DDP Enterprise Server – Virtual Edition

v9.7 – Schnellstart- und Installationshandbuch

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.

VE – Erste Schritte und Installationshandbuch

2017 - 04

Rev. A01

Inhaltsverzeichnis

Schnellstart-Handbuch für Virtual Edition

Das Schnellstart-Handbuch ist für erfahrenere Anwender konzipiert, die DDP Enterprise Server – VE schnell einrichten und starten möchten. Im Allgemeinen empfiehlt Dell, zuerst DDP Enterprise Server – VE zu installieren, gefolgt von der Installation der Clients.

Detailliertere Anweisungen finden Sie im Virtual Edition-Installationshandbuch.

Weitere Informationen zu VE-Voraussetzungen finden Sie unter DDP Enterprise Server – VE-Voraussetzungen, VE Remote-Verwaltungskonsolen-Voraussetzungen und Proxy-Modus-Voraussetzungen.

Informationen zum Aktualisieren einer vorhandenen DDP Enterprise Server – VE finden Sie unter DDP Enterprise Server – VE aktualisieren.

Installation von DDP Enterprise Server – VE

1 Navigieren Sie zum Verzeichnis, wo die Dell Data Protection-Dateien gespeichert werden, und doppelklicken Sie, um in VMware **DDP Enterprise Server – VE v9.x.x Build x.ova** zu importieren.
2 Fahren Sie DDP Enterprise Server - VE hoch.
3 Befolgen Sie die Anweisungen auf dem Bildschirm.

VE konfigurieren

Bevor Sie Benutzer aktivieren, müssen Sie folgende Konfigurationsaufgaben am DDP Enterprise Server – VE-Terminal ausführen:

- Kennwort für die Datenbank einstellen oder ändern
- SMTP-Einstellungen konfigurieren
- Import eines bestehenden Zertifikats oder Registrierung eines neuen Serverzertifikats
- DDP Enterprise Server – VE aktualisieren
- Installieren Sie einen FTP-Client, der SFTP an Port 22 unterstützt und richten Sie Dateiübertragung (FTP)-Benutzer ein.

  Wenn Ihr Unternehmen über externe Geräte verfügt, siehe Proxy-Modus installieren und konfigurieren.

ANMERKUNG: Wenn für Ihre Enterprise Edition Clients werksseitige Berechtigungen vorliegen oder Sie Lizenzen erwerben, aktivieren Sie diese Berechtigungen durch das Einrichten eines Gruppenrichtlinienobjekts auf dem Domänencontroller (das muss nicht der Server sein, auf dem Virtual Edition ausgeführt wird). Achten Sie bitte darauf, dass der ausgehende Port 443 für die Kommunikation mit dem Server verfügbar ist. Falls der Port 443 (aus irgendeinem Grund) gesperrt ist, funktioniert die Berechtigungsfunktion nicht.

VE Remote Management-Konsole öffnen

Öffnen Sie die VE Remote Management-Konsole an dieser Adresse:

https://server.domain.com:8443/webui/

Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

Eine Liste der unterstützten Webbrowser finden Sie unter Voraussetzungen für die VE Remote Management Console.

Administrative Aufgaben

Wenn Sie die VE Remote Management Console noch nicht gestartet haben, tun Sie dies jetzt. Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

Dell empfiehlt, Administratorrollen so bald wie möglich zuzuweisen. Um diese Aufgabe jetzt abzuschließen, siehe Dell Administratorrolle zuweisen.

Klicken Sie auf „?“ in der oberen rechten Ecke der VE Remote Management-Konsole, um *Dell Data Protection AdminHelp* zu starten. Die Seite „*Erste Schritte*“ wird angezeigt. Klicken Sie auf **Domänen hinzufügen**.

Für Ihre Organisation wurden grundlegende Richtlinien festgelegt, aber je nach Ihren Anforderungen müssen diese möglicherweise wie folgt geändert werden (für alle Aktivierungen sind Lizenzen und Berechtigungen erforderlich):

- Windows-Computer werden verschlüsselt.
- Computer mit selbstverschlüsselnden Laufwerken werden verschlüsselt.
- BitLocker Management ist nicht aktiviert
- Advanced Threat Protection ist nicht aktiviert
- Der Bedrohungsschutz ist aktiviert
- Externe Medien werden nicht verschlüsselt.
- An Ports angeschlossene Geräte werden nicht verschlüsselt.
- Dell Data Guardian ist aktiviert.
- Die Mobile Edition wird nicht aktiviert.

Im Hilfethema *Richtlinien verwalten* der AdminHelp finden Sie Anweisungen zum Navigieren zu Technologiegruppen und Richtlinienbeschreibungen.

Die Ersten Schritte sind damit abgeschlossen.

Virtual Edition-Installationshandbuch

Dieses Installationshandbuch soll weniger erfahrenen Benutzern bei der Installation und Konfiguration von DDP Enterprise Server – VE helfen. Im Allgemeinen empfiehlt Dell, zuerst DDP Enterprise Server – VE zu installieren, gefolgt von der Installation der Clients.

Informationen zum Aktualisieren einer vorhandenen DDP Enterprise Server – VE finden Sie unter DDP Enterprise Server – VE aktualisieren.

Über DDP Enterprise Server – VE

Der DDP Enterprise Server – VE ist die Sicherheitsverwaltungskomponente der Dell-Lösung. Über die VE Remote Management Console können Administratoren unternehmensweit den Status von Endpunkten, die Durchsetzung von Richtlinien und den Schutzstatus überwachen. Der Proxy-Modus bietet eine Front-End-DMZ-Modus-Option für die Verwendung mit DDP Enterprise Server – VE.

DDP Enterprise Server – VE hat die folgenden Funktionen:

- Zentrale Verwaltung von bis zu 3,500 Geräten
- Erstellung und Verwaltung rollenbasierter Sicherheitsrichtlinien
- Gerätewiederherstellung durch einen Administrator
- Aufteilung administrativer Aufgaben
- Automatische Verteilung von Sicherheitsrichtlinien
- Vertrauenswürdige Kommunikation zwischen Komponenten
- Generierung eindeutiger Verschlüsselungsschlüssel und automatische, sichere Schlüsselhinterlegung
- Zentrale Compliance-Prüfverfahren und -Berichterstellung
- Automatische Erzeugung von selbstsignierten Zertifikaten

Kontaktaufnahme mit dem Dell ProSupport

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

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

Halten Sie bei Ihrem Anruf Ihren Service Code 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.

Anforderungen

Voraussetzungen für <1/>DDP Enterprise Server – VE

Hardware

Der empfohlene Speicherplatz für DDP Enterprise Server – VE ist 80 GB.

Virtuelle Umgebung

DDP Enterprise Server – VE v9.6 wurde mit den folgenden Virtualisierungsumgebungen validiert.

Virtuelle Umgebungen

- VMware Workstation 12.5
  - 64-Bit-CPU erforderlich
  - 4 GB RAM empfohlen
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/workstation-11/index.jsp

- VMware Workstation 11
  - 64-Bit-CPU erforderlich
  - 4 GB RAM empfohlen
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/workstation-11/index.jsp

- VMware ESXi 6.0
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-60/index.jsp

- VMware ESXi 5.5
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-55/index.jsp.

- Hyper-V-Server (Vollständige oder Core-Installation)
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen

- Ein Betriebssystem ist nicht erforderlich
- Die Hardware muss die Mindestanforderungen für Hyper-V erfüllen.
- Mindestens 4 GB RAM für dedizierte Bildressource
- Muss als virtuelle Maschine der 1. Generation ausgeführt werden.
- Weitere Informationen finden Sie unter https://technet.microsoft.com/en-us/library/hh923062.aspx.

Voraussetzungen für die VE Remote Management Console

Internet-Browser

ANMERKUNG:
Ihr Browser muss Cookies akzeptieren.

Die folgende Tabelle führt unterstützte Internet-Browser auf.

Internet-Browser

- Internet Explorer 11.x oder höher
- Internet Explorer 41.x oder höher
- Google Chrome 46.x oder höher

Voraussetzungen für den Proxy-Modus

Hardware

Die folgende Tabelle enthält die *mindestens* erforderlichen Hardware-Anforderungen für den Proxy-Modus.

Prozessor

2 GHz Core 2 Duo-Prozessor oder besser

RAM

+-2 GB dedizierter RAM mindestens/ 4 GB dedizierter RAM empfohlen

Freier Speicherplatz

ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher)

Netzwerkkarte

Netzwerkschnittstellenkarte 10/100/1000

Sonstiges

TCP/IP installiert und aktiviert

Software

Die folgende Tabelle enthält genauere Informationen zu der Software, die zur Installation des Proxy-Modus erforderlich ist.

Voraussetzungen

- **Windows Installer 4.0 oder höher**

  Auf dem für die Installation vorgesehenen Server muss Windows Installer 4.0 oder eine spätere Version installiert sein.

