


Dell Endpoint Security Suite Enterprise for Mac

Administratorhandbuch v2.9

Hinweise, Vorsichtshinweise und Warnungen

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

 **VORSICHT:** Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

 **WARNUNG:** Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

© 2012-2021 Dell Inc. All rights reserved. Registered trademarks and trademarks used in the Dell Encryption and Endpoint Security Suite Enterprise suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

Kapitel 1: Einleitung	5
Übersicht.....	5
FileVault-Verschlüsselung.....	5
Kontaktieren des Dell ProSupports.....	5
Kapitel 2: Anforderungen	6
Encryption-Client.....	6
Encryption-Client-Hardware.....	6
Encryption Client Software.....	6
Advanced Threat Prevention.....	7
Advanced Threat Prevention – Hardware.....	7
Advanced Threat Prevention – Software.....	8
Advanced Threat Prevention – Ports.....	8
Kompatibilität.....	8
Kapitel 3: Aufgaben für den Encryption Client	11
Installation/Upgrade von dem Encryption Client.....	11
Interaktive Installation oder Upgrade.....	12
Installation/Upgrade über Befehlszeile.....	13
Aktivieren des vollständigen Festplattenzugriffs für Wechselmedien.....	15
Aktivieren von Encryption Client.....	16
Verschlüsselungsrichtlinie und Status anzeigen.....	17
Anzeigen von Richtlinie und Status in der Verwaltungskonsole.....	20
Systemlaufwerke.....	20
Verschlüsselung aktivieren.....	20
Verschlüsselungsvorgang.....	21
Austauschen der FileVault-Wiederherstellungsschlüssel.....	24
Nutzerfreundlichkeit.....	24
Wiederherstellung.....	26
Volume laden.....	26
FileVault-Wiederherstellung.....	27
Wechselmedien.....	31
Unterstützte Formate.....	31
Encryption External Media und Richtlinienaktualisierung.....	31
Verschlüsselungsausnahmen.....	31
Fehler auf der Registerkarte „Wechselmedien“.....	32
Überprüfungsmeldungen.....	32
Sammeln von Protokolldateien für Endpoint Security Suite Enterprise.....	32
Deinstallieren von dem Encryption Client for Mac.....	32
Aktivierung als Administrator.....	33
Aktivieren.....	33
Vorübergehend aktivieren.....	33
Encryption Client – Referenzdokument.....	34
Informationen zum optionalen Firmware-Kennwortschutz.....	34

Verwendung von Boot Camp.....	35
Anleitung zum Abrufen eines Firmwarepassworts.....	36
Client-Hilfsprogramm.....	37
Kapitel 4: Aufgaben.....	40
Installieren von Advanced Threat Prevention for Mac.....	40
Interaktive Installation von Advanced Threat Prevention.....	40
Installation von Advanced Threat Prevention über die Befehlszeile.....	43
Advanced Threat Prevention for Mac – Fehlerbehebung.....	44
Prüfen der Advanced Threat Prevention Installation.....	45
Sammeln von Protokolldateien für Endpoint Security Suite Enterprise.....	46
Details zu Advanced Threat Prevention anzeigen.....	46
Bereitstellung eines Mandanten.....	48
Bereitstellung eines Mandanten.....	49
Konfigurieren der automatischen Aktualisierung des Advanced Threat Prevention Agenten.....	49
Advanced Threat Prevention – Fehlerbehebung.....	49
Kapitel 5: Glossar.....	52

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](#)
- [FileVault-Verschlüsselung](#)
- [Kontaktieren des Dell ProSupports](#)

Übersicht

Die Endpoint Security Suite Enterprise for Mac bietet Advanced Threat Prevention auf der Betriebssystem- und der Speicherebene sowie Verschlüsselung. Alles wird dabei zentral über den Dell 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 – eine Software-Suite für Client-Verschlüsselung von Daten und Advanced Threat Prevention.
- [Richtlinien-Proxy](#) – wird zum Verteilen von Richtlinien verwendet
- [Sicherheitsserver](#) – wird für Aktivierungen der Client-Verschlüsselungssoftware verwendet
- Security Management Server oder Security Management Server Virtual – bieten 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 werden muss (wenn z. B. bei Verwendung von Security Management Server Virtual 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 den Encryption Client und eine für die Advanced Threat Prevention. Sie können beide oder nur eine davon installieren.

FileVault-Verschlüsselung

Dell Encryption kann die vollständige Datenträgerverschlüsselung mit Mac FileVault verwalten. Die Richtlinie für die *Dell Volume-Verschlüsselung* muss auf **Ein** festgelegt werden, damit die Verschlüsselung durchgeführt werden kann und andere Richtlinieneinstellungen funktionieren. Weitere Informationen zu zusätzlichen Richtlinien finden Sie unter *AdminHelp*.

Nur die FileVault-Verschlüsselung wird unterstützt, die von Endpoint Security Suite Enterprise verwaltet wird. Wenn auf einem Computer die Richtlinien für *Dell Volume-Verschlüsselung* auf **Ein** und *Verschlüsseln mit FileVault für Mac* auf **Aus** eingestellt sind, wird eine Meldung über einen Richtlinienkonflikt auf dem Verschlüsselungs-Client angezeigt. Der Administrator muss beide Richtlinien auf **An** einrichten.

Kontaktieren des Dell ProSupports

Telefonischen Support 24x7 für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell 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](#).

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](#)
- [Advanced Threat Prevention](#)

Encryption-Client

Encryption-Client-Hardware

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


Hardware
<ul style="list-style-type: none"> • 30 MB freier Speicherplatz
<ul style="list-style-type: none"> • Netzwerkschnittstellenkarte 10/100/1000 oder Wi-Fi
<ul style="list-style-type: none"> • Der Systemdatenträger muss mit dem Partitionsschema GUID Partition Table (GPT) partitioniert sein und kann formatiert werden mit: <ul style="list-style-type: none"> ○ Mac OS X Extended Journaled (HFS+) – wird in den Core-Speicher konvertiert, um FileVault anzuwenden. ○ Apple File System (APFS)

Encryption Client Software

Die folgende Tabelle enthält detaillierte Informationen über die unterstützte Software.

Betriebssysteme (64-Bit-Kernel)
<ul style="list-style-type: none"> • macOS High Sierra 10.13.6
<ul style="list-style-type: none"> • macOS Mojave 10.14.5 - 10.14.6
<ul style="list-style-type: none"> • macOS Catalina 10.15.5 – 10.15.6

 **ANMERKUNG:** Dell Encryption bietet keine Unterstützung für macOS Big Sur.

 **ANMERKUNG:**
Falls Sie ein Netzwerk-Nutzerkonto für die Authentifizierung verwenden möchten, muss dieses als mobiles Konto eingerichtet sein, damit die FileVault 2-Verwaltung vollständig konfiguriert werden kann.

Verschlüsselte Datenträger

Die folgende Tabelle enthält Informationen zu den unterstützten Betriebssystemen für den Zugriff auf von Dell verschlüsselte externe Medien.

 **ANMERKUNG:**

Encryption External Media unterstützt Medien, die mit:

- FAT32
- exFAT
- HFS Plus (Mac OS Extended) formatierte Medien mit Partitionsschemata Master Boot Record (MBR) oder GUID-Partitionstabelle (GPT). Siehe dazu [Aktivieren von HFS Plus](#).

i ANMERKUNG:

Um Encryption External Media zu hosten, müssen 55 MB verfügbar sein und auf dem Wechselspeichermedium muss zusätzlich freier Speicherplatz vorhanden sein, dessen Größe der größten zu verschlüsselnden Datei entspricht.

Unterstützte Windows-Betriebssysteme (32-Bit und 64-Bit) für den Zugriff auf verschlüsselte Medien
<ul style="list-style-type: none">• Microsoft Windows 7 SP1<ul style="list-style-type: none">– Enterprise– Professional– Ultimate
<ul style="list-style-type: none">• Microsoft Windows 8.1 - Windows 8.1 Update 1<ul style="list-style-type: none">– Enterprise– Professional
<ul style="list-style-type: none">• Microsoft Windows 10<ul style="list-style-type: none">– Bildungseinrichtungen– Enterprise– Pro v1607 (Anniversary Update/Redstone 1) bis v1909 (November 2019 Update/19H2)
Mac-Betriebssysteme (64-Bit-Kernel) mit Unterstützung für den Zugriff auf verschlüsselte Medien
<ul style="list-style-type: none">• macOS High Sierra 10.13.6<ul style="list-style-type: none">i ANMERKUNG: Für Encryption External Media auf macOS High Sierra 10.14.x ist Encryption Enterprise v8.16 oder höher erforderlich.
<ul style="list-style-type: none">• macOS Mojave 10.14.5 - 10.14.6
<ul style="list-style-type: none">• macOS Catalina 10.15.5 – 10.15.6

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
<ul style="list-style-type: none">• 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)	
<ul style="list-style-type: none"> Mac OS X Mavericks 10.9.5 Mac OS X Yosemite 10.10.5 macOS Sierra 10.12.6 <p>ANMERKUNG: Mac OS X Mavericks 10.9.5, Mac OS X Yosemite 10.10.5 und macOS Sierra 10.12 werden nur mit Advanced Threat Prevention und nicht mit dem Encryption Client unterstützt.</p>	
<ul style="list-style-type: none"> macOS High Sierra 10.13.6 <p>ANMERKUNG: Beziehen Sie sich auf Encryption Client Software für bestimmte macOS High Sierra Versionen, die vom Encryption Client unterstützt werden.</p>	
<ul style="list-style-type: none"> macOS Mojave 10.14.5 - 10.14.6 <p>ANMERKUNG: Sie können den ATP-Agenten auf macOS Mojave installieren, aber Speicherschutz- und Skriptsteuerungsfunktionen werden automatisch deaktiviert und derzeit nicht unterstützt.</p>	
<ul style="list-style-type: none"> macOS Catalina 10.15.3 – 10.15.4 	

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

Kompatibilität

Die folgende Tabelle zeigt die Kompatibilität mit Windows, Mac und Linux.

Nicht verfügbar – Die Technologie gilt nicht für diese Plattform.

Leeres Feld – Die Richtlinie wird nicht mit Endpoint Security Suite Enterprise unterstützt.

Funktionen	Richtlinien	Windows	macOS	Linux	
Dateimaßnahmen					
	Automatische Quarantäne (Unsicher)	x	x	x	

Funktionen	Richtlinien	Windows	macOS	Linux	
	Automatische Quarantäne (Anormal)	x	x	x	
	Automatisch hochladen	x	x	x	
	Richtlinie „Sichere Liste“	x	x	x	
Speichermaßnahmen					
	Speicherschutz	x	x	x	
Ausnutzung					
	Stapeldrehung	x	x	x	
	Stapelschutz	x	x	x	
	Code überschreiben	x	k. A.		
	RAM-Scraping	x	k. A.		
	Schädliche Nutzlast	x			
Vorgangsinjektion					
	Remote-Zuweisung von Speicher	x	x	k. A.	
	Remote-Zuordnung von Speicher	x	x	k. A.	
	Remote Schreiben in Speicher	x	x	k. A.	
	Remote Schreiben von PE in Speicher	x	k. A.	k. A.	
	Code remote überschreiben	x	k. A.		
	Zuordnung von Speicher remote aufheben	x	k. A.		
	Remote-Thread-Erstellung	x	x		
	Remote-APC geplant	x	k. A.	k. A.	
	DYLD-Injektion		x	x	
Eskalation					
	LSASS lesen	x	k. A.	k. A.	
	Null-Zuweisung	x	x		
Schutzeinstellungen					
	Ausführungssteuerung	x	x	x	
	Herunterfahren des Dienstes vom Gerät verhindern	x	x		
	Unsichere Prozesse und ihre Unterprozesse, die gerade ausgeführt werden, beenden	x	x	x	
	Entdeckung einer Hintergrundsbedrohung	x	x	x	

