DDP Enterprise Server - Virtual Edition

VE クイックスタートガイドおよびインストールガイド v9.7

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

VE クイックスタートガイドおよびインストールガイド

2017 - 04

Rev. A01

目次

1

Virtual Edition クイックスタートガイド

このクイックスタートガイドは経験のあるユーザー対象で、DDP Enterprise Server - VE を素早く準備して稼動させるためのものです。原則として、デルではまず最初に DDP Enterprise Server - VE をインストールし、その後クライアントをインストールすることをお勧めします。

詳細な手順については、「Virtual Edition インストールガイド」を参照してください。

VE の前提条件については、「DDP Enterprise Server - VE の前提条件」、「VE リモート管理コンソールの前提条件」、および「プロキシモードの前提条件」を参照してください。

既存の DDP Enterprise Server - VE のアップデート方法については、「Enterprise Server - VE のアップデート」を参照してください。

DDP Enterprise Server - VE のインストール

1 Dell Data Protection ファイルが保存されているディレクトリを参照してダブルクリックし、VMware **DDP Enterprise Server - VE v9.x.x Build x.ova** にインポートします。
2 DDP Enterprise Server - VE の電源をオンにします。
3 画面に表示される手順に従います。

VE の設定

ユーザーをアクティブ化する前に、DDP Enterprise Server - VE ターミナルで次の設定タスクを完了する必要があります。

- データベースパスワードの設定または変更
- SMTP 設定の構成
- 既存の証明書のインポートまたは新規サーバー証明書の登録
- DDP Enterprise Server - VE のアップデート
- ポート 22 で SFTP をサポートする FTP クライアントをインストールし、ファイル転送（FTP）ユーザーの設定をセットアップします。

  組織に外向きデバイスがある場合は、「プロキシモードのインストールと設定」を参照してください。

> **メモ: Enterprise Edition のクライアントライセンスが工場から付与される場合、または工場からライセンスを購入した場合において資格を有効にするには、ドメインコントローラで GPO を設定します（これは Virtual Edition を実行するものと同じサーバーではない場合があります）。サーバーとの通信に送信ポート 443 が使用可能であることを確認します。ポート 443 が何らかの理由でブロックされている場合、資格機能は機能しません。**

VE リモート管理コンソールを開く

次のアドレスから VE リモート管理コンソールを開きます。

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

デフォルトの資格情報は **superadmin/changeit** です。

サポートされる Web ブラウザのリストについては、「VE リモート管理コンソールの前提条件」を参照してください。

管理作業

VE リモート管理コンソールをまだ起動していない場合は、ここで起動してください。デフォルトの資格情報は **superadmin/changeit** です。

デルでは、なるべく早く管理者役割を割り当てることをお勧めします。このタスクをすぐに完了するには、「Dell 管理者役割の割り当て」を参照してください。

VE リモート管理コンソールの右上隅の「?」をクリックして、*Dell Data Protection AdminHelp* を起動します。はじめに ページが表示されます。**ドメインの追加** をクリックします。

組織にはベースラインポリシーが設定されていますが、次のように、特定のニーズに応じて変更する必要が生じる場合があります（ すべてのアクティブ化はライセンスおよび資格によって決まります ）。

- Windows コンピュータは暗号化されます
- 自己暗号化ドライブが搭載されたコンピュータは暗号化されます
- BitLocker 管理は無効です
- Advanced Threat Protection が有効になっていません
- Threat Protection は有効です
- 外部メディアは暗号化されません
- ポートに接続されているデバイスは暗号化されません
- Dell Data Guardian が有効になります
- Mobile Edition は無効です

Technology Group とポリシーの説明については、AdminHelp トピックの「ポリシーの管理」を参照してください。

これで、クイックスタートタスクが完了しました。

Virtual Edition インストールガイド

本インストールガイドは、専門知識をお持ちでないユーザーのために DDP Enterprise Server - VE のインストールと設定について説明するものです。原則として、デルではまず最初に DDP Enterprise Server - VE をインストールし、その後クライアントをインストールすることをお勧めします。

既存の DDP Enterprise Server - VE のアップデート方法については、「Enterprise Server - VE のアップデート」を参照してください。

DDP Enterprise Server - VE について

DDP Enterprise Server - VE は Dell ソリューションのセキュリティ管理部分です。管理者は、VE リモート管理コンソールを使用して、企業全体のエンドポイント、ポリシーの適用、および保護の状態を監視できます。プロキシモードは、DDP Enterprise Server - VE で使用するフロントエンド DMZ モードのオプションを提供します。

