Dell Data Protection | Endpoint Security Suite Enterprise for Mac

Administrator Guide v1.1

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Administrator Guide

2017 - 05

Rev. A02

Contents

1

Einleitung

Im Administratorhandbuch zu Endpoint Security Suite Enterprise for Mac sind die Informationen enthalten, die zum Bereitstellen und Installieren der Client-Software benötigt werden.

Themen:

Übersicht

Die Endpoint Security Suite Enterprise for Mac bietet fortschrittlichen Schutz vor Bedrohungen auf der Betriebssystem- und der Speicherebene sowie Verschlüsselung. Alles wird dabei zentral über den Dell Data Protection Server verwaltet. Durch die zentralisierte Verwaltung, konsolidierte Berichterstattung zur Richtlinientreue und Bedrohungsmeldungen in der Konsole können Unternehmen problemlos die Richtlinientreue all ihrer Endpunkte durchsetzen und beweisen. Sicherheits-Expertise ist durch Funktionen wie vordefinierten Richtlinien und Berichtsvorlagen integriert, damit Unternehmen Kosten und Komplexität ihrer IT reduzieren können.

- Endpoint Security Suite Enterprise for Mac ist eine Software Suite für Client-Verschlüsselung von Daten und erweiterten Schutz vor Bedrohungen.
- Richtlinien-Proxy – wird zum Verteilen von Richtlinien verwendet
- Sicherheitsserver – wird für Aktivierungen der Client-Verschlüsselungssoftware verwendet
- Enterprise Server oder Dell Enterprise Server – VE – bietet eine zentrale Verwaltung der Sicherheitsrichtlinien, Integration in die vorhandenen Enterprise-Verzeichnisse und das Erstellen von Berichten. Zum Zwecke dieses Dokuments werden beide Server als „Dell Server“ bezeichnet, sofern keine konkrete Version angegeben ist (wenn z. B. bei Verwendung des Dell Enterprise Server – VE ein anderes Verfahren notwendig ist).

  Diese nahtlos ineinandergreifenden Dell Komponenten sorgen für eine sichere mobile Umgebung, ohne die Benutzerfreundlichkeit zu beeinträchtigen.

Endpoint Security Suite Enterprise for Mac verfügt über zwei .dmg-Dateien, eine für Encryption Client und eine für Advanced Threat Prevention. Sie können beide oder nur eine davon installieren.

Dell Encryption Client und FileVault-Verschlüsselung

Die Option zum Verwalten der FileVault-Verschlüsselung ist zusammen mit dem Dell Encryption Client in der Endpoint Security Suite Enterprise for Mac enthalten. Die Wahl der jeweiligen Option ist von den Verschlüsselungsanforderungen des Unternehmens abhängig. Weitere Informationen über Verschlüsselungsrichtlinien finden Sie unter Mac-Verschlüsselung > Dell Volume-Verschlüsselung.

Kontaktieren des Dell ProSupports

Telefonischen Support rund um die Uhr für Ihr Dell Data Protection-Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Data Protection-Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport – Internationale Telefonnummern.

2

Anforderungen

In diesem Kapitel werden die Hardware- und Softwareanforderungen für den Client erläutert. Stellen Sie sicher, dass die Implementierungsumgebung die Anforderungen erfüllt, bevor Sie mit der Implementierung fortfahren.

Themen:

Encryption Client

Encryption-Client-Hardware

Die Mindestanforderungen für die Hardware müssen den Mindestspezifikationen des Betriebssystems entsprechen.

ANMERKUNG: Der Systemdatenträger muss mit dem Partitionsschema GUID Partition Table (GPT) partitioniert sein und über das Format Mac OS X Extended (Journaled) verfügen.

Hardware

- 30 MB freier Speicherplatz
- Netzwerkschnittstellenkarte 10/100/1000 oder 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

- Bevor Sie den Advanced Threat Prevention Client installieren, sollten Sie Drittanwendungen für Viren-, Malware- und Spyware-Schutz deinstallieren, um potenzielle Installationsfehler zu vermeiden.

Advanced Threat Prevention Hardware

Die Mindestanforderungen für die Hardware müssen den Mindestspezifikationen des Betriebssystems entsprechen.

Hardware

- 500 MB freier Speicherplatz, je nach Betriebssystem
- 2 GB RAM
- Netzwerkschnittstellenkarte 10/100/1000 oder Wi-Fi

Advanced Threat Prevention Software

Die folgende Tabelle enthält detaillierte Informationen über die unterstützte Software.

Betriebssysteme (64-Bit-Kernel)

- Mac OS X Mavericks 10.9.5

ANMERKUNG: Diese Version gilt nur für Advanced Threat Prevention und nicht für den Verschlüsselungs-Client.

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

ANMERKUNG: Dateisysteme, die zwischen Groß- und Kleinschreibung unterschieden, werden nicht unterstützt.

Advanced Threat Prevention – Ports

- Die Advanced Threat Prevention-Agenten werden von der SaaS-Plattform der Verwaltungskonsole verwaltet und erstatten Bericht an diese. Port 443 (https) wird für die Kommunikation verwendet und muss auf der Firewall geöffnet sein, damit die Agenten mit der Konsole kommunizieren können. Die Konsole wird von Amazon Web Services gehostet und verfügt über keine festen IP-Adressen. Sollte Port 443 gesperrt sein, können keine Aktualisierungen heruntergeladen werden. In diesem Fall ist ein ordnungsgemäßer Schutz der Computer nicht gewährleistet. Stellen Sie sicher, dass die Client-Computer wie folgt auf die URLs zugreifen können.

Verwenden Sie die Datei	Anwendungsprotokoll	Transportprotokoll	Portnummer	Ziel	Richtung
Gesamte Kommunikation	HTTPS	TCP	443	Lassen Sie den gesamten https-Datenverkehr an *.cylance.com zu.	Ausgehend

3

Aufgaben für den Encrpytion Client

Installation/Upgrade von dem Encryption Client

Dieser Abschnitt führt Sie durch Installation/Upgrade und Aktivierungsprozess von dem Encryption Client for Mac.

Es gibt zwei Methoden für die Installation/das Upgrade von dem Encryption Client for Mac. Wählen Sie **eine** der folgenden:

- Interaktive Installation/Upgrade und Aktivierung – Dies ist die einfachste Methode zum Installieren oder Aktualisieren des Client-Softwarepakets. Bei dieser Methode sind allerdings keinerlei Anpassungen möglich. Wenn Sie beabsichtigen, Boot Camp oder eine Version des Betriebssystems zu verwenden, die noch nicht vollständig durch Dell unterstützt wird (über eine .plist-Änderung), müssen Sie die Installations-/Upgrade-Methode über Befehlszeile verwenden. Weitere Informationen über die Verwendung von Boot Camp finden Sie unter Verwendung von Boot Camp.
- Installation/Upgrade über Befehlszeile – Dies ist eine fortgeschrittene Installationsmethode, die nur von Administratoren verwendet werden sollte, die sich mit Befehlszeilensyntax auskennen. Wenn Sie beabsichtigen, Boot Camp oder eine Version des Betriebssystems zu verwenden, die noch nicht vollständig durch Dell unterstützt wird (über eine .plist-Änderung), müssen Sie diese Methode zur Installation/zum Upgrade des Client-Softwarepakets verwenden. Weitere Informationen über die Verwendung von Boot Camp finden Sie unter Verwendung von Boot Camp.

  Weitere Informationen zu den Befehlsoptionen des Installationsprogramms finden Sie in der Mac OS X-Referenzbibliothek unter http://developer.apple.com. Dell empfiehlt dringend, zur Verteilung des Client-Installationspakets ein Remote-Bereitstellungstool (wie Apple Remote Desktop) zu verwenden.

> **ANMERKUNG: Apple veröffentlicht häufig neue Versionen von Betriebssystemen zwischen den Versionen von Endpoint Security Suite Enterprise for Mac. Mit dem Ziel, im Sinne möglichst vieler Kunden zu handeln, erlauben wir die Modifizierung der com.dell.ddp.plist-Datei, um einer solchen Situation Rechnung zu tragen. Sobald Apple eine neue Version veröffentlicht, beginnen wir mit dem Testen dieser Versionen, um sicherzustellen, dass sie mit dem Encryption Client for Mac kompatibel sind.**

Voraussetzungen

Dell empfiehlt, bei der Implementierung der Client-Software die Best Practices für IT zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.

Stellen Sie zunächst fest, ob folgende Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob der Dell Server und seine Komponenten bereits installiert sind.

  Wenn Sie den Dell Server noch nicht installiert haben, folgen Sie den Anweisungen in der entsprechenden nachfolgenden Anleitung.

  Enterprise Server-Installations- und Migrationshandbuch

  Erste Schritte und Installationshandbuch für Enterprise Server – Virtual Edition
- Achten Sie darauf, die Sicherheitsserver- und Richtlinien-Proxy-URL zur Hand zu haben. Beide URLs werden für die Installation und Aktivierung der Client-Software benötigt.
- Wenn Ihre Bereitstellung eine Nicht-Standard-Konfiguration verwendet, stellen Sie sicher, dass Sie die Portnummer für den Sicherheitsserver kennen. Diese wird für die Installation und Aktivierung der Client-Software benötigt.
- Stellen Sie sicher, dass der Zielcomputer über Netzwerkkonnektivität mit dem Sicherheitsserver und dem Richtlinien-Proxy verfügt.
- Stellen Sie sicher, dass Sie in der Active Directory-Installation über ein Domänen-Benutzerkonto verfügen, das für die Verwendung mit dem Dell Server konfiguriert ist. Das Domänen-Benutzerkonto wird für die Aktivierung der Client-Software benötigt. Die Konfiguration von Endpunkten für die Domänen-(Netzwerk)-Authentifizierung ist nicht erforderlich.

- Um die Verschlüsselung auf dem Client-Computer durchzusetzen, wählen Sie zunächst die für Ihr Unternehmen relevante Verschlüsselungsoption aus.

Dell Encryption	FileVault-Verschlüsselung
Wählen Sie diese Option für folgende Zwecke aus:	Wählen Sie diese Option für folgende Zwecke aus:
• Alle Partitionen auf dem Startlaufwerk verschlüsseln • Preboot-Authentifizierung überspringen • 256-Bit-Verschlüsselung verwenden	• Fusion Drives verschlüsseln • Preboot-Authentifizierung verwenden • Lösung bereitstellen, die von Apple unterstützt wird
ANMERKUNG: Wenn Sie die Dell Verschlüsselung verwenden möchten, müssen Sie die System Integrity Protection (SIP) deaktivieren. Siehe Interaktive Installation/Upgrade und Aktivierung, Schritt 4.	**ANMERKUNG: Falls ein Mac über ein Fusion Drive verfügt, müssen Sie FileVault aktivieren, um dieses Laufwerk zu verschlüsseln.**

Die Einstellungen der Verschlüsselungsrichtlinie müssen der von Ihnen ausgewählten Verschlüsselungsoption entsprechen. Vergewissern Sie sich vor dem Einrichten von Verschlüsselungsrichtlinien, dass Sie die Richtlinien *Verschlüsseln mit FileVault for Mac* und *Zur Verschlüsselung vorgesehene Volumes* verstehen. Um entweder Dell Encryption oder FileVault Verschlüsselung verwenden zu können, muss die Richtlinie *Dell Volume Encryption* auf *Ein* gesetzt sein.

Weitere Informationen über Verschlüsselungsrichtlinien finden Sie unter Mac-Verschlüsselung > Dell Volume-Verschlüsselung.

Interaktive Installation/Upgrade und Aktivierung

Führen Sie die nachfolgenden Schritte aus, um die Client-Software zu installieren, zu aktualisieren und zu aktivieren. Zur Durchführung dieser Schritte benötigen Sie ein Administratorkonto.

ANMERKUNG: Bevor Sie beginnen, speichern Sie die Arbeit des Benutzers und schließen Sie andere Anwendungen; denn sofort nachdem die Installation abgeschlossen ist, muss der Computer neu gestartet werden.

1. Laden Sie vom Dell Installationsmedium die Datei „Dell-Data-Protection-<version>.dmg“.
2. Doppelklicken Sie auf das Paket-Installationsprogramm. Die folgende Meldung wird angezeigt:
   Dieses Paket führt ein Programm aus, um festzustellen, ob die Software installiert werden kann.
3. Klicken Sie zum Fortsetzen des Vorgangs auf **Weiter**.
4. Lesen Sie die Informationen im Begrüßungsbildschirm und klicken Sie auf **Weiter**.
5. Lesen Sie den Lizenzvertrag, klicken Sie auf **Weiter** und klicken Sie dann auf **Zustimmen**, um die Bedingungen der Lizenzvereinbarung anzunehmen.
   Wenn Sie Dell Encryption mit Mac OS X v10.11 oder höher verwenden, wird ein Dialogfeld mit dem Titel *Mac OS System Integrity Protection ist aktiviert*. Sie müssen die System Integrity Protection (SIP) deaktivieren.

   Führen Sie die folgenden Schritte durch:

   a. Informationen zum Deaktivieren von SIP finden Sie unter http://www.dell.com/support/Article/us/en/19/SLN299063.
   b. Klicken Sie im Assistenten auf **OK** und fahren Sie mit *Dell Data Protection Konfiguration* fort.
6. Geben Sie in das Feld `Domänenadresse:` den vollqualifizierten Domänennamen für die Zielbenutzer ein, wie z. B. *abteilung.unternehmen.de*.
7. Geben Sie in das Feld **Anzeigename (optional):** gegebenenfalls als *Anzeigenamen* den NetBIOS-Namen (vor Windows 2000) der Domäne an, in der Regel in Großbuchstaben.
   Bei entsprechender Einstellung wird dieses Feld anstelle des Feldes „Domänenadresse“ im Dialogfeld *Aktivierung* angezeigt. Diese sorgt für übereinstimmende Domänennamen in den Dialogfeldern zur *Authentifizierung* bei Domänen, die von Windows-Computern verwaltet werden.
8. Geben Sie in das Feld **Sicherheitsserver:** den Sicherheitsserver-Hostnamen ein.

Falls Ihre Bereitstellung auf einer nicht standardmäßigen Konfiguration basiert, aktualisieren Sie die Portfelder und das Kontrollkästchen **SSL verwenden**.

Sobald eine Verbindung hergestellt ist, wechselt die Sicherheitsserver-Konnektivitätsanzeige von rot auf grün.

9 Im Feld **Richtlinien-Proxy:** wird der Richtlinien-Proxy-Hostname automatisch mit einem Richtlinien-Proxy-Host bestückt, der dem Sicherheitsserver-Host entspricht. Dieser Host wird als der Richtlinien-Proxy verwendet, wenn keine Hosts in der Richtlinien-Konfiguration festgelegt wurden.

Nachdem eine Verbindung hergestellt wurde, wechselt die Richtlinien-Proxy-Konnektivitätsanzeige von rot auf grün.

10 Sobald das Dialogfeld „Dell Konfiguration" vollständig ausgefüllt wurde und die Verbindung mit dem Sicherheitsserver und dem Richtlinien-Proxy hergestellt wurde, klicken Sie auf **Weiter**, um die Installationsart anzuzeigen.

11 Bei einigen Installationen auf bestimmten Computern wird ein Dialogfeld *Wählen Sie ein Ziel* vor dem Dialogfeld *Installationsart* angezeigt. Falls dies der Fall ist, wählen Sie den aktuellen Systemdatenträger aus der angezeigten Liste der Datenträger aus. Das Symbol für den aktuellen Systemdatenträger enthält einen grünen Pfeil, der zum Datenträger zeigt. Klicken Sie auf **Weiter**.

12 Nachdem die Installationsart angezeigt wird, klicken Sie auf **Installieren**, um mit der Installation fortzufahren.

13 Geben Sie bei entsprechender Aufforderung die Anmeldeinformationen für das Administratorkonto ein (wird vom Mac OS X-Installationsprogramm verlangt) und klicken Sie anschließend auf **OK**.

> **ANMERKUNG: Unmittelbar nach Abschluss der Installation müssen Sie einen Neustart des Computers ausführen. Wenn noch Dateien in andere Anwendungen offen sind und Sie den Neustart noch nicht durchführen möchten, klicken Sie auf Abbrechen, speichern Sie die Arbeit und schließen Sie die anderen Anwendungen.**

14 Klicken Sie auf **Mit der Installation fortfahren**. Der Installationsvorgang beginnt.

15 Wenn die Installation abgeschlossen wurde, klicken Sie auf **Neustarten**.

16 Fahren Sie fort mit der Aktivierung des Encryption Client for Mac-.

Installation/Upgrade über Befehlszeile

Führen Sie die folgenden Schritte aus, um die Client-Software unter Verwendung der Befehlszeile zu installieren.

> **ANMERKUNG: Wenn Sie die Dell Verschlüsselung auf Mac OS X v10.11.x verwenden möchten, müssen Sie SIP deaktivieren. Siehe dazu http://www.dell.com/support/Article/us/en/19/SLN299063.**

1 Laden Sie vom Dell Installationsmedium die Datei „Dell-Data-Protection-<version>.dmg".

2 Kopieren Sie das Paket **Installation von Dell Data Protection** und die Datei **com.dell.ddp.plist** auf das lokale Laufwerk.

3 Ändern Sie über die Remote-Verwaltungskonsole, falls erforderlich, die folgenden Richtlinien. Richtlinieneinstellungen überschreiben .plist-Dateieinstellungen. Verwenden Sie die .plist-Einstellungen, wenn keine Richtlinien in der Remote-Verwaltungskonsole vorhanden sind.

- **Firmwarekennwort-Modus** – Wenn Sie Boot Camp auf verschlüsselten Mac-Computern oder eine Betriebssystemversion, die von Dell noch nicht vollständig unterstützt wird, verwenden möchten, **müssen** Sie diese Richtlinie zu *Optional* ändern, um **nicht** den Firmware-Kennwortschutz zu verwenden. Weitere Informationen finden Sie unter Info zum optionalen Firmware-Kennwortschutz.

  > **ANMERKUNG:**
  > Wenn die Richtlinie „FirmwarePasswordMode" auf **optional** eingestellt ist, deaktiviert dies nur die Durchsetzung des Firmware-Kennwortschutzes durch die Client-Software. Dadurch wird jedoch ein etwaig vorhandener Firmware-Kennwortschutz **nicht** entfernt. Nachdem diese Schritte durchgeführt wurden, die Installation abgeschlossen und der Neustart des Computers erfolgt ist, können Sie vorhandene Firmwarepasswörter unter Verwendung des Mac OS X-Firmwarepasswort-Dienstprogramms entfernen.