- **Microsoft Visual C++ 2010 Redistributable Package**

  Wenn sie nicht installiert ist, installiert der Installer sie für Sie.

- **Microsoft .NET Framework Version 4.5**

  Für .NET Framework Version 4.5 wurden von Microsoft Sicherheitsupdates veröffentlicht.

In der folgenden Tabelle sind die Anforderungen an die Software für den Proxy-Modus-Server aufgelistet.

ANMERKUNG:
Deaktivieren Sie beim Verwenden von Windows Server 2008 immer die UAC. Nach der Deaktivierung des UAC, muss der Server neu gestartet werden, damit diese Änderungen in Kraft treten.

Registrierungspfad für Windows Server: HKLM\SOFTWARE\Dell.

Betriebssystem

- **Windows Server 2008 R2 SP0 bis SP1 64-Bit**

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2008 SP2 64-Bit**

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition

- **Windows Server 2016**

  - Standard Edition

  - Datacenter Edition

Herunterladen von DDP Enterprise Server – VE

Bei der Erstinstallation wird DDP Enterprise Server - VE als OVA-Datei bereitgestellt. Das Open Virtual Application-Format wird zur Bereitstellung von Software für die Ausführung auf virtuellen Maschinen verwendet. Die DDP Enterprise Server – VE-OVA-Datei steht unter www.dell.com/support auf den Produkt-Supportseiten der folgenden Dell Data Protection-Produkte bereit:

Verschlüsselung

oder

Endpoint Security Suite

oder

Endpoint Security Suite Enterprise

oder

Data Guardian

So laden Sie die OVA-Datei herunter:

1 Navigieren Sie zur Seite „Produkt-Support“ für Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise oder Data Guardian.
2 Klicken Sie auf **Treiber und Downloads**.
3 Klicken Sie zum „Anzeigen verfügbarer Aktualisierungen für <OS-Version>“ auf **OS ändern** und wählen Sie entweder **VMware ESXi 6.0, VMware ESXi 5.5** oder **VMware ESXi 5.1** aus.
4 Wählen Sie unter „Anzeige nach:“ **Alle anzeigen** aus.
5 Wählen Sie unter „Dell Data Protection“ **Herunterladen** aus.

Installation von DDP Enterprise Server – VE

Stellen Sie vor Beginn sicher, dass alle Anforderungen an die Systeme und die virtuelle Umgebung erfüllt sind.

1 Suchen Sie die Dell Data Protection-Dateien auf dem Installationsdatenträger und doppelklicken Sie sie zum Import in VMware **DDP Enterprise Server – VE v9.x.x Build x.ova**.
2 Fahren Sie DDP Enterprise Server - VE hoch.
3 Wählen Sie die Sprache für die Lizenzvereinbarung aus und wählen Sie dann **EULA anzeigen** aus.
4 Lesen Sie die Vereinbarung durch und wählen Sie **EULA akzeptieren**.
5 Falls eine Aktualisierung verfügbar ist, klicken Sie auf **Annehmen**.
6 Wählen Sie **Standardmodus** oder **Getrennten Modus**.

> **ANMERKUNG:**
> Wenn Sie **Getrennter Modus** auswählen, kann VE nicht mehr in den Standardmodus geändert werden.
>
> Der getrennte Modus isoliert VE aus dem Internet und einem ungesicherten LAN oder anderen Netzwerk. Alle Aktualisierungen müssen manuell durchgeführt werden. Weitere Informationen über die Funktionalität und die Richtlinien des getrennten Modus finden Sie in der *Administrator-Hilfe*.

7 Wenn Sie aufgefordert werden, das Standardkennwort zu ändern, wählen Sie **Ja** aus.
8 Geben Sie auf dem Bildschirm *ddpuser-Kennwort einstellen* das aktuelle (Standard-) Passwort **ddpuser** und dann ein eindeutiges Kennwort ein. Wiederholen Sie es und wählen Sie **OK** aus.

   Passwörter müssen folgende Elemente enthalten:

   - Mindestens 8 Zeichen
   - Mindestens 1 Großbuchstaben
   - Mindestens 1 Ziffer
   - Mindestens 1 Sonderzeichen

9 Verwenden Sie im Dialogfeld *Hostname konfigurieren* die Zurücktaste, um den Standardhostnamen zu entfernen. Geben Sie einen eindeutigen Hostnamen ein und wählen Sie **OK** aus.
10 Wählen Sie im Dialogfeld *Netzwerkeinstellungen konfigurieren* eine der nachstehenden Optionen aus und wählen Sie dann **OK** aus.

   - (Standard) DHCP verwenden.

- (Empfohlen) Drücken Sie im Feld „DHCP verwenden“ die Leertaste, um das X zu entfernen, und geben Sie manuell die zutreffenden folgenden Adressen ein: Statische IP-Netzwerkmaske Standard-Gateway DNS-Server 1 DNS-Server 2 DNS-Server 3

ANMERKUNG: Bei Verwendung einer statischen IP-Adresse müssen Sie auch einen Host-Eintrag auf dem DNS-Server erstellen.

11 Verwenden Sie auf dem Bildschirm *Zeitzone* die Pfeiltasten, um Ihre Zeitzone hervorzuheben und wählen Sie dann **Eingabe** aus.

12 Wenn Sie aufgefordert werden, die Zeitzone zu bestätigen, wählen Sie **OK** aus.

13 Wenn die Nachricht angibt, dass die erste Konfiguration abgeschlossen ist, wählen Sie **OK** aus.

14 Kennwort für die Datenbank einstellen oder ändern

15 SMTP-Einstellungen konfigurieren

16 Ein bestehendes Zertifikat importieren oder ein neues Serverzertifikat registrieren

17 DDP Enterprise Server – VE aktualisieren

18 Installieren Sie einen FTP-Client, der SFTP an Port 22 unterstützt und richten Sie Dateiübertragung (FTP)-Benutzer ein.

Die Installationsaufgaben der DDP Enterprise Server – VE wurden abgeschlossen.

VE Remote Management-Konsole öffnen

Öffnen Sie die VE Remote Management-Konsole an dieser Adresse:

https://server.domain.com:8443/webui/

Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

Eine Liste der unterstützten Webbrowser finden Sie unter Voraussetzungen für die VE Remote Management Console.

Proxy-Modus installieren und konfigurieren

Proxy-Modus bietet eine Front-End-Option (z. B. DMZ-Modus) für die Verwendung mit DDP Enterprise Server – VE. Wenn Sie Dell-Komponenten in Ihre DMZ implementieren möchten, vergewissern Sie sich, dass sie ausreichend vor Angriffen geschützt sind.

ANMERKUNG: Der Beacon-Dienst wird im Rahmen dieser Installation zur Unterstützung des Data Guardian-Rückrufsignals installiert. Dieser fügt zu jeder durch Data Guardian geschützten Datei beim Ausführen des geschützten Office-Modus ein Rückrufsignal hinzu. Dies ermöglicht die Kommunikation zwischen jedem Gerät an jedem Standort und dem Dell Front-End-Server. Stellen Sie vor Verwendung des Rückrufsignals sicher, dass die erforderliche Netzwerksicherheit konfiguriert ist. Das Kontrollkästchen für die Richtlinie zur Aktivierung des Rückrufsignals ist standardmäßig aktiviert.

Für diese Installation benötigen Sie den vollständig qualifizierten Hostnamen des DMZ-Servers.

1 Wechseln Sie auf dem Dell Installationsmedium in das Dell Enterprise Server-Verzeichnis. **Entpacken** (NICHT kopieren/einfügen oder ziehen) Sie Dell Enterprise Server-x64 im Stammverzeichnis des Servers, auf dem Sie VE installieren möchten. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***

2 Doppelklicken Sie auf **setup.exe**.

3 Wählen Sie im Dialogfeld *InstallShield-Assistenten* die Sprache für die Installation aus, und klicken Sie dann auf **OK**.

4 Wenn die Voraussetzungen noch nicht installiert wurden, wird eine Meldung angezeigt, die Sie darüber informiert, welche Voraussetzungen installiert werden Klicken Sie auf **Installieren**.

5 Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.

6 Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen und klicken Sie auf **Weiter**.

7 Geben Sie den Produktschlüssel ein.

8 Wählen Sie **Front-End-Installation** aus, und klicken Sie dann auf **Weiter**.

9 Klicken Sie zur Installation des Front-End-Servers im Standardverzeichnis **C:\Programme\Dell** auf **Weiter**. Klicken Sie anderenfalls auf **Ändern**, um einen anderen Speicherort auszuwählen; klicken Sie anschließend auf **Weiter**.

10 Sie können aus verschiedenen digitalen Zertifikatstypen auswählen. **Es wird dringend empfohlen, ein digitales Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zu verwenden.**

Wählen Sie entweder Option „a“ oder „b“ unten aus:

a Um ein vorhandenes Zertifikat zu verwenden, das Sie bei einer Zertifizierungsstelle erworben haben, wählen Sie **Vorhandenes Zertifikat importieren** aus, und klicken Sie dann auf **Weiter**.

Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein.

Klicken Sie auf **Weiter**.

ANMERKUNG:

Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren

b Wählen Sie zum Erstellen eines selbstsignierten Zertifikats **Ein selbstsigniertes Zertifikat erstellen und in den Schlüsselspeicher importieren und klicken Sie auf Weiter.**

Geben Sie im Dialogfeld *Selbstsigniertes Zertifikat erstellen* die folgenden Informationen ein:

Vollständiger Computername (Beispiel: computername.domain.com)

Organisation

Organisationseinheit (Beispiel: Sicherheit)

Ort

Bundesstaat (vollständiger Name)

Land: Abkürzung aus zwei Buchstaben

Klicken Sie auf **Weiter**.

ANMERKUNG:

Das Zertifikat läuft standardmäßig in einem Jahr ab.

11 Geben Sie im Dialogfeld *Front-End-Server-Setup* den vollständigen Hostnamen oder DNS-Alias des Back-End-Servers ein, wählen Sie **Enterprise Edition** aus, und klicken Sie auf **Weiter**.

12 Über das Dialogfeld *Front-End-Server-Installationseinrichtung* können Sie Hostnamen und Ports anzeigen oder bearbeiten.

- Klicken Sie zum Übernehmen der Standard-Hostnamen und -Ports im Dialogfeld *Front-End-Server-Installationseinrichtung* auf **Weiter**.
- Klicken Sie zum Anzeigen oder Bearbeiten von Hostnamen im Dialogfeld *Front-End-Server-Setup* auf **Hostnamen bearbeiten**. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

ANMERKUNG:

Im Hostnamen darf kein Unterstrich (_) enthalten sein.

Heben Sie die Auswahl eines Proxys nur dann auf, wenn Sie sicher sind, dass Sie ihn nicht für die Installation konfigurieren wollen. Wenn Sie die Auswahl eines Proxys in diesem Dialogfeld aufheben, wird er nicht installiert.

Klicken Sie anschließend auf **OK**.

- Klicken Sie zum Anzeigen oder Bearbeiten von Ports im Dialogfeld *Front-End-Server-Setup* entweder auf **Externe Ports bearbeiten** oder **Interne Ports bearbeiten**. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

  Wenn Sie die Auswahl eines Proxys im Dialogfeld *Front-End-Hostnamen bearbeiten* aufheben, wird sein Port in den Dialogfeldern für Externe Ports und Interne Ports nicht angezeigt.

  Klicken Sie anschließend auf **OK**.

13 Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.

14 Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.

VE-Terminal – Grundkonfigurationsaufgaben

Die grundlegenden Konfigurationsaufgaben werden über das Hauptmenü aufgerufen.

Ändern des Hostnamens

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie aus dem Menü *Grundkonfiguration* den **Hostnamen** aus.

2 Verwenden Sie die Zurücktaste, um den bestehenden Hostnamen von DDP Enterprise Server – VE zu entfernen und ersetzen Sie ihn durch einen neuen. Wählen Sie dann **OK** aus.

Ändern der Netzwerkeinstellungen

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Netzwerkeinstellungen** aus.

2 Wählen Sie auf dem Bildschirm *Netzwerkeinstellungen konfigurieren* eine der nachstehenden Optionen aus und wählen Sie dann **OK** aus.

- (Standard) DHCP verwenden.
- (Empfohlen) Drücken Sie im Feld „DHCP verwenden“ die Leertaste, um das X zu entfernen, und geben Sie manuell die zutreffenden folgenden Adressen ein:

  Statische IP-Adresse

  Netzwerkmaske

  Standard-Gateway

  DNS-Server 1

  DNS-Server 2

  DNS-Server 3

  ANMERKUNG: Bei Verwendung einer statischen IP-Adresse müssen Sie einen Host-Eintrag auf dem DNS-Server erstellen.

DMZ-Hostnamen festlegen

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **DMZ-Hostname** aus.
2 Geben Sie den vollständig qualifizierten Domänennamen des DMZ-Servers ein und wählen Sie **OK** aus.

ANMERKUNG: Um den Proxy-Modus (DMZ-Modus) zu verwenden, müssen Sie den Proxy-Modus installieren und konfigurieren.

Ändern der Zeitzone

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie aus dem Menü *Grundkonfiguration* die **Zeitzone** aus.
2 Verwenden Sie auf dem Bildschirm *Zeitzone* die Pfeiltasten, um Ihre Zeitzone hervorzuheben und wählen Sie dann **Eingabe** aus.
3 Wenn Sie aufgefordert werden, die Zeitzone zu bestätigen, wählen Sie **OK** aus.

DDP Enterprise Server – VE aktualisieren

Informationen zu einer bestimmten Aktualisierung finden Sie unter „VE Technical Advisories“ auf der Dell Support-Website unter http://www.dell.com/support. Um das Versions- und Installationsdatum einer Aktualisierung zu sehen, die bereits angewendet wird, wählen Sie aus dem Menü **Basiskonfiguration** zunächst **DDP Enterprise Server – VE** > **Letzte erfolgreiche Aktualisierung angewendet** .

Anweisungen zum Erhalten von E-Mail-Benachrichtigungen, wenn VE-Aktualisierungen verfügbar sind finden Sie unter SMTP-Einstellungen konfigurieren.

ANMERKUNG: Im Standardmodus sollte nach der ursprünglichen Installation von DDP Enterprise Server – VE und vor der Aktivierung der Clients eine Aktualisierung durchgeführt werden.

Wenn Richtlinienänderungen vorgenommen, jedoch nicht in der Remote-Verwaltungskonsole bestätigt wurden, übernehmen Sie vor der VE-Aktualisierung die Richtlinienänderungen:

1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.
2 Klicken Sie im linken Menü auf **Verwaltung** > **Bestätigen**.
3 Geben Sie in das Kommentarfeld eine Beschreibung der Änderung ein.
4 Klicken Sie auf **Richtlinien bestätigen**.
5 Melden Sie sich nach Abschluss der Bestätigung von der Remote-Verwaltungskonsole ab.

VE aktualisieren (Standardmodus)

1 Dell empfiehlt, eine regelmäßige Sicherung durchzuführen. Stellen Sie vor der Aktualisierung sicher, dass der Sicherungsprozess ordnungsgemäß funktioniert hat. Siehe Sichern und wiederherstellen.
2 Wählen Sie aus dem Menü **Basiskonfiguration DDP Enterprise Server – VE aktualisieren**.
3 Wählen Sie die gewünschte Aktion aus:

- Aktualisierungsserver festlegen – Wählen Sie diese Option zum Festlegen oder Ändern des Serverstandorts für die DDP Enterprise Server – VE-Aktualisierungspakete aus. Verwenden Sie auf dem Bildschirm *Aktualisierungs-Server einstellen* die Zurücktaste, um den bestehenden Server-Hostnamen oder die IP-Adresse zu entfernen. Geben Sie den neuen, vollständig qualifizierten Domänennamen oder die IP-Adresse ein und wählen Sie **OK** aus.

  Der Standard-Aktualisierungsserver ist **act.credant.com**.
- Proxy-Einstellungen festlegen - Wählen Sie diese Option aus, um die Proxy-Einstellungen zum Herunterladen von Aktualisierungen festzulegen.

  Drücken Sie im Bildschirm *Proxy-Einstellungen konfigurieren* auf die Leertaste, um ein **X** ins Feld „Proxy verwenden“ einzugeben. Geben Sie die HTTPS-, HTTP- und FTP-Proxy-Adressen ein. Falls Firewall-Authentifizierung erforderlich ist drücken Sie die Leertaste, um ein **X** ins Feld „Authentifizierung erforderlich“ einzugeben. Geben Sie den Benutzernamen und das Passwort ein, und drücken Sie dann auf **OK**.

  ANMERKUNG: Geben Sie bei der Aktualisierung über eine FTP-Site den FTP-Benutzernamen und das Passwort gefolgt von der URL ein.
- Auf Aktualisierungen überprüfen – Wählen Sie diese Option aus, um auf dem Aktualisierungsserver nach Aktualisierungspaketen für DDP Enterprise Server – VE zu suchen.
- Aktualisierung herunterladen – Wählen Sie diese Option, um eine Aktualisierung herunterzuladen, die mit „Auf Aktualisierungen überprüfen“ gefunden wurde.
- Aktualisierung übernehmen – Wählen Sie diese Option aus, wenn Sie ein DDP Enterprise Server – VE-Aktualisierungspaket übernehmen möchten, das Sie heruntergeladen haben. Wählen Sie auf dem Bildschirm *Aktualisierungsdatei (.deb) auswählen* das Aktualisierungspaket aus, das Sie installieren möchten, und drücken Sie dann auf die **Eingabetaste**.
- Letzte erfolgreich übernommene Aktualisierung - Wählen Sie diese Option aus, um die Version und das Installationsdatum der aktuellen VE-Version anzuzeigen.