Funktionen	Richtlinien	Windows	macOS	Linux	
	Nach neuen Dateien Ausschau halten	x	x	x	
	Maximale Größe der zu scannenden Archivdatei	x	x	x	
	Bestimmte Ordner ausschließen	x	x	x	
	Dateimuster kopieren	x			
Anwendungssteuerung					
	Fenster ändern	x		x	
	Ordnerausschlüsse	x			
Agenten-Einstellungen					
	Automatisches Hochladen von Protokolldateien aktivieren	x	x	x	
	Desktop-Benachrichtigungen aktivieren	x			
Skriptsteuerung					
	Aktives Skript	x			
	Powershell	x			
	Office-Makros	x		k. A.	
	Powershell-Konsolennutzung blockieren	x			
	Skripte in diesen Ordnern (und Unterordnern) genehmigen	x			
	Protokolliergrad	x			
	Selbstschutzebene	x			
	Automatische Aktualisierung	x			
	Erkennung durchführen (von Agent-UI)	x			
	In Quarantäne löschen (Agent-UI und Konsolen-UI)	x			
	Getrennter Modus	x		x	
	Detaillierte Bedrohungsdaten	x			
	Zertifizierte sichere Liste	x	x	k. A.	
	Malware-Muster kopieren	x	x	x	
	Proxy-Einstellungen	x	x	x	
	Manuelle Richtlinienüberprüfung (Agent-UI)	x	x		

Aufgaben für den Encryption Client

Themen:

- Installation/Upgrade von dem Encryption Client
- Aktivieren von Encryption Client
- Verschlüsselungsrichtlinie und Status anzeigen
- Systemlaufwerke
- Wiederherstellung
- Wechselmedien
- Sammeln von Protokolldateien für Endpoint Security Suite Enterprise
- Deinstallieren von dem Encryption Client for Mac
- Aktivierung als Administrator
- Encryption Client – Referenzdokument

Installation/Upgrade von dem Encryption Client

Dieser Abschnitt führt Sie durch den Installations-/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. Zur Unterstützung so vieler Kunden wie möglich ist eine Änderung der Datei `com.dell.ddp.plist` zur Unterstützung dieser Fälle erlaubt. Das Testen dieser Versionen beginnt, sobald Apple eine neue Version veröffentlicht, um sicherzustellen, dass sie kompatibel sind mit dem Verschlüsselungs-Client für Mac.

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.

Security Management Server Installation and Migration Guide (Installations- und Migrationshandbuch für Security Management Server)

Security Management Server Virtual Quick Start Guide and Installation Guide (Schnellanleitung und Installationshandbuch für Security Management Server Virtual)

- Achten Sie darauf, die Sicherheitsserver- und Richtlinien-Proxy-URL zur Hand zu haben. Beide 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.

Bevor Sie Verschlüsselungsrichtlinien festlegen, muss die *Dell Richtlinie für Volume-Verschlüsselung aktiviert sein*. Stellen Sie sicher, dass Sie die Richtlinien *Verschlüsseln mit FileVault for Mac* und *Zur Verschlüsselung vorgesehene Volumes* verstehen.

Weitere Informationen über Verschlüsselungsrichtlinien finden Sie unter [Mac-Verschlüsselung > Dell Volume-Verschlüsselung](#).

Interaktive Installation oder Upgrade

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

Interaktive Installation

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-Encryption-Enterprise-<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.
6. Geben Sie in das Feld *Domänenadresse* den vollqualifizierten Domännennamen für die Zielbenutzer ein, wie z. B. *abteilung.unternehmen.de*.
7. Geben Sie in das Feld *Anzeigenname (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. Dieser Name sorgt für übereinstimmende Domännennamen 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 Ports 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 der aktuellen Systemfestplatte zeigt einen grünen Pfeil, der auf die Festplatte 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. (Die Anwendung „MacOS X Installer“ erfordert Anmeldedaten.)
14. Klicken Sie 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.

15. Klicken Sie auf **Mit der Installation fortfahren**. Der Installationsvorgang beginnt.
16. Wenn die Installation abgeschlossen wurde, klicken Sie auf **Neustarten**.
17. Da es sich hier um eine neue Installation von Endpoint Security Suite Enterprise handelt, wird das Dialogfeld *Systemerweiterung blockiert* angezeigt.

Bei text-Zustimmung werden eines oder beide dieser Dialogfenster angezeigt.

Systemerweiterung blockiert	Systemerweiterung blockiert
<ol style="list-style-type: none"> a. Klicken Sie auf OK. b. Klicken Sie auf OK. c. Um diese Erweiterungen zu genehmigen, wählen Sie Systemeinstellungen > Sicherheit und Datenschutz. d. Klicken Sie auf Zulassen neben <i>System-Software vom Entwickler Credant Technologies (Dell, Inc, ehemals Credant Technologies)</i>. e. Klicken Sie auf OK. 	<p>Führen Sie diese Schritte aus, wenn die Systemerweiterung zum Laden von FDEEM-Volumes nicht geladen werden konnte.</p> <ol style="list-style-type: none"> a. Klicken Sie auf Systemeinstellungen öffnen. b. Klicken Sie auf OK. c. Klicken Sie auf der Registerkarte Allgemein auf Zulassen neben <i>Systemsoftware vom Entwickler Credant Technologies, (Dell, Inc, ehamals Credant Technologies)</i>. d. Klicken Sie auf OK.

Die Option „Zulassen“ ist nach der Installation möglicherweise nur 30 Minuten oder kürzer verfügbar. Wenn Sie diesen Schritt überspringen, wird das Dialogfeld ungefähr alle fünfundzwanzig Minuten angezeigt, bis Sie diesen Schritt abgeschlossen haben.

18. Fahren Sie fort mit der [Aktivierung des Encryption Client for Mac](#).

macOS 10.15 und höher mit Wechselmedien

Wenn ein Unternehmen Wechselmedien mit macOS 10.15 und höher verwendet, müssen Benutzer den vollständigen Festplattenzugriff für externe Medien aktivieren. Weitere Informationen finden Sie unter [Aktivieren des vollständigen Festplattenzugriffs für Wechselmedien](#).

Installation/Upgrade über Befehlszeile

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

Installation über die Befehlszeile

1. Laden Sie vom Dell Installationsmedium die Datei „Dell-Encryption-Enterprise-<version>.dmg“.
2. Kopieren Sie das Paket **Install Dell Endpoint Security Suite Enterprise** und die Datei **com.dell.ddp.plist** auf das lokale Laufwerk.
3. Ändern Sie über die Verwaltungskonsolle, falls erforderlich, die folgenden Richtlinien. Richtlinieneinstellungen überschreiben .plist-Dateieinstellungen. Verwenden Sie die .plist-Einstellungen, wenn keine Richtlinien in der Verwaltungskonsolle vorhanden sind.
 - **Liste der Benutzer ohne Authentifizierung** – In einigen Fällen möchten Sie diese Richtlinie möglicherweise bearbeiten, damit bestimmte Benutzer oder Gruppen von Benutzern keine Aktivierung 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 ausgeführt 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 am Dell Server aktiviert werden, damit Enterprise diese Eigenschaft nicht ändert. Wenn ein Benutzer jedoch Encryption External Media 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/> [Dell recommends 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>
</dict>
</plist>
```