- **Liste der Benutzer ohne Authentifizierung** – In einigen Fällen möchten Sie diese Richtlinie möglicherweise bearbeiten, damit bestimmte Benutzer oder Gruppen von Benutzern keine Aktivierung nicht am Dell Server durchführen müssen. Zum Beispiel könnten in einer Bildungseinrichtung die Lehrkräfte dazu aufgefordert werden, ihre Computer am Dell Server zu aktivieren, aber für die einzelnen Studenten/Schüler, die Labor-Computer verwenden, wäre das nicht erforderlich. Der Labor-Administrator könnte diese Richtlinie und das Konto, auf dem das Client-Hilfsprogramm ausführt wird, verwenden, damit Studenten/Schüler sich anmelden können, ohne zum Aktivieren aufgefordert zu werden. Informationen zum Client-Hilfsprogramm finden Sie unter Client-Hilfsprogramm. Wenn ein Unternehmen wissen muss, welches Benutzerkonto welchem Mac-Computer zugeordnet ist, müssen alle Benutzer sich am Dell Server aktivieren, damit Enterprise diese Eigenschaft nicht ändert. Wenn ein Benutzer jedoch EMS-Datenträger bereitstellen möchte, muss der Benutzer am Dell Server authentifiziert werden.

4 Öffnen Sie die .plist-Datei und bearbeiten Sie alle zusätzlichen Platzhalterwerte:

ANMERKUNG:

Apple veröffentlicht häufig neue Versionen von Betriebssystemen zwischen den Versionen von Endpoint Security Suite Enterprise for Mac. Mit dem Ziel, im Sinne möglichst vieler Kunden zu handeln, erlauben wir die Modifizierung der Datei „com.dell.ddp.plist“, um einer solchen Situation Rechnung zu tragen. Sobald Apple eine neue Version veröffentlicht, beginnt Dell mit dem Testen dieser Versionen, um sicherzustellen, dass sie mit dem Encryption Client for Mac kompatibel sind.

```
<?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 Speichern und schließen Sie die .plist-Datei.

6 Kopieren Sie für jeden Zielcomputer das Paket in einen temp-Ordner und die Datei „com.dell.ddp.plist“ nach **/Library/Preferences**.

7 Führen Sie eine Installation über die Befehlszeile durch, indem Sie den folgenden **Installationsbefehl** ausgeben:

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

8 Starten Sie den Computer mithilfe der folgenden Befehlszeile neu: `sudo shutdown -r now`

9 Fahren Sie fort mit der Aktivierung des Encryption Client for Mac-.

Aktivieren von Encryption Client

Der Aktivierungsprozess ordnet Netzwerkbenutzerkonten im Dell Server dem Mac-Computer zu und ruft von jedem Konto die Sicherheitsrichtlinien ab, sendet Bestandsaufnahme- und Statusaktualisierungen, ermöglicht die Wiederherstellungs-Workflows und bietet umfassende Berichterstattung zur Richtlinientreue. Die Client-Software führt den Aktivierungsvorgang für jedes Benutzerkonto durch, das sie auf dem Computer vorfindet, während sich die einzelnen Benutzer an ihrem Benutzerkonto anmelden.

ANMERKUNG: Anweisungen zum Aktivieren eines Nicht-Domänen-Mac finden Sie im KB-Artikel SLN302497.

Nachdem die Client-Software installiert und der Mac-Neustart durchgeführt wurden, meldet sich der Benutzer an:

1 Geben Sie den Benutzernamen und das Passwort an, der/das von Active Directory verwaltet wird.

Wenn für das Dialogfeld „Kennwort“ eine Zeitüberschreitung eintritt, klicken Sie auf **Aktualisieren** auf der Registerkarte „Richtlinien“. Lesen Sie unter Anzeigen von Verschlüsselungsrichtlinie und Status auf dem lokalen Computer den Schritt 1.

2 Wählen Sie die Domäne aus, bei der Sie sich anmelden möchten.

Wenn der Dell Server so konfiguriert ist, dass mehrere Domänen unterstützt werden und eine andere Domäne zur Aktivierung verwendet werden muss, verwenden Sie den Benutzerprinzipalnamen (UPN) in der Form *<Benutzername>@<Domain>*.

3 Folgende Optionen sind verfügbar:

- Klicken Sie auf **Aktivieren**.
  - Wenn die Aktivierung erfolgreich war, wird eine entsprechende Meldung angezeigt. Der Encryption Client für Mac ist jetzt voll funktionsfähig und wird durch den Dell Server verwaltet.
  - Falls die Aktivierung fehlschlägt, erlaubt die Client-Software drei Versuche zur Eingabe der korrekten Domänen-Anmeldeinformationen. Falls alle drei Versuche fehlschlagen, wird die Aufforderung zur Eingabe der Domänen-Anmeldeinformationen bei der nächsten Anmeldung des Benutzers erneut angezeigt.
- Klicken Sie auf **Jetzt nicht** zum Beenden des Dialogfelds, das noch einmal bei der nächsten Benutzeranmeldung angezeigt wird.

ANMERKUNG: Wenn der Administrator ein Laufwerk auf einem Mac-Computer entschlüsseln muss, sei es über einen Remote-Standort, durch Ausführung eines Skripts oder persönlich, fordert die Client-Software den Benutzer auf, dem Administrator Zugriff zu gewähren und sein Passwort einzugeben.

ANMERKUNG: Falls Sie den Computer für die FileVault-Verschlüsselung konfiguriert haben und Dateien verschlüsselt sind, stellen Sie sicher, dass Sie sich an einem Konto anmelden, über das Sie das System zu einem späteren Zeitpunkt starten können.

4 Führen Sie einen der folgenden Schritte aus:

- Wenn die Verschlüsselung **nicht** vor der Aktivierung aktiviert wurde, fahren Sie mit dem Verschlüsselungsverfahren fort.
- Wenn die Verschlüsselung vor der Aktivierung aktiviert **wurde**, fahren Sie mit Anzeigen von Verschlüsselungsrichtlinie und Status fort.

Verschlüsselungsrichtlinie und Status anzeigen

Die Verschlüsselungsrichtlinie und den Status sehen Sie auf dem lokalen Computer oder in der Remote-Verwaltungskonsole.

Anzeigen von Verschlüsselungsrichtlinie und Status auf dem lokalen Computer

Gehen Sie wie nachfolgend beschrieben vor, um die Verschlüsselungsrichtlinie und den Verschlüsselungsstatus auf dem lokalen Computer anzuzeigen.

1 Starten Sie die *Systemeinstellungen* und klicken Sie auf **Dell Data Protection**.

2 Klicken Sie auf die Registerkarte **Richtlinien** zum Anzeigen der aktuellen Richtlinie, die für diesen Computer festgelegt wurde. Mithilfe dieser Ansicht können Sie die einzelnen Verschlüsselungsrichtlinien überprüfen, die derzeit für den Computer gelten.

TIPP: Klicken Sie auf Aktualisieren zur Suche nach Richtlinienaktualisierungen.

Die Remote Management Console listet die Mac-Richtlinien auf, die in diesen Technologiegruppen verwendet werden:

- **Mac-Verschlüsselung**
- **Verschlüsselung von Wechselspeichermedien**

Je nach den Verschlüsselungsanforderungen in Ihrem Unternehmen können Sie Richtlinien für Dell Encryption oder die FileVault-Verschlüsselung festlegen. Diese Tabelle listet die jeweiligen Richtlinienoptionen auf.

Mac Verschlüsselung > Dell Volume-Verschlüsselung

Dell Volume-Verschlüsselung	*Ein* oder *Aus* Diese Richtlinie ist die „Master-Richtlinie“ für allen anderen Dell Volume-Verschlüsselungsrichtlinien. Diese Richtlinie muss auf *Ein* eingestellt werden, damit andere Dell Volume Verschlüsselungsrichtlinien angewendet werden können.

	Ein aktiviert die Verschlüsselung und initiieren Verschlüsselung für unverschlüsselte Volumes, gemäß den Richtlinien *Für die Verschlüsselung vorgesehene Volumes* **oder** *Verschlüsseln mit FileVault for Mac*. Die Standardeinstellung ist *Ein*. Mit der Einstellung „Aus“ wird die Verschlüsselung deaktiviert und eine Entschlüsselungssuche für alle vollständig oder teilweise verschlüsselten Volumes eingeleitet.
Verschlüsselung mit FileVault für Mac	Wenn Sie die FileVault-Verschlüsselung verwenden möchten, achten Sie darauf, zuerst die Dell Volume-Verschlüsselung auf *Ein* zu setzen. Stellen Sie sicher, dass die Richtlinie *Verschlüsselung mit FileVault for Mac* auf dem Dell Server ausgewählt ist. Nach der Aktivierung wird FileVault basierend auf der Richtlinieneinstellung *Für die Verschlüsselung vorgesehene Volumes* das Systemvolume einschließlich Fusion Drives verschlüsseln. **ANMERKUNG: Wenn Sie die Dell Verschlüsselung (nicht FileVault) verwenden und diese Richtlinie aktiviert ist, hat dies einen Richtlinienkonflikt zur Folge.** **ANMERKUNG:** Informationen zum Durchführen der Migration von der Dell Verschlüsselung zur Verschlüsselung durch FileVault finden Sie unter Migration von Dell Volume-Verschlüsselung auf FileVault-Verschlüsselung.

Mac-Verschlüsselung > Globale Mac-Einstellungen

Zur Verschlüsselung vorgesehene Datenträger	*Nur Systemvolume* oder *Alle festen Volumes* *Nur Systemvolume* bedeutet, dass nur das derzeit aktive Systemvolume geschützt wird. **Alle festen Volumes** bedeutet, dass sämtliche Mac OS Extended Volumes auf allen fest eingebauten Laufwerken sowie der derzeit aktive Systemdatenträger geschützt werden.

3 Beschreibungen aller Richtlinien finden Sie in der *AdminHelp*, die in der Dell Server Remote-Verwaltungskonsole verfügbar ist. So finden Sie eine spezifische Richtlinie in der *AdminHelp*:

a Klicken Sie auf das Suchsymbol.

b Geben Sie das Suchfeld den Richtliniennamen in Anführungszeichen ein.

c Klicken Sie auf den angezeigten Themen-Link. Der von Ihnen in Anführungszeichen eingegebene Richtlinienname wird in diesem Thema hervorgehoben.

4 Klicken Sie auf die Registerkarte **Systemvolumes**, um den Status der zur Verschlüsselung vorgesehenen Volumes anzuzeigen.

Status	Beschreibung
Ausgeschlossen	Das Volume ist von der Verschlüsselung ausgeschlossen. Dies gilt für unverschlüsselte Volumes, wenn die Verschlüsselung deaktiviert ist, für externe Volumes, für Volumes mit einem anderen Format als Mac OS X Extended (Journaled) und für Volumes, die keine Systemlaufwerke sind, wenn die Richtlinie *Für die Verschlüsselung vorgesehene Volumes* auf „Nur Systemvolume“ gesetzt ist.
Volume wird für die Verschlüsselung vorbereitet...	Die Client-Software ist gerade dabei, den Verschlüsselungsprozess für das Volume einzuleiten, hat jedoch noch nicht mit der Verschlüsselungssuche begonnen.
Volume-Größe kann nicht geändert werden	Die Client-Software kann nicht mit der Verschlüsselung beginnen, weil die Größe des Volumes nicht passend eingestellt werden kann. Nehmen Sie nach dem Erhalt dieser Nachricht Kontakt mit dem Dell ProSupport auf und stellen Sie die Protokolldateien bereit.
Vor der Verschlüsselung ist eine Reparatur erforderlich	Das Volume hat die Überprüfung durch das Datenträgerdienstprogramm nicht bestanden.

Status	Beschreibung
	Folgen Sie zum Reparieren eines Volumes den Anweisungen im Apple Support-Artikel HT1782 (http://support.apple.com/kb/HT1782).
Vorbereitung auf die Verschlüsselung abgeschlossen. Neustart steht aus...	Die Verschlüsselung beginnt nach dem Neustart.
Verschlüsselungsrichtlinienkonflikt	Der Datenträger kann nicht mit der Richtlinie in Einklang gebracht werden, weil er mit einer falschen Einstellung verschlüsselt wurde. Siehe Verschlüsselung mit FileVault for Mac.
Warte auf Hinterlegung der Schlüssel beim Server ...	Um sicherzustellen, dass alle verschlüsselten Daten wiederhergestellt werden können, beginnt die Client-Software erst dann mit dem Verschlüsselungsvorgang, wenn alle Verschlüsselungsschlüssel erfolgreich beim Dell Server hinterlegt wurden. Die Client-Software sendet eine Abfrage zur Sicherheitsserver-Verbindung, während sie in diesem Zustand ist, bis die Schlüssel hinterlegt wurden.
Verschlüsselung läuft...	Es wird gerade eine Verschlüsselungssuche durchgeführt.
Verschlüsselt	Die Verschlüsselungssuche ist abgeschlossen.
Entschlüsselung läuft...	Es wird gerade eine Entschlüsselungssuche durchgeführt.
Wiederherstellung des ursprünglichen Zustands läuft...	Die Client-Software versucht am Ende des Vorgangs „Entschlüsselung läuft ...“ das Partitionsschema auf den ursprünglichen Zustand zurückzusetzen. Dies ist bei der Entschlüsselungssuche das Äquivalent des Zustands „Volume wird für die Verschlüsselung vorbereitet...“.
Entschlüsselt	Die Entschlüsselungssuche ist abgeschlossen.

Farbe	Beschreibung
Grün	Verschlüsselter Anteil
Rot	Nicht verschlüsselter Anteil
Gelb	Anteil, der erneut verschlüsselt wird Z. B. aufgrund einer Änderung an den Verschlüsselungsalgorithmen. Die Daten sind weiterhin sicher. Sie gehen lediglich in einen anderen Verschlüsselungstyp über.

Die Registerkarte „Systemlaufwerke“ zeigt alle an den Computer angeschlossenen Volumes an, die sich auf einem mit GPT (GUID Partition Table) formatierten Datenträger befinden. Die folgende Tabelle enthält Beispiele für Volume-Konfigurationen für interne Laufwerke.

ANMERKUNG: Die Zeichen und Symbole können je nach Betriebssystem leicht unterschiedlich sein.

Zeichen	Volume-Typ und Status
	Das derzeit gestartete Mac OS X-Systemlaufwerk. Das X-Ordner-Zeichen steht für die derzeitige Startpartition. Die Dell Verschlüsselung wird nicht zusammen mit der System Integrity Protection (SIP) unterstützt. Falls diese Inkompatibilität per Richtlinie festgelegt und SIP aktiviert ist, wird auf der Registerkarte „Systemlaufwerke“ neben dem Laufwerk ein Fehler angezeigt.

Zeichen	Volume-Typ und Status
	Informationen zum Deaktivieren von SIP finden Sie unter Interaktive Installation/Upgrade und Aktivierung unter Schritt 4.
	Ein Volume, das für die Verschlüsselung konfiguriert ist. Dieses Zeichen steht für eine mit Dell verschlüsselte Partition.
	Ein Volume, das für die Verschlüsselung konfiguriert ist. Das Zeichen „Sicherheit und Datenschutz“ steht für eine mit FileVault geschützte Partition.
	Ein Nicht-Startvolume, das für die Verschlüsselung konfiguriert ist. Das Zeichen „Sicherheit und Datenschutz“ steht für eine mit FileVault geschützte Partition.
	Mehrere Laufwerke und keine Verschlüsselung. **ANMERKUNG: Das Volume-Symbol ohne Zeichen weist darauf hin, dass keine Maßnahmen am Datenträger vorgenommen worden sind. Dies ist kein Startdatenträger.**
	Mehrere Laufwerke, von denen nur das Systemlaufwerk verschlüsselt ist. In diesem Beispiel ist die Partition mit Dell verschlüsselt.

5 Klicken Sie auf die Registerkarte **Wechselmedien**, um den Status der zur Verschlüsselung vorgesehenen Volumes anzuzeigen. Die folgende Tabelle enthält Beispiele für Volume-Konfigurationen für Wechselmedien.

Die Zeichen und Symbole können je nach Betriebssystem leicht unterschiedlich sein.

Zeichen	Status
	Ein abgeblendetes Volume-Symbol weist auf ein nicht geladenes Gerät hin. Mögliche Gründe: • Der Benutzer hat beschlossen, das Volume nicht bereitzustellen. • Das Medium ist gesperrt. **ANMERKUNG: Ein Zeichen mit einem roten Kreis/Schrägstrich auf diesem Symbol weist auf eine Partition hin, die vom Schutz ausgenommen ist, weil sie nicht unterstützt wird. Dies betrifft auch FAT32-formatierte Volumes.**
	Ein ausgefülltes Volume-Symbol weist auf ein geladenes Gerät hin. Das Zeichen für „Nicht beschreibbar“ weist darauf hin, dass das Volume schreibgeschützt ist. Die Verschlüsselung ist aktiviert, aber der Datenträger wurde nicht bereitgestellt und der EMS-Zugriff auf Datenträger ohne Shield ist auf „schreibgeschützt“ eingestellt.

Zeichen	Status
	Mit EMS verschlüsseltes Medium, dargestellt durch ein Dell Emblem.

Anzeigen von Richtlinie und Status in der Remote-Verwaltungskonsole

Gehen Sie wie nachfolgend beschrieben vor, um die Verschlüsselungsrichtlinie und den Verschlüsselungsstatus in der Remote-Verwaltungskonsole anzuzeigen.

1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.

2 Klicken Sie im linken Fensterbereich auf **Bestückungen > Endpunkte**.

3 Klicken Sie bei Workstations auf eine Option im Feld „Hostname“ oder geben Sie den Hostnamen des Endpunkts, falls bekannt, in das Suchfeld ein. Sie können alternativ auch einen Filter für die Suche nach dem Endpunkt eingeben.

> **ANMERKUNG: Das Platzhalterzeichen (*) kann verwendet werden, ist jedoch am Anfang oder am Ende eines Textes nicht erforderlich. Sie können nach allgemeinem Namen, UPN (Universal Principal Name) oder SAM-Kontonamen suchen.**

4 Klicken Sie auf den entsprechenden Endpunkt.

5 Klicken Sie auf die Registerkarte **Details und Aktionen**.

Im Bereich „Endpunktdetails“ werden Informationen zum Mac-Computer angezeigt.

Der Detailbereich Shield zeigt Informationen über die Client-Software an, einschließlich der Start- und Endzeiten der Verschlüsselungssuche für diesen Computer.

Klicken Sie zum Anzeigen der derzeit wirksamen Richtlinien des Endpunkts im Bereich „Maßnahmen“ auf **effektive Richtlinien anzeigen**.

6 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien**. Über diese Registerkarte können Sie die einzelnen Richtlinientypen erweitern und ggf. einzelne Richtlinien ändern.

a Wenn Sie fertig sind, klicken Sie auf **Speichern**.

b Klicken Sie im linken Fensterbereich auf **Verwaltung** > **Festlegen**.

> **ANMERKUNG: Die Anzahl, die unter by "Offene Richtlinienänderungen" angezeigt wird, ist kumulativ. Sie enthält ggf. Änderungen, die auf anderen Endpunkten oder von anderen Administratoren vorgenommen wurden, die das gleiche Konto verwenden.**

c Geben Sie eine Beschreibung der Änderungen in das Kommentarfeld ein und klicken Sie dann auf **Richtlinien bestätigen**.

7 Klicken Sie auf die Registerkarte **Benutzer**. In diesem Bereich wird eine Liste der auf diesem Mac-Computer aktivierten Benutzer angezeigt. Klicken Sie auf den Benutzernamen, um Informationen zu allen Computern anzuzeigen, auf denen dieser Benutzer aktiviert ist.

8 Klicken Sie auf die Registerkarte **Endpunkt-Gruppen**. In diesem Bereich werden alle Endpunkt-Gruppen angezeigt, denen dieser Mac-Computer angehört.

Systemlaufwerke

Verschlüsselung aktivieren

ANMERKUNG: Nur Volumes im Format Mac OS X Extended (Journaled) und Systemdatenträger, die mit dem Partitionsschema GUID Partition Table (GPT) partitioniert wurden, werden für die Verschlüsselung unterstützt.

Verwenden Sie dieses Verfahren zur Aktivierung der Verschlüsselung auf einem Client-Computer, falls die Verschlüsselung vor der Aktivierung noch **nicht** aktiviert wurde. Mit diesem Verfahren kann die Verschlüsselung nur für einen einzigen Computer aktiviert werden. Falls erforderlich, können Sie die Verschlüsselung aller Mac-Computer auf Enterprise-Richtlinienebene aktivieren. Zusätzliche Anleitungen zur Aktivierung der Verschlüsselung auf der Richtlinienebene *Enterprise* finden Sie in der *AdminHelp*.

1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.

2 Klicken Sie im linken Fensterbereich auf **Bestückungen** > **Endpunkte**.

3 Klicken Sie bei Workstations auf eine Option in der Spalte „Hostname“ oder geben Sie den Hostnamen des Endpunkts, falls bekannt, in das Suchfeld ein. Sie können alternativ auch einen Filter für die Suche nach dem Endpunkt eingeben.

ANMERKUNG: Das Platzhalterzeichen (*) kann verwendet werden, ist jedoch am Anfang oder am Ende eines Textes nicht erforderlich. Sie können nach allgemeinem Namen, UPN (Universal Principal Name) oder SAM-Kontonamen suchen.

4 Klicken Sie auf den entsprechenden Endpunkt.

5 Klicken Sie auf der Seite *Sicherheitsrichtlinien* auf die Technikgruppe **Mac-Verschlüsselung**.

Standardmäßig ist die Master-Richtlinie *Dell Volume-Verschlüsselung* auf *Ein* gesetzt.

6 Wenn ein Mac verfügt über ein Fusion-Laufwerk verfügt, markieren Sie das Kontrollkästchen für das *Verschlüsseln mit FileVault* der Mac-Richtlinie.

ANMERKUNG: Diese Richtlinie erfordert, dass die Richtlinie *Dell Volume-Verschlüsselung* auch *Ein* gesetzt ist. Wenn die FileVault-Verschlüsselung jedoch aktiviert ist, ist keine andere Richtlinie der Gruppe wirksam. Siehe dazu Mac Verschlüsselung > Dell Volume-Verschlüsselung

7 Wenn FileVault nicht ausgewählt wurde, können Sie die anderen Richtlinien nach Bedarf ändern.

Beschreibungen aller Richtlinien finden Sie in der *AdminHelp*, die in der Dell Server Remote-Verwaltungskonsole verfügbar ist.

8 Wenn Sie fertig sind, klicken Sie auf **Speichern**.

9 Klicken Sie im linken Fensterbereich auf **Verwaltung** > **Festlegen**.

Die Anzahl, die unter by "Offene Richtlinienänderungen" angezeigt wird, ist kumulativ. Sie enthält ggf. Änderungen, die auf anderen Endpunkten oder von anderen Administratoren vorgenommen wurden, die das gleiche Konto verwenden.

10 Geben Sie eine Beschreibung der Änderungen in das Kommentarfeld ein und klicken Sie dann auf **Richtlinien bestätigen**.

11 Um die Richtlinieneinstellung auf dem lokalen Computer anzuzeigen, nachdem der Dell Server die Richtlinie gesendet hat, klicken Sie im Fensterbereich „Richtlinien“ der Dell Data Protection-Voreinstellungen auf **Aktualisieren**.

Verschlüsselungsvorgang

Der Verschlüsselungsvorgang ist von den folgenden Faktoren abhängig:

- Start des Startvolumes, wenn die Verschlüsselung aktiviert ist
- Auswahl von Dell Encryption oder FileVault-Verschlüsselung.

ANMERKUNG: Zur Wahrung der Integrität der Benutzerdaten, beginnt die Client-Software erst dann mit der Verschlüsselung eines Volumes, wenn der Überprüfungsvorgang auf dem betreffenden Volume erfolgreich abgeschlossen wurde. Schlägt die Überprüfung für ein Volume fehl, informiert die Client-Software den Benutzer und meldet den Fehler in den Dell Data Protection Voreinstellungen. Folgen Sie zum Reparieren eines Volumes den Anweisungen im Apple Support-Artikel HT1782 (http://support.apple.com/kb/HT1782). Die Client-Software führt die Überprüfung beim nächsten Startvorgang des Computers erneut durch.

Wählen Sie eine dieser Optionen aus:

- Dell Verschlüsselung eines unverschlüsselten Laufwerks
- FileVault Verschlüsselung eines unverschlüsselten Volumes
- Verwaltung eines vorhandenen mit FileVault verschlüsselten Volumes übernehmen

Dell Verschlüsselung eines unverschlüsselten Laufwerks

Nachdem die Client-Software die Verschlüsselungsrichtlinie erhalten hat, führt sie eine Überprüfung mit dem Datenträgerdienstprogramm auf den für die Verschlüsselung vorgesehenen Volumes durch und konfiguriert diese für die Verschlüsselung.

1 Die Fortschrittsleiste gibt Aufschluss über den Status der Überprüfung. Nach Abschluss der Überprüfung werden die Volumes für die Verschlüsselung konfiguriert.

   Durch diesen Vorgang kann die Reaktionsgeschwindigkeit des Computers für einige Minuten reduziert sein. Für jedes Volume, für das die Verschlüsselung aussteht, wird ein Dialogfeld angezeigt, das den Benutzer darauf hinweist, dass der Vorgang gerade durchgeführt wird.

2 Starten Sie den Computer nach Abschluss der Verschlüsselungsvorbereitung neu.

   ANMERKUNG: Je nach den Benutzerfreundlichkeitsrichtlinien, die in der Remote-Verwaltungskonsole festgelegt wurden, kann der Benutzer durch die Client-Software aufgefordert werden, den Computer neu zu starten.

3 Nach dem Neustart des Computers muss dieser mit dem Netzwerk verbunden werden, damit die Client-Software die Wiederherstellungsinformationen beim Dell Server hinterlegen kann.

Die Client-Software kann den Verschlüsselungsvorgang starten und abschließen und den Verschlüsselungsstatus an die Remote-Verwaltungskonsole melden, noch bevor sich die Benutzer anmelden. Auf diese Weise können Sie die Compliance auf allen Mac-Computern durchsetzen, ohne dass hierfür das Eingreifen des Benutzers erforderlich ist.

FileVault Verschlüsselung eines unverschlüsselten Volumes

1 Nach der Installation und Aktivierung müssen Sie sich an dem Konto anmelden, über das Sie nach Aktivierung der FileVault-Verschlüsselung starten möchten.

2 Warten Sie, bis das Laufwerk validiert und das Volume überprüft wurden.

3 Geben Sie das Passwort für das Konto ein.

   ANMERKUNG: Falls Sie die Möglichkeit der Zeitüberschreitung für dieses Dialogfeld aktiviert haben, müssen Sie einen Neustart durchführen oder sich anmelden, damit das Dialogfeld für die Eingabe des Passworts erneut angezeigt wird.

4 Klicken Sie auf **OK**.

   Falls es sich bei dem Konto, an dem der Benutzer angemeldet war, um ein nicht mobiles Netzwerkkonto handelt, wird ein Dialogfeld angezeigt. Nachdem das Startlaufwerk verschlüsselt wurde, kann das Laufwerk nur durch den Benutzer gestartet werden, der zum Zeitpunkt der FileVault-Initialisierung angemeldet war.

   Dieses Konto muss ein mobiles, lokales Konto ein mobiles Netzwerkkonto sein. Zum Ändern von nicht-mobilen Netzwerkkonten in mobile Konten, gehen Sie zu **Systemeinstellungen > Benutzer und Gruppen**. Führen Sie einen der folgenden Schritte durch:

   - Ändern Sie das Konto in ein mobiles Konto.
     ODER
   - Melden Sie sich bei einem lokalen Konto an und initialisieren Sie FileVault von dort aus.

5 Klicken Sie auf **OK**.

6 Starten Sie den Computer nach Abschluss der Verschlüsselungsvorbereitung neu.

   ANMERKUNG: Je nach den Benutzerfreundlichkeitsrichtlinien, die in der Remote-Verwaltungskonsole festgelegt wurden, kann der Benutzer durch die Client-Software aufgefordert werden, den Computer neu zu starten.

7 Nach dem Neustart des Computers muss dieser mit dem Netzwerk verbunden werden, damit die Client-Software die Wiederherstellungsinformationen beim Dell Server hinterlegen kann.

Die Client-Software kann den Verschlüsselungsvorgang starten und abschließen und den Verschlüsselungsstatus an die Remote-Verwaltungskonsole melden, noch bevor sich die Benutzer anmelden. Auf diese Weise können Sie die Compliance auf allen Mac-Computern durchsetzen, ohne dass hierfür das Eingreifen des Benutzers erforderlich ist.

Ändern der Richtlinie zum Hinzufügen von FileVault-Benutzern

FileVault sichert die Daten auf einem Laufwerk, indem diese automatisch verschlüsselt werden. Um in einem verwalteten FileVault-Startvolume mehreren Benutzern zu erlauben, das Laufwerk zu entsperren, können Sie über die Remote-Verwaltungskonsole eine Richtlinie ändern und Ihr Wörterbuch mit OpenDirectory-Datensatznamen und -werten verwenden. So können Sie den Benutzern erlauben, sich selbst zum FileVault-Laufwerk hinzuzufügen.

1 Scrollen Sie in den erweiterten Richtlinien *Globale Mac-Einstellungen* zur Richtlinie *Benutzerliste für FileVault 2 PBA*.

2 Geben Sie im Richtlinienfeld *Benutzerliste für FileVault 2 PBA* eine Regel ein, die den Benutzern entspricht, die Sie festlegen möchten. Zum Beispiel muss die Zuordnung von `<string>*</string>` für einen beliebigen Schlüssel mit allen Benutzern übereinstimmen, über die der gebundene OpenDirectory-Server verfügt.

Bei den Tags sind Groß- und Kleinschreibung zu berücksichtigen und der gesamte Wert muss ordnungsgemäß als Wörterbuch und Arrayelement in einer Eigenschaftenliste formatiert sein. Wörterbuchschlüssel sind durch UND miteinander verbunden. Arraywerte sind durch „oder“ miteinander verbunden, sodass die Zuordnung eines beliebigen Elements in einem Array mit dem gesamten Array übereinstimmt.

ANMERKUNG:
Wenn eine Richtlinie nicht korrekt gebildet wird, wird in der Registerkarte *Dell Data Protection > Einstellungen* eine Fehlermeldung angezeigt.

<dict> führt im folgenden Beispiele für zwei Schlüssel auf:

```
<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>
```

- Die Beispielschlüsseleinträge *AuthenticationAuthority* legen ein Muster von *Benutzer1*, *Benutzer2* und *Benutzer3* oder eine beliebige Benutzer-ID, die mit *z* beginnt, fest. Drücken Sie die Tasten **Control-Option-Command** am Client, um das Dialogfeld mit der korrekten Syntax für jeden Benutzer anzuzeigen. Kopieren Sie die Syntax für den Benutzer und fügen Sie diese im Server ein.

  ANMERKUNG:
  In diesem Beispiel stehen die nachgestellten Sternchen für den hinteren Teil der Datensätze zur Authentifizierungsautorität. Um eine unzureichende Angabe zu vermeiden, verwenden Sie den vollständigen Datensatz anstelle eines nachgestellten Sternchen, da das Sternchen mit allen Daten nach dem Doppelpunkt im OpenDirectory-Verzeichnis übereinstimmt.

- Der NFSHomeDirectory-Schlüssel setzt voraus, dass jeder Benutzer, der den ersten Schlüssel durchläuft, über ein Basisverzeichnis in */Benutzer/* verfügt.

  ANMERKUNG:
  Sie müssen den Basisordner erstellen, falls dieser für einen Benutzer nicht vorhanden ist.

3 Starten Sie die Computer neu.

4 Benachrichtigen Sie die Endbenutzer, damit diese das Starten von FileVault für ihr Benutzerkonto aktivieren. Der Benutzer muss über ein lokales oder mobiles Konto verfügen. Netzwerkkonten werden automatisch für mobile Konten konvertiert.

So kann ein Benutzer das FileVault-Konto aktivieren:

1 Starten Sie die **Systemeinstellungen** und klicken Sie auf **Dell Data Protection**.
2 Klicken Sie auf die Registerkarte **Systemvolumes**.
3 Klicken Sie auf das Systemvolume-Laufwerk, und wählen Sie **FileVault Benutzer zu Start von FileVault hinzufügen**.
4 Geben Sie im Suchfeld den Namen eines Benutzers ein oder scrollen Sie nach unten. Benutzerkonten werden nur angezeigt, wenn Sie die Kriterien der Richtlinie erfüllen.

   Für lokale und mobile Benutzer wird die Schaltfläche *Benutzer aktivieren* angezeigt.

   Für Benutzer im Netzwerk wird die Schaltfläche *Konvertieren & Benutzer aktivieren* angezeigt.

   ANMERKUNG:
   Ein grünes Zeichen neben den Benutzerkonten gibt an, dass FileVault gestartet werden kann.
5 Klicken Sie auf **Benutzer aktivieren** oder **Konvertieren & Benutzer aktivieren**.
6 Geben Sie das Kennwort für das ausgewählte Konto an und klicken Sie auf **OK**. Eine Fortschrittsleiste wird angezeigt.
7 Klicken Sie im Dialogfenster nach der Fertigstellung auf **Fertig**.

Verwaltung eines vorhandenen mit FileVault verschlüsselten Volumes übernehmen

Falls der Computer bereits über ein mit FileVault verschlüsseltes Volume verfügt und die FileVault-Verschlüsselung in der Remote-Verwaltungskonsole aktiviert ist, kann Dell Encryption die Verwaltung des Volumes übernehmen.

Falls Dell Encryption feststellt, dass das Startvolume bereits verschlüsselt ist, wird das Dialogfeld „Dell Data Protection“ angezeigt. Gehen Sie folgendermaßen vor, um Dell Encryption die Übernahme der Verwaltung des Volumes zu ermöglichen.

1 Wählen Sie entweder **Persönlicher Wiederherstellungsschlüssel *oder* Startfähige Konto-Anmeldeinformationen**.

   - **Persönlicher Wiederherstellungsschlüssel – falls Sie über den persönlichen Wiederherstellungsschlüssel verfügen, den Sie bei der Verschlüsselung des Laufwerks mit FileVault erhalten haben.**

     1 Geben Sie den Schlüssel ein.

       Wenn der Benutzer nicht über den bereits vorhandenen Schlüssel verfügt, kann er diesen beim Administrator anfordern.
     2 Klicken Sie auf **OK**.

       ANMERKUNG: Nach Abschluss des Übernahmevorgangs wird ein neuer persönlicher Wiederherstellungsschlüssel generiert und hinterlegt. Der vorherige Wiederherstellungsschlüssel wird entwertet und entfernt.
   - **Startfähige Konto-Anmeldeinformationen – wenn Sie über den Benutzernamen und das Kennwort für ein Konto verfügen, das derzeit für das Starten des Volume autorisiert ist.**

     1 Geben Sie den Benutzernamen und das Passwort ein.
     2 Klicken Sie auf **OK**.
2 Wenn ein Dialogfeld angezeigt wird, das darauf hinweist, dass die Verschlüsselung des Volumes nunmehr über Dell verwaltet wird, klicken Sie auf **OK**.

   Falls Dell Encryption feststellt, dass ein Nicht-Startvolume bereits verschlüsselt ist, werden Sie zur Eingabe einer Passphrase aufgefordert.

3 (Nur über FileVault verschlüsselte, Nicht-Startvolumes) Damit Dell Encryption die Verwaltung des Volumes übernehmen kann, geben Sie die Passphrase für den Zugriff auf das Volume ein. Hierbei handelt es sich um das Kennwort, das dem Volume zugewiesen wurde, als es ursprünglich mit FileVault verschlüsselt wurde.

Sobald die Volumeverschlüsselung von Dell verwaltet wird, ist das alte Kennwort nicht länger gültig. Für den unwahrscheinlichen Fall, dass Sie Unterstützung bei der Wiederherstellung benötigen, kann Ihr Dell Administrator einen Wiederherstellungsschlüssel für Ihr Volume abrufen.

Wenn Sie sich gegen die Eingabe eines Passworts entscheiden, kann auf die Inhalte des Volumes zugegriffen werden und sie werden mit FileVault verschlüsselt, jedoch wird die Verschlüsselung nicht durch Dell verwaltet.

ANMERKUNG: In der Remote-Verwaltungskonsole wird dem Administrator angezeigt, dass der Dell-Server die Verwaltung des Endpunkts übernommen hat.

Austauschen der FileVault-Wiederherstellungsschlüssel

Falls Sie Sicherheitsprobleme mit einem Wiederherstellungspaket haben sollten, oder falls ein Volume oder Schlüssel beschädigt sind, können Sie das Schlüsselmaterial für das betreffende Volume austauschen.

Sie können die Schlüssel für Startlaufwerke und Nicht-Startlaufwerke auf Mac OS X austauschen.

So tauschen Sie das Schlüsselmaterial aus:

1 Laden Sie ein Wiederherstellungspaket von der Remote-Verwaltungskonsole herunter und kopieren Sie es in den Desktop des Computers.
2 Starten Sie die *Systemeinstellungen* und klicken Sie auf **Dell Data Protection**.
3 Klicken Sie auf die Registerkarte **Systemvolumes**.
4 Ziehen Sie das Wiederherstellungspaket aus Schritt 1 in die jeweilige Partition.
Ein Dialogfeld fordert Sie dazu auf, die FileVault-Schlüssel auszutauschen.
5 Klicken Sie auf **OK**.
Ein Dialogfeld bestätigt den Austausch der Schlüssel.
6 Klicken Sie auf **OK**.

ANMERKUNG: Die Schlüssel im Wiederherstellungspaket für dieses Laufwerk sind jetzt entwertet. Sie müssen ein neues Wiederherstellungspaket aus der Remote-Verwaltungskonsole herunterladen.

Benutzerfreundlichkeit

Um maximale Sicherheit zu erreichen, deaktiviert die Client-Software die Funktion *automatische Anmeldung* auf Mac OS X Computern.

Darüber hinaus wendet die Client-Software automatisch die Mac OS X Funktion *Passwort erforderlich, wenn Energiesparmodus oder Bildschirmschoner aktiv ist*. Außerdem ist ein Zeitfenster konfigurierbar, nach dessen Ablauf die Authentifizierung nach Aktivierung des Ruhemodus/Bildschirmschoners durchgesetzt wird. Die Client-Software ermöglicht dem Benutzer die Festlegung eines Werts von maximal fünf Minuten, bevor die Authentifizierung durchgesetzt wird.

Benutzer können den Computer während der Verschlüsselungssuche ganz normal nutzen. Alle Daten, die sich auf dem derzeit gestarteten Systemlaufwerk befinden, werden verschlüsselt, einschließlich des Betriebssystems. Das Betriebssystem ist währenddessen weiterhin funktionsfähig.

Wenn der Computer neu gestartet wird oder in den Ruhemodus wechselt, wird die Verschlüsselungssuche angehalten. Nach dem Neustart bzw. Verlassen des Ruhemodus wird sie automatisch wieder aufgenommen.

Die Client-Software bietet keine Unterstützung für die Verwendung von Ruhezustandsbildern, die die Mac OS X Funktion *Safe Sleep* zum Reaktivieren des Computers verwendet, wenn der Akku während des Ruhemodus vollständig entladen wurde.

Um die Beeinträchtigung des Benutzers möglichst gering zu halten, aktualisiert die Client-Software automatisch den Systemruhemodus so, dass der Ruhezustand deaktiviert wird, und setzt diese Einstellung durch. Der Computer kann weiterhin in den Ruhemodus wechseln, allerdings wird der derzeitige Systemzustand nur im Speicher beibehalten. Der Computer wird daher komplett neu gestartet, falls er während des Ruhemodus vollständig heruntergefahren wird, was beispielsweise bei niedrigem Akkuladezustand oder beim Austauschen des Akkus der Fall sein könnte.

Whitelist-Regel kopieren

Ein ausgeblendetes Menüelement ermöglicht dem Benutzer, eine Regel für die Positivliste für externe Medien zu kopieren.

1 Starten Sie die **Systemeinstellungen** und klicken Sie auf **Dell Data Protection**.
2 Wählen Sie die Registerkarte **Wechseldatenträger**.
3 Klicken Sie mit der rechten Maustaste auf eine Laufwerkszeile und drücken Sie gleichzeitig auf die Befehlstaste.

   Ein ausgeblendetes Menüelement wird angezeigt.
4 Klicken Sie auf **Whitelist-Regel kopieren** für den aktuellen externen Datenträger. Die Regel für die Positivliste wird in die Zwischenablage kopiert.
5 Rufen Sie die Zwischenablage auf, kopieren Sie die Regel für die Positivliste und senden Sie sie an Ihren Administrator.

Wenn die Richtlinie *Mac Media Encryption* auf **Ein** geschaltet ist, werden Daten verschlüsselt, einschließlich der Thunderbolt-Laufwerke.

Falls Sie ein Gerät oder eine Gerätegruppe ausschließen möchten, um zu verhindern, dass verschlüsselte Daten auf das Thunderbolt-Laufwerk oder das EMS-Medium geschrieben werden, können Sie die Werte der Positivlistenregel ändern.

Verwenden Sie die vollständige Regel, um ein bestimmtes Laufwerk für die Aufnahme in die Positivliste auszuwählen, beispielsweise:

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

ANMERKUNG: Ersetzen Sie die Beispielwerte durch die Informationen für Ihr Laufwerk.

ANMERKUNG: Sie müssen HFS Plus aktivieren. Siehe dazu Aktivieren von HFS Plus.

So schließen Sie bei einer Verbindung über Thunderbolt SATA-Geräte von der Durchsetzung der EMS-Richtlinie aus:

tbolt=1;bus=SATA

Sie haben außerdem die Möglichkeit, Medien anhand der folgenden Kriterien auf die Positivliste zu setzen oder aus EMS zu entfernen:

- **Mediengröße**

  Positivlistenregel für den Ausschluss großer Medien aus dem EMS-Schutz:

  size <Operant> <Größenfestlegung>

  <Operant> kann die folgenden Werte haben: =, <=, >=, <, >

  <Größenfestlegung> in der Form einer dezimale Ganzzahl mit einem optionalen Suffix aus {K, M, G, T}, abgestimmt auf 1.000, nicht auf 1.024. Um beispielsweise Medien oder ein Laufwerk mit einer Größe über 500.000.000 Byte aus EMS auszuschließen, verwenden Sie den folgenden Befehl:

  size >= 500000000

  size >= 500000K

  size >= 500M
- **Dateisystemtyp**

Positivlistenregel:

fstype=<fstype>

Mögliche Werte für <fstype> sind ExFAT, FAT oder HFS+

Um beides auszuschließen, finden Sie hier ein Beispiel für ein HFS+-Medium ab 1 TB:

size>=1T;fstype=HFS+

Wiederherstellung

Eventuell benötigen Sie gelegentlich Zugriff auf Daten auf verschlüsselten Laufwerken. Als Dell Administrator können Sie auf verschlüsselte Laufwerke zugreifen, ohne diese entschlüsseln zu müssen. So sparen Sie wertvolle Zeit.

Es kann aus verschiedenen Gründen erforderlich sein, auf die verschlüsselten Daten eines Benutzers zuzugreifen. Hier einige Fallbeispiele:

- Sie müssen die verschlüsselten Daten eines Benutzers im Rahmen einer Hardware-Aktualisierung auf einen anderen Mac verschieben.
- Sie müssen auf einen verschlüsselten Datenträger zugreifen, weil das Systemlaufwerk aufgrund eines Betriebssystemfehlers nicht mehr startet und Sie verschiedene Dienstprogramme zur Reparatur des Betriebssystems ausführen müssen.
- Der Benutzer hat eine unzulässige Konfigurationsänderung vorgenommen und Sie müssen die Situation korrigieren.

Dieser Abschnitt führt Sie durch den Vorgang der Verwendung **einer** der drei verfügbaren Wiederherstellungsvorgänge.

Wählen Sie **eine** der folgenden Optionen:

- Volume laden
- Neue Systemkonfiguration übernehmen
- FileVault Recovery – nur verwenden, wenn Sie die FileVault-Verschlüsselung auf dem Endpunkt einsetzen, der wiederhergestellt werden soll. FileVault kann verwendet werden, wenn der Encryption Client unter Mac OS X 10.10.5 oder höher ausgeführt wird. Die FileVault-Wiederherstellung wird auch auf Fusion Drives verwendet.

Volume laden

Voraussetzungen

- Unverschlüsseltes, externes Wiederherstellungsvolume oder Computer, auf dem das Wiederherstellungsdienstprogramm ausgeführt wird
- FireWire- oder Thunderbolt-Kabel, je nach Hardware
- Die Geräte-ID/Eindeutige ID des Computers – In der Regel finden Sie den für die Wiederherstellung vorgesehenen Computer in der Remote-Verwaltungskonsole. Suchen Sie nach dem Benutzernamen des Besitzers und zeigen Sie die für diesen Benutzer verschlüsselten Geräte an. Das Format für die Eindeutige ID/Geräte-ID lautet „Peter Schmidt's MacBook.Z4291LK58RH“.
- Die Dell Installationsmedien

Verfahren

1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.

2 Klicken Sie im linken Bereich auf **Verwaltung > Endpunkt wiederherstellen**.

3 Geben Sie in das Suchfeld den vollständig qualifizierten Domänennamen (FQDN) des Endpunktes ein und klicken Sie auf das Symbol zum Suchen.

4 Klicken Sie auf den Link zum **Wiederherstellen** des Geräts.

5 Wenn für den Endpunkt eine erweiterte Wiederherstellung erforderlich ist, werden Sie über ein Dialogfeld dazu aufgefordert, ein Passwort einzugeben. Weisen Sie dem Schlüsselpaket, das Sie herunterladen möchten, ein neues Passwort zu.

ANMERKUNG: Sie müssen sich dieses Passwort für den Zugriff auf die Wiederherstellungsschlüssel merken.

6 Zum Speichern des Wiederherstellungspakets auf dem externen Wiederherstellungsvolume oder Computer, auf dem das Wiederherstellungsprogramm für den Wiederherstellungsvorgang ausgeführt wird, klicken Sie auf **Herunterladen** und klicken Sie auf **Speichern**.

Anschließend wird die Wiederherstellungsdatei <Computername.Domäne>.csv heruntergeladen.

> **ANMERKUNG: Falls auf dem Computer der Firmwarepasswortschutz aktiviert ist, werden Sie zur Eingabe des Firmwarepassworts aufgefordert, um Zugriff auf den Preboot Startup Manager zu erhalten. Sie finden das Firmwarekennwort für diesen Computer im Wiederherstellungspaket, das Sie unter Speichern des Wiederherstellungspakets heruntergeladen haben. Siehe Anleitung zum Aktivieren von Mac OS X Boot Camp für weitere Informationen.**

7 Starten Sie den Zielcomputer über ein zuvor erstelltes, externes Wiederherstellungsvolume. Sie erreichen dies, indem Sie entweder den Bereich „Startlaufwerk“ in der Systemeinstellung starten und das Wiederherstellungsvolume auswählen oder indem Sie die Taste **Option** während des Neustarts dieses Computers gedrückt halten und das Wiederherstellungsvolume vor dem Starten im Start-Manager auswählen.

oder

Starten Sie den für die Wiederherstellung vorgesehenen Computer im Zieldatenträgermodus. Sie erreichen dies, indem Sie entweder den Bereich „Startlaufwerk“ in der Systemeinstellung starten und auf **Ziellaufwerkmodus** klicken oder indem Sie die Taste **T** während des Neustarts dieses Computers gedrückt halten.

> **ANMERKUNG: Der Firmwarepasswortschutz blockiert die Verwendung der Taste T beim Starten zum Aufrufen des Zieldatenträgermodus. Weitere Informationen zum Zieldatenträgermodus erhalten Sie von Apple unter http://support.apple.com/kb/HT1661.**

Schließen Sie diesen Computer jetzt mithilfe eines Firewire- oder Thunderbolt-Kabels (je nach Hardware) an den Host-Computer an, auf dem der Wiederherstellungsvorgang durchgeführt werden wird.

8 Laden Sie Dell-Data-Protection-<Version>.dmg.

