l'unità in un altro Mac perché l'utente ha danneggiato lo schermo. Utilizzando questo metodo, si istruisce il software client ad accettare questa "nuova" configurazione come valida.

Prerequisiti

- Un volume o computer di ripristino esterno non crittografato in cui verrà eseguita l'Utilità di ripristino
- Un cavo FireWire o Thunderbolt, in base all'hardware in dotazione
- L'ID dispositivo/ID univoco del computer destinato al ripristino: nella maggior parte dei casi, è possibile trovare il computer destinato al ripristino nella Remote Management Console cercando il nome utente del proprietario e visualizzando i dispositivi crittografati per tale utente. Il formato dell'ID univoco/ID dispositivo è "MacBook.Z4291LK58RH di Mario Rossi".
- Supporti di installazione Dell

Procedura

1 Eseguire l'accesso alla Remote Management Console come amministratore Dell.

2 Nel riquadro sinistro, fare clic su **Popolamenti > Endpoint**.

3 Cercare il dispositivo da ripristinare.

4 Fare clic sul nome del dispositivo per aprire la pagina Dettagli endpoint.

5 Fare clic sulla scheda **Dettagli e azioni**.

6 In dettagli Shield, fare clic sul collegamento **chiavi di ripristino dispositivo**.

7 Per salvare il pacchetto di ripristino su un volume o computer di ripristino esterno che avrà in esecuzione l'utilità di ripristino per eseguire l'operazione di ripristino, fare clic su **Download** e quindi su **Salva**.

> **N.B.: Se nel computer è abilitata la protezione con password del firmware, all'utente verrà richiesta la password del firmware per accedere a Startup Manager di preavvio. È possibile trovare la password del firmware di questo computer nel pacchetto di ripristino scaricato al passaggio 7. Consultare Come abilitare il Boot Camp per Mac OS X per ulteriori informazioni.**

8 Avviare il computer di destinazione da un volume di installazione del SO completo esterno creato in precedenza. È possibile portarlo a termine tramite l'avvio del riquadro del disco di avvio nelle Preferenze di sistema e selezionando il volume di installazione del SO completo, o tenendo premuta la chiave **Opzione** mentre si riavvia il computer e selezionando il volume di installazione del SO completo esterno nello Startup Manager di preavvio. Per creare un volume avviabile, fare riferimento a https://support.apple.com/en-us/HT202796.

Oppure

Avviare il computer destinato al ripristino in Modalità disco di destinazione. È possibile portarlo a termine tramite l'avvio del riquadro del disco di avvio nelle Preferenze di sistema e facendo clic su **Modalità disco di destinazione**, o tenendo premuta la chiave **T** mentre si riavvia il computer.

> **N.B.: La protezione con password del firmware blocca la possibilità di utilizzare il tasto T all'avvio per entrare in Modalità disco di destinazione. Maggiori informazioni sulla Modalità disco di destinazione sono rese disponibili da Apple alla pagina all'indirizzo http://support.apple.com/kb/HT1661.**

9 Eseguire una delle azioni seguenti:

- Connettere il computer al computer host che eseguirà l'operazione di ripristino utilizzando un cavo FireWire o Thunderbolt, in base al proprio hardware.

  Oppure

- Passare l'avvio a un qualsiasi disco con un'installazione del SO completa.

10 Montare Dell-Data-Protection-<version>.dmg.

> **N.B.: La versione della Recovery Utility deve essere la stessa o più recente rispetto a quella del software client installato nel computer destinato al ripristino.**

11 Nella cartella Utilità collocata nel supporto di installazione Dell, avviare l'utilità di ripristino Dell.

Viene visualizzato un messaggio che informa: "È necessario caricare il kext [testo del kernel] di DDP per modificare i dischi crittografati. Digitare la password per consentire la modifica."

12 Immettere la password per l'amministratore o l'utente.

Viene visualizzato un messaggio che informa, "È necessario installare il ripristino."

13 Fare clic su **Installa**.

14 Selezionare il volume o l'unità che necessita di ripristino e fare clic su **Continua**.

La selezione dell'unità ripristinerà tutti i volumi nell'unità in una volta sola.

Viene visualizzata la finestra di selezione dei file.

15 Selezionare il pacchetto di ripristino (salvato nel passaggio 7) e fare clic su **Apri**.
Viene visualizzata la finestra di dialogo *selezionare l'operazione di ripristino*.

16 Selezionare l'opzione **Accetta nuova configurazione di sistema**.

17 Fare clic su **Continua** per confermare *Accetta nuova configurazione di sistema*.

18 Immettere la password per reimpostare la proprietà e accettare la nuova configurazione di sistema.

19 Fare clic su **OK**.

Il messaggio di ripristino completo viene visualizzato quando viene avviato il volume di sistema interno originale. Il messaggio richiederà all'utente di riavviare di nuovo il computer. Il software client ha ora accettato la configurazione di sistema aggiornata ed è possibile accedere normalmente al computer.

Ripristino FileVault

Il ripristino di un volume gestito crittografato tramite FileVault è considerevolmente differente dal ripristino di un volume crittografato tramite il volume crittografato Dell. Il processo di ripristino è dettato da Apple ed è automatizzato laddove possibile, ma sono necessari alcuni altri passaggi.

L'utilità Dell Recovery semplifica l'operazione degli strumenti di ripristino di Apple con script che assistono nel montaggio di un volume o, in alcuni casi, nella decrittografia dello stesso. La funzionalità di ripristino FileVault è determinata dal sistema operativo installato nel Recovery HD e dalla partizione di destinazione associata.

Un volume crittografato tramite FileVault può essere ripristinato solo da una partizione Recovery HD scritta in tutte le unità disco che hanno in esecuzione Mac OS X 10.9.5 o successive. Questo requisito elimina la possibilità di eseguire un'operazione di ripristino direttamente dall'utilità Dell Recovery.

Esistono due metodi di ripristino, a seconda che la chiave di ripristino di FileVault sia una chiave di ripristino personale o istituzionale. Esiste sempre una chiave di ripristino valida. Generalmente, è consigliato utilizzare prima la chiave di ripristino personale più recente. Nel caso in cui quella chiave non funzioni, utilizzare il portachiavi di ripristino istituzionale.

- Chiave di ripristino personale - La crittografia FileVault esistente viene gestita dal server Dell. Questo è il metodo preferito.

  Se la voce più recente nel pacchetto di ripristino contiene una voce RecoveryKey, seguire i passaggi Chiave di ripristino personale. Qui di seguito un esempio di RecoveryKey:

  ```
  RecoveryKey</key><string>C73W-CX2B-ANFY-HH3K-RLRE-LVAK</string>
  ```

- Portachiavi di ripristino - Questo metodo di ripristino si basa sull'uso di una chiave di ripristino FileVault istituzionale.

  Se la voce più recente nel pacchetto di ripristino contiene una voce KeychainKey, seguire i passaggi Portachiavi di ripristino. Qui di seguito un esempio di KeychainKey:

  ```
  KeychainKey</key><data>a3ljaAABAAAAA...
  ```

Chiave di ripristino personale

Generalmente, la procedura consigliata è di ripristinare il volume di avvio prima di ripristinare i volumi non di avvio. Il ripristino del volume di avvio generalmente corregge gli errori nei volumi non di avvio.

Prerequisiti

- Un'unità avviabile esterna
- ID dispositivo/ID univoco del computer destinato al ripristino. Nella maggior parte dei casi, è possibile trovare il computer destinato al ripristino nella Remote Management Console cercando il nome utente del proprietario e visualizzando i dispositivi crittografati per tale utente. Il formato dell'ID univoco/ID dispositivo è "MacBook.Z4291LK58RH di Mario Rossi".