DDP Enterprise Server - VE には次の機能があります。

- 最大 3500 台のデバイスの一元管理
- 役割ベースのセキュリティポリシーの作成と管理
- 管理者がサポートするデバイス復元
- 管理者職務の分割
- セキュリティポリシーの自動分配
- コンポーネント間での通信のための信頼済みパス
- 固有暗号化キーの生成および自動かつセキュアなキーエスクロー
- 一元的なコンプライアンス監査とレポート
- 自己署名証明書の自動生成

Dell ProSupport へのお問い合わせ

Dell Data Protection 製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 431003）に電話をかけてください。

さらに、dell.com/support で Dell Data Protection 製品のオンラインサポートもご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の国際電話番号をチェックしてください。

要件

DDP Enterprise Server - VE 前提条件

ハードウェア

DDP Enterprise Server - VE に推奨されるディスク容量は 80 GB です。

仮想環境

DDP Enterprise Server - VE v9.6 は、以下の仮想環境で検証されました。

仮想環境

- VMware Workstation 12.5
  - 64 ビット CPU（必須）
  - 4 GB RAM（推奨）
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/workstation-11/index.jsp を参照してください。

- VMware Workstation 11
  - 64 ビット CPU（必須）
  - 4 GB RAM（推奨）
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/workstation-11/index.jsp を参照してください。

- VMware ESXi 6.0
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-60/index.jsp を参照してください。

- VMware ESXi 5.5
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-55/index.jsp を参照してください。

- Hyper-V Server（フルまたはコアインストール）
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ

仮想環境

- 最小 8 GB RAM（推奨）
- オペレーティングシステムは必要ありません
- ハードウェアは Hyper-V 最小要件を満たしている必要があります
- イメージ専用リソース用に最小 4 GB の RAM
- 第 1 世代の仮想マシンとして実行する必要があります
- 詳細については、https://technet.microsoft.com/en-us/library/hh923062.aspx を参照してください。

VE リモート管理コンソールの前提条件

インターネットブラウザ

メモ:
お使いのブラウザで cookie を受け入れる必要があります。

次の表は、サポートされるインターネットブラウザの詳細を説明しています。

インターネットブラウザ

- Internet Explorer 11.x 以降
- Mozilla Firefox 41.x 以降
- Google Chrome 46.x 以降

プロキシモードの前提条件

ハードウェア

次の表では、プロキシモードの最小ハードウェア要件の詳細を説明しています。

プロセッサ

2 GHz Core 2 Duo 以上

RAM

最小 +-2 GB の専用 RAM / 4 GB の専用 RAM 推奨

空きディスク容量

+-1.5 GB の空きディスク容量（その他仮想ページング領域が必要）

ネットワークカード

10/100/1000 ネットワークインタフェースカード

その他

TCP/IP がインストールされアクティブ化されている

ソフトウェア

次の表では、プロキシモードをインストールする前にインストールしておく必要があるソフトウェアの詳細を説明しています。

前提条件

- **Windows インストーラ 4.0 以降**

  Windows インストーラ 4.0 以降が、インストールを実行するサーバー上にインストールされている必要があります。

- **Microsoft Visual C++ 2010 再頒布可能パッケージ**

  インストールされていない場合、インストーラが自動でインストールします。

- **Microsoft .NET Framework バージョン 4.5**

  Microsoft は、.NET Framework バージョン 4.5 のセキュリティアップデートを公開しました。

次の表では、プロキシモードサーバーのソフトウェア要件の詳細を説明しています。

メモ:
Windows Server 2008 を使用するときは UAC を常に無効にしてください。UAC を無効化した後は、変更を有効にするためにサーバーを再起動する必要があります。

Windows Server のレジストリの場所：HKLM\SOFTWARE\Dell。

オペレーティングシステム

- **Windows Server 2008 R2 SP0-SP1 64 ビット**

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2008 SP2 64 ビット**

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition

- **Windows Server 2016**

  - Standard Edition

  - Datacenter Edition

DDP Enterprise Server - VE のダウンロード

DDP Enterprise Server - VE は初期インストール時に OVA ファイルとして配信されます (Open Virtual Application (オープン仮想アプリケーション) は仮想マシンで実行されるソフトウェアを配信するために使用されます)。以下の Dell Data Protection 製品における DDP Enterprise Server - VE OVA ファイルは、www.dell.com/support の製品サポートページからダウンロードできます。

暗号化

または

Endpoint Security Suite

または

Endpoint Security Suite Enterprise

または

Data Guardian

OVA ファイルのダウンロード手順

1 Encryption、Endpoint Security Suite、Endpoint Security Suite Enterprise または Data Guardian の製品のサポートページに移動します。
2 **Drivers & downloads**（**ドライバおよびダウンロード**）をクリックします。
3 「<OS バージョン> のすべての利用可能なアップデートを表示」の隣にある **OS の変更** をクリックし、**VMware ESXi 6.0、VMware ESXi 5.5** または **VMware ESXi 5.1** のどれか 1 つを選択します。
4 「表示基準：」で **すべて表示** を選択します。
5 Dell Data Protection で **ダウンロード** を選択します。