```

</array>
<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>

```

- Speichern und schließen Sie die .plist-Datei.
- Kopieren Sie für jeden Zielcomputer das Paket in einen temp-Ordner und die Datei „com.dell.ddp.plist“ nach **/Library/Preferences**.
- Führen Sie eine Installation über die Befehlszeile durch, indem Sie den folgenden **Installationsbefehl** ausgeben:
sudo installer -pkg "Install Dell Endpoint Security Suite Enterprise.pkg" -target /
- Starten Sie den Computer mithilfe der folgenden Befehlszeile neu: **sudo shutdown -r now**

ANMERKUNG:

System Integrity Protection (SIP) wurde in macOS High Sierra (10.13) erweitert, damit Benutzer Kernel-Erweiterungen von Dritten genehmigen müssen. Weitere Informationen zum Genehmigen von Kernel-Erweiterungen unter macOS High Sierra finden Sie in folgendem Artikel der Knowledge Base: [SLN307814](#).

- Fahren Sie fort mit der [Aktivierung des Encryption Client for Mac](#).

macOS 10.15 und höher mit Wechselmedien

Wenn ein Unternehmen Wechselmedien mit macOS 10.15 und höher verwendet, müssen Benutzer den vollständigen Festplattenzugriff für externe Medien aktivieren. Weitere Informationen finden Sie unter [Aktivieren des vollständigen Festplattenzugriffs für Wechselmedien](#).

Aktivieren des vollständigen Festplattenzugriffs für Wechselmedien

Wenn ein Unternehmen Wechselmedien mit macOS 10.15 und höher verwendet, müssen Benutzer den vollständigen Festplattenzugriff für externe Medien aktivieren. Benutzer sehen eine der folgenden Aufforderungen:

- Nach der Installation der Client-Software werden Sie dazu aufgefordert, dass Sie Wechselmedien vollständigen Festplattenzugriff gewähren müssen. Klicken Sie auf die Schaltfläche **Sicherheit und Datenschutz aufrufen** und fahren Sie mit den nachfolgenden Schritten fort.
- Wenn die Benutzer nicht nach der Installation dazu aufgefordert werden, vollständigen Festplattenzugriff zu gewähren, erhalten sie die entsprechende Aufforderung beim ersten Laden der Wechselmedien. Es wird eine Meldung angezeigt, dass Dell Encryption External Media oder EMS Explorer auf Dateien auf einem Wechseldatenträger zugreifen möchten. Klicken Sie auf **OK** und fahren Sie mit den nachfolgenden Schritten fort.

Weitere Informationen finden Sie im [KB-Artikel SLN319972](#).

- Klicken Sie unter *Systemeinstellungen* > *Sicherheit und Datenschutz* auf die Registerkarte **Datenschutz**.
- Wählen Sie im linken Bereich die Option **Vollständiger Festplattenzugriff** aus.
Die *Dell Encryption External Media* App wird nicht angezeigt.
- Klicken Sie unten auf das Schlosssymbol und geben Sie die Anmeldeinformationen für ein lokales Administratorkonto ein.

Im linken Fenster > **Dateien und Ordner** kann der Benutzer die externen Medien (EMS)-Komponenten überprüfen, um die erforderlichen Berechtigungen zu geben.

4. Wählen Sie im linken Bereich die Option **Vollständiger Festplattenzugriff** aus.

Die *External Media Dell Encryption App* wird jetzt angezeigt. Wenn jedoch die Genehmigungsanforderung noch aussteht, wird das Kontrollkästchen für diese App nicht ausgewählt.

5. Erteilen Sie die Berechtigung, indem Sie das Kontrollkästchen aktivieren.

Wenn die *Dell Encryption externe Medien App* nicht angezeigt wird:

- a. Klicken Sie auf das Plus-Symbol (+) im rechten Fensterbereich.
- b. Gehen Sie zu **/Library/Dell/EMS** und wählen Sie **Dell Encryption External Media** aus.
- c. Klicken Sie auf **Öffnen**.
- d. Aktivieren Sie unter **Vollständiger Festplattenzugriff** das Kontrollkästchen für *Dell Encryption External Media*.

6. Schließen Sie die **Sicherheit und Datenschutz**.

Aktivieren von Encryption Client

Der Aktivierungsprozess ordnet Netzwerkbenutzerkonten im Dell Server dem Mac-Computer zu und ruft von jedem Konto die jeweiligen Sicherheitsrichtlinien ab, sendet Bestandsaufnahme- und Statusaktualisierungen, ermöglicht 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.

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 for Mac ist jetzt voll funktionsfähig und wird durch den Dell Server verwaltet.

ANMERKUNG:

Wenn eine Warnung bezüglich einer erforderlichen Encryption External Media-Ressource angezeigt wird, klicken Sie auf die Schaltfläche **Sicherheit und Datenschutz aufrufen** und klicken Sie dann für jede von Ihrer Organisation benötigte Systemerweiterung auf **Zulassen**. Sie müssen diese Erweiterung aktivieren, damit Encryption External Media ordnungsgemäß funktioniert.

- 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 [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 Encryption Enterprise**.
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.

ANMERKUNG:

Klicken Sie auf **Aktualisieren** zur Suche nach Richtlinienaktualisierungen.

Die Verwaltungskonsole listet die Mac-Richtlinien auf, die in diesen Technologiegruppen verwendet werden:

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

Richtlinien, die Sie festlegen, hängen von den Verschlüsselungsanforderungen Ihres Unternehmens ab.

Diese Tabelle listet die Richtliniengruppen auf.

Mac Verschlüsselung > Dell Volume-Verschlüsselung	
Für High Sierra und höher müssen beide Richtlinien aktiviert sein. Informationen zu Sierra und früheren Versionen finden Sie in den vorherigen Versionen der Dokumentation.	
Dell Volume-Verschlüsselung	<p><i>Ein oder Aus</i></p> <p>Diese Richtlinie ist die „Master-Richtlinie“ für allen anderen Dell Volume-Verschlüsselungsrichtlinien. Diese Richtlinie muss auf <i>Ein</i> eingestellt werden, damit andere Dell Volume Verschlüsselungsrichtlinien angewendet werden können.</p> <p><i>Ein</i> aktiviert die Verschlüsselung und initiiert die Verschlüsselung für unverschlüsselte Volumes gemäß den Richtlinien <i>Für die Verschlüsselung vorgesehene Volumes</i> oder <i>Verschlüsseln mit FileVault für Mac</i>. Die Standardeinstellung ist <i>Ein</i>.</p> <p>Mit der Einstellung „Aus“ wird die Verschlüsselung deaktiviert und eine Entschlüsselungssuche für alle vollständig oder teilweise verschlüsselten Volumes eingeleitet.</p>
Verschlüsselung mit FileVault für Mac	<p>Wenn Sie die FileVault-Verschlüsselung verwenden möchten, achten Sie darauf, zuerst die Dell Volume-Verschlüsselung auf <i>Ein</i> zu setzen.</p> <p>Stellen Sie sicher, dass die Richtlinie <i>Verschlüsselung mit FileVault für Mac</i> in der Verwaltungskonsole ausgewählt ist.</p> <p>Nach der Aktivierung wird FileVault basierend auf der Richtlinieneinstellung <i>Für die Verschlüsselung vorgesehene Volumes</i> das Systemvolume einschließlich Fusion Drives verschlüsseln.</p>
Mac-Verschlüsselung > Globale Mac-Einstellungen	
Zur Verschlüsselung vorgesehene Datenträger	<p><i>Nur Systemvolume</i> oder <i>Alle festen Volumes</i></p> <p><i>Nur Systemvolume</i> bedeutet, dass nur das derzeit aktive Systemvolume geschützt wird.</p> <p>Alle festen Volumes bedeutet, dass sämtliche Mac OS Extended Volumes auf allen fest eingebauten Laufwerken sowie der derzeit aktive Systemdatenträger geschützt werden.</p>

3. Beschreibungen aller Richtlinien finden Sie in der *AdminHelp*, die in der Dell Server Verwaltungskonsole verfügbar ist. So finden Sie eine spezifische Richtlinie in der *AdminHelp*:
 - a. Klicken Sie auf das Suchsymbol.
 - b. Geben Sie in die *Suche* den Richtliniennamen in Anführungszeichen ein.
 - c. Klicken Sie auf den angezeigten Themen-Link. Der von Ihnen in Anführungszeichen eingegebene Richtliniennamen 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 <i>Für die Verschlüsselung vorgesehene Volumes</i> 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. 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 Dell Server	Um sicherzustellen, dass alle verschlüsselten Daten wiederhergestellt werden können, beginnt der Client erst dann mit dem Verschlüsselungsvorgang, wenn alle Verschlüsselungsschlüssel erfolgreich beim Dell Server hinterlegt wurden. Der Client sendet eine Abfrage zur Sicherheitserver-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 <i>Entschlüsselung läuft</i> das Partitionsschema auf den ursprünglichen Zustand zurückzusetzen. Dies ist bei der Entschlüsselungssuche das Äquivalent des Zustands <i>Volume wird für die Verschlüsselung vorbereitet</i> .
Entschlüsselt	Die Entschlüsselungssuche ist abgeschlossen.






Farbe	Beschreibung
Grün	Verschlüsselter Anteil
Rot	Nicht verschlüsselter Anteil
Gelb	Anteil, der erneut verschlüsselt wird

Farbe	Beschreibung
	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.
	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.

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: <ul style="list-style-type: none"> 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 Encryption External Media Zugriff auf unverschlüsselte Datenträger ist auf „schreibgeschützt“ eingestellt.

Zeichen	Status
	Durch Encryption External Media verschlüsselte Medien, erkennbar an dem Dell Emblem.

Anzeigen von Richtlinie und Status in der Verwaltungskonsole

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

1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsole 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 die *Suche* 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. Geben Sie den allgemeinen Namen, UPN (Universal Principal Name) oder SAM-Kontonamen ein.

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

Die Verschlüsselung wird für die folgenden Volumes unterstützt:

- Volumes im Format Apple File System (APFS), die gemeinsame physische Datenträger mit dem Startvolume haben.
- Volumes im Format Mac OS X Extended (Journaled) und Systemdatenträger, die mit dem Partitionsschema GUID Partition Table (GPT) partitioniert wurden

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-Ebene aktivieren. Zusätzliche Anleitungen zur Aktivierung der Verschlüsselung auf *Enterprise*-Ebene finden Sie in der AdminHelp.

1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsole 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 die *Suche* 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. Geben Sie den allgemeinen Namen, UPN (Universal Principal Name) oder SAM-Kontonamen ein.

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, 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 ist (macOS Sierra und frühere Versionen), ändern Sie weitere Richtlinien wie gewünscht.
Beschreibungen aller Richtlinien finden Sie in der *AdminHelp*, die in der Dell Server 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 Encryption Enterprise-Voreinstellungen auf **Aktualisieren**.

Verschlüsselungsvorgang

Der Verschlüsselungsvorgang variiert je nach Zustand des Startvolumens, wenn die Verschlüsselung aktiviert ist.

ANMERKUNG:

Zur Wahrung der Integrität der Benutzerdaten, beginnt die Client-Software erst dann mit der Verschlüsselung eines Volumens, 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 Volumens 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:

- [FileVault Verschlüsselung eines unverschlüsselten Volumens](#)
- [Verwaltung eines vorhandenen mit FileVault verschlüsselten Volumens übernehmen](#)

FileVault-Verschlüsselung eines unverschlüsselten Volumens

Mit FileVault-Verschlüsselung wird ein zusätzlicher unbenannter Benutzer im PBA angezeigt. Löschen Sie diesen Benutzer nicht, da er dem Dell Server erlaubt, die Richtlinien auf dem Gerät durchzusetzen. Wenn der PBA-Benutzer entfernt wird, muss der Benutzer Maßnahmen ergreifen, um richtlinienunterstellte Entschlüsselungen zu starten.

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**.
5. Vergewissern Sie sich, dass jeder Benutzer über ein sicheres Token verfügt. Siehe <https://www.dell.com/support/article/us/en/19/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en>.

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.

6. Klicken Sie auf **OK**.
7. Starten Sie den Computer nach Abschluss der Verschlüsselungsvorbereitung neu.

ANMERKUNG:

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

8. 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 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 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 Eigenschaftsliste 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 Regel nicht korrekt gebildet wird, wird in der Registerkarte *Dell Encryption Enterprise > 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 in der Verwaltungskonsole 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.

- Starten Sie die Computer neu.
- Benachrichtigen Sie die Benutzer, 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:

- Starten Sie die **Systemeinstellungen** und klicken Sie auf **Dell Encryption Enterprise**.
- Klicken Sie auf die Registerkarte **Systemvolumes**.
- Klicken Sie auf das Systemvolume-Laufwerk und wählen Sie **FileVault Benutzer zu Start von FileVault hinzufügen**.
- Geben Sie unter *Suche* 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.

- Klicken Sie auf **Benutzer aktivieren** oder **Konvertieren & Benutzer aktivieren**.
- Geben Sie das Kennwort für das ausgewählte Konto an und klicken Sie auf **OK**. Eine Fortschrittsleiste wird angezeigt.
- 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 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 Encryption Enterprise“ angezeigt. Gehen Sie folgendermaßen vor, um Dell Encryption die Übernahme der Verwaltung des Volumes zu ermöglichen.

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

ANMERKUNG:

Für macOS High Sierra und Apple File System (APFS) müssen Sie **Startfähige Konto-Anmeldeinformationen** auswählen.

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

- Geben Sie den Schlüssel ein.

Wenn der Benutzer nicht über den bereits vorhandenen Schlüssel verfügt, kann er diesen beim Administrator anfordern.

- b. Klicken Sie auf **OK**.

i ANMERKUNG:

Nach Abschluss des Übernahmeprozesses 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 Volumes autorisiert ist.**

- a. Geben Sie den Benutzernamen und das Passwort ein.
- b. 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.

i ANMERKUNG:

In der 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 Verwaltungskonsole herunter und kopieren Sie es in den Desktop des Computers.
2. Starten Sie die *Systemeinstellungen* und klicken Sie auf **Dell Encryption Enterprise**.
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**.

i ANMERKUNG:

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

Nutzerfreundlichkeit

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 Nutzer die Festlegung eines Werts von maximal fünf Minuten, bevor die Authentifizierung durchgesetzt wird.

Nutzer 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 Nutzers 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 Akkuladestatus oder beim Austauschen des Akkus der Fall sein könnte.

Zulassungsregel kopieren

Ein ausgeblendetes Menüelement ermöglicht dem Nutzer, eine Regel für die Zulassungsregel für Wechselmedien zu kopieren.

1. Starten Sie die **Systemeinstellungen** und klicken Sie auf **Dell Encryption Enterprise**.
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 **Zulassungsregel kopieren** für das aktuelle Wechselmedium. Die Regel für die Zulassungsliste wird in die Zwischenablage kopiert.
5. Rufen Sie die Zwischenablage auf, kopieren Sie die Regel für die Zulassungsliste und senden Sie sie an Ihren Administrator.

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

Um ein Gerät oder eine Gerätegruppe auszuschließen und zu verhindern, dass verschlüsselte Daten auf das Thunderbolt-Laufwerk oder das Encryption External Media geschrieben werden, ändern Sie die Werte der Zulassungslistenregel.

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

```
bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101  
II;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSENUM=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 Mac Media Encryption-Richtlinie aus:

```
tbolt=1;bus=SATA
```

Sie haben außerdem die Möglichkeit, Medien anhand der folgenden Kriterien auf die Zulassungsliste zu setzen oder aus Encryption External Media zu entfernen:

• **Mediengröße**

Zulassungslistenregel für den Ausschluss großer Medien aus dem Encryption External Media-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 Encryption External Media auszuschließen, verwenden Sie den folgenden Befehl:

```
size >= 500000000
```

size >= 500000K

size >= 500M

- **Dateisystemtyp**

Zulassungsregel:

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:

- Ein Mitarbeiter verlässt das Unternehmen und informiert niemanden über das Passwort.
- Ein Benutzer kann sich nicht mehr an das Passwort erinnern.

Dieser Abschnitt enthält Informationen zur Verwendung der [FileVault-Wiederherstellung](#), wenn der wiederherzustellende Endpunkt per FileVault-Verschlüsselung verschlüsselt ist. FileVault kann verwendet werden, wenn der Encryption Client unter macOS Sierra 10.12.6 ausgeführt wird. Die FileVault-Wiederherstellung wird auch auf Fusion Drives verwendet.

Volume laden

Voraussetzungen

- Unverschlüsseltes, externes Wiederherstellungsvolume oder Computer zum Ausführen des Wiederherstellungsdienstprogramms
- 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 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 Verwaltungskonsole an.
2. Klicken Sie im linken Bereich auf **Verwaltung > Endpunkt wiederherstellen**.
3. Geben Sie in die *Suche* den vollständig qualifizierten Domännennamen (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 Verschlüsselungsschlüsselpaket, 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.

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 auf

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-Encryption-Enterprise-<version>.dmg.

ANMERKUNG:

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

9. 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.

10. Wählen Sie das Wiederherstellungspaket (das Sie in [Schritt 6](#) gespeichert haben) und klicken Sie auf **Öffnen**.

11. 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.