VE aktualisieren (getrennter Modus)

1 Dell empfiehlt, eine regelmäßige Sicherung durchzuführen. Stellen Sie vor der Aktualisierung sicher, dass der Sicherungsprozess ordnungsgemäß funktioniert hat. Siehe Sichern und wiederherstellen.

2 Rufen Sie die .deb-Datei ab, die die neueste VE-Aktualisierung von der Dell Support-Website enthält.

  VE-Downloads befinden sich im Ordner **Treiber & Downloads** unter

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

  oder

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

3 Speichern Sie die .deb-Datei im Ordner „/Aktualisierungen“ auf dem sicheren FTP-Server des VE.

  Stellen Sie sicher, dass der FTP-Client SFTP an Port 22 unterstützt und ein FTP-Benutzer eingerichtet wird. Siehe File Transfer (FTP)-Benutzer einrichten.

4 Wählen Sie aus dem Menü **Basiskonfiguration DDP Enterprise Server – VE aktualisieren**.

5 Wählen Sie **Aktualisierung anwenden** und drücken Sie **Eingabe**.

  Wenn die .deb-Datei nicht angezeigt wird, stellen Sie sicher, dass die .deb-Datei am richtigen Speicherort gespeichert ist.

6 Wählen Sie die .deb Aktualisierungsdatei aus, die Sie installieren möchten und drücken Sie **Eingabe**.

Benutzerkennwörter ändern

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Sie können die Passwörter für die folgenden Benutzer ändern:

- ddpuser (DDP Enterprise Server – VE-Terminal-Administrator) – Diese Benutzer hat Zugang zum VE-Terminal und der darin enthaltenen Menüs.
- ddpconsole (DDP Enterprise Server – VE-Shellzugriff) – Dieser Benutzer hat VE-Shellzugriff. Shell-Zugriff steht für einen Netzwerkadministrator zur Verfügung, um die Netzwerkkonnektivität zu überprüfen und allfällige Probleme zu beheben.
- dpsupport (Dell ProSupport Administrator) – Dieser Benutzer existiert nur für die Nutzung von Dell ProSupport. Sie kontrollieren das Kennwort für dieses Konto aus Sicherheitsgründen.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Benutzerpasswörter ändern** aus.
2 Wählen Sie auf dem Bildschirm *Benutzerpasswörter ändern* das zu ändernde Benutzerpasswort aus und wählen Sie dann **Eingabe** aus.
3 Geben Sie auf dem Bildschirm *Passwort einstellen* das aktuelle Passwort ein. Dann geben Sie das neue Passwort ein, wiederholen Sie es zur Bestätigung und wählen dann **OK** aus.

   Passwörter müssen folgende Elemente enthalten:

   - Mindestens 8 Zeichen
   - Mindestens 1 Großbuchstaben
   - Mindestens 1 Ziffer
   - Mindestens 1 Sonderzeichen

File Transfer (FTP)-Benutzer einrichten

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Sie können bis zu drei Benutzern Zugriff auf den sicheren FTP-Server von DDP Enterprise Server – VE für Sicherungs- und Wiederherstellungsaufgaben gewähren. Der VE-FTP-Server kann auch zum Speichern und Hochladen von Aktualisierungen auf den DDP Enterprise Server – VE genutzt werden.

1 Wählen Sie im Menü *Grundkonfiguration* **File Transfer (FTP)-Benutzer** aus.
2 Um einen FTP-Benutzer zu aktivieren, verwenden Sie auf dem Bildschirm *FTP-Benutzer konfigurieren* die Leertaste, um ein **X** im Statusfeld für den Benutzer einzugeben. Um einen FTP-Benutzer zu deaktivieren, drücken Sie die Leertaste, um das **X** im Statusfeld für den Benutzer zu entfernen.
3 Geben Sie einen Benutzernamen und ein Passwort für den SFTP-Benutzer ein.

   Passwörter müssen folgende Elemente enthalten:

   - Mindestens 8 Zeichen
   - Mindestens 1 Großbuchstaben
   - Mindestens 1 Ziffer
   - Mindestens 1 Sonderzeichen
4 Wenn Sie mit der Eingabe der SFTP-Benutzer fertig sind, wählen Sie **OK** aus.

Aktivierung von SSH

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Sie können SSH für die Support-Administrator-Anmeldung, Shell-Zugriff auf DDP Enterprise Server – VE und die Befehlszeilenschnittstelle des VE-Terminals aktivieren.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **SSH-Einstellungen** aus.
2 Markieren Sie den Benutzer, für den Sie SSH aktivieren möchten und drücken Sie die Leertaste, um ein **X** in sein Feld einzugeben und wählen Sie **OK** aus.

VE-Dienste starten oder beenden

Führen Sie diese Aufgabe nur bei Bedarf aus. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Um alle VE-Dienste gleichzeitig hoch- oder herunterzufahren, wählen Sie aus dem Menü *Grundkonfiguration* entweder **Anwendung starten** oder **Anwendung beenden** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.

ⓘ | **ANMERKUNG: Es kann bis zu zwei Minuten dauern, bis der Serverstatus geändert wird.**

Neustart von VE

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Gerät neu starten** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.
3 Melden Sie sich nach dem Neustart bei DDP Enterprise Server – VE an.

Herunterfahren von VE

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Scrollen Sie im Menü *Grundkonfiguration* nach unten und wählen Sie **Gerät herunterfahren** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.
3 Melden Sie sich nach dem Neustart bei DDP Enterprise Server – VE an.

VE-Terminal – Erweiterte Konfigurationsaufgaben

Die erweiterten Konfigurationsaufgaben werden über das Hauptmenü aufgerufen.

Kennwort für die Datenbank einstellen oder ändern

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Datenbank-Passwort** aus.
2 Geben Sie ein Passwort für den Zugang auf die Datenbank ein und wählen Sie dann **OK** aus.
Passwörter müssen folgende Elemente enthalten:

- Mindestens 8 Zeichen
- Mindestens 1 Großbuchstaben
- Mindestens 1 Ziffer
- Mindestens 1 Sonderzeichen

ANMERKUNG: Dell empfiehlt, nach Abschluss der Installation Sicherheitskopien der Passwörter zu erstellen.

SMTP-Einstellungen konfigurieren

Wenn Sie E-Mail-Benachrichtigungen von DDP Enterprise Server – VE empfangen **oder** Data Guardian verwenden möchten, befolgen Sie die Schritte in diesem Abschnitt zur Konfiguration der SMTP-Einstellungen. E-Mail-Benachrichtigungen der Art „DDP Enterprise Server – VE“ informieren die Empfänger über den Fehlerstatus bei DDP Enterprise Server – VE, über Kennwortaktualisierungen, über die Verfügbarkeit von Aktualisierungen bei DDP Enterprise Server – VE sowie über Kundenlizenzprobleme.

Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Führen Sie zur Konfiguration von SMTP-Einstellungen die folgenden Schritte aus:

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* die Option **E-Mail-Benachrichtigungen** aus.
2 Um E-Mail-Warnungen zu aktivieren, drücken Sie auf dem Bildschirm *E-Mail-Benachrichtigungen einrichten* auf die Leertaste, um ein **X** in das Feld „E-Mail-Warnungen aktivieren“ einzugeben.
3 Geben Sie den vollständigen Domänennamen des SMTP-Servers ein.
4 Geben Sie den SMTP-Port ein.
5 Geben Sie im Feld „Von Benutzer“ das E-Mail-Konto an, von dem die E-Mail-Benachrichtigungen gesendet werden sollen.
6 Geben Sie im Feld „Benutzer eingeben“ die E-Mail-Kontodaten an, die zu Änderungen an den konfigurierten E-Mail-Benachrichtigungen berechtigen.
7 Geben Sie unter „Passwort“ ein Passwort ein, das zu Änderungen an den konfigurierten E-Mail-Benachrichtigungen berechtigt.
8 Geben Sie in die Mail-ID-Felder für VE-Zustand, Passwort-Aktualisierungen und Verfügbare Aktualisierungen die Listen der Empfänger für jeden Benachrichtigungstyp ein. Halten Sie bei der Auflistung der Empfänger die folgenden Konventionen ein:
   - Geben Sie E-Mail-Adressen im Format empfänger@dell.com ein.
   - Trennen Sie Empfänger durch Komma oder Semikolon.
9 Drücken Sie zum Aktivieren von Erinnerungen im Feld „Dienste-Erinnerungsalarm“ die Leertaste, um ein **X** in das Feld zu setzen, und legen Sie anschließend das Erinnerungsintervall in Minuten fest. Nach dem Senden einer Benachrichtigung zu einem Problem in Zusammenhang mit dem Systemzustand wird nach Verstreichen des Erinnerungsintervalls ein Dienste-Erinnerungsalarm ausgelöst und der Host bzw. Dienst verbleibt im gleichen Zustand.
10 Wählen Sie zum Aktivieren von Berichten von Benachrichtigungen im Feld „Zusammenfassungsbericht“ das gewünschte Intervall aus (Täglich, Wöchentlich oder Monatlich), und drücken Sie dann die Leertaste, um ein **X** in das Feld zu setzen.
11 Wählen Sie **OK**.