DDP Enterprise Server - VE のインストール

作業を開始する前に、すべてのシステムと仮想環境の要件が満たされていることを確認してください。

1 インストールメディア内の Dell Data Protection ファイルを見つけてダブルクリックし、VMware **DDP Enterprise Server - VE v9.x.x Build x.ova** にインポートします。
2 DDP Enterprise Server - VE の電源をオンにします。
3 ライセンス契約の言語を選択し、**EULA を表示する** を選択します。
4 ライセンス契約を読み、**EULA に同意する** を選択します。
5 アップデートが利用可能な場合、**同意する** を選択します。
6 **デフォルトモード** または **切断モード** を選択します。

> **メモ:**
> **切断モード**を選択した場合、VE をデフォルトモードに変更することはできません。
>
> 切断モードは、インターネットおよびセキュアではない LAN または他のネットワークから VE を分離します。すべてのアップデートを手動で実行する必要があります。切断モードの機能およびポリシーの詳細については、*AdminHelp* を参照してください。

7 デフォルトパスワードの変更プロンプトが表示されたら、**はい** を選択します。
8 *ddpuser* パスワードの設定 画面で現在の（デフォルトの）パスワードである **ddpuser** を入力し、次に固有のパスワードを入力して、同じ固有のパスワードを再入力してから **OK** を選択します。

パスワードには次の文字が含まれている必要があります。

- 少なくとも 8 文字
- 少なくとも 1 つの大文字
- 少なくとも 1 つの数字
- 少なくとも 1 つの特殊文字

9 ホスト名の設定 ダイアログで、Backspace キーを使用してデフォルトホスト名を削除します。固有のホスト名を入力して、**OK** を選択します。
10 ネットワークの設定 ダイアログで、以下のいずれかのオプションを選択し、**OK** を選択します。

- （デフォルト）DHCP を使用する。

- （推奨）DHCP の使用 フィールドで、スペースバーを押して X を削除し、該当する場合は、静的 IP、ネットワークマスク、デフォルトゲートウェイ、DNS サーバー 1、DNS サーバー 2、DNS サーバー 3 の各アドレスを手動で入力します。

メモ: 静的 IP を使用する場合は、DNS サーバーにもホストエントリを作成する必要があります。

11 タイムゾーン 画面で、矢印キーを使用してタイムゾーンを選択し、**Enter** を選択します。

12 タイムゾーンの確認プロンプトで、**OK** を選択します。

13 初期設定が完了したことを示すメッセージが表示されたら、**OK** を選択します。

14 データベースパスワードの設定または変更。

15 SMTP 設定の構成。

16 既存の証明書のインポートまたは新規サーバ証明書の登録。

17 DDP Enterprise Server - VE のアップデート。

18 ポート 22 で SFTP をサポートする FTP クライアントをインストールし、ファイル転送（FTP）ユーザーの設定をセットアップします。

これで DDP Enterprise Server - VE インストールタスクは完了です。

VE リモート管理コンソールを開く

次のアドレスから VE リモート管理コンソールを開きます。

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

デフォルトの資格情報は **superadmin/changeit** です。

サポートされる Web ブラウザのリストについては、「VE リモート管理コンソールの前提条件」を参照してください。

プロキシモードのインストールと設定

プロキシモードは、DDP Enterprise Server - VE を使用するフロントエンド（DMZ モード）オプションを提供します。DMZ 内に Dell コンポーネントをデプロイする場合は、攻撃から適切に保護されていることを確認してください。

メモ: ビーコンサービスは、保護 Office モードを実行する際に、Data Guardian によって保護されるすべてのファイルにコールバックビーコンを挿入する Data Guardian コールバックビーコンをサポートするこのインストールの一部としてインストールされます。これによって、任意の場所の任意のデバイスと Dell Front End Server 間の通信が可能になります。コールバックビーコンを使用する前に、必要なネットワークセキュリティが設定されていることを確認します。コールバックビーコンの有効化ポリシーはデフォルトで有効です。

このインストールを実行するには、DMZ サーバーの完全修飾ホスト名が必要になります。

1 Dell インストールメディアで、Dell Enterprise Server ディレクトリに移動します。Dell Enterprise Server-x64 を、VE をインストールするサーバのルートディレクトリに**解凍**（コピー / 貼り付けまたはドラッグ / ドロップではなく）します。**コピー /貼り付けまたはドラッグ /ドロップを行うと、エラーが発生し、インストールが失敗します。**