FileVault-Wiederherstellung

Die Wiederherstellung eines verwalteten, mit FileVault verschlüsselten Volumes 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. Wenn ein persönlicher Wiederherstellungsschlüssel vorhanden ist, empfiehlt Dell, dass Sie den neuesten Eintrag für diesen Schlüssel verwenden. Falls dieser nicht funktioniert, verwenden Sie die institutionelle Wiederherstellungsschlüsselkette.

- [Persönlicher Wiederherstellungsschlüssel](#) – Die vorhandene FileVault-Verschlüsselung wird durch den Dell Server verwaltet. 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](#) (selten verwendet) – 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>a31jaAABAAAAA...
```

Persönlicher Wiederherstellungsschlüssel

Im Allgemeinen gilt es als Best Practice, das Startvolume vor der Wiederherstellung von Nicht-Startvolumes wiederherzustellen, da dadurch alle anderen Volumes geladen werden, die verschlüsselt wurden. 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 Verwaltungskonsole. Suchen Sie nach dem Benutzernamen des Besitzers und zeigen Sie die für diesen Benutzer verschlüsselten Geräte an. Das Format für die Geräte-ID/Eindeutige ID lautet „Peter Schmidts MacBook.Z4291LK58RH“.
- Die Dell Installationsmedien

Verwaltungskonsole – Wiederherstellungspaket speichern

1. Öffnen Sie die Verwaltungskonsole.
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**.

Prozess – .dmg laden

1. Kopieren Sie das Wiederherstellungspaket und die Datei **Dell-Encryption-Enterprise-<version>.dmg** auf das startfähige USB-Laufwerk.
2. Starten Sie den Zielcomputer von einem im Voraus erstellten, externen Installations-Volume mit vollständigem Betriebssystem aus, indem Sie die Taste **Option** während des Neustarts dieses Computers gedrückt halten und das externe Installations-Volume mit dem vollständigen Betriebssystem vor dem Starten im Start-Manager auswählen. Weitere Informationen zum Erstellen eines startfähigen Volumes finden Sie unter <https://support.apple.com/en-us/HT202796>.
3. Laden Sie **Dell-Encryption-Enterprise-<version>.dmg**.

Prozess – Dell Recovery Utility starten und FileVault Volume wiederherstellen

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

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

ANMERKUNG:

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

2. Wählen Sie unter *Dell Recovery Utility > Volumes auswählen* das FileVault-Volume aus.
 - Bei der Wiederherstellung eines Betriebssystems ist die beste Methode, auf einem Computer mit dem gleichen oder einem höheren Betriebssystem zu starten.
 - Wenn Sie Nicht-Startvolumes verschlüsselt haben, müssen Sie in der Regel zuerst die Startpartition wiederherstellen.
3. Klicken Sie auf **Weiter**.
4. Suchen und wählen Sie das (zuvor gespeicherte) Wiederherstellungspaket aus und klicken Sie auf **Öffnen**.
5. Wenn das Dialogfeld *Wiederherstellungsdatensatz auswählen* angezeigt wird, sehen Sie sich die Spalte *Hinterlegungsdatum* an, wählen Sie 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.

Das *Ergebnis des Wiederherstellungsvorgangs* wird 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. Eine Schaltfläche zum Entsperren wird bereitgestellt, um das Volume zu entsperren und zu laden.
6. Führen Sie einen der folgenden Schritte aus:
 - Wiederherstellen des Startvolumes (am häufigsten verwendet)
 - Wiederherstellen eines Nicht-Startvolumes (selten verwendet)

Wiederherstellen des Startvolumes (am häufigsten verwendet)

Für die meisten Wiederherstellungsfälle verwenden Sie diese Option, um das Startvolumen wiederherzustellen:

1. Schreiben Sie den Schlüssel entweder auf oder klicken Sie auf **Wiederherstellungsschlüssel drucken**.
2. Klicken Sie auf **Schließen**.
3. Starten Sie das Volume, das Sie wiederherstellen möchten, unter Verwendung des Preboot Startup Managers, falls erforderlich.
Der Computer zeigt Symbole für mehrere Benutzer an oder verlangt ein Kennwort.
4. Wählen Sie ggf. einen Benutzer aus und klicken Sie dann auf **?** im Anmeldebildschirm.
5. Klicken Sie auf den angezeigten Pfeil.
6. Geben Sie den Wiederherstellungsschlüssel ein und drücken Sie die **Eingabetaste**.
7. Geben Sie in das Dialogfeld ein neues Passwort für den Benutzer ein.

Optionen zum Wiederherstellen von Nicht-Startvolumen (selten verwendet) – Führen Sie eine der folgenden Aktionen aus:

Wiederherstellen eines Nicht-Startvolumen

Wenn das Startvolumen beschädigt oder gelöscht wurde und sekundäre Volumes vorhanden sind, können Sie diese Nicht-Startvolumen laden.

1. Klicken Sie auf **Entsperren**. Das Volume wird geladen.
2. Klicken Sie auf **Schließen**.

Volume entschlüsseln – klicken Sie auf die Schaltfläche

1. Klicken Sie auf **Entschlüsseln**. Ein Dialogfeld und eine Fortschrittsleiste zeigen den Entschlüsselungsprozess an.
2. Wenn er abgeschlossen ist, klicken Sie auf **Schließen**.
3. Starten Sie das entschlüsselte Volume, um es zu verwenden.

Volume entschlüsseln – führen Sie den Befehl über das Terminal aus

1. Kopieren Sie den Befehl in den Bereich *Volume entschlüsseln*.
2. Klicken Sie auf **Schließen**.
3. Führen Sie den Befehl im Terminal aus.

Wiederherstellungsschlüsselkette

Das Dell Wiederherstellungsdienstprogramm muss über ein unverschlüsseltes Wiederherstellungsvolumen gestartet und ausgeführt werden.

Voraussetzungen

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

Verwaltungskonsole – Wiederherstellungspaket speichern

1. Öffnen Sie die Verwaltungskonsole.
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 Wiederherstellungsvolumen 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**.

Verfahren

1. Schließen Sie ein externes Laufwerk an das System an, damit es wiederhergestellt werden kann.
Das externe Laufwerk muss über ein Mac OS-Startvolumen verfügen.

2. Starten Sie über das externe Laufwerk, indem Sie die Taste **Option** gedrückt halten, und verwenden Sie die Startauswahl, um dieses Volume auszuwählen und darüber zu starten.
3. Kopieren Sie das Wiederherstellungspaket aus der Verwaltungskonsole.
4. Laden Sie die Installationsdatei .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 Wechseldatenträgers, z. B. eines USB-Sticks, 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:

Das Speichern der Dateien in der Nähe des Stamms eines Volumes verkürzt den einzugebenden Pfad.

Bei Ergebnis des Wiederherstellungsvorgangs wird der Schlüssel angezeigt.

Das 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 sowie während des Computerstarts.
oder auf
- Für frühere Versionen von Apple: Drücken Sie die **Wahltaste** 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 Encryption External Media. 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 Zulassungsliste 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 Nutzer seine Zulassungslistenregel kopieren und sie Ihnen zusenden, um seinen Time Machine-Datenträger für die Zulassungsliste anzugeben. Siehe [Zulassungslistenregel kopieren](#).

Encryption External Media und Richtlinienaktualisierung

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

Verschlüsselungsausnahmen

Erweiterte Attribute werden auf einem Wechselmedium 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 Encryption External Media überschrieben wird und wenn Sie die Datei anschließend in Encryption External Media 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:
 1. Notieren Sie sich die Größe des Speicherplatzes, der auf dem Gerät freigegeben werden muss. Der Bericht enthält eine Liste der Dateien und ihre Größe.
 2. Leeren Sie den Papierkorb. Während Sie Speicherplatz freigeben, verschlüsselt Encryption External Media automatisch zusätzliche Dateien.
 3. Wenn Sie Dateien oder Ordner löschen, müssen Sie den Papierkorb anschließend leeren, um Speicherplatz freizugeben.

Überprüfungsmeldungen

Überprüfungsmeldungen werden an den Dell Server gesendet.

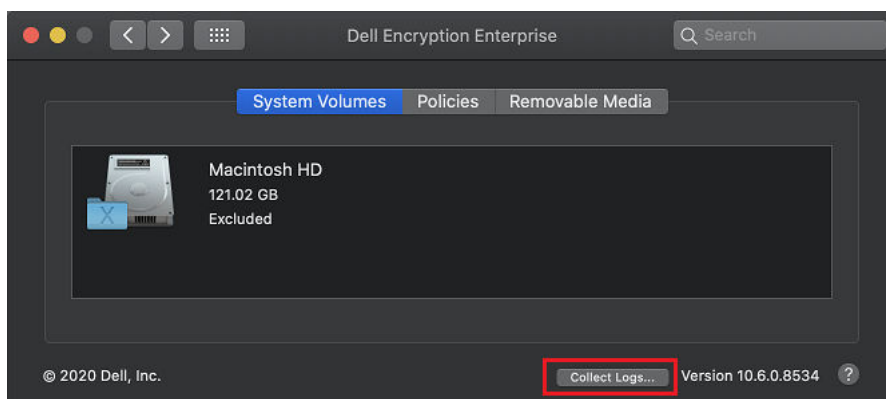
Um bei Endpoint Security Suite Enterprise for Mac Audit-Meldungen anzuzeigen:

1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsolle an.
2. Klicken Sie im linken Fensterbereich auf **Bestückungen > Enterprise oder Endpunkte**.
3. Wählen Sie die Registerkarte **Erweiterte Bedrohungsereignisse** aus.

Weitere Informationen finden Sie unter *AdminHelp*.

Sammeln von Protokolldateien für Endpoint Security Suite Enterprise

In den *Systemeinstellungen > Dell Encryption Enterprise > -System-Volumes* kann ein Administrator über die Schaltfläche „Protokolle erfassen“ unten rechts vorab Protokolle für den Support erstellen. Diese Maßnahme kann sich auf die Performance auswirken, während Protokolle erfasst werden.



DellLogs.zip enthält die Protokolle für Mac Encryption Enterprise und 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 Encryption Enterprise 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 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 Encryption Enterprise deinstallieren** (diese befindet sich im Ordner „Dienstprogramme“ in der Dell-Encryption-Enterprise-<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 Server kommen.

Voraussetzungen

- Der Encryption Client for Mac muss 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 Encryption Enterprise-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.

Damit 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 verschlüsselt Dell Encryption Enterprise das Windows Betriebssystem nicht. Außerdem verschlüsselt Encryption Enterprise nur das primäre Volume, wenn zwei oder mehr startfähige macOS-Partitionen auf dem Gerät vorhanden sind.

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 8.1 und 8.1 Pro (64-Bit)

ANMERKUNG:

Windows 7 unterstützt Boot Camp 4 oder 5.1. Windows 8.1 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 den Encryption Client for Mac mit FileVault2 verschlüsselt werden. Anweisungen dazu finden Sie unter [Installation/Upgrade über Befehlszeile](#).

ANMERKUNG:

Falls es sich bei Ihrer Windows-Partition um einen Kandidaten für Encryption External Media handelt, stellen Sie sicher, dass sie Teil der Zulassungsliste ist, um eine Verschlüsselung zu verhindern. Siehe [Zulassungslistenregel 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 for Windows auf Boot Camp

Um Endpoint Security Suite Enterprise for 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 Verwaltungskonsole. Suchen Sie nach dem Benutzernamen des Besitzers und zeigen Sie die für diesen Benutzer verschlüsselten Geräte an. Das Format für die Geräte-ID/Eindeutige ID lautet „Peter Schmidts 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 Verwaltungskonsole das Wiederherstellungspaket auf eines der Folgenden:

- Startfähiges USB-Laufwerk
oder auf


- 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. Um den Computer über das externe Boot Camp-Laufwerk zu starten, führen Sie eine der folgenden Aktionen aus:

- Drücken und halten Sie gleichzeitig die Taste **Befehl** und **R** (Befehl-R), bevor der Signalton für das Einschalten/den Selbsttest erklingt sowie während des Computerstarts.
oder
 - Für frühere Versionen von Apple drücken Sie die **Wahltaste**, während Sie den Computer einschalten.
Das Dialogfeld *Mac OS X Dienstprogramme* wird angezeigt.
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 Encryption Enterprise“ eine Option aus:
 - *Mein System lässt sich nicht booten* – Wenn der Benutzer das System nicht starten kann, wählen Sie die erste Option aus.
oder auf
 - *Mein System lässt mich keine verschlüsselten Daten anzeigen* – Wenn der Benutzer auf einige verschlüsselte Dateien bei der Anmeldung am System nicht zugreifen kann, wählen Sie die zweite Option.
 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 Verwaltungskonsole 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\$vn8WDn</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\ Encryption\ Enterprise.prefPane/Contents/Helpers/client -at domainAccount domainPassword
```