Import eines bestehenden Zertifikats oder Registrierung eines neuen Serverzertifikats

Zertifikate müssen eingerichtet sein, bevor Sie Benutzer für DDP Enterprise Server – VE aktivieren können.

Sie können ein bestehendes Zertifikat importieren oder eine Zertifikatsanforderung über den DDP Enterprise Server – VE erstellen.

Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Import eines bestehenden Zertifikats

1 Exportieren Sie das bestehende Zertifikat mit der vollständigen Zertifikatkette aus dem Schlüsselspeicher.

> **ANMERKUNG: Bewahren Sie das Export-Kennwort auf. Sie müssen es eingeben, wenn Sie das Zertifikat in DDP Enterprise Server – VE importieren.**

2 Speichern Sie auf dem FTP-Server von DDP Enterprise Server – VE das Zertifikat unter **/opt/dell/vsftpd/files/certificates**.

3 Wählen Sie aus dem Menü *Erweiterte Konfiguration* des DDP Enterprise Server – VE **Server-Zertifikate** aus.

4 Wählen Sie **Bestehendes Zertifikat importieren** aus.

5 Wählen Sie eine in DDP Enterprise Server – VE zu installierende Zertifikatdatei aus.

6 Geben Sie auf Aufforderung das Zertifikat-Export-Passwort ein und wählen Sie dann **OK**.

7 Nach Abschluss des Imports wählen Sie **OK** aus.

Registrierung eines neuen Serverzertifikats

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Server-Zertifikate** aus.

2 Wählen Sie **Neues Server-Zertifikat** aus.

3 Wählen Sie **Zertifikatanforderung erstellen** aus.

4 Füllen Sie die Felder auf dem Bildschirm *Zertifikatanforderung erstellen* aus:

- Name des Landes: Zweistelliger Ländercode.
- *Bundesstaat bzw. Bundesland*: Geben Sie den Namen des Bundesstaats oder -landes ohne Abkürzungen ein (Beispiel: Bayern).
- *Ort/Stadt*. Geben Sie den entsprechenden Wert ein (z. B. Dallas).
- *Organisation*: Geben Sie den entsprechenden Wert ein (Beispiel: Dell).
- *Organisationseinheit*: Geben Sie den entsprechenden Wert ein (Beispiel: Sicherheit).
- *Allgemeiner Name:* Geben Sie den vollständig qualifizierten Domänennamen des Servers ein, auf dem DDP Enterprise Server – VE installiert ist. Zum vollständigen Namen gehören der Hostname und der Domänenname (Beispiel: server.domäne.com).
- *E-Mail-ID:* Geben Sie die E-Mail-Adresse ein, an die Ihr CSR gesendet wird.

5 Befolgen Sie Ihr Organisationsverfahren zum Erwerb eines SSL-Serverzertifikats bei einer Zertifizierungsstelle. Senden Sie den Inhalt der Zertifikatanforderungsdatei zum Signieren.

6 Wenn Sie das signierte Zertifikat erhalten haben, exportieren Sie es als .p7b-Datei und laden Sie die vollständige Zertifikatkette im .der-Format herunter.

7 Erstellen Sie Sicherungskopien des Zertifikats und der vollständigen Zertifikatkette.

8 Laden Sie die Zertifikatsdatei und die vollständige Vertrauenskette auf den FTP-Server von DDP Enterprise Server – VE.

9 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Server-Zertifikate** aus.

10 Wählen Sie **Neues Server-Zertifikat** aus.

11 Wählen Sie `Zertifikateintragung abschließen` aus.

12 Wählen Sie die in DDP Enterprise Server – VE zu installierende Zertifikatdatei aus.

13 Geben Sie bei entsprechender Aufforderung das Zertifikatkennwort ein: **changeit**.

Um die Vertrauensvalidierung auf Windows-basierten Encryption-Clients zu aktivieren, siehe „Manager-Vertrauenskettenprüfung aktivieren“.

Erstellen und Installieren eines selbstsignierten Zertifikats

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* des DDP Enterprise Server – VE **Server-Zertifikate** aus.
2 Wählen Sie **Erstellen und Installieren eines selbstsignierten Zertifikats** aus.
3 Um zu bestätigen, dass Sie das vorinstallierte Zertifikat mit einem neuen Zertifikat ersetzen möchten, klicken Sie auf **Ja**.
4 Geben Sie das Zertifikatkennwort ein: **changeit**.
5 Wählen Sie nach der Installation des neuen Zertifikats **OK** aus, und warten Sie bis die Dienste neu starten.

Die VE-Services werden automatisch neu gestartet.

Konfigurieren des Protokollrotators

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Standardmäßig ist die tägliche Protokollrotation aktiviert. Um die Standard-Protokollrotation zu ändern, wählen Sie aus dem Menü *Erweiterte Konfiguration* **Protokollrotations-Konfiguration** aus.

Um die Protokollrotation zu deaktivieren, verwenden Sie die Leertaste, um ein **X** in das Rotationsfeld „Nein“ einzugeben, und wählen Sie dann **OK**.

Führen Sie zur Aktivierung des Protokollrotators die folgenden Schritte aus:

1 Um tägliche, wöchentliche oder monatliche Rotation zu aktivieren, geben Sie mit der Leertaste ein **X** in das entsprechende Feld ein. Geben Sie bei der wöchentlichen oder monatlichen Rotation den entsprechenden Tag der Woche oder des Monats als Zahl ein, wobei Montag = 1 ist.
2 Geben Sie eine Uhrzeit für die Rotation in das Feld „Protokollrotationszeit“ ein.
3 Wählen Sie **OK**.

Sichern und wiederherstellen

Sicherungen können jederzeit konfiguriert oder durchgeführt werden und sind nicht erforderlich, um DDP Enterprise Server – VE verwenden zu können. Dell empfiehlt, einen regelmäßigen Sicherungsprozess zu konfigurieren.

Sicherungen können auf einem externen sicheren FTP-Server (empfohlen) oder auf DDP Enterprise Server – VE gespeichert werden. Wenn bei einem Speichern auf dem VE-Server die Festplattenkapazität auf 90 % steht, werden keinen neuen Sicherungen gespeichert. Sie erhalten eine Benachrichtigung per E-Mail, aus der hervorgeht, dass der Speicherplatz auf der Festplatte nicht mehr ausreicht.

ANMERKUNG:
Um Speicherplatz von Festplattenpartitionen einzusparen und das automatische Löschen von Sicherungen zu verhindern, entfernen Sie unnötige Sicherungen von DDP Enterprise Server - VE.

Sicherungen werden standardmäßig täglich ausgeführt. Dell empfiehlt, Sicherungen auf einem externen sicheren FTP-Server mit einer Häufigkeit zu speichern, die die Anforderungen der Organisation für Sicherungen und eine angemessene Nutzung von Speicherplatz erfüllt.

Zur Konfiguration eines Sicherungsplans wählen Sie aus dem Menü *Erweiterte Konfiguration* **Sicherung und Wiederherstellung > Konfiguration** aus und gehen folgendermaßen vor:

1 Zur Aktivierung täglicher, wöchentlicher oder monatlicher Sicherungen geben Sie mithilfe der Leertaste ein **X** in das entsprechende Feld ein. Geben Sie bei der wöchentlichen oder monatlichen Sicherung den entsprechenden Tag der Woche oder des Monats als Zahl ein, wobei Montag = 1 ist. Um die Sicherungen zu deaktivieren, geben Sie mithilfe der Leertaste ein **X** in das Feld „Keine Sicherungen“ ein und wählen Sie dann **OK**.

2 Geben Sie eine Uhrzeit für die Sicherung in das Feld „Sicherungszeit“ ein.

3 Wählen Sie **OK**.

Um eine sofortige Sicherung durchzuführen, wählen Sie im Menü *Erweiterte Konfiguration* **Sicherung und Wiederherstellung > Jetzt sichern** aus. Wenn „Sicherung bestätigen“ angezeigt wird, wählen Sie **OK**.

ANMERKUNG:

Bevor Sie eine Wiederherstellung beginnen, müssen alle VE-Server-Services laufen. **Serverstatus prüfen**. Wenn nicht alle Services laufen, starten Sie die Services neu. Weitere Informationen finden Sie unter **VE-Dienste starten oder beenden**. Beginnen Sie die Wiederherstellung ***nur***, wenn ***alle*** Dienste laufen.