2 **setup.exe** をダブルクリックします。

3 *InstallShield* ウィザードでインストールの言語を選択し、**OK** をクリックします。

4 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

5 ようこそ ダイアログで **次へ** をクリックします。

6 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

7 プロダクトキーを入力します。

8 **フロントエンドインストール** を選択し、**次へ** をクリックします。

9 フロントエンドサーバーをデフォルトの **C:\Program Files\Dell** にインストールする場合は、**次へ** をクリックします。それ以外の場所にインストールする場合は、**変更** をクリックして異なる場所を選択し、**次へ** をクリックします。

10 使用するデジタル証明書のタイプを選択することができます。**デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。**

以下のオプション「a」または「b」を選択します。

a CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。
参照 をクリックして、証明書のパスを入力します。

この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。

次へ をクリックします。

> **メモ:**
> この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。
>
> - Personal Information Exchange - PKCS#12 (.PFX)
> - 可能な場合は証明書パスにすべての証明書を含める
> - すべての拡張プロパティをエクスポートする

b 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。
Create Self-Signed Certificate (自己署名証明書の作成) ダイアログで、次の情報を入力します。

完全修飾コンピュータ名 (例 : computername.domain.com)

組織

組織単位 (例 : Security)

都市

州 (正式名)

国 : 国を表す 2 文字の略語

次へ をクリックします。

> **メモ:**
> **証明書は、デフォルトで 1 年で期限切れになります。**

11 フロントエンドサーバーセットアップ ダイアログでバックエンドサーバーの完全修飾ホスト名または DNS エイリアスを入力して **Enterprise Edition** を選択し、**次へ** をクリックします。

12 フロントエンドサーバーインストールの設定ダイアログから、ホスト名とポートを表示または編集できます。

- デフォルトのホスト名とポートを使用する場合は、フロントエンドサーバーインストールの設定 ダイアログで、**次へ** をクリックします。
- ホスト名を表示または編集する場合は、フロントエンドサーバーセットアップ ダイアログで **ホスト名の編集** をクリックします。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。

> **メモ:**
> **ホスト名に下線 (「_」) は使用できません。**

プロキシはインストールに設定する必要がない場合のみ非選択にしてください。このダイアログでプロキシを選択しないとインストールされません。

終了したら、**OK** をクリックします。

- ポートを表示または編集する場合は、フロントエンドサーバーセットアップダイアログで **外向きポートの編集**、または **内部接続ポートの編集** のいずれかをクリックします。必要に応じて、ポートを編集します。Dell はデフォルトの使用を推奨します。

フロントエンドのホスト名の編集 ダイアログでプロキシの選択を解除すると、そのポートは 外部ポート または 内部ポート ダイアログには表示されません。

終了したら、**OK** をクリックします。

13 プログラムインストールの準備完了 ダイアログで、**インストール** をクリックします。

14 インストールが完了したら、**終了** をクリックします。

VE ターミナル - 基本設定タスク

基本設定タスクは、メインメニューからアクセスできます。

ホスト名の変更

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 基本設定 メニューから **ホスト名** を選択します。

2 Backspace キーを使用して既存の DDP Enterprise Server - VE ホスト名を削除してから、新しいホスト名に置き換えて **OK** を選択します。

ネットワーク設定の変更

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 基本設定メニューから **ネットワーク設定** を選択します。

2 ネットワークの設定 画面で以下のいずれかのオプションを選択し、**OK** を選択します。

- （デフォルト）DHCP を使用する。
- （推奨）DHCP を使用する フィールドでスペースバーを押して X を削除し、手動で次の該当するアドレスを入力します。

  静的 IP

  ネットワークマスク

  デフォルトゲートウェイ

  DNS サーバー 1

  DNS サーバー 2

  DNS サーバー 3

メモ: 静的 IP を使用する場合は、DNS サーバーにホストエントリを作成する必要があります。

DMZ ホスト名の設定

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 基本設定メニューから **DMZ ホスト名** を選択します。

2 DMZ サーバーの完全修飾ドメインネームを入力して、**OK** を選択します。

メモ: プロキシモード（DMZ モード）を使用するには、プロキシモードのインストールと設定を行う必要があります。

タイムゾーンの変更

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 基本設定 メニューから **タイムゾーン** を選択します。
2 タイムゾーン 画面で、矢印キーを使用してタイムゾーンを選択し、**Enter** を選択します。
3 タイムゾーンの確認プロンプトで、**OK** を選択します。

DDP Enterprise Server - VE のアップデート

特定のアップデートの詳細については、http://www.dell.com/support のデルサポートサイトにある VE 技術アドバイザリーを参照してください。**基本設定** メニューで既に適用されているアップデートのバージョンおよびインストール日時を参照するには、**DDP Enterprise Server - VE のアップデート** > **正常に適用された最新のアップデート** を選択してください。

VE のアップデートが利用可能になったときに電子メール通知を受け取るには、「SMTP 設定の構成.」を参照してください。

メモ: デフォルトモードで、アップデートは DDP Enterprise Server - VE の初回インストール後に、かつクライアントがアクティブ化される前に実行する必要があります。