- Supporti di installazione Dell

Procedura

1 Aprire la Remote Management Console.

2 Nel riquadro sinistro, fare clic su **Popolamenti > Endpoint**.

3 Cercare il dispositivo da ripristinare.

4 Fare clic sul nome del dispositivo per aprire la pagina Dettagli endpoint.

5 Fare clic sulla scheda **Dettagli e azioni**.

6 In dettagli Shield, fare clic sul collegamento **chiavi di ripristino dispositivo**.

7 Per salvare il pacchetto di ripristino su un volume o computer di ripristino esterno che avrà in esecuzione l'utilità di ripristino per eseguire l'operazione di ripristino, fare clic su **Download** e quindi su **Salva**.

8 Immettere una posizione per il pacchetto di ripristino e fare clic su **Salva**.

9 Copiare il pacchetto di ripristino e il file **Protezione dati Dell- <version> .dmg** sull'unità USB di avvio.

10 Avviare il computer di destinazione da un volume di installazione del SO completo esterno creato precedentemente tenendo premuto la chiave **Opzione** mentre si riavvia il computer, quindi selezionare il volume di installazione del SO completo esterno nello Startup Manager di preavvio. Per creare un volume avviabile, fare riferimento a https://support.apple.com/en-us/HT202796.

11 Montare Dell-Data-Protection-<version>.dmg.

> **N.B.:**
> La versione della Recovery Utility deve essere la stessa o più recente rispetto a quella del software client installato nel computer destinato al ripristino.

12 Nella cartella Utilità collocata nel supporto di installazione Dell, avviare l'utilità di ripristino Dell.
Viene visualizzata la finestra di dialogo *Utilità di ripristino Dell > Seleziona volume.*

13 Selezionare il volume di FileVault.

- Per decrittografare e montare l'unità, è necessario disporre di una partizione di avvio nella versione 10.9.5 o successiva. In caso contrario, è possibile ottenere solamente la chiave di ripristino personale.
- Se si hanno volumi non di avvio crittografati, generalmente verrà ripristinata prima la partizione di avvio.

14 Fare clic su **Continua.**

Viene visualizzata la finestra di dialogo *Scegli il pacchetto di ripristino*.

15 Selezionare il pacchetto di ripristino (salvato nel passaggio 9) e fare clic su **Apri**.

Viene visualizzata la finestra di dialogo *selezionare la registrazione di ripristino*.

16 Nella colonna Data deposito, selezionare la data più recente per il tipo di chiave di ripristino personale, e fare clic su **Continua.**

> **N.B.:**
> La chiave con una data di deposito obsoleta potrebbe non essere più valida.

La finestra Risultato dell'operazione di ripristino visualizza la chiave.

- Per le unità di avvio, lo strumento di ripristino fornisce una chiave di ripristino personale che consente all'utente di avviare utilizzando il normale ripristino FileVault di Apple. È possibile avviare nella partizione di destinazione e immettere la chiave di ripristino personale per l'autenticazione di preavvio, che può variare a seconda del SO.
- Per unità non di avvio, viene visualizzata solo la chiave di ripristino personale. Per montare un volume non di avvio, immettere la chiave di ripristino nella finestra di dialogo di richiesta della password del sistema operativo. Se la finestra di dialogo è stata chiusa in precedenza, è ora possibile selezionare Sblocca tramite l'Utility Disco per montare la partizione crittografata.

17 Stampare o annotare la chiave.

18 Fare clic su **Chiudi**.

19 Avviare nel volume di avvio esterno tenendo premuto la chiave **Opzione**.

20 Se necessario, immettere la password del firmware. Selezionare il volume di avvio esterno.

21 Al termine del riavvio del sistema, fare clic su **?** nella schermata di accesso.

22 Fare clic sulla freccia che viene visualizzata.

23 Digitare la chiave di ripristino e premere **Invio**.

24 Nella finestra di dialogo, immettere una nuova password.

Portachiavi di ripristino

È necessario eseguire Dell Recovery Utility mentre è avviata in un volume di ripristino non crittografato. Non eseguire Dell Recovery Utility da un volume di avvio esterno crittografato.

Prerequisiti

- Un volume di ripristino esterno o un computer che avrà in esecuzione l'utilità di ripristino
- Un'unità USB
- Un cavo Firewire
- Supporti di installazione Dell

Procedura

1 Collegare un'unità esterna al sistema da ripristinare.

L'unità esterna deve disporre di un volume di avvio Mac OS.

2 Avviare nel volume di avvio esterno tenendo premuto la chiave **Opzione**.

3 Se necessario, immettere la password del firmware. Selezionare il volume di avvio esterno.

4 Montare il file .dmg.

5 Nella cartella Utilities, eseguire Dell Recovery Utility.

Viene visualizzata la finestra di dialogo *Utilità di ripristino Dell > Seleziona volume.*

6 Selezionare il volume di FileVault da ripristinare e fare clic su **Continua.**

Viene visualizzata la finestra di dialogo *Scegli il pacchetto di ripristino*.

7 Selezionare il pacchetto di ripristino e fare clic su **Apri**.

Se esiste più di una chiave di ripristino per il disco, viene visualizzata la schermata *Selezionare la registrazione di ripristino.*

8 Nella colonna Data di deposito, selezionare la data più recente per il tipo di portachiavi di ripristino, e fare clic su **Continua.**

> **N.B.:**
> La chiave con una data di deposito obsoleta potrebbe non essere più valida.

Viene visualizzata la finestra di dialogo *istruzioni di ripristino FileVault.*

9 Leggere le istruzioni e fare clic su **Continua**.

Viene visualizzata la finestra di dialogo *conferma l'operazione di ripristino*.

10 Evidenziare il volume di FileVault da ripristinare e fare clic su **Continua.**

Viene visualizzata la finestra di dialogo *scegliere la posizione per i file di ripristino*, che richiede di selezionarne una per archiviare i file di ripristino.

È necessario che il percorso sia quello che verrà utilizzato per il ripristino poiché gli script contengono percorsi assoluti ai file di dati. **Non** copiare questi file in Recovery HD.

Dell consiglia di salvare questi file nella radice di un'unità esterna, come un'unità USB.

> **N.B.:**
> Verificare che tutti gli utenti abbiano accesso in lettura/scrittura all'USB o ad un altro disco utilizzato per archiviare la chiave di ripristino, e che il disco disponga di spazio sufficiente. Se non si possiedono i diritti per un disco selezionato o se il disco non dispone di spazio sufficiente, viene visualizzato un errore che indica che le chiavi di ripristino non sono state archiviate.

11 Selezionare un percorso e fare clic su **Salva**.

Viene visualizzata la finestra di dialogo *Risultato dell'operazione di ripristino*, che indica che i file sono stati creati.

12 Fare clic su **Chiudi**.

13 Al termine dell'avvio del volume Recovery HD, immettere il nome e il percorso dello script.

> **N.B.:**
> Archiviare i file in un percorso vicino alla directory principale di un volume abbrevia il percorso da digitare.

La finestra Risultato dell'operazione di ripristino visualizza la chiave.

L'utilità Dell Recovery invia i file al percorso selezionato, quindi mostra i comandi esatti che sarà necessario eseguire dal volume Recovery HD per montare o decrittografare il volume di FileVault.

14 Una volta che tali file sono stati generati, copiare le stringhe di comando mostrate nella finestra di dialogo Risultato dell'operazione di ripristino.

15 Riavviare dal Recovery HD in uno dei seguenti modi:

- Tenere premute contemporaneamente le chiavi **comando** e **R** (Comando-R) prima della suoneria di accensione/autotest e durante l'avvio del computer.

  Oppure
- Premere la chiave **Opzione** e utilizzare la selezione di avvio per selezionare il Recovery HD.

  Viene visualizzata la finestra di dialogo *Utilità per Mac OS X*.

16 Dal menu Strumenti, selezionare **Utilità > Terminale**.

17 Per montare il volume in modo da poter copiare i file dal terminale o un'immagine del disco dall'utilità del disco: nel terminale, digitare il percorso completo e il nome dello script **fv2mount.sh**, ad esempio:

/Volumes/recoveryFOB/fv2mount.sh

18 Riavviare il sistema.

Supporto rimovibile

Formati supportati

I supporti formattati con FAT32, exFAT o HFS Plus (Mac OS Esteso) con gli schemi di partizione Master Boot Record (MBR) o Tabella di partizione GUID (GPT), sono supportati. È necessario abilitare HFS Plus.