Zur Wiederherstellung einer Sicherungsdatei wählen Sie aus dem Menü *Erweiterte Konfiguration* die Optionen **Sicherung und Wiederherstellung > Wiederherstellen** und dann die gewünschte wiederherzustellende Sicherungsdatei aus. Wählen Sie auf dem Bestätigungsbildschirm **Ja** aus.

VE startet neu und die Sicherung ist wiederhergestellt.

Sicherungen auf einem sicheren FTP-Server speichern

Um Sicherungen auf einem FTP-Server zu speichern, muss der FTP-Client SFTP auf Port 22 unterstützen.

Entsprechend den Sicherungsanforderungen der Organisation können Sicherungen auf die folgende Arten heruntergeladen werden:

- Manuell
- Durch automatisches Skript
- Durch die zugelassene Sicherungslösung der Organisation

Um Sicherungen mithilfe der Sicherungslösung der Organisation herunterzuladen, können Sie detaillierte Anweisungen vom Anbieter Ihrer Sicherungslösung erhalten.

ANMERKUNG:

Virtual Edition beruht auf Linux Debian Ubuntu x64.

Melden Sie sich bei VE als „ddpsupport“ an, und verwenden Sie den Befehl „sudo“ zum Konfigurieren Ihrer Sicherungslösung:

`sudo` <Anleitungen vom Anbieter der Sicherungslösung>

Sicherungsinhalte der folgenden Ordner:

/opt/dell/vsftpd/files/backup (erforderlich)

/opt/dell/vsftpd/files/certificates (dringend empfohlen)

/opt/dell/vsftpd/files/support (optional)

Wenn der sudo-Vorgang läuft, geben Sie **Beenden** ein und drücken Sie die **Eingabetaste** bis die Anmeldeaufforderung erscheint.

Remotezugriff auf die Datenbank aktivieren

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

ANMERKUNG: Dell empfiehlt, den Remotezugriff auf die Datenbank nur bei Bedarf zu aktivieren.

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Remote-Zugriff auf die Datenbank** aus.
2 Geben Sie mithilfe der Leertaste ein **X** in das Feld „Remotezugriff auf die Datenbank aktivieren“ ein und wählen Sie dann **OK** aus. Wenn das Datenbankpasswort noch nicht konfiguriert wurde, wird eine Aufforderung für das Datenbankpasswort angezeigt.
3 Geben Sie das Datenbankpasswort ein.
4 Geben Sie das Datenbankpasswort erneut ein.

DDP-Anwendungskomponenten werden automatisch gestoppt.

DMZ-Serverunterstützung aktivieren

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von DDP Enterprise Server – VE ist nicht erforderlich. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **DMZ Server-Support aktivieren** aus.
2 Geben Sie mithilfe der Leertaste ein **X** in das Feld „DMZ Server-Support“ ein und wählen Sie dann **OK** aus.

ANMERKUNG: Um den Proxy-Modus (DMZ-Modus) zu verwenden, müssen Sie den Proxy-Modus installieren und konfigurieren.

3

DDP Enterprise Server – VE-Administratoraufgaben

DDP Enterprise Server – VE-Terminal-Sprache festlegen oder ändern

Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie im Hauptmenü **Sprache einstellen** aus.
2 Wählen Sie mithilfe der Pfeiltasten die gewünschte Sprache aus.

Serverstatus prüfen

Um den Status der DDP Enterprise Server – VE-Dienste zu prüfen, wählen Sie aus dem Hauptmenü **Serverstatus** aus.

Die folgende Tabelle zeigt die einzelnen Dienste und deren Funktion.

Name	Beschreibung
Dell Message Broker	Enterprise Server-Bus
Dell Identity Server	Verarbeitet Authentifizierungsanforderungen für die Domäne.
Dell Compatibility Server	Ein Dienst für die Verwaltung der Unternehmensarchitektur.
Dell Security Server	Stellt den Mechanismus für die Steuerung von Befehlen und die Kommunikation mit Active Directory bereit. Wird zur Kommunikation mit dem Dell Policy Proxy verwendet.
Dell Compliance Reporter	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität.
Dell Core Server	Ein Dienst für die Verwaltung der Unternehmensarchitektur.
Dell Core Server HA (High Availability - Hohe Verfügbarkeit)	Ein High-Availability-Dienst, der beim Verwalten der Enterprise-Architektur eine höhere Sicherheit und Leistung von HTTPS-Verbindungen ermöglicht.
Dell Inventory Server	Verarbeitet die Bestandswarteschlange.
Dell Forensic Server	Bietet Web-Services für die forensische API.
Dell-Richtlinien-Proxy	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden.

DDP Enterprise Server – VE überwacht und startet seine Dienste, falls erforderlich.

ANMERKUNG: Wenn der Datenbankanpassungsvorgang fehlschlägt, werden die Server in den Status „Fehler bei der Ausführung“ versetzt. Zur Überprüfung der Datenbankanpassung wählen Sie im Hauptmenü die Option „Protokolle anzeigen“ aus.

Anzeigen von Protokollen

Wenn Sie die folgenden Protokolle prüfen möchten, wählen Sie im Hauptmenü **Protokolle anzeigen** aus.

Syslog Log Mail Log Auth Log (SSH) Postgres Log Monitor Log

- Systemprotokolle

  Syslog-Protokoll

  E-Mail-Protokoll

  Autorisierungsprotokoll (SSH)

  Postgres-Protokoll

  Überwachungsprotokoll
- Serverprotokolle

  Compatibility Server

  Security Server

  Message Broker

  Core Server

  Core Server HA

  Compliance Reporter

  Identity Server

  Inventory Server

  Forensics Server

  Policy Proxy
- Protokoll der Datenbankanpassung

Öffnen der Befehlszeilenschnittstelle

Zum Öffnen der Befehlszeilenschnittstelle wählen Sie im Hauptmenü **Shell starten** aus.

Wenn Sie die Befehlszeilenschnittstelle verlassen möchten, geben Sie **Beenden** ein und drücken dann die **Eingabetaste**.

Erstellen eines Systemmomentaufnahme-Protokolls

Wenn Sie ein System-Schnappschuss-Protokoll für Dell ProSupport erstellen möchten, wählen Sie aus dem Hauptmenü **Support-Tools** aus.

1 Wählen Sie im Menü *Support-Tools* **System Schnappschuss-Protokoll erstellen** aus.
2 Wenn angezeigt wird, dass die Datei erstellt wurde, wählen Sie **OK** aus.

Wenn der ddpsupport-Benutzer aktiviert ist, kann Dell ProSupport das Protokoll vom SFTP-Server von DDP Enterprise Server – VE abrufen. Wenn der ddpsupport-Benutzer nicht aktiviert ist, wenden Sie sich an den Dell ProSupport. Weitere Informationen finden Sie unter Dell ProSupport kontaktieren.

4

DDP Enterprise Server – VE Wartung

Sie müssen unnötige DDP Enterprise Server – VE-Sicherungen entfernen.

Nur die letzten zehn Sicherungskopien werden erhalten. Wenn der freie Speicherplatz auf der Partition zehn Prozent oder weniger beträgt, werden keine Sicherungskopien mehr gespeichert. In diesem Fall erhalten Sie eine Benachrichtigung per E-Mail, dass der Speicherplatz auf der Festplatte nicht mehr ausreicht.

5

Fehlerbehebung für DDP Enterprise Server – VE

Wenn ein Fehler auftritt und Sie die E-Mail-Benachrichtigungen konfiguriert haben, erhalten Sie eine Benachrichtigung per E-Mail. Führen Sie je nach den Informationen in der E-Mail-Benachrichtigung die folgenden Schritte aus:

1 Überprüfen der verfügbaren Protokolldateien.
2 Bei Bedarf Neustart der Dienste. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.
3 Systemmomentaufnahme-Protokoll erstellen.
4 Kontaktieren Sie den Dell ProSupport. Weitere Informationen finden Sie unter Dell ProSupport kontaktieren.

Konfigurationsaufgaben nach der Installation

Nach der Installation müssen einige Komponenten Ihrer Umgebung möglicherweise konfiguriert werden. Dies hängt von der Dell Data Protection-Lösung ab, die Ihre Organisation verwendet.

VE für Data Guardian konfigurieren

Um VE für die Unterstützung von Data Guardian zu konfigurieren, stellen Sie in der VE Remote-Verwaltungskonsole die Schutzrichtlinie „Cloud Encyrption“ auf „Ein“. Um den Modus „geschützte Office-Dokumente“ für Data Guardian zu aktivieren, stellen Sie die Richtlinie „geschützter Office-Dokumente“ auf „Ein“.

Informationen zum Installieren des Data Guardian-Client finden Sie im *Enterprise Edition Erweitertes Installationshandbuch*, *Enterprise Edition Grundlegendes Installationshandbuch*, oder im *Data GuardianBenutzerhandbuch*.