ポリシーが変更されたが Remote Management Console でコミットされていない場合は、VE: をアップデートする前にポリシーの変更を適用してください。

1 リモート管理コンソールに Dell 管理者としてログインします。
2 左側のメニューで、**管理** > **コミット** をクリックします。
3 コメント フィールドで変更の説明を入力します。
4 **ポリシーのコミット** をクリックします。
5 コミットが完了したら、リモート管理コンソールからログオフします。

VE のアップデート (デフォルトモード)

1 デルは定期的にバックアップすることをお勧めします。アップデートする前に、バックアッププロセスが正常であることを確認します。「バックアップと復元」を参照してください。
2 **基本設定** メニューから **DDP Enterprise Server - VE のアップデート** を選択します。
3 目的のアクションを選択します。
   - アップデートサーバーの設定 - DDP Enterprise Server - VE アップデートパッケージのサーバーの場所を設定または変更するには、このオプションを選択します。アップデートサーバーの設定 画面で、Backspace キーを使用して既存のサーバーホスト名または IP アドレスを削除します。新しい完全修飾ドメインネームまたは IP アドレスを入力して、**OK** を選択します。

     デフォルトのアップデートサーバーは **act.credant.com** です。
   - プロキシ設定 - アップデートのダウンロードに関するプロキシサーバーを設定するには、このオプションを選択します。

     プロキシサーバーの設定 画面で、スペースバーを押して プロキシの使用 フィールドに **X** を入力します。HTTPS、HTTP、および FTP プロキシアドレスを入力します。ファイアウォール認証が必要な場合は、スペースバーを押して 認証必須 フィールドに **X** を入力します。ユーザー名とパスワードを入力して、**OK** を押します。

     メモ: FTP サイトからアップデートを行うには、FTP ユーザー名とパスワードを入力し、続いて URL を入力します。
   - アップデートのチェック - DDP Enterprise Server - VE アップデートパッケージ用のアップデートサーバーをチェックするには、このオプションを選択します。
   - アップデートのダウンロード - アップデートのチェックによってアップデートが検出されたあとでアップデートをダウンロードするには、このオプションを選択します。

- アップデートの適用 - ダウンロードした DDP Enterprise Server - VE アップデートパッケージを適用したい場合は、このオプションを選択します。アップデート *(.deb)* ファイルの選択 画面で、インストールするアップデートパッケージを選択し、**Enter** を押します。
- 正常に適用された最新のアップデート - 現在の VE バージョンとインストール日を表示するには、このオプションを選択します。

VE のアップデート (切断モード)

1 デルは定期的にバックアップすることをお勧めします。アップデートする前に、バックアッププロセスが正常であることを確認します。「バックアップと復元」を参照してください。

2 デルサポートサイトで最新の VE を含む .deb ファイルを取得します。
VE のダウンロードは以下のサイトの **ドライバおよびダウンロード** フォルダにあります

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

または

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

または

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

または

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

3 VE のセキュア FTP サーバの /updates フォルダの .deb ファイルを取得します。
FTP クライアントがポート 22 の SFTP をサポートし、FTP ユーザーがセットアップされていることを確認します。ファイル転送 (FTP) ユーザーの設定を参照してください。

4 **基本設定** メニューから **DDP Enterprise Server - VE のアップデート** を選択します。

5 **アップデートの適用** を選択し、**Enter** を押します。
.deb ファイルが表示されない場合は、.deb ファイルが適切な場所に保存されていることを確認してください。

6 インストールする .deb アップデートファイルを選択し、**Enter** を押します。

ユーザーパスワードの変更

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

次のユーザーのパスワードを変更できます。

- ddpuser (DDP Enterprise Server - VE ターミナル管理者) - このユーザーは、VE ターミナルとそのメニューにアクセスする権限があります。
- ddpconsole (DDP Enterprise Server - VE シェルアクセス) - このユーザーには VE シェルアクセスがあります。シェルアクセスは、ネットワーク管理者がネットワーク接続をチェックしてトラブルシューティングを行うために使用できます。
- ddpsupport (Dell ProSupport 管理者) - このユーザーは、Dell ProSupport 専用です。セキュリティ上の理由により、このアカウントのパスワードは管理者自身でコントロールします。

1 基本設定 メニューから、**ユーザーパスワードの変更** を選択します。

2 ユーザーパスワードの変更 画面で変更するユーザーパスワードを選択し、**Enter** を選択します。

3 パスワードの設定 画面で現在のパスワードを入力し、新規パスワードを入力して同じ新規パスワードを再入力してから **OK** を選択します。
パスワードには次の文字が含まれている必要があります。