> **N.B.: Mac attualmente non supporta la masterizzazione di CD/DVD per EMS. Tuttavia, l'accesso alle unità CD/DVD non è bloccato, anche se il criterio "Blocca accesso di EMS a supporti non protetti" è selezionato.**

Abilita HFS Plus

Per abilitare HFS Plus, aggiungere quanto segue .plist.

<key>EMSHFSPlusOptIn</key>

<true/>

N.B.: Dell consiglia di testare questa configurazione prima di introdurla nell'ambiente di produzione.

HFS Plus non supporta:

- Versioni - I dati esistenti delle versioni vengono rimossi dal disco.
- Collegamenti reali - Durante la ricerca di crittografia dei supporti rimovibili, il file non viene crittografato. Una finestra di dialogo consiglia di espellere il supporto.
- Supporti contenenti i backup di Time Machine:
  - I supporti identificati dai computer come una destinazione di backup Time Machine vengono automaticamente inseriti nell'elenco degli elementi consentiti, per permettere ai backup di continuare.
  - Tutti gli altri supporti rimovibili con i backup di Time Machine sono basati su criteri che disciplinano i supporti non sottoposti a provisioning e quelli non protetti. Consultare *Accesso EMS ai supporti non schermati* e *Blocca accesso EMS ai supporti non schermati*.

    N.B.: Per una nuova unità che non dispone ancora dei backup, l'utente deve copiare la propria regola dell'elenco elementi consentiti e inviare la regola per specificare l'unità di Time Machine da ammettere nell'elenco dei dispositivi consentiti. Consultare Copiare la regola dell'elenco elementi consentiti.

EMS e aggiornamenti criteri

Nel sistema in cui il supporto è stato sottoposto a provisioning (o ripristinato), i criteri vengono aggiornati nel supporto al momento del montaggio.

Eccezioni alla crittografia

Nei supporti esterni, gli attributi estesi non vengono crittografati.

Errori nella scheda Supporto rimovibile

- In un computer non protetto, non sostituire un file crittografato con una versione decrittografata del file. In seguito, questo potrebbe impedire la decrittografia. Potrebbe anche essere visualizzato come errore nella scheda Supporto rimovibile.
- Se un indicatore di fine file viene invalidato, per esempio se un file viene sovrascritto con un nuovo contenuto al di fuori del controllo EMS, e successivamente si esegue un montaggio in EMS, nella scheda Supporto rimovibile viene visualizzato un errore di fine file.
- Quando i file vengono convertiti, il supporto deve disporre di una quantità di spazio libero superiore alle dimensioni del file più grande da convertire. Se viene visualizzato un triangolo di avviso giallo nell'area di stato di Supporto rimovibile, fare clic su di esso. Se un messaggio indica *spazio libero insufficiente*, effettuare le operazioni seguenti:

  a Annotare la quantità di spazio che deve essere liberata nel dispositivo. Il rapporto mostra un elenco di file e la dimensione.

  b Svuotare il cestino. Man mano che si libera spazio, EMS crittografa automaticamente ulteriori file.

  c Se vengono eliminati file e cartelle, assicurarsi di svuotare di nuovo il cestino.

Messaggi di controllo

I messaggi di controllo vengono inviati al server Dell.

Per Endpoint Security Suite Enterprise per Mac, vedere la Remote Management Console e selezionare **Popolamenti > Enterprise o endpoint**. Quindi selezionare la scheda **Eventi di minaccia avanzati**. Per maggiori informazioni, consultare *AdminHelp*.

Raccogliere i file di registro per Endpoint Security Suite Enterprise

DellLogs.zip contiene i registri per la Crittografia client e Advanced Threat Prevention.

Per informazioni su come raccogliere i registri, consultare http://www.dell.com/support/article/us/en/19/SLN303924.

Disinstallare Encryption Client per Mac

Il software client può essere disinstallato eseguendo l'applicazione **disinstallare la protezione dei dati Dell**. Per disinstallare il software client, seguire la procedura seguente.

N.B.: Prima di eseguire l'applicazione di disinstallazione, è necessario che il disco venga decrittografato completamente.

1 Se il disco è attualmente crittografato, impostare il criterio crittografia dei volumi Dell su **disattivato** per la Remote Management Console e il commit del criterio.

Viene visualizzata una finestra di dialogo per richiedere l'accesso alle Preferenze di sistema e il controllo del computer in modo che il software client possa decrittografare il disco.

a Fare clic su **Aprire le Preferenze di Sistema**.

Se la **negazione** è selezionata, non vengono eseguite la disinstallazione e la decrittografia.

b Immettere la password amministratore.

2 Al completamento della decrittografia del disco, riavviare il sistema (quando richiesto).

3 Dopo che il computer viene riavviato, avviare l'applicazione **disinstallare la protezione dati Dell** (che si trova nella cartella Utilità in Dell-Data-Protection-<version>.dmg nei supporti di installazione Dell).

Vengono visualizzati dei messaggi sullo stato della disinstallazione.

Encryption Client for Mac è disinstallato e il computer può essere utilizzato normalmente.

Attivazione come amministratore

Client Tool offre all'amministratore nuovi metodi per l'attivazione del software client in un computer Mac e per l'analisi del software client. Sono disponibili due metodi di attivazione:

- Attivazione tramite le credenziali di amministratore
- Attivazione temporanea che emula l'utente senza lasciare footprint in quel computer.

Entrambi i metodi possono essere utilizzati direttamente tramite una shell o in uno script.

N.B.: Non attivare il software client in più di cinque computer con lo stesso account di rete. Ne potrebbero conseguire gravi vulnerabilità di sicurezza e prestazioni diminuite Server.

Prerequisiti

- Encryption Client per Mac deve essere installato sul computer remoto.
- Non attivare tramite l'interfaccia utente del client prima di tentare di attivare da una postazione remota.

Attiva

Utilizzare questo comando per attivare il client come amministratore.

Esempio:

client -a *username@domain.com password admin admin*

Activate Temporarily

Utilizzare questo comando per attivare il client senza lasciare footprint nel computer.

1 Aprire una shell oppure utilizzare uno script per attivare il software client:

client - a *username@domain.com password*

2 Utilizzare Client Tool per recuperare le informazioni sul software client, i suoi criteri, lo stato del disco, l'account utente e altro. Per maggiori informazioni su Client Tool, consultare Strumento client.

> **N.B.: Dopo l'attivazione, le informazioni sul software client, inclusi criteri, stato del disco e informazioni sull'utente, sono disponibili anche in Preferenze di sistema nelle preferenze di Dell Data Protection.**

Riferimento del client di crittografia

Informazioni sulla protezione della password del firmware opzionale

> **N.B.: Computer Mac più recenti non supportano la protezione con password del firmware. La protezione con password del firmware è supportata nei modelli seguenti:**
>
> - iMac10.*
> - iMac11.*
> - Macmini4.*
> - MacBook7.*
> - MacBookAir2.*
> - MacBookPro7.*
> - MacPro5.*
> - XServe3.*
>
> Ad esempio, iMac10.1, iMac R11.1 e iMac11.2 supportano la protezione della password del firmware opzionale (come indicato dal *), a differenza di iMac12.1 o versioni successive.

> **N.B.: Quando l'opzione della chiave FirmwarePasswordMode è impostata su opzionale, si disabilita solo l'applicazione client della protezione della password del firmware. Non rimuovere un'eventuale protezione della password del firmware esistente. È possibile rimuovere eventuali protezioni con password del firmware esistenti utilizzando l'Utility Password Firmware di Mac OS X.**

Se si intende utilizzare il Boot Camp (consultare in che modo è possibile attivare Mac OS X Boot Camp per le istruzioni) su computer Mac crittografati, è **necessario** configurare il client per **non** utilizzare la protezione della password del firmware.