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

```
/Library/PreferencePanes/Dell\ Encryption\ Enterprise.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 Domänenanmeldedaten 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 <i>Liste der Benutzer ohne Authentifizierung</i> zum Erstellen von Benutzerklassen verwenden, die gegebenenfalls nicht beim 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 Datenträger-ID, Verschlüsselungsstatus und Richtlinien Wenn leere Klammern ausgegeben werden, weist dies darauf hin, dass keine

Tabelle 1. Client-Tool-Befehle (fortgesetzt)

Befehl	Zweck	Syntax	Ergebnisse
			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 lokales Konto 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\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -p -plist**

Zum Abrufen der Richtlinien vom Client und Drucken der Richtlinien.

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

Zum temporären Aktivieren des Clients und dem Drucken des Ergebnisses.

Library/PreferencePanes/Dell\ Encryption\Enterprise.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\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -d -plist**

Zum Abrufen des Client-Datenträgerstatus und Drucken.

Globale Rückgabecodes

Kein Fehler 0

Parameterfehler 4

Befehl nicht erkannt 5

Socketzeitüberschreitung 8

Interner Fehler 9

Aufgaben

Themen:

- [Installieren von Advanced Threat Prevention for Mac](#)
- [Prüfen der Advanced Threat Prevention Installation](#)
- [Sammeln von Protokolldateien für Endpoint Security Suite Enterprise](#)
- [Details zu Advanced Threat Prevention anzeigen](#)
- [Bereitstellung eines Mandanten](#)
- [Konfigurieren der automatischen Aktualisierung des Advanced Threat Prevention Agenten](#)
- [Advanced Threat Prevention – Fehlerbehebung](#)

Installieren von Advanced Threat Prevention for Mac

Dieser Abschnitt führt Sie durch die Installation von Advanced Threat Prevention.

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

- [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.
Installations- und Migrationshandbuch für Security Management Server
Schnellanleitung und Installationshandbuch für Security Management Server Virtual
- Stellen Sie sicher, dass Sie über den Dell Server-Hostnamen und -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.

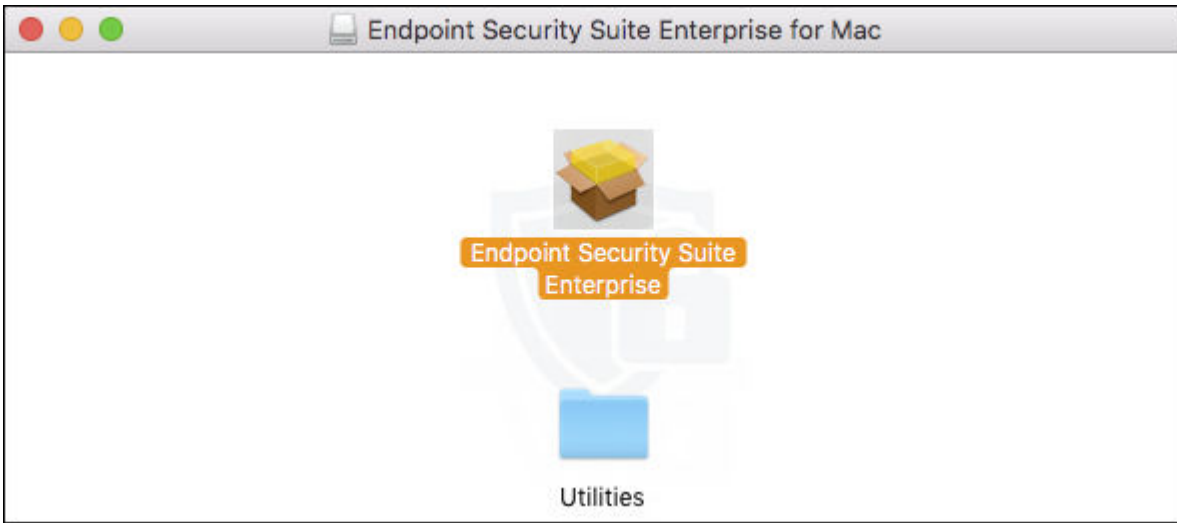
Interaktive Installation ist die einfachste Methode zum Installieren oder Aktualisieren des Client-Softwarepakets. Bei dieser Methode sind allerdings keinerlei Anpassungen möglich.

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

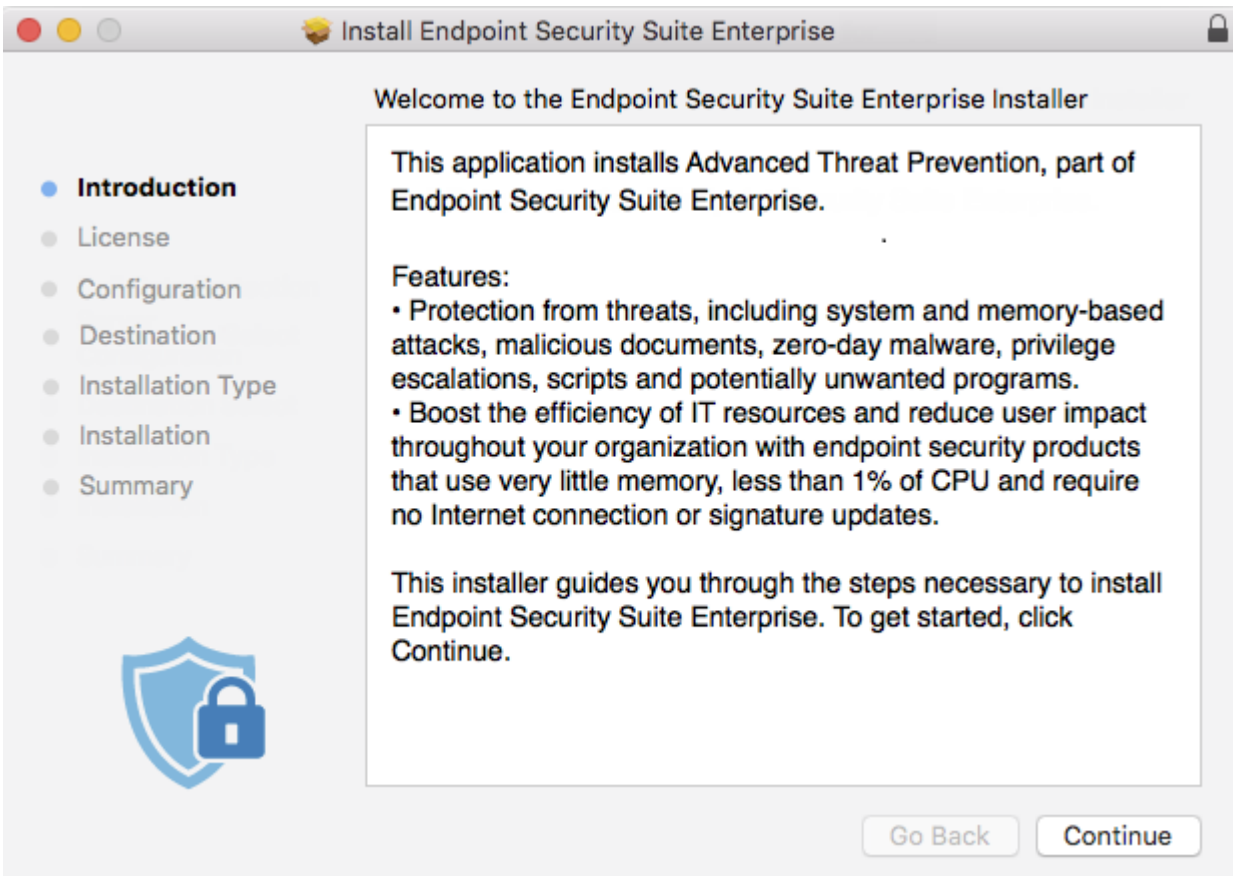
ANMERKUNG:

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

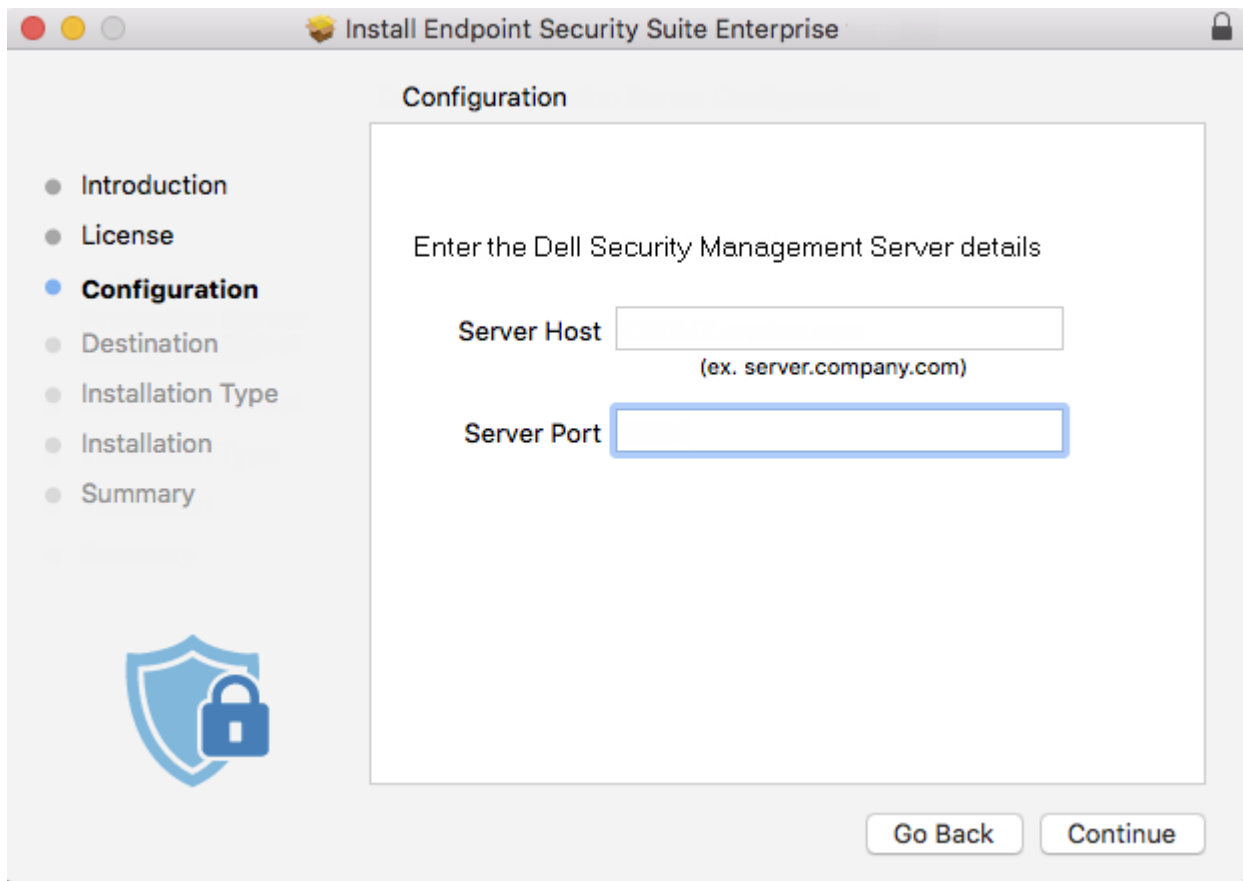
1. Laden Sie vom Dell Installationsmedium die Datei **Endpoint-Security-Suite-Enterprise-<version>.dmg**.
Das Paket Endpoint Security Suite Enterprise for Mac wird geöffnet.



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 *Serverhost* den vollqualifizierten Hostnamen des Dell Server 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 **Software installieren**.
10. Wenn die Installation abgeschlossen ist, klicken Sie auf **Schließen**. Der Advanced Threat Prevention Client for Mac wurde installiert.
11. Schließen Sie das Paket.
12. Siehe [Prüfen der Installation von Advanced Threat Prevention](#).

Wenn das System nicht am Dell Server registriert ist, lesen Sie die Protokolle, um zu ermitteln, ob Sie auf Ihrem Dell Server über ein gültiges Zertifikat verfügen. Siehe [Deaktivieren von SSL Trust Certificate für Advanced Threat Prevention](#).

Interaktive Deinstallation des Advanced Threat Prevention Client

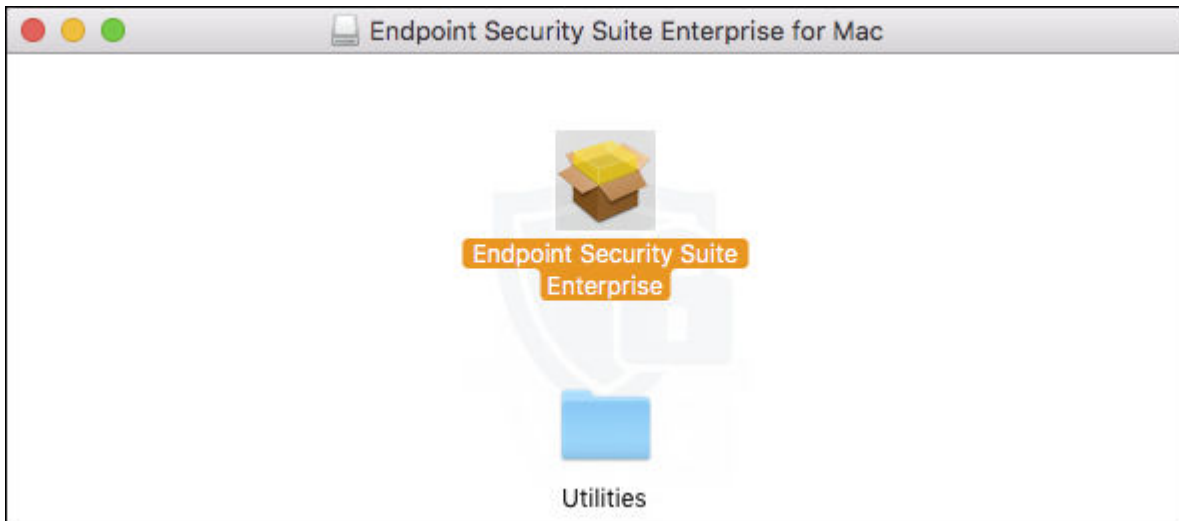
Die Client-Software kann durch Ausführen der Anwendung **Endpoint Security Suite Enterprise deinstallieren** deinstalliert werden. Führen Sie die nachfolgenden Schritte aus, um die Client-Software zu deinstallieren.

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

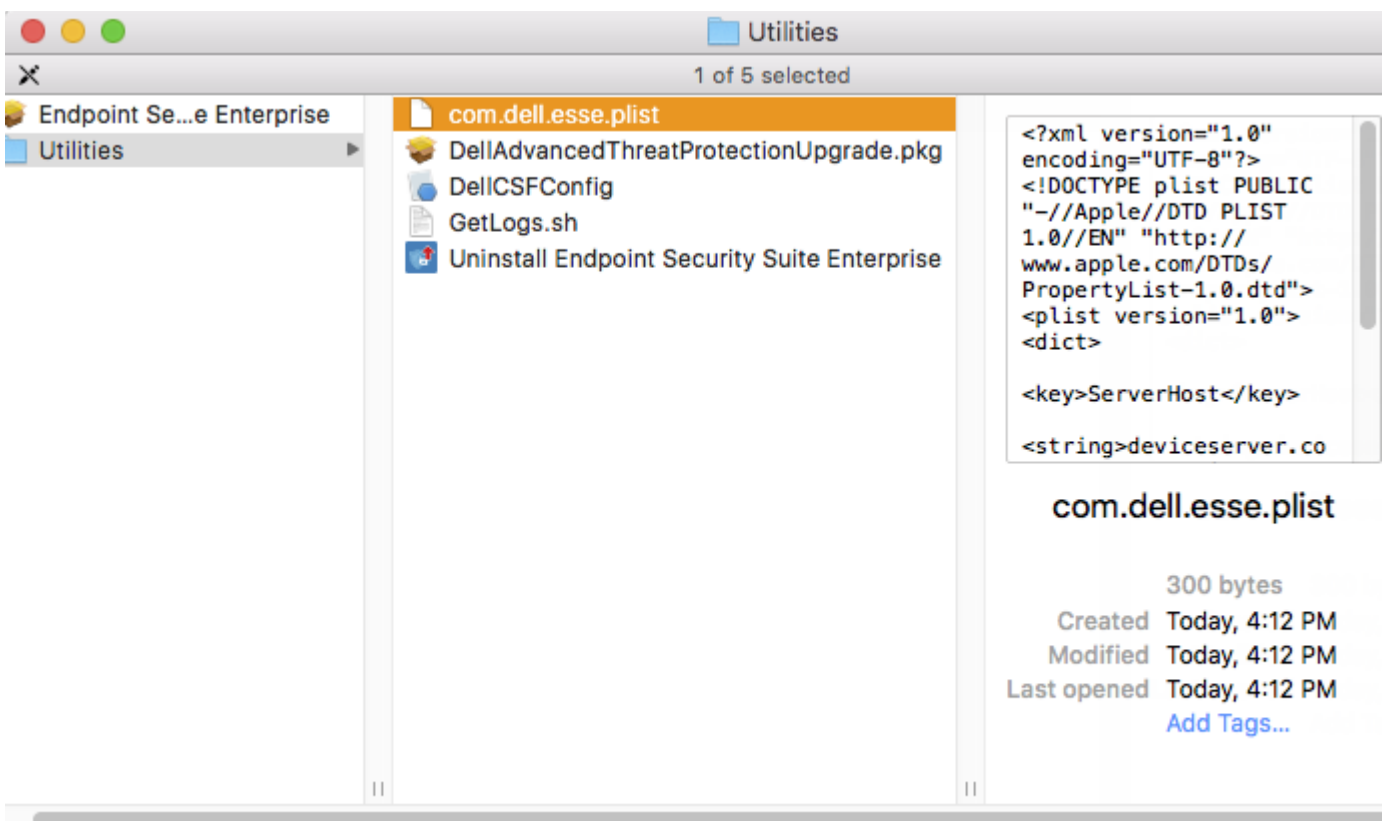
Installation von Advanced Threat Prevention über die Befehlszeile

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 Server, der die Verwaltung des Zielbenutzers übernimmt, wie z. B. server.unternehmen.de, 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>server.organization.com</string>
  <key>ServerPort</key>
  <string>8888</string>
  <array>
</dict>
</plist>
```