- 少なくとも 8 文字
- 少なくとも 1 つの大文字

- 少なくとも 1 つの数字
- 少なくとも 1 つの特殊文字

ファイル転送（FTP）ユーザーの設定

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

バックアップタスクおよび復元タスクのため、DDP Enterprise Server - VE のセキュア FTP サーバーに最大 3 つのユーザーアクセスを付与することができます。VE FTP サーバーは、DDP Enterprise Server - VE に対するアップデートを保存またはアップロードするためにも使用できます。

1 基本設定 メニューから、**ファイル転送（FTP）ユーザー** を選択します。
2 FTP ユーザーを有効にするには、*FTP* ユーザーの設定 画面で、スペースバーを押してユーザーの ステータス フィールドに **X** を入力します。FTP ユーザーを無効にするには、スペースバーを押してユーザーの ステータス フィールドから **X** を外します。
3 SFTP ユーザーのユーザー名とパスワードを入力します。
パスワードには次の文字が含まれている必要があります。

- 少なくとも 8 文字
- 少なくとも 1 つの大文字
- 少なくとも 1 つの数字
- 少なくとも 1 つの特殊文字

4 SFTP ユーザーの入力が終わったら、**OK** を選択します。

SSH の有効化

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

SSH は、サポート管理者のログイン、DDP Enterprise Server - VE のシェルアクセス、および VE ターミナルのコマンドラインインタフェース用に有効化することができます。

1 基本設定 メニューから、**SSH 設定** を選択します。
2 SSH を有効にするユーザーをハイライトし、スペースバーを押してそのフィールドに **X** を入力して、**OK** を選択します。

VE サービスの開始または停止

この作業は、必要な場合にのみ実行するようにしてください。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 すべての VE サービスを同時に開始または停止するには、基本設定 メニューから **アプリケーションの起動** または **アプリケーションの停止** のいずれかを選択します。
2 確認プロンプトで **はい** を選択します。

メモ: サーバー状態の変更には、最大 2 分かかる場合があります。

VE の再起動

この作業は、必要な場合にのみ実行するようにしてください。

1 基本設定 メニューから、**アプライアンスの再起動** を選択します。
2 確認プロンプトで **はい** を選択します。
3 再起動後に、DDP Enterprise Server - VE にログインします。

VE のシャットダウン

この作業は、必要な場合にのみ実行するようにしてください。

1 基本設定 メニューから、下にスクロールして **アプライアンスのシャットダウン** を選択します。
2 確認プロンプトで **はい** を選択します。
3 再起動後に、DDP Enterprise Server - VE にログインします。

VE ターミナル - 詳細設定タスク

詳細設定タスクは、メインメニューからアクセスします。

データベースパスワードの設定または変更

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 詳細設定 メニューから、**データベースパスワード** を選択します。
2 データベースにアクセスするためのパスワードを入力して、**OK** を選択します。
パスワードには次の文字が含まれている必要があります。

- 少なくとも 8 文字
- 少なくとも 1 つの大文字
- 少なくとも 1 つの数字
- 少なくとも 1 つの特殊文字

メモ: デルでは、インストール完了後に各パスワードをバックアップすることをお勧めします。

SMTP 設定の構成

DDP Enterprise Server - VE の電子メール通知を受け取る、**または** Data Guardian を使用するには、本項の手順に従って SMTP 設定を構成します。DDP Enterprise Server - VE の電子メール通知は、DDP Enterprise Server - VE サーバーのステータスエラー状態、パスワードアップデート、DDP Enterprise Server - VE アップデートの使用可能性、およびクライアントライセンスの問題を受信者に通知します。

設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

SMTP を設定するには、次の手順に従います。

1 詳細設定 メニューから、**電子メール通知** を選択します。
2 電子メールアラートを有効にするには、電子メール通知のセットアップ画面で、スペースバーを押して 電子メールアラートの有効化 フィールドに **X** を入力します。
3 SMTP サーバーの完全修飾ドメインネームを入力します。
4 SMTP ポートを入力します。
5 差出人ユーザー フィールドに、電子メール通知を送信する電子メールアカウント ID を入力します。
6 ユーザーの入力 フィールドに、設定済み電子メール通知を変更するためのアクセス用電子メールアカウント ID を入力します。
7 パスワード フィールドに、設定済み電子メール通知を変更するためのアクセス用パスワードを入力します。
8 VE ステータス、パスワードアップデート、およびアップデート可用性の メール ID フィールドに、各通知タイプに対する受信者のリストを入力します。受信者をリストするときは、これらの規則に従ってください。
   - 電子メールアドレスのフォーマットは、recipient@dell.com です。
   - 受信者はコンマ、またはセミコロンで区切ります。
9 サービスアラートリマインダのフィールドでリマインダを有効にしたい場合は、スペースバーを押してフィールドに **X** を入力し、分単位のリマインダ間隔を設定します。サービスアラートリマインダは、システム正常性の問題について通知が送信された時点からリマインダ間隔が経過してもホストまたはサービスが同じ状態にある場合、トリガされます。
10 サマリレポートのフィールドで通知レポートを有効にするには、お望みの間隔 (毎日、毎週または毎月) を選択し、スペースバーを押してフィールドに「**X**」を入力します。
11 **OK** を選択します。

