Dell Data Security

EnCase Integrationsanleitung

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

© 2012–2018 Dell Inc. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

In den Dokumenten zu Dell Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise und Data Guardian verwendete eingetragene Marken und Marken: Dell™ und das Logo von Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® und KACE™ sind Marken von Dell Inc. Cylance®, CylancePROTECT und das Cylance Logo sind eingetragene Marken von Cylance, Inc. in den USA. und anderen Ländern. McAfee® und das McAfee-Logo sind Marken oder eingetragene Marken von McAfee, Inc. in den USA und anderen Ländern. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, und Xeon® sind eingetragene Marken der Intel Corporation in den USA und anderen Ländern. Adobe®, Acrobat® und Flash® sind eingetragene Marken von Adobe Systems Incorporated. Authen Tec® und Eikon® sind eingetragene Marken von Authen Tec. AMD® ist eine eingetragene Marke von Advanced Micro Devices, Inc. Microsoft®, Windows® und Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, und Visual C++® sind entweder Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern. VMware® ist eine eingetragene Marke oder eine Marke von VMware, Inc. in den USA oder anderen Ländern. Box® ist eine eingetragene Marke von Box. DropboxSM ist eine Dienstleistungsmarke von Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® und Google™ Play sind entweder Marken oder eingetragene Marken von Google Inc. in den Vereinigten Staaten oder anderen Ländern. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® und Siri® sind entweder Dienstleistungsmarken, Marken oder eingetragene Marken von Apple, Inc. in den Vereinigten Staaten oder anderen Ländern. GO ID®, RSA® und SecurID® sind eingetragene Marken von Dell EMC. EnCaseTM™ und Guidance Software® sind entweder Marken oder eingetragene Marken von Guidance Software. Entrust® ist eine eingetragene Marke von Entrust®, Inc. in den USA und anderen Ländern. InstallShield® ist eine eingetragene Marke von Flexera Software in den USA, China, der EU, Hong Kong, Japan, Taiwan und Großbritannien. Micron® und RealSSD® sind eingetragene Marken von Micron Technology, Inc. in den USA und anderen Ländern. Mozilla® Firefox® ist eine eingetragene Marke von Mozilla Foundateion in den USA und/oder anderen Ländern. iOS® ist eine Marke oder eingetragene Marke von Cisco Systems, Inc. in den USA und bestimmten anderen Ländern und wird in Lizenz verwendet. Oracle® und Java® sind eingetragene Marken von Oracle und/oder seinen Tochtergesellschaften. Andere Namen können Marken ihrer jeweiligen Inhaber sein. SAMSUNGTM™ ist eine Marke von SAMSUNG in den USA oder anderen Ländern. Seagate® ist eine eingetragene Marke von Seagate Technology LLC in den USA und/oder anderen Ländern. Travelstar® ist eine eingetragene Marke von HGST, Inc. in den USA und anderen Ländern. UNIX® ist eine eingetragene Marke von The Open Group. VALIDITYTM™ ist eine Marke von Validity Sensors, Inc. in den USA und anderen Ländern. VeriSign® und andere zugehörige Marken sind Marken oder eingetragene Marken von VeriSign, Inc. oder seinen Tochtergesellschaften und verbundenen Unternehmen in den USA und anderen Ländern und werden von der Symantec Corporation in Lizenz verwendet. KVM on IP® ist eine eingetragene Marke von Video Products. Yahoo!® ist eine eingetragene Marke von Yahoo! Inc. Dieses Produkt verwendet Teile des Programms 7-Zip. Der Quellcode ist unter 7-zip.org verfügbar. Die Lizenzierung erfolgt gemäß der GNU LGPL-Lizenz und den unRAR-Beschränkungen (7-zip.org/license.txt).

EnCase Integrationsanleitung

2018 - 03

Rev. A01

Inhaltsverzeichnis

1

Einleitung

Dell Data Security ist mit digitalen forensischen EnCase V6.15-Produkten von Guidance Software, Inc. integrierbar, um die Online-Untersuchungen von Dell verschlüsselten Dateien zu unterstützen. Mit dieser Integration können forensische Ermittler von Dell gesicherte Daten anzeigen, exportieren oder durchsuchen. Mit den richtigen Anmeldeinformationen für einen forensischen Administrator werden alle Dell gesicherten Daten, unabhängig von den zur Verschlüsselung verwendeten Schlüsseln, entschlüsselt und dem Ermittler ohne weitere Benutzerinteraktion präsentiert. Die Anmeldeinformationen des forensischen Administrators werden im sicheren Speicher von EnCase abgelegt und aufbewahrt, sodass sie nicht erneut eingegeben werden müssen.