> **ANMERKUNG: Die Version des Wiederherstellungsdienstprogramms muss mindestens der Version der Client-Software entsprechen, die auf dem wiederherzustellenden Computer installiert ist.**

9 Starten Sie das Dell Recovery Dienstprogramm im Ordner Dienstprogramme auf der Dell Installations-CD.

Es wird folgende Meldung angezeigt: „Die DDP-Kext [Kernel-Erweiterung] muss geladen werden, damit verschlüsselte Datenträger modifiziert werden können. Geben Sie Ihr Passwort ein, um diesen Vorgang zuzulassen.“

10 Geben Sie das Passwort für den Administrator oder den Benutzer ein.

Es wird folgende Meldung angezeigt: „Installation erforderlich: Recovery muss installiert werden."

11 Klicken Sie auf **Installieren**.

12 Wählen Sie das Volume oder Laufwerk aus, das wiederhergestellt werden soll, und klicken Sie auf **Weiter**.

Durch Auswählen des Laufwerks werden alle darauf befindlichen Volumes gleichzeitig wiederhergestellt.

13 Wählen Sie das Wiederherstellungspaket (das Sie in Schritt 6 gespeichert haben) und klicken Sie auf **Öffnen**.

14 Wählen Sie die Option **Volume laden**.

15 Klicken Sie zur Bestätigung auf **Weiter**, um die Option *Volume laden* auszuführen. Eine Erfolgsmeldung wird angezeigt.

16 Klicken Sie auf **Schließen**.

Sie können jetzt ein Finder-Fenster öffnen und genau wie bei einem normalen Volume auf die Daten des verschlüsselten Volumes zugreifen. Sämtliche Daten werden mit der Übertragung der Dateien zwischen den Volumes transparent verschlüsselt und entschlüsselt.

Neue Systemkonfiguration übernehmen

Falls der Verschlüsselungsschlüssel auf einem verschlüsselten Computer durch ein neues Firmwarepasswort oder eine andere Änderung an der Systemkonfiguration entwertet wurde, können Sie die aktualisierte Systemkonfiguration mithilfe dieser Option beim nächsten Neustart übernehmen und den Zugriff auf den Computer wiederherstellen.

Da die Verschlüsselung an eine bestimmte Gerätekonfiguration gebunden ist, wird der Verschlüsselungsschlüssel der Client-Software entwertet, wenn Änderungen an der Konfiguration vorgenommen werden. Durch Auswahl der Option zum Übernehmen der neuen Systemkonfiguration wird die Client-Software angewiesen, die Sicherheit basierend auf der neuen Konfiguration wiederherzustellen.

Beispiel: Sie müssen das Laufwerk zu einem anderen Mac transferieren, weil der Bildschirm eines Benutzers beschädigt ist. Mit der Option weisen Sie die Client-Software an, diese „neue“ Konfiguration als gültig zu betrachten.

Voraussetzungen

- Unverschlüsseltes, externes Wiederherstellungsvolume oder Computer, auf dem das Wiederherstellungsdienstprogramm ausgeführt wird
- FireWire- oder Thunderbolt-Kabel, je nach Hardware
- Die Geräte-ID/Eindeutige ID des Computers – In der Regel finden Sie den für die Wiederherstellung vorgesehenen Computer in der Remote-Verwaltungskonsole. Suchen Sie nach dem Benutzernamen des Besitzers und zeigen Sie die für diesen Benutzer verschlüsselten Geräte an. Das Format für die Eindeutige ID/Geräte-ID lautet „Peter Schmidt's MacBook.Z4291LK58RH“.
- Die Dell Installationsmedien

Verfahren

1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.

2 Klicken Sie im linken Fensterbereich auf **Bestückungen > Endpunkte**.

3 Suchen Sie nach dem wiederherzustellenden Gerät.

4 Klicken Sie auf den Gerätenamen, um die Seite mit den Endpunktdetails aufzurufen.

5 Klicken Sie auf die Registerkarte **Details und Aktionen**.

6 Unter dem Punkt „Shield“ klicken Sie auf den Link **Geräte-Wiederherstellungsschlüssel**.

7 Zum Speichern des Wiederherstellungspakets auf dem externen Wiederherstellungsvolume oder Computer, auf dem das Wiederherstellungsprogramm für den Wiederherstellungsvorgang ausgeführt wird, klicken Sie auf **Herunterladen** und klicken Sie auf **Speichern**.

> **ANMERKUNG: Falls auf dem Computer der Firmwarepasswortschutz aktiviert ist, werden Sie zur Eingabe des Firmwarepassworts aufgefordert, um Zugriff auf den Preboot Startup Manager zu erhalten. Sie finden das Firmwarekennwort für diesen Computer im Wiederherstellungspaket, das Sie in Schritt 7 heruntergeladen haben. Siehe Anleitung zum Aktivieren von Mac OS X Boot Camp für weitere Informationen.**

8 Starten Sie den Zielcomputer über ein zuvor erstelltes Installationsvolume mit vollständigem Betriebssystem. Sie erreichen dies, indem Sie entweder den Bereich „Startlaufwerk“ in der Systemeinstellung starten und das Installations-Volume mit dem vollständigen BS auswählen oder indem Sie die Taste **Option** während des Neustarts dieses Computers gedrückt halten und das externe Installations-Volume mit dem vollständigen BS vor dem Starten im Start-Manager auswählen. Weitere Informationen zum Erstellen eines startfähigen Volumes finden Sie unter https://support.apple.com/en-us/HT202796.

oder

Starten Sie den für die Wiederherstellung vorgesehenen Computer im Zieldatenträgermodus. Sie erreichen dies, indem Sie entweder den Bereich „Startlaufwerk“ in der Systemeinstellung starten und auf **Ziellaufwerkmodus** klicken oder indem Sie die Taste **T** während des Neustarts dieses Computers gedrückt halten.

> **ANMERKUNG: Der Firmwarepasswortschutz blockiert die Verwendung der Taste T beim Starten zum Aufrufen des Zieldatenträgermodus. Weitere Informationen zum Zieldatenträgermodus erhalten Sie von Apple unter http://support.apple.com/kb/HT1661.**

9 Führen Sie einen der folgenden Schritte aus:

- Schließen Sie diesen Computer jetzt mithilfe eines Firewire- oder Thunderbolt-Kabels (je nach Hardware) an den Host-Computer an, auf dem der Wiederherstellungsvorgang durchgeführt werden wird.

  oder

- Wechseln Sie den Startvorgang auf eine Festplatte mit einem vollständig installierten Betriebssystem.

10 Laden Sie Dell-Data-Protection-<Version>.dmg.

> **ANMERKUNG: Die Version des Wiederherstellungsdienstprogramms muss mindestens der Version der Client-Software entsprechen, die auf dem wiederherzustellenden Computer installiert ist.**

11 Starten Sie das Dell Recovery Dienstprogramm im Ordner Dienstprogramme auf der Dell Installations-CD.

Es wird folgende Meldung angezeigt: „Die DDP-Kext [Kernel-Erweiterung] muss geladen werden, damit verschlüsselte Datenträger modifiziert werden können. Geben Sie Ihr Passwort ein, um diesen Vorgang zuzulassen.“

12 Geben Sie das Passwort für den Administrator oder den Benutzer ein.
Es wird folgende Meldung angezeigt: „Installation erforderlich: Recovery muss installiert werden."

13 Klicken Sie auf **Installieren**.

14 Wählen Sie das Volume oder Laufwerk aus, das wiederhergestellt werden soll, und klicken Sie auf **Weiter**.
Durch Auswählen des Laufwerks werden alle darauf befindlichen Volumes gleichzeitig wiederhergestellt.

Das Fenster für die Dateiauswahl wird angezeigt.

15 Wählen Sie das Wiederherstellungspaket (das Sie in Schritt 7 gespeichert haben) und klicken Sie auf **Öffnen**.
Das Dialogfeld *Wiederherstellungsvorgang auswählen* wird angezeigt.

16 Wählen Sie die Option **Neue Systemkonfiguration akzeptieren**.

17 Klicken Sie auf **Fortfahren**, um den Vorgang *Neue Systemkonfiguration akzeptieren* zu bestätigen.

18 Geben Sie Ihr Passwort ein, um das Eigentum wiederherzustellen und die neue Systemkonfiguration zu übernehmen.

19 Klicken Sie auf **OK**.

Die Meldung *Wiederherstellung abgeschlossen* erscheint, wenn vom ursprünglichen internen System-Volume gestartet wird. Mit dieser Meldung werden Sie aufgefordert, einen weiteren Neustart des Computers durchzuführen. Die Client-Software hat die aktualisierte Systemkonfiguration jetzt übernommen und Sie können wie gewohnt auf Ihren Computer zugreifen.

FileVault-Wiederherstellung

Die Wiederherstellung eines verwalteten, mit FileVault verschlüsselten Volumes unterscheidet sich erheblich von der eines mit Dell verschlüsselten Volumes. Der Wiederherstellungsprozess wird von Apple vorgegeben und ist weitestgehend automatisiert. Es sind jedoch einige zusätzliche Schritte erforderlich.

Das Dell Recovery Utility vereinfacht den Betrieb der Apple Wiederherstellungstools durch Skripte, die dem Laden eines Volumes oder, in manchen Fällen, dem Entschlüsseln eines Volumes dienen. Die FileVault-Wiederherstellungsfunktionalität richtet sich nach dem Betriebssystem, das auf der Recovery HD und der gekoppelten Zielpartition installiert ist.

Ein mit FileVault verschlüsseltes Volume kann nur über eine Recovery HD-Partition wiederhergestellt werden, die an alle Festplattenlaufwerke geschrieben wird, auf denen Mac OS X 10.9.5 oder höher ausgeführt wird. Diese Anforderung hat zur Folge, dass die Durchführung eines Wiederherstellungsvorgangs direkt über das Dell Recovery Utility nicht mehr möglich ist.

Es gibt zwei Wiederherstellungsmethoden, die sich danach richten, ob es sich bei dem FileVault-Wiederherstellungsschlüssel um einen persönlichen oder einen institutionellen Schlüssel handelt. Ein gültiger Wiederherstellungsschlüssel ist immer vorhanden. Sie sollten grundsätzlich immer zuerst den neusten persönlichen Wiederherstellungsschlüssel verwenden. Falls dieser nicht funktioniert, verwenden Sie die institutionelle Wiederherstellungsschlüsselkette.

- Persönlicher Wiederherstellungsschlüssel – vorhandene FileVault-Verschlüsselung, die durch den Dell Server verwaltet wird. Dies ist die bevorzugte Methode.

  Falls der neueste Eintrag im Wiederherstellungspaket einen RecoveryKey-Eintrag enthält, befolgen Sie die Schritte unter Persönlicher Wiederherstellungsschlüssel. Hier ist ein Beispiel für RecoveryKey:

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

- Wiederherstellungsschlüsselkette – Diese Wiederherstellungsmethode basiert auf der Verwendung eines institutionellen FileVault-Wiederherstellungsschlüssels.

  Falls der neueste Eintrag im Wiederherstellungspaket einen KeychainKey-Eintrag enthält, befolgen Sie die Schritte unter Wiederherstellungsschlüsselkette. Hier ist ein Beispiel für KeychainKey:

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

Persönlicher Wiederherstellungsschlüssel

Es hat sich bewährt, das Startvolume vor anderen Volumes wiederherzustellen, die keine Startvolumes sind. Durch die Wiederherstellung des Startvolumes werden in der Regel Probleme mit Nicht-Startvolumes behoben.

Voraussetzungen

- Externes, startfähiges Laufwerk
- Geräte-ID/Eindeutige ID des für die Wiederherstellung vorgesehenen Computers In der Regel finden Sie den für die Wiederherstellung vorgesehenen Computer in der Remote-Verwaltungskonsole. Suchen Sie nach dem Benutzernamen des Besitzers und zeigen Sie die für diesen Benutzer verschlüsselten Geräte an. Das Format für die Eindeutige ID/Geräte-ID lautet „Peter Schmidt's MacBook.Z4291LK58RH“.
- Die Dell Installationsmedien

Verfahren

1 Öffnen Sie die Remote Management Console.

2 Klicken Sie im linken Fensterbereich auf **Bestückungen > Endpunkte**.

3 Suchen Sie nach dem wiederherzustellenden Gerät.

4 Klicken Sie auf den Gerätenamen, um die Seite mit den Endpunktdetails aufzurufen.

5 Klicken Sie auf die Registerkarte **Details und Aktionen**.

6 Unter dem Punkt „Shield“ klicken Sie auf den Link **Geräte-Wiederherstellungsschlüssel**.

7 Zum Speichern des Wiederherstellungspakets auf dem externen Wiederherstellungsvolume oder Computer, auf dem das Wiederherstellungsprogramm für den Wiederherstellungsvorgang ausgeführt wird, klicken Sie auf **Herunterladen** und klicken Sie auf **Speichern**.

8 Geben Sie einen Speicherort für das Wiederherstellungspaket ein und klicken Sie auf **Speichern**.

9 Kopieren Sie das Wiederherstellungspaket und die Datei **Dell-Data-Protection-<version>.dmg** auf das startfähige USB-Laufwerk.

10 Starten Sie den Zielcomputer von einem im Voraus erstellten, externen Installations-Volume mit vollständigem BS aus, indem Sie die Taste **Option** während des Neustarts dieses Computers gedrückt halten und das externe Installations-Volume mit dem vollständigen BS vor dem Starten im Start-Manager auswählen. Weitere Informationen zum Erstellen eines startfähigen Volumes finden Sie unter https://support.apple.com/en-us/HT202796.

11 Laden Sie Dell-Data-Protection-<Version>.dmg.

> **ANMERKUNG:**
> Die Version des Wiederherstellungsdienstprogramms muss mindestens der Version der Client-Software entsprechen, die auf dem wiederherzustellenden Computer installiert ist.

12 Starten Sie das Dell Recovery Dienstprogramm im Ordner Dienstprogramme auf der Dell Installations-CD.
Das Dialogfeld *Dell Recovery Utility > Volumes auswählen* wird angezeigt.

13 Wählen Sie das FileVault-Volume aus.

- Um das Laufwerk entschlüsseln und laden zu können, benötigen Sie eine Startpartition ab Version 10.9.5. Ansonsten steht Ihnen nur der persönliche Wiederherstellungsschlüssel zur Verfügung.
- Wenn Sie Nicht-Startvolumes verschlüsselt haben, müssen Sie in der Regel zuerst die Startpartition wiederherstellen.

14 Klicken Sie auf **Weiter**.

Das Dialogfeld *Wiederherstellungspaket auswählen* wird angezeigt.

15 Wählen Sie das Wiederherstellungspaket (das Sie in Schritt 9 gespeichert haben) und klicken Sie auf **Öffnen**.

Das Dialogfeld *Wiederherstellungsdatensatz auswählen* wird angezeigt.

16 Wählen Sie in der Spalte „Hinterlegungsdatum“ das aktuellste Datum für den Typ „Persönlicher Wiederherstellungsschlüssel“ aus und klicken Sie auf **Weiter**.

ANMERKUNG:
Bei Verwendung eines älteren Hinterlegungsdatums kann es sein, dass der Schlüssel nicht mehr gültig ist.

Bei „Ergebnis des Wiederherstellungsvorgangs“ wird der Schlüssel angezeigt.

- Für Startlaufwerke stellt das Wiederherstellungstool einen persönlichen Wiederherstellungsschlüssel bereit, mit dem Sie unter Verwendung der standardmäßigen Wiederherstellung mit Apple FileVault starten können. Sie können über die Zielpartition starten und dort den persönlichen Wiederherstellungsschlüssel für Pre-Boot-Authentication eingeben, der je nach Betriebssystem variieren kann.
- Für Nicht-Startlaufwerke wird nur der persönliche Wiederherstellungsschlüssel angezeigt. Geben Sie zum Laden eines Nicht-Startvolumes den Wiederherstellungsschlüssel in das Dialogfeld „Passwort“ des Betriebssystems ein. Falls Sie das Dialogfeld zuvor verlassen haben, können Sie jetzt mithilfe der Option „Entsperren über Datenträgerdienstprogramm“ die verschlüsselte Partition laden.

17 Drucken oder notieren Sie den Schlüssel.

18 Klicken Sie auf **Schließen**.

19 Starten Sie über das externe Startvolume, indem Sie beim Start die Taste **Option** gedrückt halten.

20 Geben Sie gegebenenfalls das Firmwarepasswort ein. Wählen Sie das externe Startvolume aus.

21 Klicken Sie nach dem Neustart des Systems auf das **?** im Anmeldebildschirm.

22 Klicken Sie auf den angezeigten Pfeil.

23 Geben Sie den Wiederherstellungsschlüssel ein und drücken Sie die **Eingabetaste**.

24 Geben Sie in das Dialogfeld ein neues Passwort ein.

Wiederherstellungsschlüsselkette

Das Dell Wiederherstellungsdienstprogramm muss über ein unverschlüsseltes Wiederherstellungsvolume gestartet und ausgeführt werden. Das Dell Wiederherstellungsdienstprogramm kann nicht über ein verschlüsseltes, externes Startvolume ausgeführt werden.

Voraussetzungen

- Externes Wiederherstellungsvolume oder Computer, auf dem das Wiederherstellungsdienstprogramm ausgeführt wird
- USB-Laufwerk
- Firewire-Kabel
- Die Dell Installationsmedien

Verfahren

1 Schließen Sie ein externes Laufwerk an das System an, damit es wiederhergestellt werden kann.

Das externe Laufwerk muss über ein Mac OS-Startvolume verfügen.

2 Starten Sie über das externe Startvolume, indem Sie beim Start die Taste **Option** gedrückt halten.