Installieren und Konfigurieren des EAS-Managements für Mobile Edition

Bei der Verwendung von Mobile Edition müssen Sie EAS-Management installieren und konfigurieren. Wenn Sie Mobile Edition nicht verwenden möchten, überspringen Sie diesen Abschnitt.

Voraussetzungen

- Die Anmeldedaten für den EAS Mailbox Manager-Dienst müssen Berechtigungen zum Erstellen/Ändern der Exchange ActiveSync-Richtlinie, zur Zuweisung von Richtlinien an die Postfächer der Benutzer und zum Abfragen von Informationen über ActiveSync-Geräte umfassen.
- Das EAS-Konfigurationsprogramm muss mit Administrator-Berechtigungen zum Ändern von Dateien und zum Neustart von Diensten ausgeführt werden.
- Netzwerkverbindung zum DDP Enterprise Server – VE ist erforderlich.
- Halten Sie den Hostnamen oder die IP-Adresse von DDP Enterprise Server – VE bereit.
- Microsoft Message Queuing (MSMQ) muss bereits auf dem Server installiert/konfiguriert sein, auf dem die Exchange-Umgebung gehostet wird. Ist dies nicht der Fall, dann installieren Sie MSMQ 4.0 auf Windows Server 2008 oder Windows Server 2008 R2 (auf dem Server, der die Exchange-Umgebung hostet) – http://msdn.microsoft.com/en-us/library/aa967729.aspx

Während der Implementierung

Wenn Sie Exchange ActiveSync verwenden möchten, um Mobilgeräte über Mobile Edition zu verwalten, muss Ihre Exchange Server-Umgebung konfiguriert werden.

Installation des EAS-Geräte-Managers

1 Navigieren Sie auf dem Mobile Edition-Installationsmedium zum Ordner „EAS-Management“. Kopieren Sie vom Ordner EAS-Gerätemanager „setup.exe“ in Ihre(n) *Exchange Client-Zugangsserver*.

2 Doppelklicken Sie auf **setup.exe**, um mit der Installation zu beginnen. Wenn Ihre Umgebung mehr als einen *Exchange Client Zugangsserver* enthält, führen Sie dieses Installationsprogramm auf jedem davon aus.

3 Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

4 Klicken Sie auf **Weiter**, wenn der *Startbildschirm* angezeigt wird.

5 Lesen Sie die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.

6 Klicken Sie auf **Weiter**, um den EAS-Geräte-Manager am Standardspeicherort **C:\Inetpub\wwwroot\Dell\EAS Device Manager\ zu installieren.**

7 Klicken Sie auf **Installieren** auf dem Bildschirm *Bereit für Installation*.

Der Installationsfortschritt wird in einem Statusfenster angezeigt.

8 Markieren Sie nach Wunsch das Kontrollkästchen, um das Windows Installationsprotokoll anzuzeigen und klicken Sie auf **Fertigstellen**.

Installation des EAS-Postfach-Managers

1 Navigieren Sie auf dem Mobile Edition-Installationsmedium zum Ordner „EAS-Management“. Kopieren Sie setup.exe aus dem Ordner „EAS-Postfachmanagement“ in Ihre(n) *Exchange Mailbox-Server*.

2 Doppelklicken Sie auf **setup.exe**, um mit der Installation zu beginnen. Sollte Ihre Umgebung mehr als einen *Exchange Mailbox Server* enthalten, führen Sie dieses Installationsprogramm auf jedem davon aus.

3 Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

4 Klicken Sie auf **Weiter**, wenn der *Startbildschirm* angezeigt wird.

5 Lesen Sie die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.

6 Klicken Sie auf **Weiter**, um den EAS-Postfachmanager am Standardspeicherort **C:\Program Files\Dell\EAS Mailbox Manager** zu installieren.

7 Geben Sie auf dem *Anmeldebildschirm* die Anmeldeinformationen für das Benutzerkonto ein, über das auf diesen Dienst zugegriffen werden soll.

Benutzername: DOMÄNE\Benutzername

Passwort: das mit diesem Benutzernamen verknüpfte Passwort

Klicken Sie auf **Weiter**.

8 Klicken Sie auf **Installieren** auf dem Bildschirm *Bereit für Installation*.

Der Installationsfortschritt wird in einem Statusfenster angezeigt.

9 Markieren Sie nach Wunsch das Kontrollkästchen, um das Windows Installationsprotokoll anzuzeigen und klicken Sie auf **Fertigstellen**.

Verwendung des EAS-Konfigurationsprogramms

1 Gehen Sie auf demselben Rechner zu **Start** > **Dell** > **EAS-Konfigurationshilfsprogramm** > **EAS-Konfiguration** und führen Sie das EAS-Konfigurationshilfsprogramm aus.

2 Klicken Sie auf **Setup**, um die EAS-Management-Einstellungen zu konfigurieren.

3 Geben Sie die folgenden Informationen ein:

Hostname für DDP Enterprise Server – VE

Intervall für Dell Policy Proxy-Abfragen (die Standardeinstellung ist 1 Minute)

Aktivieren Sie das Kontrollkästchen für die Ausführung des EAS-Geräte-Managers im Berichtsmodus (während der Implementierung empfohlen).

> **ANMERKUNG:**
> Im Berichtsmodus erhalten unbekannte Geräte/Benutzer Zugriff auf Exchange ActiveSync, aber Sie empfangen die Berichte zum Datenverkehr. Sobald Ihre Implementierung abgeschlossen ist, können Sie diese Einstellung ändern, um die Sicherheit zu erhöhen.

Klicken Sie auf **OK**.

4 Eine Erfolgsmeldung wird angezeigt. Klicken Sie auf **Ja**, um IIS- und EAS-Postfach-Manager-Dienste neu zu starten.

5 Klicken Sie nach Abschluss auf **Beenden**.

Nach der Implementierung

Führen Sie nach Abschluss der Implementierung die folgenden Schritte aus, um die Sicherheit zu erhöhen.

Auf Ihrem/Ihren Exchange-Postfachserver(n)

1 Gehen Sie zu **Start** > **Dell** > **EAS-Konfigurationshilfsprogramm** > **EAS-Konfiguration** und führen Sie das EAS-Konfigurationshilfsprogramm aus.

2 Klicken Sie auf **Setup**, um die EAS-Management-Einstellungen zu konfigurieren.

3 Geben Sie die folgenden Informationen ein:

Hostname für DDP Enterprise Server – VE

Intervall für Dell Policy Proxy-Abfragen (die Standardeinstellung ist 1 Minute)

Deaktivieren Sie das Kontrollkästchen für die Ausführung des EAS-Geräte-Managers im Berichtsmodus

Klicken Sie auf **OK**.

4 Eine Erfolgsmeldung wird angezeigt. Klicken Sie auf **Ja**, um IIS und EAS Mailbox Manager Dienste neu zu starten.

5 Klicken Sie nach Abschluss auf **Beenden**.

Manager-Vertrauenskettenprüfung aktivieren

Wenn ein selbstsigniertes Zertifikat auf VE-Server für SED oder BitLocker Manager verwendet wird, muss die SSL-/TLS-Vertrauensprüfung auf dem Client-Computer ***deaktiviert*** bleiben. Vor dem Aktivieren der SSL/TLS-Vertrauensprüfung auf dem Client müssen die folgenden Voraussetzungen erfüllt sein:

- Ein durch eine Stammzertifizierungsstelle, wie beispielsweise Ensign oder Verisign signiertes Zertifikat muss in VE-Server importiert werden. Siehe Import eines bestehenden Zertifikats oder Registrierung eines neuen Serverzertifikats.
- Die vollständige Vertrauenskette des Zertifikats muss im Microsoft Keystore des Client-Computers gespeichert werden.

Um die SSL/TLS-Trust-Validierung auf dem Clientcomputer zu aktivieren, ändern Sie den Wert des folgenden Registry-Eintrags in 0:

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):0

Aufgaben des Administrators der VE Remote Management-Konsole

Dell Administratorrolle zuweisen

1 Melden Sie sich als Dell Administrator an der Remote Management Console an. Verwenden Sie dazu die folgende Adresse: https://server.domain.com:8443/webui/. Die Standardanmeldeinformationen lauten **superadmin/changeit**.

2 Klicken Sie im linken Bereich auf **Bestückung** > **Domänen**.

3 Klicken Sie auf eine Domäne, der Sie einen Benutzer hinzufügen möchten.

4 Klicken Sie auf der Seite „Domänendetails“ auf die Registerkarte **Mitglieder**.

5 Klicken Sie auf **Benutzer hinzufügen**.

6 Geben Sie einen Filter ein, um den Benutzernamen nach allgemeinem Namen, UPN (Universal Principal Name) oder SAM-Kontonamen zu suchen. Der Platzhalter ist *.