Die forensische Integration von EnCase V6.15 (32-Bit) unterstützt:

- Dell Data Security Encryption Enterprise für Windows V7.0.x oder höher
- Dell Security Management Server V7.0.1 oder höher

ANMERKUNG: Dell Data Security Encryption Enterprise für Mac unterstützt forensische Untersuchungen mit EnCase nicht.

Kontaktaufnahme mit dem Dell ProSupport

Telefonischen Support rund um die Uhr 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.

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

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

2

Integration mit EnCase

Aktivieren der EnCase-API

ANMERKUNG: Verwenden Sie diese API nicht mit Dell Device Servern, die in einer DMZ bereitgestellt sind. Verwenden Sie zur Wahrung der Sicherheit für die EnCase-Integration einen internen Dell Device Server mit Zugangsbeschränkung.

Vor V7.7 Security Management Server

1 Öffnen Sie **<Dell Installationsverzeichnis>\Enterprise Edition\Device Server\conf\context.properties**.

2 Aktivieren Sie die forensische Integrations-API.

service.forensic.enable=true

3 Beenden Sie den Dell Device Server und starten Sie ihn über das Startmenü neu.

Zum Deaktivieren der forensischen Integration setzen Sie service.forensic.enable=false.

V7.7 Security Management Server und höher

- Dieser Dienst ist auf dem Dell Server standardmäßig aktiviert.
- Zum Deaktivieren der forensischen Integration setzen Sie xapi.service.forensic.enable=false.

Beenden Sie den Dell Device Server und starten Sie ihn über das Startmenü neu.

Installieren von EnCase Integration Adapter

1 Doppelklicken Sie auf einem Computer mit EnCase auf **CMGEnCaseIntegration.exe**.

2 Wenn das Dialogfeld mit dem Bibliotheksinstallationsprogramm angezeigt wird, stellen Sie sicher, dass der EnCase-Zielordner korrekt ist.

3 Klicken Sie auf **Fertigstellen**, um die CEGetBundle- und Integration Adapter-Dateien in \Programme\EnCase6 \Lib\Credant Technologies\CMG zu extrahieren.

Verwenden von Dell Data Security mit EnCase

Verschlüsselungsschlüssel beziehen

Verwenden Sie die Benutzerschnittstelle von EnCase Enterprise, um Verschlüsselungsschlüssel von der Dell Remote Management Console zu beziehen und alle Dell verschlüsselten Daten für diesen Computer oder diese Beweisdatei zu entschlüsseln.

1 Wählen Sie das Kontrollkästchen **Online**.

2 Geben Sie den **Benutzernamen** des forensischen Administrators ein.

3 Geben Sie das **Kennwort** des forensischen Administrators ein.

4 Geben Sie die URL zum Dell Server mit aktivierter EnCase-API ein. Beispiel:

https://cred01.somedomain.com:8443/xapi/ (wenn Ihr Security Management Server V7.7 oder höher ist)

https://cred01.somedomain.com:8081/xapi (wenn Ihr Security Management Server älter als V7.7 ist)

Suchen Sie die Dell Server-URI unter HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet.

ANMERKUNG: Am Dell Server muss die EnCase-API aktiviert sein, um Schlüssel zu exportieren. Wahlweise können Sie einen alternativen Dell Device Server ausschließlich für die EnCase-Integration einsetzen.

5 Geben Sie die Machine-ID (auch bekannt als MCID und Eindeutige ID) für den Zielcomputer oder die Beweisdatei ein.

Suchen Sie die MCID in der Registrierung des Zielcomputers unter HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Winlogon\CMGShield

von der Dell Remote Management Console aus, klicken Sie im linken Fensterbereich auf **Populationen > Endpunkte.**

- Klicken Sie auf das Symbol Details des entsprechenden Geräts.
- Klicken Sie im obersten Menü auf **Details und Aktionen**.
- Suchen Sie die Eindeutige ID im Bereich *Endpunktdetails*.