3 Geben Sie gegebenenfalls das Firmwarepasswort ein. Wählen Sie das externe Startvolume aus.

4 Laden Sie die Datei .dmg.

5 Starten Sie im Ordner „Dienstprogramme“ das Dell Wiederherstellungsdienstprogramm.

Das Dialogfeld *Dell Recovery Utility > Volumes auswählen* wird angezeigt.

6 Wählen Sie das wiederherzustellende FileVault-Volume aus und klicken Sie auf **Weiter**.

Das Dialogfeld *Wiederherstellungspaket auswählen* wird angezeigt.

7 Wählen Sie das Wiederherstellungspaket aus und klicken Sie auf **Öffnen**.

Wenn mehr als ein Wiederherstellungsschlüssel für dieses Laufwerk vorhanden ist, wird der Bildschirm *Wiederherstellungsdatensatz auswählen* angezeigt.

8 Wählen Sie in der Spalte „Hinterlegungsdatum“ das aktuellste Datum für den Wiederherstellungstyp „Schlüsselkette“ aus und klicken Sie auf **Weiter**.

> **ANMERKUNG:**
> Bei Verwendung eines älteren Hinterlegungsdatums kann es sein, dass der Schlüssel nicht mehr gültig ist.

Das Dialogfeld *Anweisungen zur FileVault-Wiederherstellung* wird angezeigt.

9 Lesen Sie die Anweisungen und klicken Sie auf **Weiter**.

Das Dialogfeld *Wiederherstellungsvorgang bestätigen* wird angezeigt.

10 Markieren Sie das wiederherzustellende FileVault-Volume und klicken Sie auf **Weiter**.

Das Dialogfeld *Ort für Wiederherstellungsdateien auswählen* wird mit der Aufforderung angezeigt, einen Speicherort für die Wiederherstellungsdateien auszuwählen.

Diesen Speicherort müssen Sie für die Wiederherstellung verwenden, da die Skripte absolute Pfade zu den Datendateien enthalten. Kopieren Sie diese Dateien **nicht** auf die Recovery HD.

Dell empfiehlt, diese Dateien im Stammverzeichnis eines externen Laufwerks, z. B. eines USB-Laufwerks, zu speichern.

> **ANMERKUNG:**
> Stellen Sie sicher, dass alle Benutzer Lese-/Schreibzugriff auf das USB-Laufwerk bzw. den Datenträger mit dem Wiederherstellungsschlüssel haben und dass darauf genügend Speicherplatz verfügbar ist. Wenn Sie keine Rechte für einen ausgewählten Datenträger besitzen, oder wenn darauf nicht genügend Speicherplatz verfügbar ist, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die Wiederherstellungsschlüssel nicht gespeichert wurden.

11 Wählen Sie einen Speicherort aus und klicken Sie auf **Speichern**.

Das Dialogfeld *Ergebnis des Wiederherstellungsvorgangs* mit den Dateien, die erstellt wurden, wird angezeigt.

12 Klicken Sie auf **Schließen**.

13 Geben Sie nach dem Start des Recovery HD-Volumes den Namen und den Pfad des Skripts ein.

> **ANMERKUNG:**
> Wenn Sie die Dateien in der Nähe des Stamms eines Volumes speichern, müssen Sie an dieser Stelle einen weniger langen Pfad eingeben.

Bei „Ergebnis des Wiederherstellungsvorgangs“ wird der Schlüssel angezeigt.

Das Dell Recovery Utility gibt die Dateien am ausgewählten Speicherort aus und zeigt die genauen Befehle an, die Sie auf dem Recovery HD-Volume ausführen müssen, um das FileVault-Volume zu laden oder zu entschlüsseln.

14 Nachdem diese Dateien generiert wurden, kopieren Sie die Befehlszeichenfolgen, die im abschließenden Dialogfeld „Ergebnis des Wiederherstellungsvorgangs“ angezeigt werden.

15 Wählen Sie eine der folgenden Methoden aus, um einen Neustart über die Recovery HD durchzuführen:

- Drücken und halten Sie gleichzeitig die Taste **Befehl** und **R** (Befehl-R), bevor der Signalton für das Einschalten/den Selbsttest erklingt und während des Computerstarts.

  oder

- Drücken Sie die Taste **Option** und nutzen Sie die Startauswahl zur Auswahl der Recovery-HD.

  Das Dialogfeld *Mac OS X Dienstprogramme* wird angezeigt.

16 Wählen Sie aus dem Extras-Menü die Option **Dienstprogramme > Terminal**.

17 So laden Sie das Volume, damit Sie Dateien aus dem Terminal kopieren oder ein Abbild der Festplatte mit Disk Utility erstellen können: Geben Sie im Terminalmodus den vollständigen Pfad und den Skriptnamen **fv2mount.sh** ein, zum Beispiel:

/Volumes/recoveryFOB/fv2mount.sh

18 Starten Sie den Computer neu.

Wechselmedien

Unterstützte Formate

Medien, die mit FAT32, exFAT oder HFS Plus (Mac OS Extended) und den Partitionsschemata Master Boot Record (MBR) oder GUID Partition Table (GPT) formatiert sind, werden unterstützt. Sie müssen HFS Plus aktivieren.

ANMERKUNG: Mac bietet derzeit keine Unterstützung für das CD/DVD-Brennen für EMS. Der Zugriff auf CD/DVD-Laufwerke ist jedoch nicht gesperrt, selbst wenn die Richtlinie *EMS Zugriff auf Medien sperren, die nicht durch Shield geschützt werden können* ausgewählt ist.

HFS Plus aktivieren

Zum Aktivieren HFS Plus fügen Sie die folgenden Zeilen zur .plist-Datei hinzu.

<key>EMSHFSPlusOptIn</key>

<true/>

ANMERKUNG: Dell empfiehlt, diese Konfiguration vor der Einführung in die Produktionsumgebung zu testen.

HFS Plus bietet keine Unterstützung für:

- Versionskontrolle – vorhandenen Versionskontrolle-Daten werden vom Datenträger entfernt.
- Harte Links – Bei einer Verschlüsselungssuche der Wechselmedien wird die Datei nicht verschlüsselt. Ein Dialogfeld empfiehlt das Auswerfen des Datenträgers.
- Speichermedium mit Time Machine-Sicherungen:
  - Ein Medium, das vom Computer als Time Machine-Sicherungsziel erkannt wird, wird automatisch auf eine Whitelist gesetzt, um weiterhin Sicherungen zuzulassen.
  - Alle anderen Wechselmedien mit Time Machine-Sicherungen werden basierend auf den Richtlinien für nicht bereitgestellte Datenträger und nicht geschützte Datenträger behandelt. Siehe die Richtlinien *EMS Zugriff auf Datenträger ohne Shield* und *EMS Zugriff auf Medien sperren, die nicht durch Shield geschützt werden können*.

    ANMERKUNG: Um einen neuen Datenträger zu nutzen, auf dem noch keine Sicherungen vorhanden sind, muss der Benutzer seine Whitelist-Regel kopieren und sie Ihnen zusenden, um seinen Time Machine-Datenträger für die Whitelist anzugeben. Siehe Whitelist-Regel kopieren.

EMS und Richtlinienaktualisierungen

Auf dem System, auf dem das Medium bereitgestellt (oder wiederhergestellt) wurde, werden die Richtlinien beim Laden auf dem Medium aktualisiert.

Verschlüsselungsausnahmen

Auf externen Medien werden erweiterte Attribute nicht verschlüsselt.

Fehler auf der Registerkarte „Wechselmedien“

- Ersetzen Sie auf einem Computer ohne Shield eine verschlüsselte Datei nicht durch eine entschlüsselte Version der Datei. Dies könnte eine spätere Entschlüsselung verhindern. Möglicherweise wird auch auf der Registerkarte „Wechselmedien“ ein Fehler angezeigt.
- Bei der Entwertung einer Dateiende-Markierung, z. B. wenn eine Datei mit neuem Inhalt außerhalb von EMS überschrieben wird und wenn Sie die Datei anschließend in EMS laden, wird auf der Registerkarte „Wechselmedien“ ein Dateiende-Fehler angezeigt.
- Wenn Sie Dateien konvertieren, muss auf dem Medium mehr Speicherplatz verfügbar sein, als die größte zu konvertierende Datei benötigt. Falls ein gelbes Warndreieck im Statusbereich der Registerkarte „Wechselmedien“ angezeigt wird, klicken Sie darauf. Wenn eine Warnmeldung darauf hinweist, dass *Nicht genügend Speicherplatz* vorhanden ist, gehen Sie wie folgt vor:

  a Notieren Sie sich die Größe des Speicherplatzes, der auf dem Gerät freigegeben werden muss. Der Bericht enthält eine Liste der Dateien und ihre Größe.

  b Leeren Sie den Papierkorb. Während Sie Speicherplatz freigeben, verschlüsselt EMS automatisch zusätzliche Dateien.

  c Wenn Sie Dateien und Ordner löschen, müssen Sie den Papierkorb anschließend erneut leeren, um Speicherplatz freizugeben.

Überprüfungsmeldungen

Überprüfungsmeldungen werden an den Dell Server gesendet.

Endpoint Security Suite Enterprise for Mac finden Sie in der Remote-Verwaltungskonsole unter **Bestückung > Enterprise oder Endpunkte**. Wählen Sie dann die Registerkarte **Advanced Threat Events** aus. Weitere Informationen finden Sie unter *AdminHelp*.

Sammeln von Protokolldateien für Endpoint Security Suite Enterprise

DellLogs.zip enthält die Protokolle für Client Encryption and Advanced Threat Prevention.

Informationen über das Sammeln der Protokolle finden Sie unter http://www.dell.com/support/article/us/en/19/SLN303924.

Deinstallieren von dem Encryption Client for Mac

Die Client-Software kann durch Ausführen der Anwendung **Dell Data Protection deinstallieren** deinstalliert werden. Führen Sie die nachfolgenden Schritte aus, um die Client-Software zu deinstallieren.

ANMERKUNG: Damit Sie die Deinstallationsanwendung ausführen können, muss der Datenträger vollständig entschlüsselt sein.

1 Wenn die Festplatte gegenwärtig verschlüsselt ist, setzen Sie die Richtlinie **Dell Volume Encryption** des Computers in der Remote-Verwaltungskonsole auf **Aus** und bestätigen die Richtlinie.

  Es wird ein Dialogfeld angezeigt, in dem der Zugriff auf die Systemvoreinstellungen und die Steuerung des Computers angefordert werden, damit die Client-Software den Datenträger entschlüsseln kann.

  a Klicken Sie auf **Systemeinstellungen öffnen**.

  Wenn **Verweigern** ausgewählt wurde, kann die Deinstallation und Entschlüsselung nicht fortgesetzt werden.

  b Geben Sie das Administrator-Passwort ein.

2 Nachdem der Datenträger vollständig entschlüsselt wurde, führen Sie (bei entsprechender Aufforderung) einen Neustart des Computers durch.

3 Nachdem der Computer neu gestartet wurde, starten Sie die Anwendung **Dell Data Protection deinstallieren** (diese befindet sich im Ordner „Utilities“ in der Dell-Data-Protection-<version>.dmg des Dell Installationsmediums).

  Der Fortschritt des Deinstallationsvorgangs wird durch verschiedene Meldungen angezeigt.

der Encryption Client for Mac ist jetzt deinstalliert und der Computer kann normal verwendet werden.

Aktivierung als Administrator

Das Client-Tool bietet dem Administrator neue Methoden zum Aktivieren der Client-Software auf einem Mac-Computer sowie zum Untersuchen der Client-Software. Es stehen zwei Aktivierungsmethoden zur Verfügung:

- Aktivierung unter Verwendung von Administrator-Anmeldeinformationen
- Vorübergehende Aktivierung, die den Benutzer emuliert, ohne Fußabdrücke auf dem Computer zu hinterlassen.

Beide Methoden können direkt über eine Shell oder in einem Skript verwendet werden.

ANMERKUNG: Aktivieren Sie die Client-Software über ein und dasselbe Netzwerkkonto auf maximal fünf Computern. Anderenfalls kann es zu Sicherheits- und Leistungsbeeinträchtigungen Ihres Dell Servers kommen.

Voraussetzungen

- Der Encryption Client for Mac müssen auf dem Remote-Computer installiert sein.
- Versuchen Sie die Aktivierung immer zuerst über einen Remote-Standort und dann über die Client-Benutzeroberfläche.

Aktivieren

Verwenden Sie diesen Befehl, um den Client als Administrator zu aktivieren.

Beispiel:

client -a *benutzername@domäne.com kennwort admin admin*

Vorübergehend aktivieren

Verwenden Sie diesen Befehl, um den Client zu aktivieren, ohne Fußabdrücke auf dem Computer zu hinterlassen.

1 Öffnen Sie eine Shell, oder verwenden Sie ein Skript, um die Client-Software zu aktivieren:

client *-bei benutzername@domäne.com kennwort*

2 Mithilfe des Client-Tools können Sie unter anderem Informationen zur Client-Software, zu Richtlinien, zum Datenträgerstatus und zum Benutzerkonto anzeigen. Weitere Informationen zum Client-Hilfsprogramm finden Sie unter Client-Hilfsprogramm.

ANMERKUNG: Nach der Aktivierung stehen die Informationen zu Client-Software, Richtlinien, Datenträgerstatus und Benutzer auch bei den Systemvoreinstellungen in den Dell Data Protection-Voreinstellungen zur Verfügung.

Encryption Client – Referenzdokument

Informationen zum optionalen Firmware-Kennwortschutz

ANMERKUNG: Neuere Mac-Computer bieten keine Unterstützung für den Firmwarepasswortschutz. Der Firmwarepasswortschutz wird auf folgenden Modellen unterstützt:

- iMac10.*
- iMac11.*
- Macmini4.*
- MacBook7.*
- MacBookAir2.*
- MacBookPro7.*
- MacPro5.*
- XServe3.*

Zum Beispiel iMac10.1, iMac11.1 und iMac11.2 unterstützen den optionalen Firmware-Kennwortschutz (durch * angegeben), aber iMac12.1 und höher nicht.

ANMERKUNG: Wenn die Schlüsseloption „FirmwarePasswordMode“ auf optional eingestellt ist, deaktiviert dies nur die Durchsetzung des Firmware-Kennwortschutzes durch den Client. Dadurch wird jedoch ein etwaig vorhandener Firmware-Kennwortschutz nicht entfernt. Sie können jedes bereits vorhandene Firmwarepasswort unter Verwendung des Mac OS X-Firmwarepasswort-Dienstprogramms entfernen.

Wenn Sie beabsichtigen Boot Camp (Anweisungen siehe Anleitung zum Aktivieren von Mac OS X Boot Camp) auf verschlüsselten Mac-Computer zu verwenden, **müssen** Sie den Client so konfigurieren, dass er den Firmware-Kennwortschutz **nicht** verwendet.

Mac-Computer verwenden den Firmwarepasswortschutz zur Verbesserung der Zugriffssicherheit des Computers. Auf Mac-Computern ist der Schutz per Standardeinstellung auf *AUS* gesetzt. Während der Client-Installation können Sie sowohl bei einer neuen Installation als auch bei einem Upgrade von einer früheren Client-Version die bestehende Datei com.dell.ddp.plist bearbeiten, damit der Schlüssel *FirmwarePasswordMode* entweder auf *Erforderlich* oder auf *Optional* eingestellt wird. Die Option *Erforderlich* ist die Standardeinstellung und setzt den Firmware-Kennwortschutz durch, während die Einstellung *Optional* bewirkt, dass der Firmware-Kennwort nicht durchgesetzt wird. Im Anschluss an die Installation bzw. Aktualisierung prüft der Client die modifizierte Installationsdatei com.dell.ddp.plist bei Neustart.

ANMERKUNG: Um zu verhindern, dass Benutzer die Sicherheitseinstellung des Computers ändern, akzeptiert der Client nach der Installation der Client-Software keinerlei Änderungen am Schlüssel FirmwarePasswordMode.

Sie können den Wert dieses Schlüssels nach erfolgter Installation oder Aktualisierung ändern, indem Sie eine Datenträgerentschlüsselung einleiten und die Verschlüsselung anschließend erneut aktivieren.

Wenn Sie möchten, dass der Mac OS X Firmware-Kennwortschutz **erforderlich** ist, befolgen Sie den normalen Installations-/Upgradevorgang für den Client, wie er unter Installation/Upgrade von Encryption Client for Mac beschrieben ist.

Verwendung von Boot Camp

Unterstützung für Mac OS X Boot Camp

ANMERKUNG: Bei Verwendung von Boot Camp kann das Windows-Betriebssystem nicht verschlüsselt werden.

Boot Camp ist ein in Mac OS X integriertes Dienstprogramm, das Sie bei der Installation von Windows auf Mac-Computern mit dualer Startkonfiguration unterstützt. Boot Camp wird mit den folgenden Windows-Betriebssystemen unterstützt:

- Windows 7 und 7 Home Premium, Professional und Ultimate (64-Bit)
- Windows 8 und 8 Pro (64-Bit)
- Windows 8.1 und 8.1 Pro (64-Bit)

ANMERKUNG: Windows 7 unterstützt Boot Camp 4 oder 5.1. Windows 8 und höher unterstützt nur Boot Camp 5.1.

Damit Endpoint Security Suite Enterprise for Windows in Boot Camp auf einem Computer mit Endpoint Security Suite Enterprise for Mac verwendet werden kann, muss das Systemlaufwerk über the Encryption client for Mac entweder mit Dell Client Encryption oder FileVault2 verschlüsselt werden. Konfigurieren Sie zuerst die Client-Installation so, dass sie **nicht** den Firmware Kennwortschutz verwendet. Anweisungen dazu finden Sie unter Installation/Upgrade über Befehlszeile.

ANMERKUNG:

Falls es sich bei Ihrer Windows-Partition um einen EMS-Kandidaten handelt, stellen Sie sicher, dass sie Teil der Positivliste ist, um zu vermeiden, dass sie verschlüsselt wird. Siehe Whitelist-Regel kopieren.

ANMERKUNG:

Stellen Sie sicher, dass Windows installiert ist, bevor Sie Client-Richtlinien bereitstellen, die eine Verschlüsselung zulassen. Nachdem der Client den Verschlüsselungsvorgang aufgenommen hat, sind von Boot Camp verlangte Datenträgerpartitionierungen nicht mehr möglich.

Wiederherstellung von Endpoint Security Suite Enterprise für Windows auf Boot Camp

Um die Endpoint Security Suite Enterprise für Windows, das auf einem Boot Camp-Volume ausgeführt wird, wiederherzustellen, müssen Sie auch auf einem externen Laufwerk ein Boot Camp-Volume erstellen.

Voraussetzungen

- Externes, startfähiges Laufwerk
- Geräte-ID/Eindeutige ID des für die Wiederherstellung vorgesehenen Computers In der Regel finden Sie den für die Wiederherstellung vorgesehenen Computer in der Remote-Verwaltungskonsole. Suchen Sie nach dem Benutzernamen des Besitzers und zeigen Sie die für diesen Benutzer verschlüsselten Geräte an. Das Format für die Eindeutige ID/Geräte-ID lautet „Peter Schmidt's MacBook.Z4291LK58RH“.

Verfahren

1 Erstellen Sie auf einem externen Laufwerk ein Boot Camp-Volume.

   Die hierfür erforderlichen Schritte entsprechen denen für die Erstellung eines Boot Camp-Volumes auf dem lokalen System. Siehe dazu http://www.apple.com/support/bootcamp/.

2 Kopieren Sie aus der Remote-Verwaltungskonsole das Wiederherstellungspaket auf eines der Folgenden:

   - Startfähiges USB-Laufwerk

     oder

   - FAT-Partition auf dem externen Boot Camp-Volume

3 Fahren Sie den Computer mit dem wiederherzustellenden Boot Camp-Volume herunter.

4 Schließen Sie das externe Laufwerk an den Computer an.

   Das Laufwerk enthält das in Schritt 1 erstellte Boot Camp Volume.

5 Zum Starten des Computers vom externen Boot Camp Laufwerk, drücken Sie die Taste **Option** während Sie den Computer einschalten.

6 Wählen Sie das Boot Camp-Volume (Windows) aus, das sich auf dem externen Laufwerk befindet.

7 Klicken Sie mit der rechten Maustaste im USB-Laufwerk oder der FAT-Partition auf das Wiederherstellungspaket (aus Schritt 2) und wählen Sie **Als Administrator ausführen**.

8 Klicken Sie auf **Ja**.

9 Wählen Sie im Dialogfeld „Dell Data Protection-Verschlüsselung“ eine Option aus:

- *Mein System lässt sich nicht starten...* – Wenn der Benutzer das System nicht starten kann, wählen Sie die erste Option aus.

  oder

- *Mein System lässt den Zugriff auf verschlüsselte Daten nicht zu...* – Wenn der Benutzer beim Anmelden am System auf bestimmte verschlüsselte Daten nicht zugreifen kann, wählen Sie die zweite Option aus.

10 Klicken Sie auf **Weiter.**

Der Bildschirm „Sicherungs-/Wiederherstellungsinformationen“ wird angezeigt.

11 Klicken Sie auf **Weiter.**

12 Wählen Sie das wiederherzustellende Boot Camp-Volume aus.

ANMERKUNG: Dies ist nicht das externe Boot Camp-Volume.

13 Klicken Sie auf **Weiter.**

14 Geben Sie das Passwort für die Datei ein.

15 Klicken Sie auf **Weiter.**

16 Klicken Sie auf **Wiederherstellen.**

17 Klicken Sie auf **Fertigstellen**.

18 Wenn Sie dazu aufgefordert werden, neu zu starten, klicken Sie auf **Ja**.

19 Das System wird neu gestartet und Sie können sich bei Windows anmelden.

Anleitung zum Abrufen eines Firmwarepassworts

Selbst wenn der Client-Computer für die Erzwingung des Firmwarepassworts konfiguriert ist, kann dieses für die Wiederherstellung verzichtbar sein. Falls der wiederherzustellende Computer startfähig ist, stellen Sie das Startziel im Bereich für Systemvoreinstellungen bei „Startdatenträger“ ein.

Falls das Firmwarepasswort für die Wiederherstellung erforderlich ist (wenn der Computer nicht startfähig ist und der Firmwarepasswortschutz erzwungen wird), führen Sie die nachfolgenden Schritte aus.

Um ein Firmwarekennwort abzurufen, müssen Sie zuerst das Wiederherstellungspaket abrufen, in dem die Verschlüsselungsschlüssel des Datenträgers enthalten sind.

1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.

2 Klicken Sie im linken Fensterbereich auf **Bestückungen > Endpunkte**

3 Suchen Sie nach dem wiederherzustellenden Gerät.

4 Klicken Sie auf den Gerätenamen, um die Seite mit den Endpunktdetails aufzurufen.

5 Klicken Sie auf die Registerkarte **Details und Aktionen**.

6 Unter dem Punkt „Shield“ klicken Sie auf den Link *Geräte-Wiederherstellungsschlüssel.*

7 Zum Speichern des Wiederherstellungspakets auf dem externen Wiederherstellungsvolume oder Computer, auf dem das Wiederherstellungsprogramm für den Wiederherstellungsvorgang ausgeführt wird, klicken Sie auf **Herunterladen** und klicken Sie auf **Speichern**.

8 Öffnen Sie das Wiederherstellungspaket, um das Firmwarepasswort für den wiederherzustellenden Computer abzurufen. Das Firmwarekennwort befindet sich innerhalb der String-Tags nach dem Schlüssel **FirmwarePassword**.

Beispiel:

<key>FirmwarePassword</key>

<string>Bo$vun8WDn</string>

Client-Hilfsprogramm

Das Client-Tool ist ein Shell-Befehl, der auf einem Mac-Endpunkt ausgeführt wird. Es wird verwendet, um den Client von einem Remote-Standort aus zu aktivieren, oder ein Skript über ein Remote-Verwaltungsdienstprogramm auszuführen. Als Administrator können Sie einen Client aktivieren und folgende Maßnahmen durchführen:

- Als Administrator aktivieren
- Vorübergehend aktivieren
- Informationen vom Mac-Client abrufen

Um das Client-Tool manuell zu verwenden, öffnen Sie eine ssh-Sitzung und geben Sie den gewünschten Befehl in die Befehlszeile ein.

Beispiel:

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at** *DomänenKonto DomänenKennwort*

Geben Sie nur **Client** zur Anzeige der Nutzungsanleitung ein.

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

Tabelle 1. Client-Tool-Befehle

Befehl	Zweck	Syntax	Ergebnisse
Aktivieren	Aktiviert einen Mac-Client auf dem Dell Server, jedoch nicht über die Benutzeroberfläche. Für die Aktivierung müssen Sie einen gültigen Domänenbenutzernamen und ein Passwort eingeben. Mit dem Client-Tool können Sie einen anderen lokalen Benutzer als den, der aktuell angemeldet ist, anmelden und die Domänenanmeldeinformationen mit dem Benutzer verknüpfen.	-a domainAccount domainPassword -a localAccount* domainAccount domainPassword **DomänenKonto** ist das Konto zur Aktivierung über das Client-Hilfsprogramm. **LokalesKonto** ist optional und entspricht dem aktuellen Benutzer, sofern keines angegeben wurde. Der Aktivierungsbefehl hat das folgende Format: client -a <zu aktivierender Benutzer*> <Domänenbenutzer> <Domänenpasswort> Wenn Sie die Richtlinie *Liste der Benutzer ohne Authentifizierung* zum Erstellen von Benutzerklassen verwenden, die nicht für den Dell Server aktiviert werden, können Sie optional das Client-Hilfsprogramm zur Angabe eines anderen lokalen Kontos als dem, mit dem Sie sich angemeldet haben, verwenden. Siehe Richtlinie „Liste der Benutzer ohne Authentifizierung“ in Schritt 3.	0 = Erfolgreich 2 = Aktivierung fehlgeschlagen und Grund des Fehlers 6 = Benutzer nicht gefunden
Vorübergehend aktivieren	Aktiviert einen Mac-Client, ohne einen Fußabdruck zu hinterlassen.	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
Datenträger	Status des Datenträgers abfragen	-d	Der Datenträgerstatus wird angezeigt, einschließlich

Befehl	Zweck	Syntax	Ergebnisse
			Datenträger-ID, Verschlüsselungsstatus und Richtlinien Wenn leere Klammern ausgegeben werden, weist dies darauf hin, dass keine Datenträger verschlüsselt sind.
FileVault-Wiederherstellung ändern	Wiederherstellungsschlüssel für FileVault-Volumes austauschen	-fc deviceId recoveryPassphrase -fc deviceId personalRecoveryKey -fc deviceId pathToKeychain keychainPassword -fc deviceId recoveryFile **ANMERKUNG: deviceId muss eine Logische Volume-UUID sein oder als exakt eine LVUUID aufgelöst sein. Häufig funktioniert ein Bereitstellungspunkt oder devnode.**	0 = Erfolgreich 7 = LVUUID nicht gefunden 10 = Fehlerhafte Anmeldeinformation 11 = Hinterlegung fehlgeschlagen
Richtlinien	Richtlinien des Mac-Clients abfragen	-p	Richtlinien werden angezeigt.
Server	Fragt den Dell Server im Namen des Mac-Clients nach aktualisierten Richtlinien ab **ANMERKUNG: Die Abfrage kann mehrere Minuten in Anspruch nehmen.**	-s	0 = Erfolgreich Alle anderen Werte weisen darauf hin, dass entweder der Dell Server oder die Mac-Client-Software ausgelastet waren oder nicht reagiert haben.
Test	Aktivierungsstatus des Mac-Clients testen	-t localAccount*	0 (domainAccount) = Erfolgreich 1 = Nicht aktiviert 6 = Benutzer nicht gefunden
Benutzer	Benutzerinformationen anfordern	-u localAccount*	Die Kontoinformationen des Benutzers werden angezeigt: 0 (Kontoinformationen) = Erfolgreich 6 = Benutzer nicht gefunden
Version	Version des Mac-Clients anfordern	-v	Die Version des Mac-Clients wird angezeigt. Beispiel: 8.x.x.xxxx

*Das Konto, das das Client-Hilfsprogramm ausführt, wird als lokalesKonto verwendet, es sei denn, ein anderes wurde angegeben.

Plist-Option

Die -plist-Option druckt die Ergebnisse des Befehls, mit dem sie kombiniert ist. Sie folgt nach dem Befehl und muss vor den zugehörigen Argumenten positioniert sein, damit die Ergebnisse als plist gedruckt werden.

Beispiele

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

Zum Abrufen der Richtlinien vom Client und Drucken der Richtlinien.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at -plist** *lokalesKonto DomänenKonto DomänenKennwort*

Zum temporären Aktivieren des Clients und dem Drucken des Ergebnisses.

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

Zum Abfragen des Dell Server für aktualisierte Richtlinien im Namen des Clients und deren Anzeige auf dem Bildschirm.

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

Zum Abrufen des Client-Datenträgerstatus und Drucken.

Globale Rückgabecodes

Kein Fehler 0

Parameterfehler 4

Befehl nicht erkannt 5

Sockelzeitüberschreitung 8

Interner Fehler 9

Aufgaben für die Advanced Threat Prevention

Installieren von Advanced Threat Prevention for Mac

Dieser Abschnitt führt Sie durch die Installation der Advanced Threat Prevention for Mac.

Es gibt zwei Möglichkeiten für die Installation von Advanced Threat Prevention for Mac.

- Interaktive Installation – Mit dieser Methode ist die Installation am einfachsten. Bei dieser Methode sind allerdings keinerlei Anpassungen möglich.
- Installation über Befehlszeile – Dies ist eine fortgeschrittene Installationsmethode, die nur von Administratoren verwendet werden sollte, die sich mit Befehlszeilensyntax auskennen.

Voraussetzungen

Dell empfiehlt, bei der Implementierung der Client-Software die Best Practices für IT zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.

Stellen Sie zunächst fest, ob folgende Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob der Dell Server und seine Komponenten bereits installiert sind.

  Wenn Sie den Dell Server noch nicht installiert haben, folgen Sie den Anweisungen in der entsprechenden nachfolgenden Anleitung.

  Enterprise Server-Installations- und Migrationshandbuch

  Erste Schritte und Installationshandbuch für Enterprise Server – Virtual Edition
- Stellen Sie sicher, dass Sie über den Server-Hostnamen und den Port verfügen. Beides wird für die Installation der Client-Software benötigt.
- Stellen Sie sicher, dass der Zielcomputer über Netzwerkkonnektivität zum Dell Server verfügt.
- Wenn ein Client-Serverzertifikat fehlt oder selbst signiert ist, müssen Sie die Funktion „SSL Certificate Trust“ nur auf der Client-Seite deaktivieren.

Interaktive Installation von Advanced Threat Prevention

Dieser Abschnitt führt Sie durch den Installationsvorgang der Advanced Threat Prevention for Mac.

Interaktive Installation ist die einfachste Methode zum Installieren oder Aktualisieren des Client-Softwarepakets. Bei dieser Methode sind allerdings keinerlei Anpassungen möglich.

Führen Sie die nachfolgenden Schritte aus, um die Client-Software zu installieren. Zur Durchführung dieser Schritte benötigen Sie ein Administratorkonto.

ANMERKUNG: Bevor Sie beginnen, speichern Sie die Arbeit des Benutzers und schließen Sie andere Anwendungen.

1 Laden Sie vom Dell Installationsmedium die Datei **Endpoint-Security-Suite-Enterprise-<version>.dmg**.
Das Paket „Endpoint Security Suite Enterprise for Mac“ wird geöffnet.

2 Doppelklicken Sie auf das Paket-Installationsprogramm **Endpoint Security Suite Enterprise**. Die folgende Meldung wird angezeigt:
Dieses Paket führt ein Programm aus, um festzustellen, ob die Software installiert werden kann.

3 Klicken Sie auf **Weiter**.

4 Lesen Sie die Informationen im Begrüßungsbildschirm und klicken Sie auf **Weiter**.

5 Lesen Sie den Lizenzvertrag, klicken Sie auf **Weiter** und klicken Sie dann auf **Zustimmen**, um die Bedingungen der Lizenzvereinbarung anzunehmen.

6 Geben Sie im Feld **Server-Host** den vollständigen Hostnamen des Dell-Servers ein, mit dem der Zielbenutzer verwaltet werden soll, z. B. server.unternehmen.de.

7 Geben Sie in das Feld **Server-Port** den Wert **8888** ein und klicken Sie auf **Weiter**.
Sobald eine Verbindung hergestellt ist, wechselt die Konnektivitätsanzeige von rot auf grün.

ANMERKUNG: Der Port ist der konfigurierbare Serviceport des Kernservers. Die Standardportnummer ist 8888.

8 Klicken Sie im Installationsfenster auf **Installieren**.

9 Geben Sie bei entsprechender Aufforderung die Anmeldeinformationen für das Administratorkonto ein (wird vom Mac OS X-Installationsprogramm verlangt) und klicken Sie anschließend auf **OK**.

10 Wenn die Installation abgeschlossen ist, klicken Sie auf **Schließen**.
Der Advanced Threat Prevention Client for Mac wurde installiert.

11 Siehe Prüfen der Installation von Advanced Threat Prevention.

Wenn die Installation fehlschlägt, prüfen Sie, ob Sie über ein gültiges Zertifikat auf Ihrem Dell Server verfügen. Siehe Deaktivieren von SSL Trust Certificate für Advanced Threat Prevention.

Interaktive Deinstallation des Advanced Threat Prevention Client

Die Client-Software kann durch Ausführen der Anwendung **Endpoint Security Enterprise deinstallieren** deinstalliert werden. Führen Sie die nachfolgenden Schritte aus, um die Client-Software zu deinstallieren.

1 Laden Sie die Datei Endpoint-Security-Suite-Enterprise-<Version>.dmg.

2 Starten Sie im Ordner „Dienstprogramme“ die Anwendung **Endpoint Security Suite Enterprise deinstallieren**.

3 Klicken Sie auf **Deinstallieren**.

4 Geben Sie bei entsprechender Aufforderung die Anmeldeinformationen für das Administratorkonto ein (wird vom Mac OS X-Installationsprogramm verlangt) und klicken Sie anschließend auf **OK**.
Der Fortschritt des Deinstallationsvorgangs wird durch verschiedene Meldungen angezeigt.

5 Klicken Sie nach der Erfolgsbestätigung auf **OK**.
Advanced Threat Prevention für Mac ist jetzt deinstalliert und der Computer kann normal verwendet werden.

Installation von Advanced Threat Prevention über die Befehlszeile

Führen Sie die folgenden Schritte aus, um den Advanced Threat Prevention Client unter Verwendung der Befehlszeile zu installieren.

1 Laden Sie vom Dell Installationsmedium die Datei „Endpoint-Security-Suite-Enterprise-<version>.dmg “. Das Paket „Endpoint Security Suite Enterprise for Mac“ wird geöffnet.

2 Kopieren Sie aus dem Ordner „Dienstprogramme“ die Datei **com.dell.esse.plist** auf das lokale Laufwerk.

3 Öffnen Sie die .plist-Datei.

4 Bearbeiten Sie die Platzhalterwerte mit dem vollqualifizierten Hostnamen des Dell Servers, der die Verwaltung des Zielbenutzers übernimmt, wie z. B. server.organization.com, und die Portnummer **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>
```