I computer Mac utilizzano la protezione con password del firmware per potenziare la protezione di accesso del computer. Nei computer Mac, per impostazione predefinita, la protezione è DISATTIVATA. Durante l'installazione del client, se si tratta di una nuova installazione o di un aggiornamento da una versione client precedente, si avrà la possibilità di modificare il file esistente .com dell.ddp.plist per consentire che la chiave *FirmwarePasswordMode* venga impostata su *Obbligatorio o opzionale*. L'opzione *Obbligatorio* è l'impostazione predefinita che applica la protezione della password del firmware, mentre l'impostazione *opzionale* provoca l'inapplicabilità della password del firmware. In seguito all'installazione o all'aggiornamento, il client valuta il file modificato com.dell.ddp.plist durante il riavvio.

N.B.: Per impedire agli utenti di modificare il livello di sicurezza del computer, il client non accetta modifiche alla chiave FirmwarePasswordMode dopo l'installazione del software client.

È possibile modificare il valore di tale chiave dopo l'installazione o l'aggiornamento avviando un processo di decrittografia del disco, e quindi riabilitando la crittografia.

Se si desidera che la protezione della password del firmware per Mac OS X venga **richiesta**, seguire le procedure normale di installazione/aggiornamento client indicate in Installare/aggiornare Encryption Client per Mac.

Utilizzare il Boot Camp

Supporto Mac OS X Boot Camp

N.B.: Quando si utilizza Boot Camp, il sistema operativo Windows non può essere crittografato.

Boot Camp è un'utilità inclusa in Mac OS X che assiste l'utente nell'installazione di Windows nei computer Mac con configurazione ad avvio doppio. Boot Camp supportato dai seguenti sistemi operativi Windows:

- Windows 7 e 7 Home Premium, Professional e Ultimate (a 64 bit)
- Windows 8 e 8 Pro (a 64 bit)
- Windows 8.1 e 8.1 Pro (a 64 bit)

N.B.: Windows 7 è Boot Camp 4 o 5.1. Windows 8 e versioni successive sono solo Boot Camp 5.1.

Per utilizzare Endpoint Security Suite Enterprise per Windows in Boot Camp in un computer con Endpoint Security Suite Enterprise per Mac, il volume del sistema deve essere crittografato mediante Encryption Client per Mac con Dell Client Encryption o FileVault2. È necessario configurare il client di installazione **senza** utilizzare la protezione della password del firmware. Consultare Installazione/aggiornamento dalla riga di comando per le istruzioni.

N.B.:

Se la partizione di Windows è destinata all'EMS, assicurarsi di includerla nell'elenco delle partizioni consentite altrimenti verrà crittografata. Consultare Copiare la regola dell'elenco elementi consentiti.

N.B.:

È necessario assicurarsi che Windows sia installato prima di distribuire i criteri del client che abilitano la crittografia. Dopo che il client avvia il processo di crittografia, disabilita le operazioni di partizione del disco richieste da Boot Camp.

Ripristino di Endpoint Security Suite Enterprise per il Boot Camp di Windows

Per ripristinare Endpoint Security Suite Enterprise per Windows in esecuzione in un volume di Boot Camp, è inoltre necessario creare un volume di Boot Camp in un'unità esterna.

Prerequisiti

- Un'unità avviabile esterna
- ID dispositivo/ID univoco del computer destinato al ripristino. Nella maggior parte dei casi, è possibile trovare il computer destinato al ripristino nella Remote Management Console cercando il nome utente del proprietario e visualizzando i dispositivi crittografati per tale utente. Il formato dell'ID univoco/ID dispositivo è "MacBook.Z4291LK58RH di Mario Rossi".

Procedura

1 Su un'unità esterna, creare un volume di Boot Camp.

La procedura è simile a quella usata dall'utente per creare un volume di Boot Camp nel proprio sistema locale. Consultare http://www.apple.com/support/bootcamp/.

2 Dalla Remote Management Console, è possibile copiare il pacchetto di ripristino su uno di questi:

- Unità USB avviabile

  Oppure

- Partizione FAT nel volume di Boot Camp esterno

3 Arrestare il computer con il volume di Boot Camp da ripristinare.

4 Connettere l'unità esterna al computer.

Tale unità contiene il volume di Boot Camp creato nel passaggio 1.

5 Per l'avvio del computer dall'unità esterna Boot Camp, premere la chiave Opzione mentre si accende il computer.

6 Selezionare il volume di Boot Camp (Windows) che si trova nell'unità esterna.

7 Nell'unità USB o nella partizione FAT, fare clic con il pulsante destro del mouse sul pacchetto di ripristino (dal passaggio 2) e selezionare **Esegui come amministratore**.

8 Fare clic su **Sì.**

9 Nella finestra di dialogo di Dell Data Protection Encryption, selezionare un'opzione:

- *Il sistema non viene avviato....* - Se l'utente non riesce ad avviare il sistema, selezionare la prima opzione

  Oppure

- *Il sistema non consente di accedere ai dati crittografati....* - Se l'utente non riesce ad accedere ad alcuni file crittografati quando effettua l'accesso al sistema, selezionare la seconda opzione.

10 Fare clic su **Avanti.**

Viene visualizzata la schermata Informazioni di backup e ripristino.

11 Fare clic su **Avanti.**

12 Selezionare il volume di Boot Camp da ripristinare.

N.B.: Non si tratta del volume esterno di Boot Camp.

13 Fare clic su **Avanti.**

14 Immettere la password associata al file.

15 Fare clic su **Avanti.**

16 Fare clic su **Ripristina.**

17 Fare clic su **Fine**.

18 Quando richiesto di riavviare, fare clic su **Sì**.

19 Il sistema si riavvia e l'utente è in grado di effettuare l'accesso a Windows.

Come recuperare una password del firmware

Anche se il computer client è configurato per l'applicazione della password del firmware, questa potrebbe non essere necessaria per il ripristino. Se il computer da ripristinare è avviabile, impostare la destinazione di avvio nel riquadro delle preferenze di sistema Disco di avvio.

Nel caso in cui la password del firmware sia necessaria per portare a termine il ripristino (se il computer non è avviabile ed è applicata la protezione con password del firmware), seguire la procedura seguente.

Per recuperare una password del firmware, è prima necessario recuperare il pacchetto di ripristino contenente le chiavi di crittografia del disco.

1 Eseguire l'accesso alla Remote Management Console come amministratore Dell.

2 Nel riquadro sinistro, fare clic su **Popolamenti > Endpoint**

3 Cercare il dispositivo da ripristinare.

4 Fare clic sul nome del dispositivo per aprire la pagina Dettagli endpoint.

5 Fare clic sulla scheda **Dettagli e azioni**.

6 In dettagli Shield, fare clic sul collegamento *chiavi di ripristino dispositivo*.

7 Per salvare il pacchetto di ripristino su un volume o computer di ripristino esterno che avrà in esecuzione l'utilità di ripristino per eseguire l'operazione di ripristino, fare clic su **Download** e quindi su **Salva**.

8 Aprire il pacchetto di ripristino per recuperare la password del firmware del computer destinato al ripristino. La password del firmware si trova all'interno dei tag delle stringhe dopo la chiave **FirmwarePassword**.

Per esempio:

<key>FirmwarePassword</key>

<string>Bo$vun8WDn</string>

Strumento client

Client Tool è un comando shell in esecuzione in un endpoint Mac. Viene utilizzato per attivare il client da una postazione remota o per eseguire uno script tramite un'utilità di gestione remota. Come amministratore, l'utente può attivare un client ed eseguire le operazioni seguenti:

- Attivare come amministratore
- Activate temporarily
- Recuperare le informazioni dal client Mac

Per utilizzare Client Tool manualmente, aprire una sessione ssh e immettere il comando desiderato nella riga di comando.

Esempio:

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

Immettere il **client** da solo per visualizzare l'utilizzo delle istruzioni.