ANMERKUNG:

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

- Speichern und schließen Sie die Datei.
- Kopieren Sie für jeden Zielcomputer das Paket-Installationsprogramm für **Endpoint Security Suite Enterprise for Mac** in einen temporären Ordner und die geänderte Datei **com.dell.esse.plist** in **/Library/Preferences**.
- Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeinformationen ein.
- Öffnen Sie ein Terminalfenster.
- 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.

- Drücken Sie die **Eingabetaste**.
- Siehe [Prüfen der ESSE Advanced Threat Prevention Installation](#).

Deinstallieren von Advanced Threat Prevention for Mac über Befehlszeile

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

- Öffnen Sie ein Terminalfenster.
- 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.

- Drücken Sie die **Eingabetaste**.
Advanced Threat Prevention for Mac ist jetzt deinstalliert und der Computer kann normal verwendet werden.

Advanced Threat Prevention for Mac – Fehlerbehebung

Deaktivieren von SSL Trust Certificate oder PolicyCheck 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.

Deaktivieren Sie PolicyCheck, wenn Sie selbstsignierte Zertifikate in Ihrer Umgebung ausführen.

Wenn Sie selbstsignierte Zertifikate in Ihrer Umgebung haben und das Zertifikat nicht in die Schlüsselkette auf Ihren Macs importiert haben, setzen Sie DisableCertTrust und DisablePolicyCheck auf „False“.

- Starten Sie auf dem Client ein Terminalfenster.
- Geben Sie den Pfad zur DellCSFConfig.App ein:

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

- Führen Sie die DellCSFConfig.App aus:

```
sudo DellCSFConfig.app/Contents/MacOS/DellCSFConfig
```