既存の証明書のインポートまたは新規サーバー証明書の登録

証明書は、DDP Enterprise Server - VE に対してユーザーを有効化する前に設定しておく必要があります。

既存の証明書のインポートまたは証明書要求の作成は、DDP Enterprise Server - VE を介して行うことができます。

設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

既存サーバー証明書のインポート

1 既存の証明書とその完全な信頼チェーンをキーストアからエクスポートします。

   メモ: DDP Enterprise Server - VE への証明書のインポート時に入力するため、エクスポートパスワードは保管しておいてください。

2 DDP Enterprise Server - VE の FTP サーバー上で、証明書を **/opt/dell/vsftpd/files/certificates** に保存します。
3 DDP Enterprise Server - VE の 詳細設定 メニューから、**サーバー証明書** を選択します。
4 **既存証明書のインポート** を選択します。
5 DDP Enterprise Server - VE にインストールする証明書ファイルを選択します。
6 プロンプトが表示されたら、証明書のエクスポートパスワードを入力して **OK** を選択します。
7 インポートが完了したら、**OK** を選択します。

新規サーバー証明書の登録

1 詳細設定 メニューから、**サーバー証明書** を選択します。
2 **新しいサーバー証明書** を選択します。
3 **証明書要求の作成** を選択します。
4 証明書要求の作成 画面の各フィールドに情報を入力します。

   - 国名：2 文字の国コード。
   - 都道府県/州：省略形でない都道府県の名前を入力します (たとえば、Texas)。

- 市区町村名。適切な値を入力します（例：Dallas）。
- 組織：該当する値を入力します（例：Dell）。
- 組織単位：適切な値を入力します（たとえば、Security）。
- 共通名 *:*DDP Enterprise Server -VE がインストールされているサーバーの完全修飾ドメイン名を入力します。この完全修飾名には、ホスト名とドメイン名を含めます（例：server.domain.com）。
- 電子メール *ID:* CSR が送信される電子メールアドレスを入力します。

5 証明機関からの SSL サーバー証明書の取得には、所属組織のプロセスに従います。署名用に CSR ファイルの内容を送信します。

6 署名済みの証明書を受け取ったら、その証明書を .p7b ファイルとしてエクスポートし、完全な信頼チェーンを .der フォーマットでダウンロードします。

7 証明書と信頼チェーンのバックアップコピーを作成します。

8 証明書ファイル、およびその証明書の完全な信頼チェーンを DDP Enterprise Server - VE の FTP サーバーにアップロードします。

9 詳細設定 メニューから、**サーバー証明書** を選択します。

10 **新しいサーバー証明書** を選択します。

11 証明書登録の完了 を選択します。

12 DDP Enterprise Server - VE にインストールする証明書ファイルを選択します。

13 プロンプトが表示されたら、証明書のパスワードを入力します: **changeit**。

Windows ベースの Encryption クライアント上で信頼検証を有効化するには、「マネージャの信頼チェーンチェックの有効化」を参照してください。

自己署名証明書の作成とインストール

1 DDP Enterprise Server - VE の 詳細設定 メニューから、**サーバー証明書** を選択します。

2 **自己署名証明書の作成とインストール** を選択します。

3 事前にインストールされた証明書の新規証明書との置き換えを確認するには、**はい** をクリックします。

4 証明書パスワードを入力します：**changeit**。

5 新しい証明書がインストールされた後、「**OK**」を選択してサービスが再起動するのを待ちます。

VE サービスが自動的に再起動します。

ログローテーションの設定

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

デフォルトでは、日次ログローテーションが有効になっています。デフォルトのログローテーションを変更するには、詳細設定メニューから **ログローテーション設定** を選択します。

ログローテーションを無効にするには、スペースバーを使用して ローテーションなし フィールドに **X** を入力し、**OK** を選択します。

ログローテーションを有効にするには、次の手順に従います。

1 日次、週次、または月次ローテーションを有効にするには、スペースバーを使用して適切なフィールドに **X** を入力します。週次または月次ローテーションについては、適切な曜日または日付を数字（月曜日 = 1）で入力します。

2 ローテーションを行う時間を、ログローテーション時間 フィールドに入力します。

3 **OK** を選択します。

バックアップと復元

バックアップの設定と実行はいつでも可能であり、DDP Enterprise Server - VE の使用を開始する必要はありません。デルは定期的なバックアッププロセスを構成することをお勧めします。