Auf dem Unternehmensverzeichnisserver muss für jeden Benutzer ein allgemeiner Name, ein UPN (Universal Principal Name) und ein SAM-Kontoname definiert sein. Wenn ein Benutzer einer Domäne oder Gruppe angehört, aber nicht in der Liste der Domänen- oder Gruppenmitglieder im Management aufgeführt wird, überprüfen Sie, ob alle drei Namen für diesen Benutzer auf dem Unternehmensverzeichnisserver korrekt definiert sind.

Bei der Abfrage wird automatisch zunächst nach dem allgemeinen Namen, dann nach dem UPN und dann nach dem SAM-Kontonamen gesucht, bis ein Treffer gefunden wurde.

7 Wählen Sie die Benutzer, die Sie zur Domäne hinzufügen möchten, aus der *Verzeichnisbenutzerliste* aus. Verwenden Sie <Umschalt><Klick> oder <Strg><Klick>, um mehrere Benutzer auszuwählen.

8 Klicken Sie auf **Hinzufügen**.

9 Klicken Sie in der Menüleiste auf die Registerkarte **Details und Aktionen** des angegebenen Benutzers.

10 Scrollen Sie durch die Menüleiste und wählen Sie die Registerkarte **Admin**.

11 Wählen Sie die Administratorrollen aus, die Sie diesem Benutzer zuweisen möchten.

12 Klicken Sie auf **Speichern**.

Mit Dell Administratorrolle anmelden

1 Melden Sie sich von der Remote Management Console des Enterprise Servers ab.

2 Melden Sie sich mit den Anmeldeinformationen eines Domänenbenutzers bei der Remote Management Console des Enterprise Servers an.

Klicken Sie auf „?“ in der oberen rechten Ecke der Remote Management Console, um die *Dell Data Protection AdminHelp* zu starten. Die Seite *Erste Schritte* wird angezeigt. Klicken Sie auf **Domänen hinzufügen**.

Für Ihre Organisation wurden grundlegende Richtlinien festgelegt, aber je nach Ihren Anforderungen müssen diese möglicherweise wie folgt geändert werden (für alle Aktivierungen sind Lizenzen und Berechtigungen erforderlich):

- Windows-Computer werden verschlüsselt.
- Computer mit selbstverschlüsselnden Laufwerken werden verschlüsselt.
- Windows-Computer mit Hardware Crypto Accelerator werden verschlüsselt.
- BitLocker Management ist nicht aktiviert
- Advanced Threat Protection ist nicht aktiviert

- Der Bedrohungsschutz ist aktiviert
- Externe Medien werden nicht verschlüsselt.
- An Ports angeschlossene Geräte werden nicht verschlüsselt.
- Data Guardian ist aktiviert.
- Die Mobile Edition wird nicht aktiviert.

  Im Hilfethema *Richtlinien verwalten* der AdminHelp finden Sie Anweisungen zum Navigieren zu Technologiegruppen und Richtlinienbeschreibungen.

Richtlinien bestätigen

Wenn die Installation abgeschlossen ist, bestätigen Sie die Richtlinien.

Um Richtlinien nach der Installation oder später, nachdem die Richtlinienänderungen gespeichert sind, zu bestätigen, führen Sie die folgenden Schritte aus:

1 Klicken Sie im linken Fensterbereich auf **Verwaltung** > **Festlegen**.
2 Geben Sie in das Kommentarfeld eine Beschreibung der Änderung ein.
3 Klicken Sie auf **Richtlinien bestätigen**.

8

Lösungsports

In der folgenden Tabelle werden die einzelnen Komponenten mit ihren Funktionen aufgeführt.

Name	Standardport	Beschreibung	Erforderlich für
Compliance Reporter	HTTP(S)/8084	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität. Eine Komponente des DDP Enterprise Server – VE.	Berichterstellung
Remote Management Console	HTTPS/8443	Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung. Eine Komponente des DDP Enterprise Server – VE.	Alle
Core Server	HTTPS/8888	Verwaltet den Richtlinienablauf, Lizenzen und die Registrierung für die Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Protection Verarbeitet Bestandslistendaten zur Verwendung durch den Compliance Reporter und die Remote-Management-Konsole. Sammelt und speichert Authentifizierungsdaten Steuert den rollenbasierten Zugriff. Eine Komponente des DDP Enterprise Server – VE.	Alle
Core Server HA (High Availability - Hohe Verfügbarkeit)	HTTPS/8888	Ein High-Availability-Dienst, der eine höhere Sicherheit und Leistung von HTTPS-Verbindungen mit der Remote-Management-Konsole, Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Protection ermöglicht. Eine Komponente des DDP Enterprise Server – VE.	Alle
Security Server	HTTPS/8443	Kommuniziert mit dem Policy Proxy; verwaltet Abrufungen von Forensic Keys, Aktivierungen von Clients, Data Guardian-Produkte und die SED-PBA-Kommunikation. Eine Komponente des DDP Enterprise Server – VE.	Alle
Compatibility Server	TCP/1099 (geschlossen)	Ein Dienst für die Verwaltung der Unternehmensarchitektur. Sammelt und speichert anfängliche Bestandslistendaten während der Aktivierung und Richtliniendaten während Migrationen. Verarbeitet Daten auf	Alle

Name	Standardport	Beschreibung	Erforderlich für
		Grundlage von Benutzergruppen in diesem Dienst. Eine Komponente des DDP Enterprise Server – VE.	
Message Broker-Service	TCP/61616 und STOMP/61613 (geschlossen, andernfalls ist 61613 bei Konfiguration für DMZ offen)	Handhabt die Kommunikation zwischen Diensten des DDP Enterprise Server – VE. Stellt durch den Compatibility Server für Policy-Proxy-Warteschlangen erzeugte Richtlinieninformationen bereit. Eine Komponente des DDP Enterprise Server – VE.	Alle
Identity Server	HTTPS/8445	Handhabt Domänen-Authentifizierungsanfragen, einschließlich der Authentifizierung des SED Manager. Erfordert ein Active-Directory-Konto. Eine Komponente des DDP Enterprise Server – VE.	Alle
Forensics Server	HTTPS/8448	Ermöglicht es Administratoren mit entsprechenden Berechtigungen, Verschlüsselungsschlüssel von der Remote-Management-Konsole zur Verwendung beim Entsperren von Daten oder Entschlüsselungsaufgaben zu erhalten. Eine Komponente des DDP Enterprise Server – VE.	Forensic API
Inventory Server	8887	Verarbeitet die Bestandswarteschlange. Eine Komponente des DDP Enterprise Server – VE.	Alle
Policy Proxy	TCP/ 8000/8090	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden. Eine Komponente des DDP Enterprise Server – VE.	Enterprise Edition für Mac Enterprise Edition für Windows Mobile Edition
LDAP	389/636, 3268/3269 RPC – 135, 49125+	**Port 3268** – Dieser Port wird für Abfragen verwendet, die spezifisch für den globalen Katalog vorgesehen sind. LDAP-Anfragen, die an Port 3268 gesandt wurden, können zur Suche nach Objekten im ganzen Wald verwendet werden. Es können jedoch nur die Attribute zurückgegeben werden, die zur Replikation im globalen Katalog markiert sind. Das Departement eines Benutzers kann beispielsweise nicht unter Verwendung von Pport 3268 zurückgegeben werden, da dieses Attribut nicht in den globalen Katalog repliziert wurde. **Port 389** - Dieser Port wird zur Anforderung von Informationen vom lokalen Domänencontroller verwendet. LDAP-Anfragen, die an Port 389	Alle

Name	Standardport	Beschreibung	Erforderlich für
		gesandt wurden, können nur zur Suche nach Objekten innerhalb der Startdomäne des globalen Katalogs verwendet werden. Die anfordernde Anwendung kann jedoch alle Attribute für diese Objekte ermitteln. Eine Anfrage an Port 389 könnte beispielsweise zur Ermittlung des Departements eines Benutzers verwendet werden.	
Client-Authentifizierung	HTTPS/8449	Ermöglicht Client-Servern die Authentifizierung bei Dell Enterprise Server – VE.	Server-Verschlüsselung
Rückrufsignal	HTTP/8446	Ermöglicht die Einführung eines Rückrufsignals in jeder geschützten Office-Datei während Data Guardian im Modus für gesichertes Office ausgeführt wird.	Data Guardian
Advanced Threat Prevention	HTTPS/TCP/443	Client-Kommunikation bei Verwendung von Advanced Threat Prevention	Advanced Threat Prevention
EAS-Geräte-Manager	k. A.	Aktiviert die over-the-air-Funktionalität. Ist auf dem Exchange-Client-Zugriffsserver installiert.	Exchange ActiveSync-Verwaltung von Mobilgeräten.
EAS Mailbox Manager	k. A.	Der Postfach-Agent, der auf dem Exchange-Postfachserver installiert ist.	Exchange ActiveSync-Verwaltung von Mobilgeräten.

NTP-Uhrzeitsynchronisierung: TCP und UDP/123 (weitere Informationen finden Sie unter https://help.ubuntu.com/lts/serverguide/NTP.html.)