ANMERKUNG: Der Port ist der konfigurierbare Serviceport des Kernservers. Die Standardportnummer ist 8888.

5 Speichern und schließen Sie die Datei.

6 Kopieren Sie für jeden Zielcomputer das Paket Installationsprogramm für **Endpoint Security Suite Enterprise for Mac** in einen temporären Ordner und die geänderten Datei **com.dell.esse.plist** in **/Library/Preferences**.

7 Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeinformationen ein.

8 Öffnen Sie ein Terminalfenster.

9 Führen Sie eine Installation über die Befehlszeile durch, indem Sie den folgenden **Installationsbefehl** ausgeben:

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

ANMERKUNG: Der „-pkg“-Pfad ist der Pfad zum .pkg-Installationsprogramm, der in der .dmg-Datei gefunden werden kann.

10 Drücken Sie die **Eingabetaste.**

11 Siehe Prüfen der ESSE Advanced Threat Prevention Installation.

Deinstallieren von Advanced Threat Prevention for Mac über Befehlszeile

Führen Sie die folgenden Schritte aus, um die Client-Software unter Verwendung der Befehlszeile zu deinstallieren.

1 Öffnen Sie ein Terminalfenster.

2 Führen Sie eine Deinstallation über die Befehlszeile durch, indem Sie den folgenden **Deinstallationsbefehl** verwenden:

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

ANMERKUNG: Stellen Sie sicher, dass der --noui Switch am Ende des Befehls enthalten ist.

3 Drücken Sie die **Eingabetaste.**

Advanced Threat Prevention für Mac ist jetzt deinstalliert und der Computer kann normal verwendet werden.

Advanced Threat Prevention for Mac – Fehlerbehebung

Deaktivieren von SSL Trust Certificate für Advanced Threat Prevention

Wenn ein Client-Serverzertifikat fehlt oder selbst signiert ist, müssen Sie die Funktion „SSL Certificate Trust“ nur auf der Client-Seite deaktivieren.

1 Starten Sie auf dem Client ein Terminalfenster.

2 Geben Sie den Pfad zur DellCSFConfig.App ein:

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

3 Führen Sie die DellCSFConfig.App aus:

```
sudo ./DellCSFConfig
```

Das Folgende stellt die Standardeinstellungen dar:

```
Current Settings:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False
```

4 Geben Sie **-help** ein, um eine Liste mit den Optionen anzuzeigen.

5 Zum Deaktivieren von SSL Certificate Trust auf dem Client ändern Sie `DisableSSLCertTrust` in **True**.

Hinzufügen von XML-Bestandsaufnahme und Richtlinienänderungen zu den Protokollordnern

So fügen Sie die inventory.xml oder polocies.xml-Dateien dem Protokollordner hinzu:

1 Führen Sie die DellCSFConfig.app wie oben beschrieben aus.

2 Ändern Sie DumpXmlInventory in **True**.

3 Ändern Sie DumpPolicies in **True**.
Die Richtliniendateien werden nur ausgegeben, wenn eine Richtlinienänderung aufgetreten ist.

4 Zum Anzeigen der Protokolldateien inventory.xml und policies.xml gehen Sie zu **/Library/Application\ Support/Dell/Dell\ Data\ Protection/**.

Prüfen der Advanced Threat Prevention Installation

Optional können Sie die Installation überprüfen.

1 Bestätigen Sie, dass das Dell Advanced Threat Prevention Symbol mit einem grünen Zeichen  in der Befehlsleiste aufgeführt wird.

2 Wenn ein Ausrufezeichen am Symbol angezeigt wird, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Details anzeigen**. Dies kann bedeuten, dass Sie nicht registriert sind.

Auf Updates prüfen – Sucht nach Updates für die Advanced Threat Prevention Engine, nicht nach Updates der Dell Server-Richtlinie.

Info – Umfasst Folgendes:

- Version
- Richtlinie – [online] zeigt die Server-basierte Richtlinie an und [offline] zeigt die Air Gap oder offline-basierte Richtlinie an
- Seriennummer – Verwenden Sie diese beim technischen Support. Dies ist die eindeutige Kennung für die Installation.

3 Im Ordner „/Anwendungen“ wird der Dell Advanced Threat Prevention Ordner erstellt.

Sammeln von Protokolldateien für Endpoint Security Suite Enterprise

DellLogs.zip enthält die Protokolle für Client Encryption and Advanced Threat Prevention.

Informationen über das Sammeln der Protokolle finden Sie unter http://www.dell.com/support/article/us/en/19/SLN303924.

Details zu Advanced Threat Prevention anzeigen

Nachdem der Advanced Threat Prevention-Client auf einem Endpunktcomputer installiert wurde, wird dieser durch den Dell-Server als Agent erkannt.

Klicken Sie mit der rechten Maustaste auf das Symbol für Advanced Threat Prevention  in der Befehlsleiste und wählen Sie **Details anzeigen**. Der Bildschirm „Details zu Advanced Threat Prevention“ verfügt über die folgenden Registerkarten.

Registerkarte „Bedrohungen“

Die Registerkarte „Bedrohungen“ zeigt alle auf dem Gerät erkannten Bedrohungen sowie die durchgeführten Maßnahmen an. „Bedrohungen“ sind eine Kategorie von Ereignissen, die als potenziell unsichere Dateien oder Programme neu erfasst wurden und eine geführte Fehlerbehebung erfordern.

Die Spalte „Kategorie“ kann Folgendes enthalten.

- **Unsicher** – Eine verdächtige Datei, die wahrscheinlich Malware enthält
- **Anormal** – Eine verdächtige Datei, die Malware enthalten könnte
- **In Quarantäne** – Eine Datei, die vom ursprünglichen Speicherort in den Quarantäne-Ordner verschoben und daran gehindert wurde, auf dem Gerät ausgeführt zu werden.
- **Freigegeben** – Eine Datei, die auf dem Gerät ausgeführt werden darf.
- **Zugelassen** – Eine Datei, die innerhalb der Organisation zugelassen wurde. Zu den zugelassenen Dateien gehören Dateien mit dem Status „Freigegeben“, Dateien, die zur Liste „Sicher“ hinzugefügt wurden und Dateien, die aus dem Ordner „Quarantäne“ auf dem Gerät gelöscht wurden.

Weitere Informationen zur Klassifizierung von Bedrohungen durch die Advanced Threat Prevention finden Sie in der *AdminHelp*, die in der Dell Server Remote-Verwaltungskonsole verfügbar ist.

Registerkarte „Exploits“

Unter der Registerkarte „Exploits“ werden Exploits aufgelistet, die als Bedrohungen eingestuft wurden.

Die Dell Server-Richtlinien bestimmen die Maßnahmen bei einem Feststellen eines Exploits unternommen werden:

- **Ignorieren** – Es werden keine Maßnahmen zum Schutz vor identifizierten Speicherangriffen durchgeführt.
- **Warnung** – Der Speicherangriff wird erfasst und an den Dell Server gemeldet.
- **Blockieren** – Der Prozessaufruf wird blockiert, falls eine Anwendung versucht, einen Prozess zur Durchführung eines Arbeitsspeicherangriffs aufzurufen. Die Anwendung, die den Aufruf initiiert hat, darf weiterhin ausgeführt werden.
- **Beenden** – Der Prozessaufruf wird blockiert, falls eine Anwendung versucht, einen Prozess zur Durchführung eines Arbeitsspeicherangriffs aufzurufen. Die Anwendung, die den Aufruf durchgeführt hat, wird beendet.

Die folgenden Exploittypen werden erkannt:

- Stapeldrehung
- Stapelschutz
- Scanner-Speicher-Suche
- Schädliche Nutzlast

Weitere Informationen über Exploit-Richtlinien finden Sie in der *AdminHelp*, die in der Dell Server Remote-Verwaltungskonsole verfügbar ist.

Registerkarte „Ereignisse“

ANMERKUNG: Ein Ereignis ist nicht unbedingt eine Bedrohung. Ein Ereignis wird generiert, wenn eine erkannte Datei oder ein erkanntes Programm in Quarantäne verschoben, sicher gelistet oder nicht angewendet wird.

Auf der Registerkarte „Ereignisse“ werden alle Bedrohungs-Ereignisse angezeigt, die auf dem Gerät auftreten. Sie werden nach dem Ereignistyp geordnet, der ihnen durch die Advanced Threat Prevention zugewiesen worden ist. Die Daten werden gelöscht, wenn das System neu gestartet wurde.