6 Geben Sie die Shield-ID (auch bekannt als Geräte-ID, DCID, Recovery-ID oder SCID) für den Zielcomputer oder die Beweisdatei ein.

Suchen Sie die DCID in der Registrierung des Zielcomputers unter HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Winlogon\CMGShield

von der Dell Remote Management Console aus, klicken Sie im linken Fensterbereich auf **Populationen > Endpunkte.**

- Klicken Sie auf das Symbol **Details** des entsprechenden Geräts.
- Klicken Sie im obersten Menü auf **Details und Aktionen**.
- Suchen Sie die Recovery-ID im Bereich *Shield*.

ANMERKUNG: Geben Sie die MCID, die DCID oder beide IDs an. Der importierte Fall enthält alle Schlüsselinformationen für die angegebene Machine-ID, Shield-ID oder beide IDs.

7 Klicken Sie auf **OK**.

Die Entschlüsselung wird nun durchgeführt.

Sobald die Entschlüsselung abgeschlossen ist, sind die Dateien für die forensische Untersuchung zugänglich. Die entschlüsselten Dateien können nur über das EnCase-Modul angezeigt werden, die ursprünglichen Quelldateien bleiben unverändert und verschlüsselt.

Verwendung von EnCase mit Dell Data Security

CEGetBundle

CEGetBundle ist ein Dienstprogramm, das es forensischen Administratoren ermöglicht, Schlüsselinformationen von einem Dell Server zu beziehen. Dieses Dienstprogramm ist über den Dell ProSupport erhältlich.

Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter.

Parameter
-L = Legacy-Modus für das Exportieren von Schlüsseln von einem CMG 5.3.x-Server
URL = Device Server-URL (<securityserver.organization.com>)
AdminName = Administrator-Benutzername
AdminPwd = Administrator-Kennwort
AdminDomain = Administrator-Domäne
MCID = Machine-ID für das Zielgerät (auch bekannt als Eindeutige ID oder Host-Name)
SCID = Shield Credant-ID für Ziel-Shield (auch bekannt als DCID oder Recovery-ID)
Benutzername = Zielbenutzer für Export der Schlüsselinformationen (nur Legacy-Modus)
OutputFile = Dateiname für das exportierte Schlüsselpaket
OutputPwd = Kennwort für das exportierte Schlüsselpaket
-R = Verwendung des Sicherungsdatei-Modus
BackupFile = die ausführbare Datei, welche die Sicherungsschlüssel enthält
BackupPwd = das für die Sicherungsdatei verwendete Administratorkennwort

ANMERKUNG: Der Parameter AdminDomain sollte nur für das Exportieren von Schlüsseln von CMG Enterprise Edition 6.0 und höheren, zur Unterstützung mehrerer Domänen konfigurierten Servern bereitgestellt werden.

ANMERKUNG: Im Legacy-Modus müssen die MCID, die SCID sowie der Benutzername angegeben werden. Die Schlüsselinformationen nur für den angegebenen Benutzer werden der Ausgabedatei angehängt. Sie müssen dieses Tool mit demselben Ausgabedateinamen für jeden Benutzer auf dem für die Entschlüsselung vorgesehenen Gerät ausführen, wenn Benutzer- oder Benutzer-Roaming-Verschlüsselung aktiviert ist. Die Schlüsselinformationen jedes Benutzers werden der Ausgabedatei angehängt.

Beispiel für eine Befehlszeile

- Im folgenden Beispiel wird die MCID, SCID oder beides verwendet. Alle Schlüsselinformationen im Zusammenhang mit der angegebenen Maschine (MCID) oder SCID oder beidem werden in die Ausgabedatei gespeichert, die überschrieben wird, wenn sie bereits existiert.

```
CEGetBundle [-L] -XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dMCID] [-sSCID] [-uUsername] -
oOutputFile -iOutputPwd
```

- Im folgenden Beispiel werden Schlüsselinformationen aus der vom Installationsprogramm exportierten Sicherungsdatei extrahiert.

```
CEGetBundle -R -bBackupFile -ABackupPwd -oOutputFile -iOutputPwd
```