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/client

Tabella 1. Comandi di Client Tool

Comando	Scopo	Sintassi	Risultati
Attiva	Attiva un client Mac con il server Dell ma senza passare tramite l'interfaccia utente. Per l'attivazione devono essere immessi un nome utente e una password di dominio validi. Con lo strumento client è possibile attivare un utente locale diverso da quello che ha eseguito l'accesso e associare le credenziali	-a AccountDominio PasswordDominio -a AccountLocale* AccountDominio PasswordDominio **domainAccount** è l'account utilizzato per l'attivazione tramite lo strumento client. **Localaccount** è opzionale ed è l'utente corrente se nessuno è stato specificato. Il comando di attivazione ha questo formato: client -a <utente da attivare*> <utente dominio> <password dominio>	0 = Azione riuscita 2 = Attivazione non riuscita e motivo dell'errore 6 = Utente non trovato

Comando	Scopo	Sintassi	Risultati
	di dominio a quell'utente.	Se si utilizza il criterio *Elenco utenti senza autenticazione* per creare classi di utenti che non vengono attivati sul server Dell, se si desidera, è possibile utilizzare lo strumento client per specificare un account locale diverso rispetto a quello connesso. Consultare la sezione Elenco utenti senza autenticazione al punto 3.	
Activate temporarily	Attivare un client Mac senza lasciare un footprint.	-at AccountDominio PasswordDominio -at AccountLocale* AccountDominio PasswordDominio	
Disk	Richiedere lo stato del disco	-d	Viene visualizzato lo stato del disco, inclusi l'ID, lo stato di crittografia e i criteri del disco Se vengono restituite parentesi graffe vuote significa che nessun disco è crittografato.
FileVault Change Recovery	Ripetere in sequenza le chiavi di ripristino per i volumi di FileVault	-fc IdDispositivo PassphraseRipristino -fc IdDispositivo ChiaveRipristinoPersonale -fc IdDispositivo PercorsoKeychain PasswordKeychain -fc IdDispositivo FileRipristino **N.B.: IdDispositivo deve essere un UUID del volume logico o trasformato esattamente in un UUID del volume logico. Spesso, un punto di montaggio o devnode funziona.**	0 = Azione riuscita 7= UUID del volume logico non trovato 10 = Errore credenziali 11 = Deposito non riuscito
Criterio	Richiedere i criteri del client Mac	-p	Vengono visualizzati i criteri
Server	Eseguire il polling del server Dell per i criteri aggiornati da parte del client Mac **N.B.: Possono essere necessari diversi minuti per eseguire il polling.**	-s	0 = Azione riuscita Qualsiasi altro valore indica che il server Dell o il software client Mac era impegnato o non rispondeva.
Test	Testare lo stato di attivazione del client Mac	-t AccountLocale*	0 (AccountDominio) = Azione riuscita 1 = Non attivato 6 = Utente non trovato
Utente	Richiedere informazioni sull'utente	-u AccountLocale*	Vengono visualizzate le informazioni sull'account utente:

Comando	Scopo	Sintassi	Risultati
			0 (informazioni account) = Azione riuscita 6 = Utente non trovato
Versione	Richiedere la versione del client Mac	-v	Viene visualizzata la versione del client Mac: Esempio: 8.x.x.xxxx

* L'account che esegue lo strumento client viene utilizzato per l'account locale a meno che un altro non venga specificato.

L'opzione Plist

L'opzione -plist stampa i risultati del comando con cui è combinata. Segue il comando e deve apparire prima dei suoi argomenti affinché i risultati vengano stampati come plist.

Esempi

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -p -plist**

Per recuperare i criteri dal client e stamparli.

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at -plist** *localAccount domainAccount domainPassword*

Per attivare temporaneamente il client e stampare il risultato.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -s ; echo$?**

Eseguire il polling del server Dell per i criteri aggiornati per conto del client e visualizzarli sullo schermo.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -d -plist**

Per recuperare lo stato del disco del client e stamparlo.

Codici restituiti globali

Nessun errore 0

Errore parametro 4

Comando non riconosciuto 5

Timeout del socket 8

Errore interno 9

Attività per Advanced Threat Prevention

Installazione Advanced Threat Prevention per Mac

Questa sezione guida l'utente nell'installazione Advanced Threat Prevention.

Vi sono due metodi per eseguire l'installazione di Advanced Threat Prevention.

- Installazione interattiva - Questo metodo è il più semplice da installare. Tuttavia, questo metodo non consente alcuna personalizzazione.
- Installazione dalla riga di comando - Si tratta di un metodo di installazione/aggiornamento avanzato che dovrebbe essere utilizzato solo dagli amministratori esperti con la sintassi dalla riga di comando.

Prerequisiti

Dell invita a seguire le procedure consigliate durante la distribuzione del software client. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e distribuzioni scaglionate agli utenti.

Prima di iniziare questo processo, accertarsi che siano soddisfatti i seguenti prerequisiti:

- Assicurarsi che il server Dell e i suoi componenti siano già installati.

  Se non è ancora stato installato il server Dell, seguire le istruzioni nella guida appropriata di seguito.

  Guida alla migrazione e all'installazione di Enterprise Server

  Guida introduttiva e all'installazione di Enterprise Server - Virtual Edition
- Assicurarsi di disporre del nome e della porta host del Server. Saranno entrambi necessari per l'installazione del software client.
- Verificare che il computer di destinazione abbia connettività di rete al Server Dell.
- Se un certificato del server del client è mancante o presenta una firma automatica, è necessario disattivare l'abilitazione del certificato SSL sul lato client.

Installazione interattiva per Advanced Threat Prevention

Questa sezione guida l'utente nel processo di installazione Advanced Threat Prevention per Mac.

L'installazione interattiva è il metodo più semplice per installare o aggiornare il pacchetto software client. Tuttavia, questo metodo non consente alcuna personalizzazione.

Per installare il software client, seguire la procedura seguente. Per eseguire la procedura, è necessario disporre di un account amministratore.

N.B.: Prima di iniziare, salvare il lavoro dell'utente e chiudere le altre applicazioni.

1 Dal supporto di installazione Dell, montare il file **Endpoint-Security-Suite-Enterprise-<version>.dmg**.
Endpoint Security Suite Enterprise per il pacchetto Mac si apre.

2 Fare doppio clic sul programma di installazione del pacchetto **Endpoint Security Suite Enterprise**. Viene visualizzato il seguente messaggio:

Il pacchetto eseguirà un programma per determinare se il software può essere installato.

3 Fare clic su **Continua.**

4 Leggere il testo iniziale e fare clic su **Continua**.

5 Per verificare il contratto di licenza, fare clic su **Continua**, quindi su **Accetto** per accettare i termini del contratto di licenza.

6 Nel campo **Host server**, immettere il nome host completo di Dell Server che gestirà l'utente di destinazione, ad esempio server.organizzazione.com.

7 Nel campo **Porta server**, immettere **8888** e fare clic su **Continua**.

Una volta stabilita la connessione, l'indicatore della connettività cambia da rosso a verde.

N.B.: La porta di servizio del Core Server configurabile. Il numero di porta predefinito è 8888.

8 Nella schermata di installazione, fare clic su **Installa**.

9 Quando richiesto, immettere le credenziali dell'account amministratore (richieste dall'applicazione del programma di installazione di Mac OS X), quindi fare clic su **OK**.

10 Al completamento dell'installazione, fare clic su **Chiudi**.

Client di Advanced Threat Prevention per Mac installato.

11 Consultare Verificare l'installazione di Advanced Threat Prevention.

Se l'installazione non riesce, verificare di avere un certificato valido sul server Dell. Consultare Disattivare il certificato di attendibilità SSL per Advanced Threat Prevention.

Disinstallazione interattiva del client di Advanced Threat Prevention

Il software client può essere disinstallato eseguendo l'applicazione **disinstallare Endpoint Security Suite Enterprise.** Per disinstallare il software client, seguire la procedura seguente.