Das Folgende stellt die Standardeinstellungen dar:

```
Current Settings:
ServerHost = deviceserver.company.com
ServerPort = 8888
DisableCertTrust = False
DisablePolicyCheck = 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 `DisableCertTrust` in **True**.
6. Zum Deaktivieren von Policy Signing Check auf dem Client ändern Sie `DisablePolicyCheck` 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**.

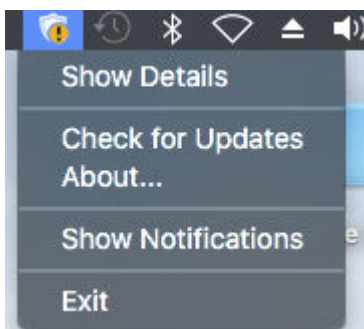
Die Richtliniendateien werden nur ausgegeben, wenn eine Richtlinienänderung aufgetreten ist.

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 Symbol für Advanced Threat Prevention 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.

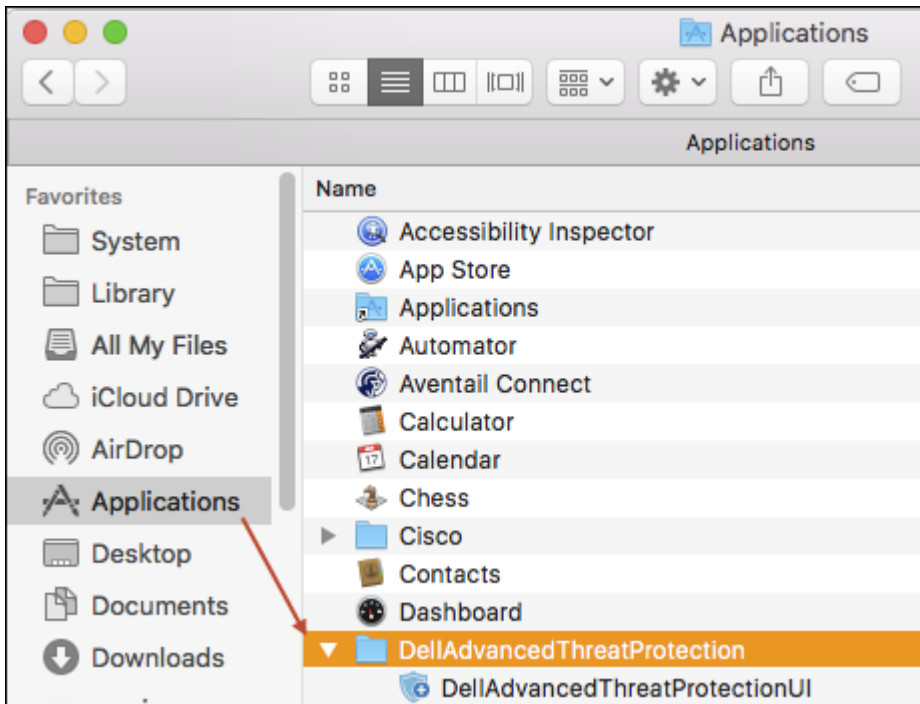


Auf Updates prüfen – Sucht nach Updates für die Advanced Threat Prevention Engine, nicht nach Updates der Dell Server-Richtlinie.

Info – Umfasst Folgendes:

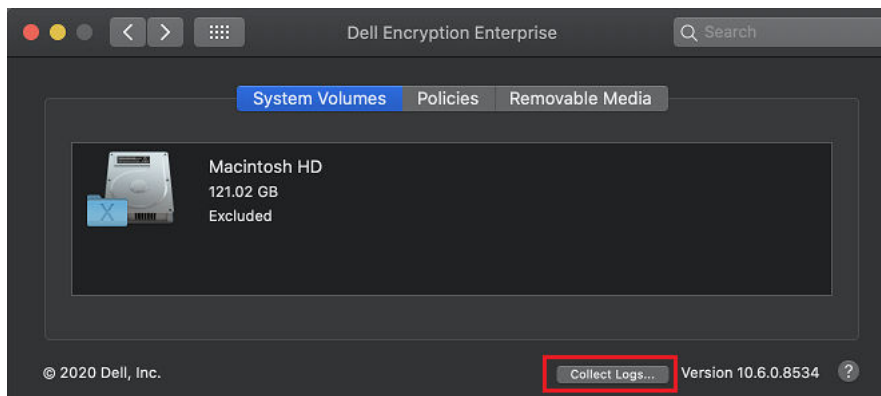
- Version
- Richtlinie – [online] zeigt die Server-basierte Richtlinie an und [offline] zeigt die Air Gap oder offline-basierte Richtlinie an
- Seriennummer – Verwenden Sie diese beim technischen Support. Dies ist die eindeutige Kennung für die Installation.

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



Sammeln von Protokolldateien für Endpoint Security Suite Enterprise


In den *Systemeinstellungen* > *Dell Encryption Enterprise* > *-System-Volumes* kann ein Administrator über die Schaltfläche „*Protokolle erfassen*“ unten rechts vorab Protokolle für den Support erstellen. Diese Maßnahme kann sich auf die Performance auswirken, während Protokolle erfasst werden.



DellLogs.zip enthält die Protokolle für Mac Encryption Enterprise und Advanced Threat Prevention. Informationen über das Sammeln der Protokolle finden Sie unter <http://www.dell.com/support/article/us/en/19/SLN303924>.

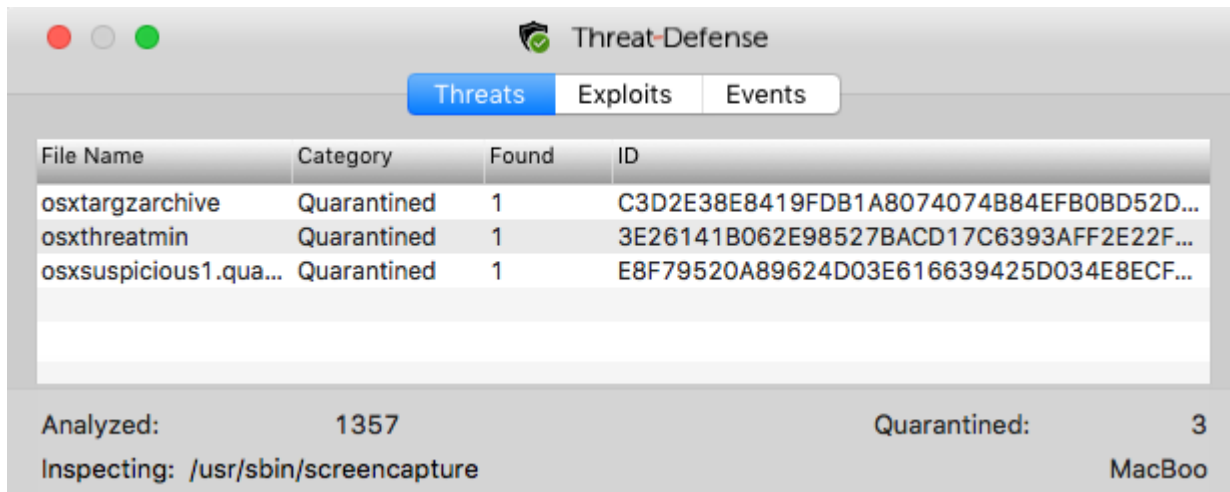
Details zu Advanced Threat Prevention anzeigen

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.



File Name	Category	Found	ID
osxtargzarchive	Quarantined	1	C3D2E38E8419FDB1A8074074B84EFB0BD52D...
osxthreatmin	Quarantined	1	3E26141B062E98527BACD17C6393AFF2E22F...
osxsuspicious1.qua...	Quarantined	1	E8F79520A89624D03E616639425D034E8ECF...

Analyzed: 1357 Quarantined: 3
Inspecting: /usr/sbin/screenshoture MacBoo

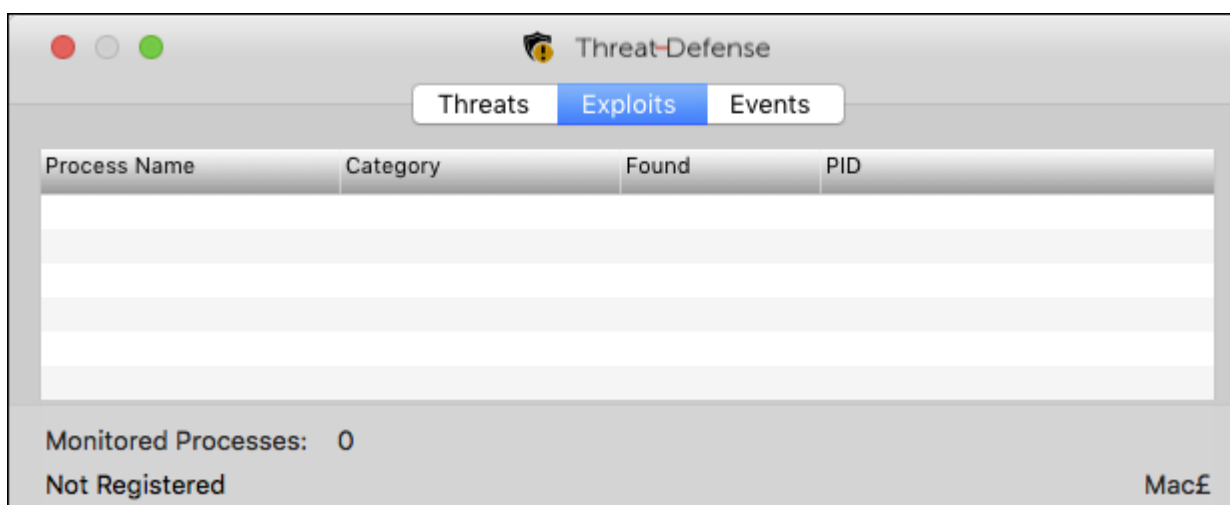
Die Spalte „Kategorie“ kann Folgendes enthalten.

- **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.
- **Gelöscht** - Eine Datei, die innerhalb der Organisation gelöscht 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 Advanced Threat Prevention finden Sie in der *AdminHelp*, die in der Verwaltungskonsole verfügbar ist.

Registerkarte „Exploits“

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



Process Name	Category	Found	PID
--------------	----------	-------	-----

Monitored Processes: 0
Not Registered Mac

Die Dell Server-Richtlinien bestimmen die Maßnahmen, die beim 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

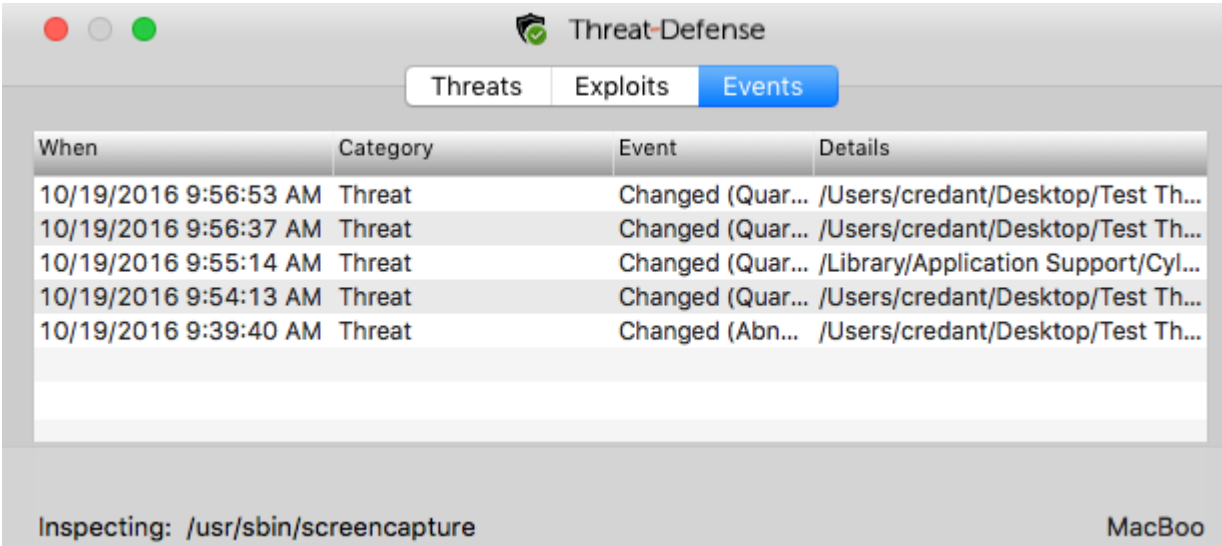
Weitere Informationen über diese Exploit-Richtlinien finden Sie in der *AdminHelp*, die in der Verwaltungskonsole verfügbar ist.

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 Advanced Threat Prevention zugewiesen worden ist. Die Daten werden gelöscht, wenn das System neu gestartet wurde.



When	Category	Event	Details
10/19/2016 9:56:53 AM	Threat	Changed (Quar...	/Users/credant/Desktop/Test Th...
10/19/2016 9:56:37 AM	Threat	Changed (Quar...	/Users/credant/Desktop/Test Th...