Beispiele für Ereignistypen umfassen:

Bedrohung gefunden

Bedrohung entfernt

Unter Quarantäne gestellte Bedrohungen

Bedrohung freigegeben

Bedrohung geändert

Bereitstellung eines Mandanten für Advanced Threat Prevention

Wenn Ihr Unternehmen Advanced Threat Prevention verwendet, muss ein Mandant auf dem Dell-Server bereitgestellt werden, bevor die Durchsetzung der Advanced Threat Prevention-Richtlinien aktiv wird.

Voraussetzungen

- Muss durch einen Administrator mit der Systemadministratorrolle durchgeführt werden.
- Muss über eine Verbindung mit dem Internet verfügen, um auf dem Dell Server bereitgestellt zu werden.
- Muss über eine Verbindung mit dem Internet auf dem Client verfügen, um die Online-Dienst-Integration von Advanced Threat Prevention in der Remote-Verwaltungskonsole anzuzeigen.
- Die Bereitstellung basiert auf einem Token, das im Rahmen der Bereitstellung aus einem Zertifikat generiert wird.
- Die Lizenzen für Advanced Threat Prevention müssen auf dem Dell Server vorhanden sein.

Bereitstellen eines Mandanten

1. Melden Sie sich bei der Remote Management Console an, und wechseln Sie zu **Dienstverwaltung**.
2. Klicken Sie auf **Advanced Threat Protection-Dienst einrichten**. Importieren Sie Ihre ATP-Lizenzen, falls an dieser Stelle ein Fehler auftritt.
3. Das geführte Setup beginnt, sobald die Lizenzen importiert wurden. Klicken Sie zum Starten auf **Weiter**.
4. Lesen und akzeptieren Sie die Endbenutzerlizenzvereinbarung (EULA) (das Kontrollkästchen ist standardmäßig **deaktiviert**), und klicken Sie auf **Weiter**.
5. Geben Sie für die Bereitstellung des Mandanten Anmeldeinformationen auf dem DDP-Server ein. Klicken Sie auf **Weiter**. *Die Bereitstellung eines vorhandenen Mandanten der Marke Cylance wird nicht unterstützt.*
6. Laden Sie das Zertifikat herunter. Dies ist erforderlich, um bei einem Notfallszenario auf dem DDP-Server eine Wiederherstellung durchführen zu können. Dieses Zertifikat wird nicht automatisch über den v9.2 „Upgrader“ gesichert. Sichern Sie das Zertifikat an einem sicheren Speicherplatz auf einem anderen Computer. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie das Zertifikat gesichert haben, und klicken Sie auf **Weiter**.
7. Die Einrichtung ist abgeschlossen. Klicken Sie auf **OK**.

Konfigurieren der automatischen Aktualisierung des Advanced Threat Prevention-Agenten

Sie können sich in der Dell Server Remote-Verwaltungskonsole anmelden, um automatische Aktualisierungen für den Advanced Threat Prevention-Agenten zu erhalten. Durch die Anmeldung für den Empfang automatischer Agent-Aktualisierungen können Clients Aktualisierungen automatisch herunterladen und über den Advanced Threat Prevention-Server anwenden. Aktualisierungen werden monatlich herausgegeben.

ANMERKUNG: Die automatischen Aktualisierungen des Agenten werden ab Dell Server Version 9.4.1 unterstützt.

Automatische Aktualisierungen für den Agenten empfangen

So melden Sie sich an, um automatische Agent-Aktualisierungen zu erhalten:

1 Klicken Sie im linken Bereich der Remote Management-Konsole auf **Verwaltung** > **Dienstverwaltung**.

2 Auf der Registerkarte **Advanced Threats** unter „Automatische Agent-Aktualisierung“ klicken Sie auf die Schaltfläche **Ein** und dann auf die Schaltfläche **Einstellungen speichern**.

Es kann einige Minuten dauern, bis die Bestückung mit Informationen abgeschlossen ist und die automatischen Aktualisierungen angezeigt werden.

Beenden des Empfangs von automatischen Agent-Aktualisierungen

So beenden Sie den Empfang von automatischen Agent-Aktualisierungen:

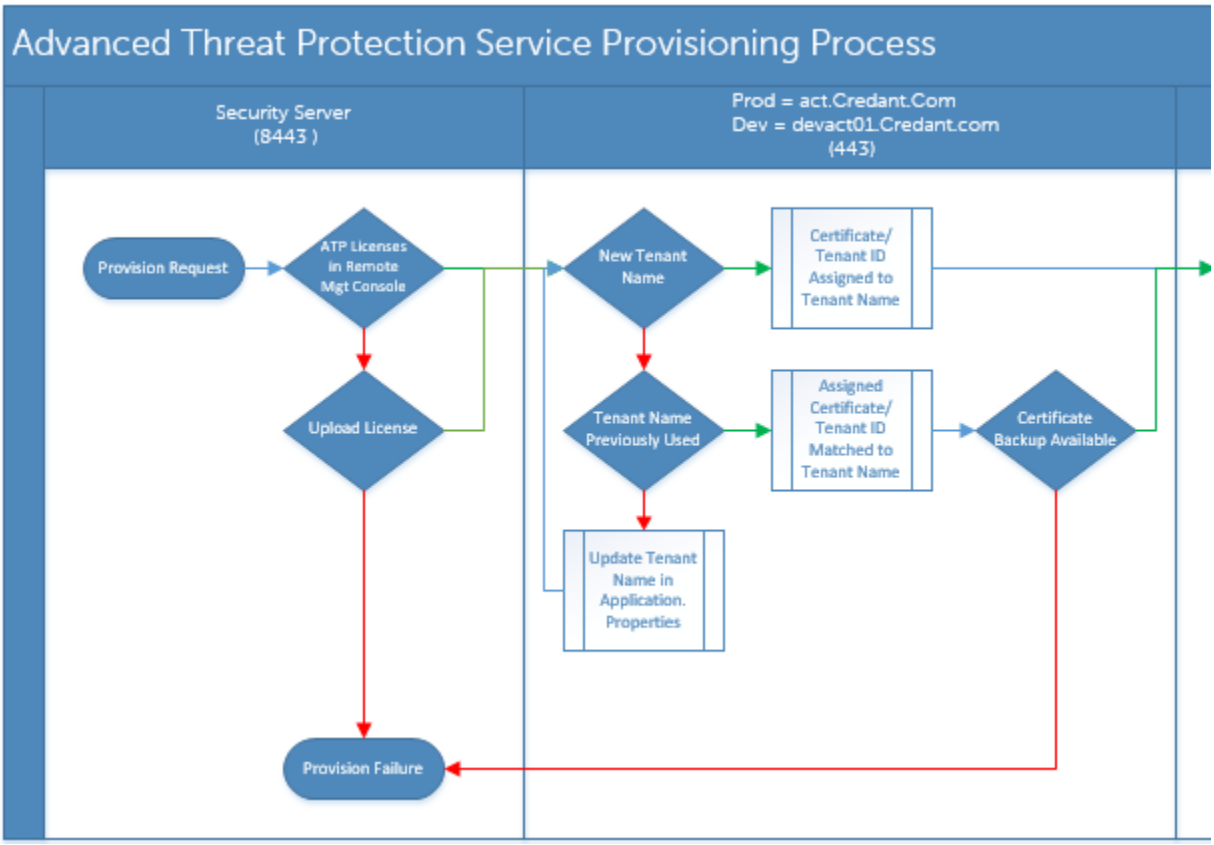
1 Klicken Sie im linken Bereich der Remote Management-Konsole auf **Verwaltung** > **Dienstverwaltung**.

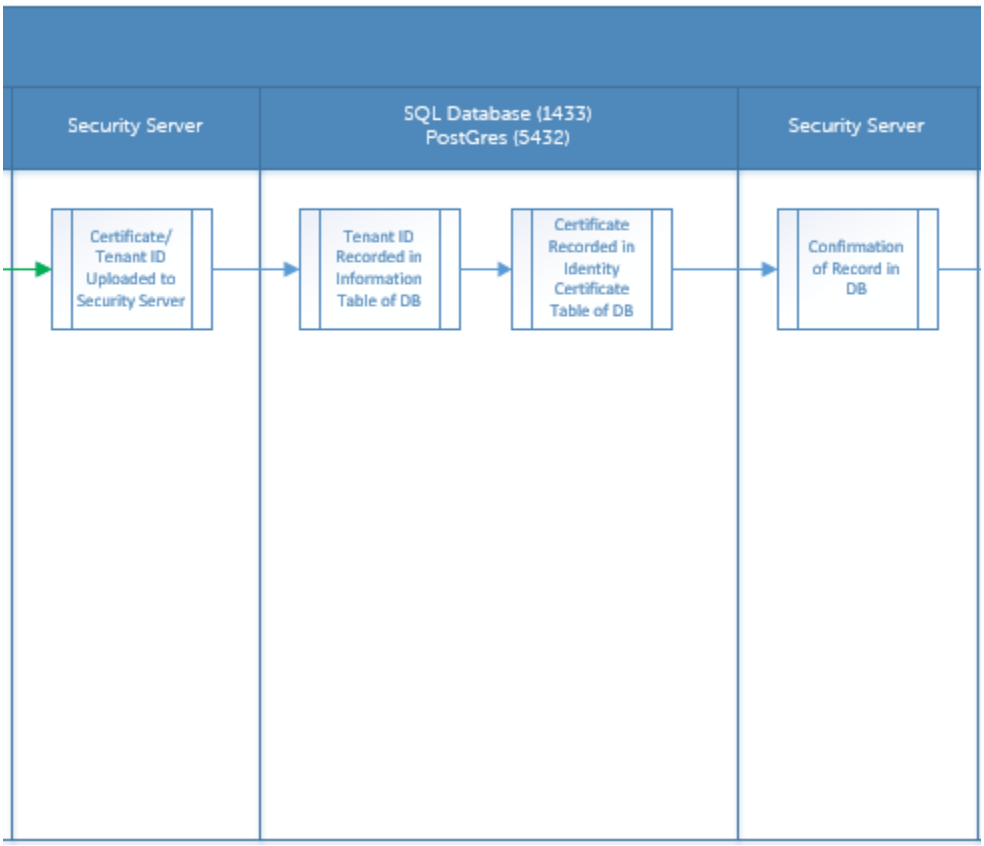
2 Auf der Registerkarte **Advanced Threats** unter „Automatische Agent-Aktualisierung“ klicken Sie auf die Schaltfläche **Aus** und dann auf die Schaltfläche **Einstellungen speichern**.

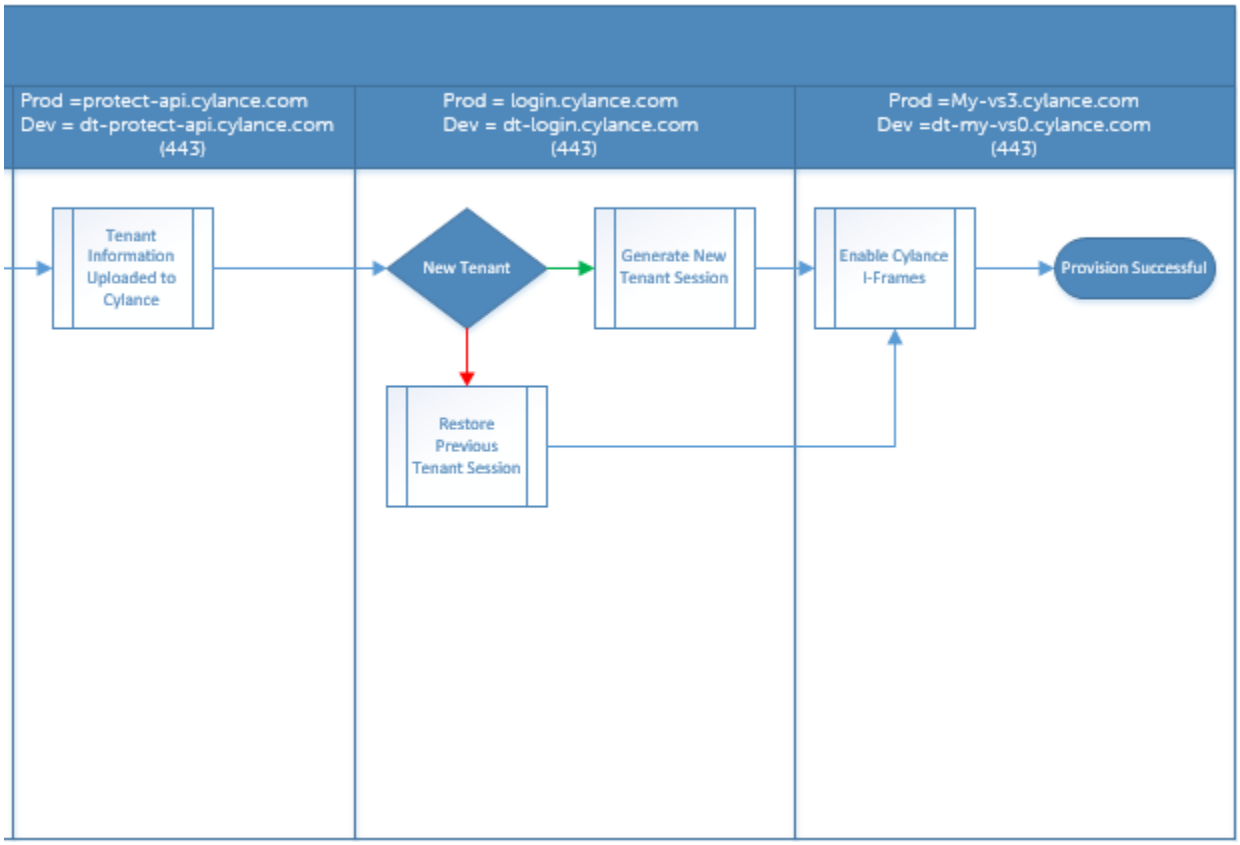
Advanced Threat Prevention Client – Fehlerbehebung

Bereitstellung von Advanced Threat Prevention und Agentenkommunikation

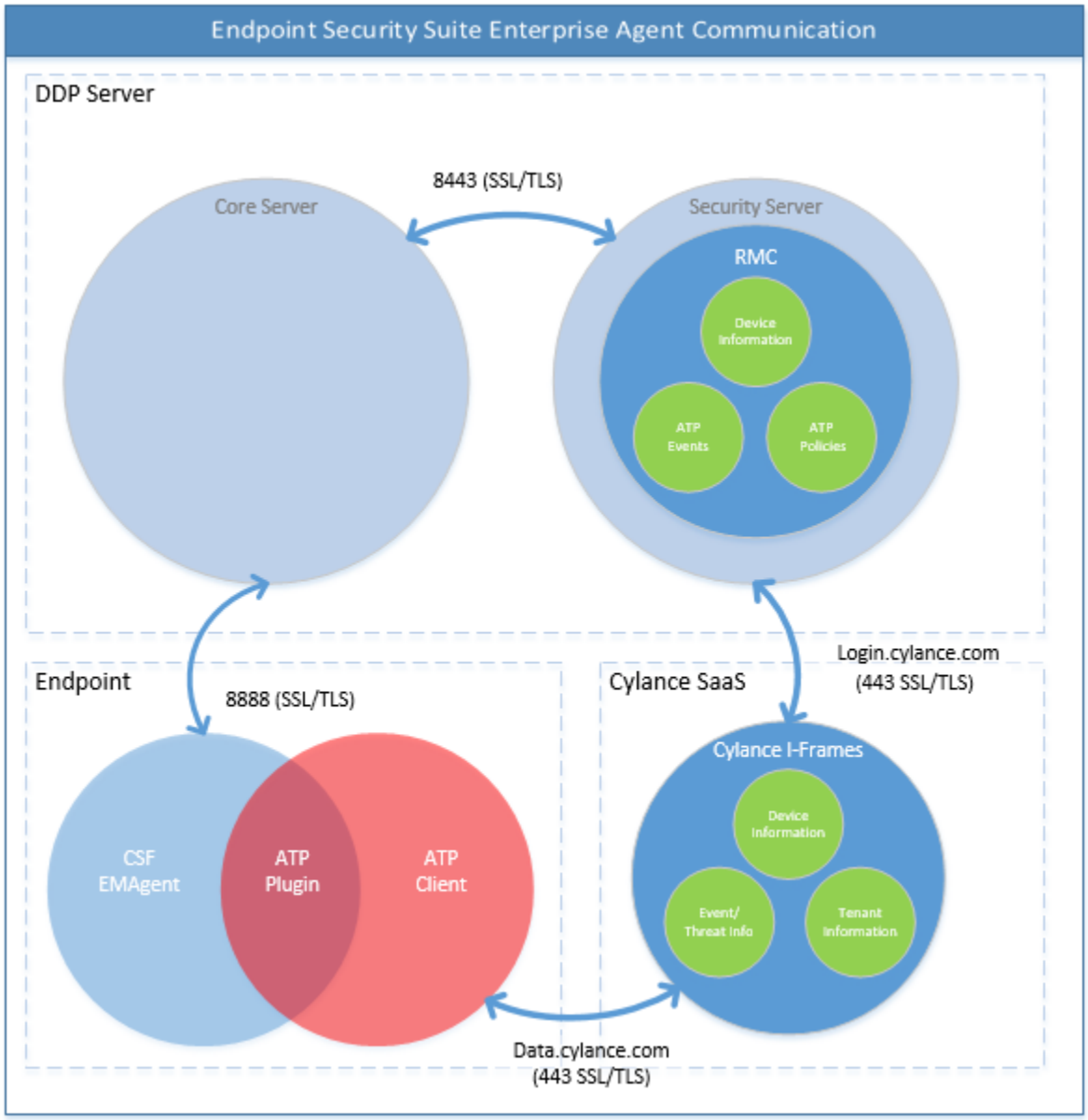
Die folgenden Diagramme veranschaulichen die Bereitstellung des Advanced Threat Prevention Dienstes.


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



Das folgende Diagramm veranschaulicht die Agentenkommunikation für 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

Glossar

Sicherheitsserver – wird für Aktivierungen der Client-Verschlüsselung verwendet.

Richtlinien-Proxy – wird verwendet, um Richtlinien an die Endpoint Security Enterprise for Mac Client-Software zu verteilen.

Remote-Verwaltungskonsole – Die Verwaltungskonsole für die gesamte Enterprise Bereitstellung.

Shield – Ab und an kann in der Dokumentation und auf der Client-Benutzeroberfläche der Begriff „Shield“ auftauchen. „Shield“ steht für die Client-Software.