1 Montare il file Endpoint-Security-Suite-Enterprise-<versione>.dmg.

2 Nella cartella Utility, avviare l'applicazione **disinstallazione Endpoint Security Suite Enterprise**.

3 Fare clic su **Uninstall** (Disinstalla).

4 Quando richiesto, immettere le credenziali dell'account amministratore (richieste dall'applicazione del programma di installazione di Mac OS X), quindi fare clic su **OK**.

Vengono visualizzati dei messaggi sullo stato della disinstallazione.

5 Sul messaggio di conferma, fare clic su **OK**.

Advanced Threat Prevention per Mac è disinstallata, e il computer può essere utilizzato normalmente.

Installazione per Advanced Threat Prevention dalla riga di comando

Per installare il client di Advanced Threat Prevention utilizzando la riga di comando, seguire la procedura seguente.

1 Dal supporto di installazione Dell, montare il file Endpoint-Security-Suite-Enterprise-<version>.dmg. Endpoint Security Suite Enterprise per il pacchetto Mac si apre.

2 Dalla cartella Utility, copiare la **com.dell.esse denominato release.plist** file per l'unità locale.

3 Aprire il file .plist.

4 Modificare i valori variabile con il nome host completo del server Dell che gestisce l'utente di destinazione, come ad esempio server.organizzazione.com, e il numero di porta **8888**:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
```

```
<dict>
  <key>ServerHost</key>
  <string>deviceserver.company.com</string>
  <key>ServerPort</key>
  <array>
</dict>
</plist>
```

N.B.: La porta di servizio del Core Server configurabile. Il numero di porta predefinito è 8888.

5 Salvare e chiudere i file.

6 Per ogni computer di destinazione, copiare il pacchetto di installazione **Endpoint Security Suite Enterprise per Mac** in una cartella temporanea e il file modificato **com.dell.esse.plist** in **/Libreria/Preferenze.**

7 Se richiesto, immettere le proprie credenziali.

8 Avviare una finestra terminale.

9 Eseguire un'installazione del pacchetto dalla riga di comando utilizzando il comando del **programma di installazione**:

```
sudo installer -pkg /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Endpoint\ Security\ Suite\ Enterprise.pkg -target /
```

N.B.: Il percorso -pkg è il percorso per il programma di installazione .pkg trovato nel file .dmg.

10 Premere **Invio**.

11 Consultare Verificare l'installazione di Advanced Threat Prevention di ESSE.

Disinstallazione dalla riga di comando Advanced Threat Prevention per Mac

Per disinstallare il client di Advanced Threat Prevention utilizzando la riga di comando, seguire la procedura seguente.

1 Avviare una finestra terminale.

2 Eseguire la disinstallazione del pacchetto dalla riga di comando utilizzando il comando del programma di **disinstallazione**:

```
sudo /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/Uninstall\ Endpoint\ Security\ Suite\ Enterprise.app/Contents/MacOS/Uninstall\ Endpoint\ Security\ Suite\ Enterprise --noui
```

N.B.: Verificare che lo switch --noui è incluso al termine del comando.

3 Premere **Invio**.

Advanced Threat Prevention per Mac è disinstallata, e il computer può essere utilizzato normalmente.

Risoluzione dei problemi Advanced Threat Prevention per Mac

Disattivare il certificato di attendibilità SSL per Advanced Threat Prevention

Se un certificato del server del client è mancante o presenta una firma automatica, è necessario disattivare l'abilitazione del certificato SSL sul lato client.

1 Sul client, avviare una finestra terminale.

2 Inserire il percorso per DellCSFConfig.app:

```
cd /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/DellCSFConfig.app/Contents/MacOS/
```

3 Eseguire DellCSFConfig.app:

```
sudo ./DellCSFConfig
```

Di seguito vengono visualizzate le impostazioni predefinite:

```
Current Settings:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False
```

4 Tipo **- aiutare** ad elencare le opzioni disponibili.

5 Per disabilitare l'attendibilità del certificato SSL, cambiare `DisableSSLCertTrust` a **Vero**.

Aggiungere l'inventario XML e le modifiche ai criteri per la cartella Accessi

Per aggiungere i file inventory.xml o policies.xml alla cartella Accessi:

1 Eseguire DellCSFConfig.app come descritto di seguito.

2 Modifica DumpXmlInventory su **Vero**.

3 Modifica FirmwarePassword su **Vero**.

I file dei criteri sono messi da parte solo se si è verificata una modifica dei criteri.

4 Per visualizzare i file di accesso inventory.xml e policies.xml, andare a **/Libreria/applicazione\/Supporto Dell/Dell\ Dati\ Protezione/**.

Verificare l'installazione di Advanced Threat Prevention

Facoltativamente, verificare l'installazione.

1 Confermare che l'icona Advanced Threat Prevention di Dell abbia un badge  nella barra dei comandi.

2 Se viene visualizzato un punto esclamativo sull'icona, fare clic con il pulsante destro del mouse, quindi selezionare **Mostra dettagli**. Può indicare che non si è registrati.

Verificare gli aggiornamenti - Verificare gli aggiornamenti del motore di ricerca per Advanced Threat Prevention, non degli aggiornamenti dei criteri del Server di Dell.

Informazioni su - La fase di implementazione prevede i seguenti passaggi:

- Versione
- Criterio - [online] indica un criterio basato su server e [offline] indica un criterio basato su offline o airgap
- N. seriale - Utilizzarlo quando si contatta il supporto tecnico. Il presente è l'identificatore univoco dell'installazione.

3 Nelle applicazioni viene creata la cartella Advanced Threat Prevention di Dell.

Raccogliere i file di registro per Endpoint Security Suite Enterprise

DellLogs.zip contiene i registri per la Crittografia client e Advanced Threat Prevention.

Per informazioni su come raccogliere i registri, consultare http://www.dell.com/support/article/us/en/19/SLN303924.

Visualizzare i dettagli su Advanced Threat Prevention

Dopo l'installazione del client Advanced Threat Prevention in un computer endpoint, viene riconosciuto dal server Dell come agente.

Fare clic con il pulsante destro del mouse sull'icona Advanced Threat Prevention  nella barra dei comandi, quindi selezionare **Mostra dettagli**. La schermata dei dettagli di Advanced Threat Prevention presenta le seguenti schede.

Scheda Minacce

La scheda Minacce visualizza tutte le minacce individuate nel dispositivo e l'azione intrapresa. Le minacce sono una categoria di eventi appena rilevati come file o programmi potenzialmente pericolosi e necessitano di misure correttive.

La colonna Categoria può includere le seguenti informazioni.

- **Non sicuro** - Un file sospetto di essere un probabile malware
- Anormale - Un file sospetto che può essere un malware
- **Spostato in quarantena** - Un file spostato dalla sua posizione originale, memorizzato nella cartella Quarantena e la cui esecuzione viene impedita sul dispositivo.
- **Ignorato** - un file la cui esecuzione è consentita sul dispositivo.
- **Cancellato** - un file cancellato all'interno dell'organizzazione. I file cancellati includono quelli ignorati che vengono aggiunti all'Elenco file sicuri ed eliminati dalla cartella Quarantena nel dato dispositivo.

Per ulteriori informazioni sulle classificazioni delle minacce di Advanced Threat Prevention consultare *AdminHelp*, disponibile nella Remote Management Console di Dell.