10/19/2016 9:55:14 AM	Threat	Changed (Quar...	/Library/Application Support/Cyl...
10/19/2016 9:54:13 AM	Threat	Changed (Quar...	/Users/credant/Desktop/Test Th...
10/19/2016 9:39:40 AM	Threat	Changed (Abn...	/Users/credant/Desktop/Test Th...

Inspecting: /usr/sbin/screenshot MacBoo

Beispiele für Ereignistypen umfassen:

Bedrohung gefunden

Bedrohung entfernt

Unter Quarantäne gestellte Bedrohungen

Bedrohung freigegeben

Bedrohung geändert

Bereitstellung eines Mandanten

Ein Tenant muss im Dell Server bereitgestellt werden, bevor die Durchsetzung von 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 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.

Bereitstellung eines Mandanten

1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2. Klicken Sie im linken Bereich der Verwaltungskonsole auf Verwaltung > Servicemanagement.
3. Klicken Sie auf **Advanced Threat Protection-Dienst einrichten**. Importieren Sie Ihre Advanced Threat Prevention Lizenzen, wenn zu diesem Zeitpunkt ein Fehler auftritt.
4. Die geführte Einrichtung beginnt, sobald die Lizenzen importiert wurden. Klicken Sie zum Starten auf **Weiter**.
5. Lesen Sie die EULA, stimmen Sie ihr zu und klicken Sie dann auf **Weiter**.
6. Geben Sie die Anmeldeinformationen für den Dell Server ein, um den Mandanten bereitzustellen. Klicken Sie auf **Weiter**. *Die Bereitstellung eines vorhandenen Mandanten der Marke Cylance wird nicht unterstützt.*
7. Laden Sie das Zertifikat herunter. Dies ist erforderlich, um eine Wiederherstellung im Falle von Notfallszenarien mit dem Dell Server durchzuführen. Dieses Zertifikat wird nicht automatisch gesichert. Sichern Sie das Zertifikat auf einem sicheren Speicherplatz auf einem anderen Computer. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie das Zertifikat gesichert haben, und klicken dann Sie auf **Weiter**.
8. Die Einrichtung ist abgeschlossen. Klicken Sie auf **OK**.

Konfigurieren der automatischen Aktualisierung des Advanced Threat Prevention Agenten

Sie können sich in der 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 Dienst 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 Verwaltungskonsole 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:

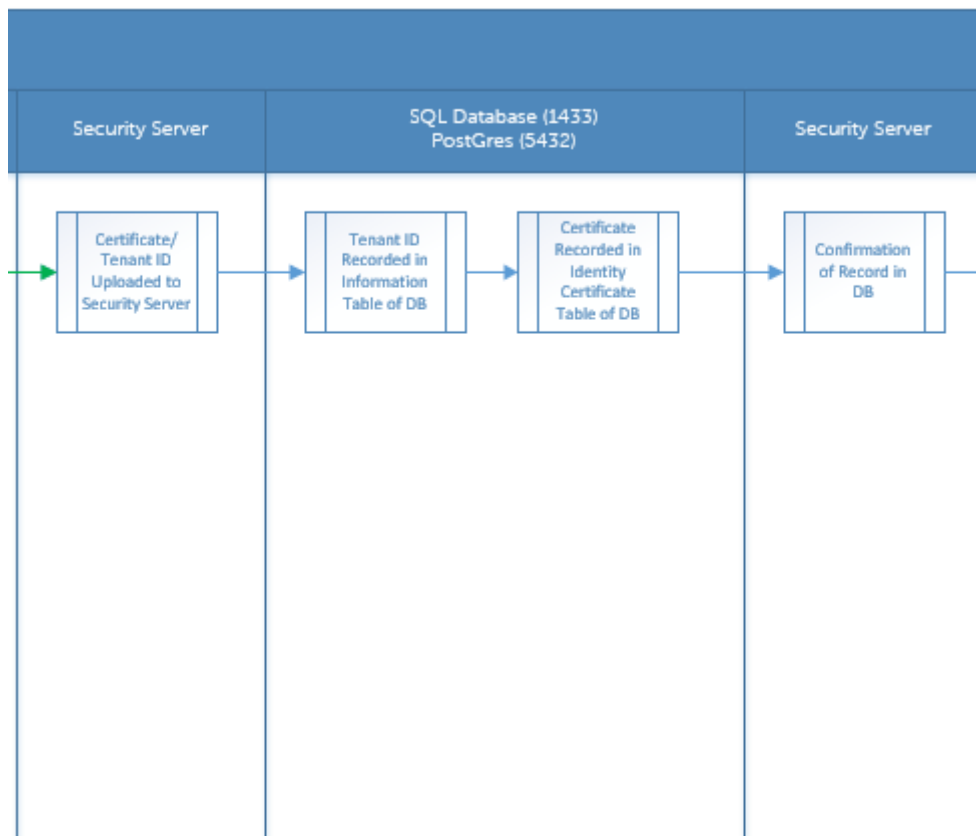
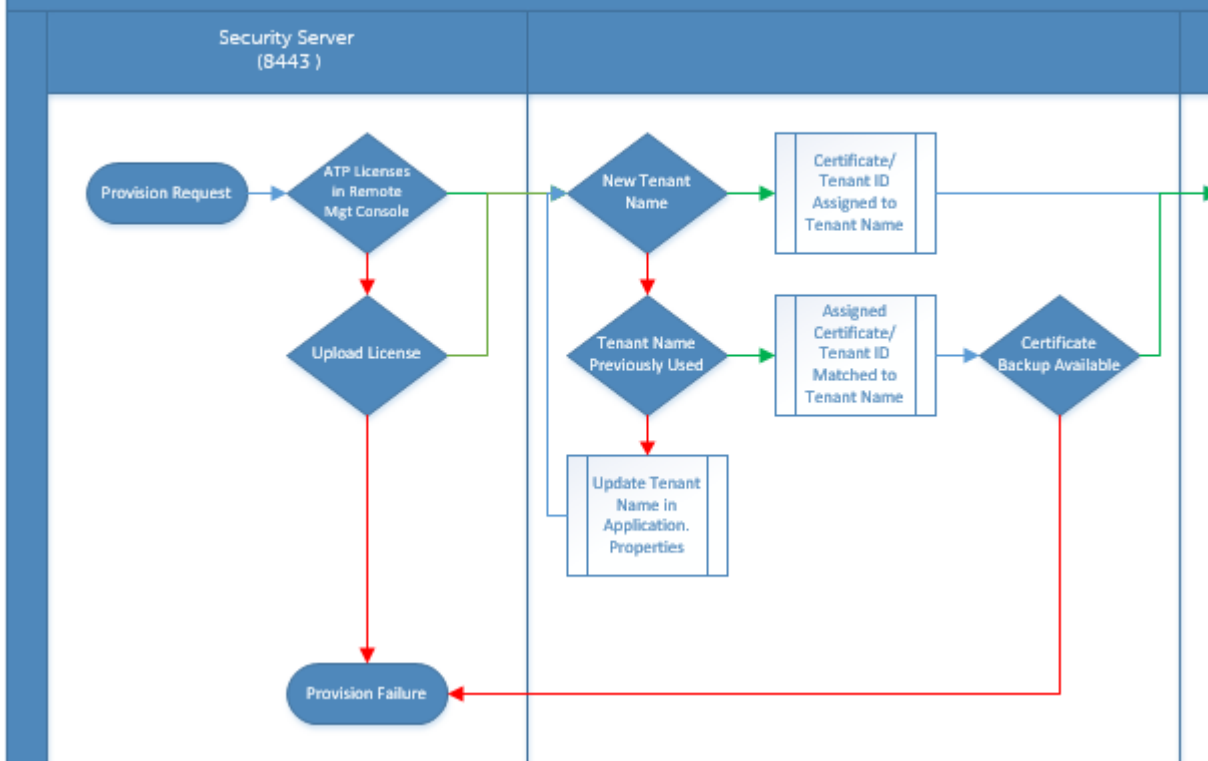
1. Klicken Sie im linken Bereich der Verwaltungskonsole auf **Verwaltung > Dienstverwaltung**.
2. Auf der Registerkarte *Advanced Threats* unter *Automatische Agent-Aktualisierung* klicken Sie auf die Schaltfläche **Aus** und dann auf die Schaltfläche **Einstellungen speichern**.

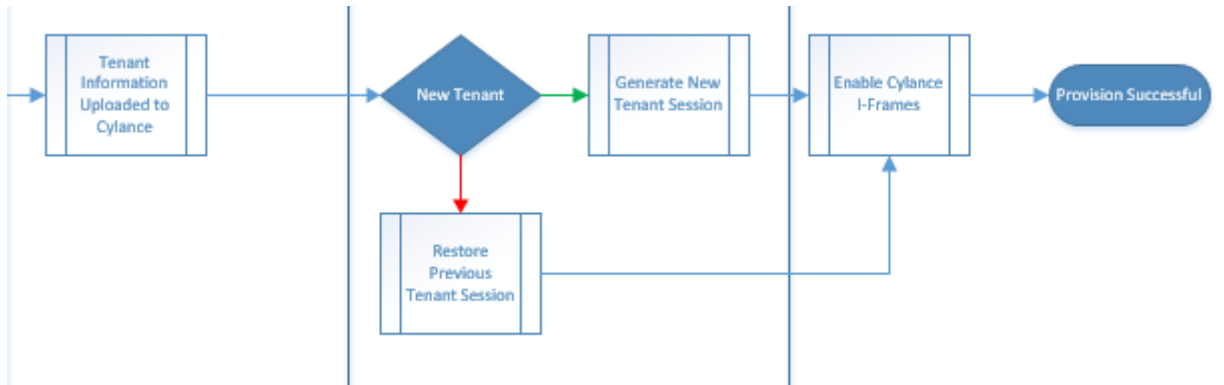
Advanced Threat Prevention – Fehlerbehebung

Bereitstellung von Advanced Threat Prevention und Agentenkommunikation

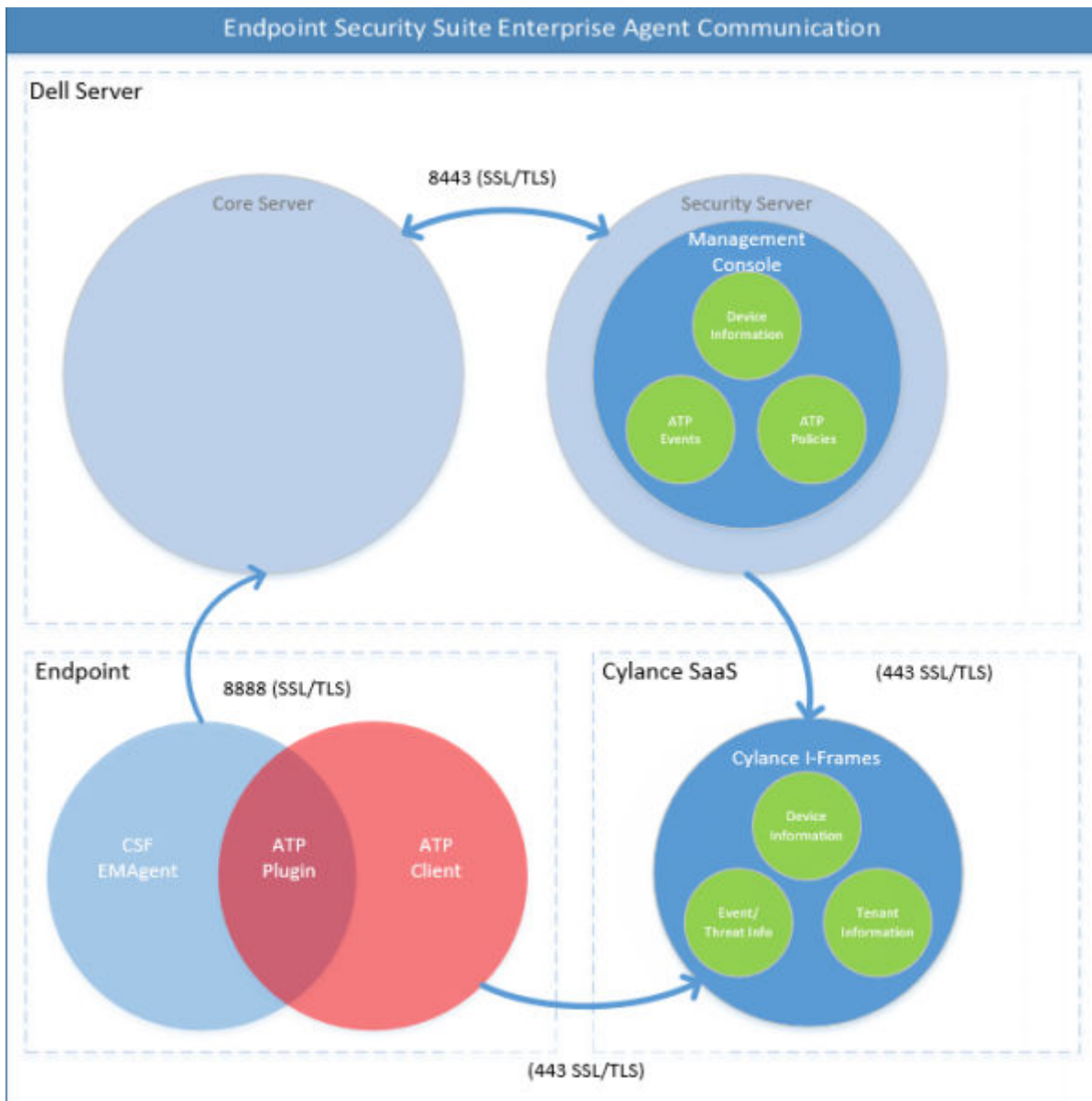
Die folgenden Diagramme veranschaulichen die Bereitstellung des Advanced Threat Prevention Dienstes.

Advanced Threat Prevention Service Provisioning Process





Das folgende Diagramm veranschaulicht die Agentenkommunikation für Advanced Threat Prevention.



Glossar

Sicherheitsserver – wird für Aktivierungen von Dell Encryption verwendet.

Richtlinien-Proxy – wird zum Verteilen von Richtlinien für Clientsoftware verwendet.

Verwaltungskonsole – die Verwaltungskonsole des Dell Servers für die gesamte Enterprise Bereitstellung.

Shield – Ab und an kann in der Dokumentation und auf den Benutzeroberflächen der Begriff „Shield“ auftauchen. „Shield“ steht für Dell Encryption.