Scheda exploit

La scheda exploit elenca gli exploit considerati minacce.

I criteri del Server Dell determinano l'azione eseguita quando viene rilevato un exploit:

- **Ignora** - Non viene posta in essere alcuna azione rispetto alle violazioni della memoria identificate.
- **Avviso** - La violazione della memoria viene registrata e segnalata al server Dell.
- **Blocca** - Se un'applicazione tenta di chiamare un processo di violazione della memoria, la chiamata al processo viene bloccata. L'applicazione che ha compiuto la chiamata può continuare a essere eseguita.
- **Termina** - Se un'applicazione tenta di chiamare un processo di violazione della memoria, la chiamata al processo viene bloccata. L'applicazione che ha effettuato la chiamata è terminata.

Vengono rilevati i seguenti tipi di exploit:

- Manipolazione dello stack
- Protezione dello stack
- Ricerca memoria scanner
- Payload dannoso

Per ulteriori informazioni sui criteri di exploit consultare *AdminHelp*, disponibile nella Remote Management Console di Dell.

Scheda Eventi

N.B.: Un evento non è necessariamente una minaccia. Un evento viene generato quando un file o programma riconosciuto viene messo in quarantena, nell'elenco di file sicuri o ignorato.

La scheda degli eventi visualizza tutti gli eventi di minaccia che si verificano sul dispositivo e li visualizza per tipo di evento, assegnato da Advanced Threat Prevention. I dati vengono rimossi quando viene riavviato il sistema.

Gli esempi dei tipi di eventi includono:

Minaccia trovata

Minaccia rimossa

Minaccia in quarantena

Minaccia ignorata

Minaccia modificata

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

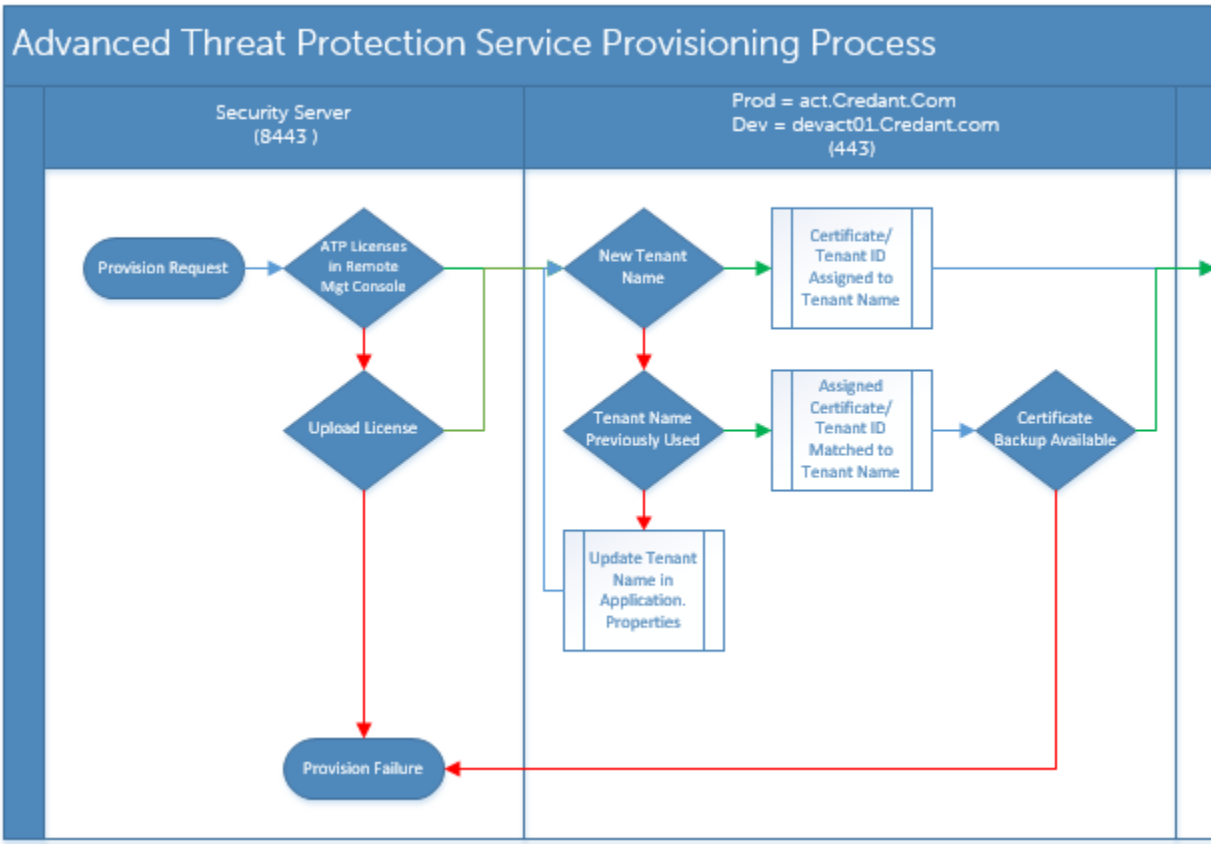
Per interrompere la ricezione degli aggiornamenti automatici dell'agente:

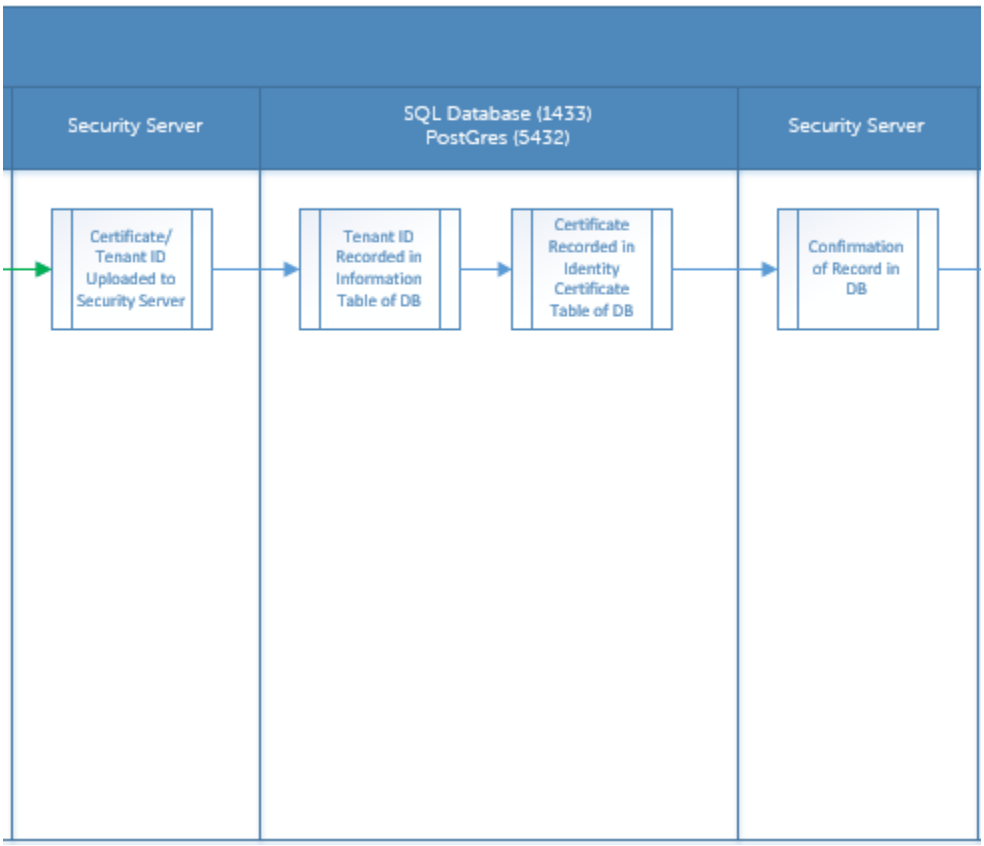
1. Nel riquadro sinistro della Remote Management Console, fare clic su **Gestione** > **Gestione dei servizi**.
2. Nella scheda **Minacce avanzate**, sotto Aggiornamento automatico agente, fare clic sul pulsante **Disattivato** e quindi sul pulsante **Salva preferenze**.

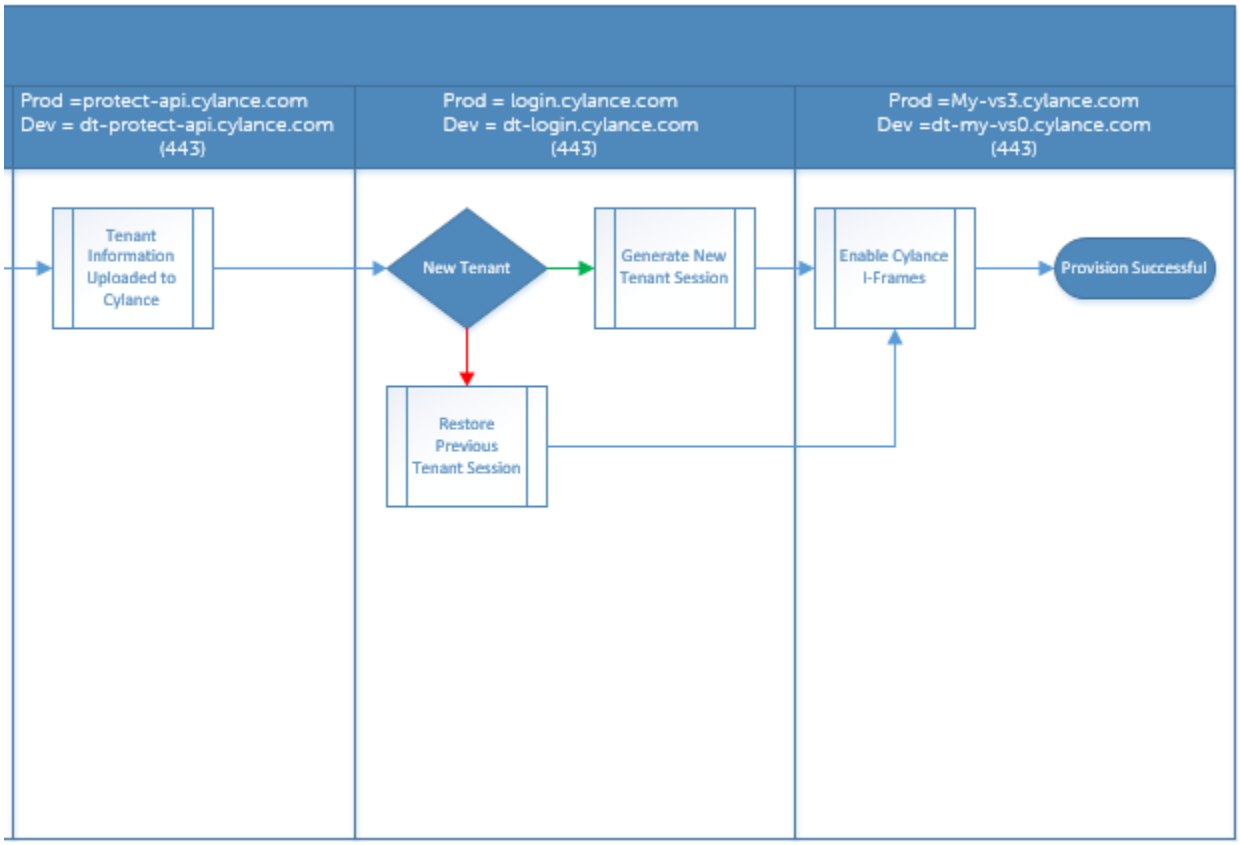
Risoluzione dei problemi del client di Advanced Threat Prevention

Provisioning di Advanced Threat Prevention e comunicazione agente

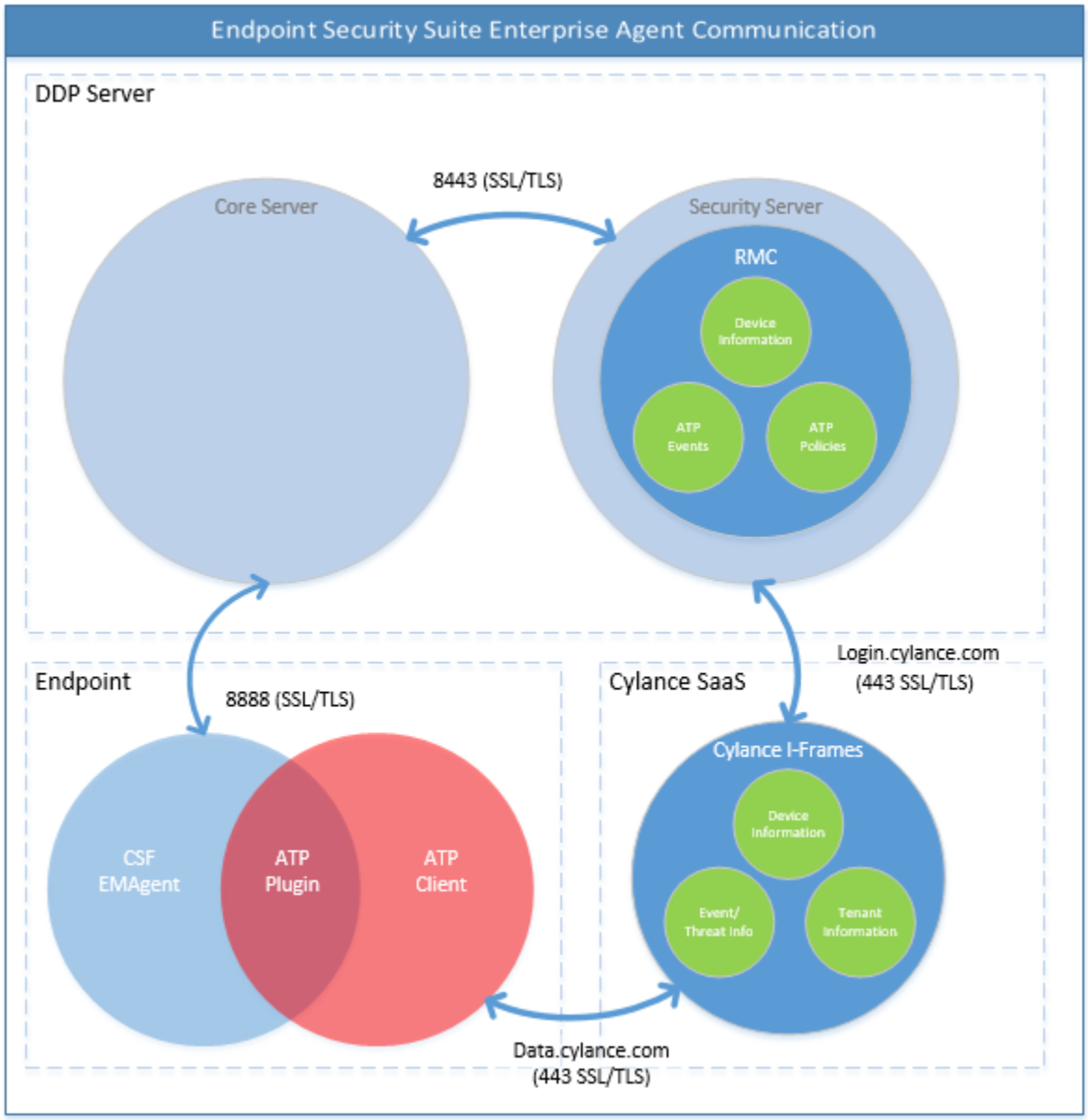
I diagrammi seguenti illustrano il processo di provisioning del servizio di Advanced Threat Prevention.


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


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



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


Endpoint Security Suite Enterprise Agent Communication
DDP Server
8443 (SSL/TLS)
Core Server
Security Server
RMC
Device Information
ATP Events
ATP Policies
Endpoint
8888 (SSL/TLS)
Cylance SaaS
Login.cylance.com
(443 SSL/TLS)
CSF EMAgent
ATP Plugin
ATP Client
Cylance I-Frames
Device Information
Event/ Threat Info
Tenant Information
Data.cylance.com
(443 SSL/TLS)

5

Glossario

Security Server - Utilizzato per le attivazioni della crittografia client.

Policy Proxy - Utilizzata per distribuire i criteri a Endpoint Security Suite Enterprise per il software client di Mac.

Remote Management Console - La console di amministrazione per l'intera distribuzione enterprise.

Shield - Occasionalmente, è possibile vedere questo termine nella documentazione e nell'interfaccia utente del client. "Shield" è un termine usato per rappresentare il software client.