バックアップは、外部のセキュア FTP サーバー（推奨）、または DDP Enterprise Server - VE に保存できます。VE サーバー上に保存する場合、ディスク使用量が 90 パーセントに達すると、それ以上新しいバックアップは保存されません。ディスク割り当て容量が少なくなっているという電子メール通知が送信されます。

メモ:
ディスクパーティションの容量を維持し、かつバックアップの自動削除を回避するには、DDP Enterprise Server - VE から不要なバックアップを削除してください。

バックアップは、デフォルトで毎日実行されます。デルでは、バックアップの保存を、バックアップとストレージ容量の適切な使用に対する組織の要件を満たす頻度で、外部のセキュア FTP サーバーに対して行うことを推奨しています。

バックアップスケジュールを設定するには、詳細設定 メニューから **バックアップと復元 > 設定** を選択し、次の手順に従います。

1 日次、週次、または月次バックアップを有効にするには、スペースバーを使用して適切なフィールドに **X** を入力します。週次または月次バックアップについては、適切な曜日または日付を数字（月曜日 = 1）で入力します。バックアップを無効にするには、スペースバーを使用して バックアップなし フィールドに **X** を入力し、**OK** を選択します。

2 バックアップを行う時間を、バックアップ時間 フィールドに入力します。

3 **OK** を選択します。

ただちにバックアップを行うには、詳細設定 メニューから **バックアップと復元 > 今すぐバックアップ** を選択します。バックアップの確認が表示されたら、**OK** を選択します。

メモ:
復元操作を開始する前に、すべての VE サーバーサービスが実行されている必要があります。**サーバーステータスのチェック**.すべてのサービスが 実行中 ではない場合、サービスを再起動してください。詳細については、「**VE サービスの開始または停止**」を参照してください。復元は、**すべて**のサービスが実行されている場合に**限り**、開始するようにしてください。

バックアップから復元するには、詳細設定 メニューから **バックアップと復元 > 復元** を選択して、復元するバックアップファイルを選択します。確認画面で **はい** を選択します。

VE が再起動され、バックアップが復元されます。

セキュア FTP サーバーへのバックアップの保存

FTP サーバーにバックアップを保存するには、FTP クライアントがポート 22 上の SFTP をサポートする必要があります。

バックアップは、組織のバックアップに対する要件に応じて、次の方法でダウンロードすることができます。

- 手動
- 自動化スクリプト経由
- 組織が承認したバックアップソリューション経由

組織のバックアップソリューションを使用してバックアップをダウンロードするには、お使いのバックアップソリューションのベンダーから詳細な手順を入手してください。

メモ:
Virtual Edition は Linux Debian Ubuntu x64 をベースにしています。

ddpsupport として VE にログオンし、sudo コマンドを使用してバックアップソリューションの設定を行います。

`sudo` <バックアップソリューションベンダーから入手した手順>

次のフォルダの内容をバックアップします。

/opt/dell/vsftpd/files/backup（必須）

/opt/dell/vsftpd/files/certificates（強く推奨）

/opt/dell/vsftpd/files/support（オプション）

sudo プロセスが完了したら、**exit** と入力し、ログインプロンプトが表示されるまで **Enter** を押します。

データベースリモートアクセスの有効化

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

メモ: デルでは、必要な場合にのみデータベースリモートアクセスを有効にすることをお勧めします。

1. 詳細設定 メニューから、**データベースリモートアクセス** を選択します。
2. スペースバーを使用して データベースリモートアクセスの有効化 フィールドに **X** を入力し、**OK** を選択します。データベースのパスワードがまだ構成されていない場合は、データベースのパスワードのプロンプトが表示されます。
3. データベースのパスワードを入力します。
4. データベースのパスワードを再入力します。
   DDP アプリケーションのコンポーネントは自動的に停止します。

DMZ サーバーサポートの有効化

このタスクはいつでも完了できます。DDP Enterprise Server - VE の使用を開始する必要はありません。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1. 詳細設定 メニューから、**DMZ サーバーサポートの有効化** を選択します。
2. スペースバーを使用して DMZ サーバーサポートの有効化 フィールドに **X** を入力し、**OK** を選択します。

メモ: プロキシモード（DMZ モード）を使用するには、プロキシモードのインストールと設定を行う必要があります。

DDP Enterprise Server - VE 管理者タスク

DDP Enterprise Server - VE ターミナル言語の設定または変更

設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 メインメニューで、**言語の設定** を選択します。
2 矢印キーを使用して使用する言語を選択します。

サーバーステータスのチェック

DDP Enterprise Server - VE サービスのステータスをチェックするには、メインメニューで **サーバーステータス** を選択します。

以下の表では、各サービスとその機能について説明しています。

名前	説明
Dell Message Broker	Enterprise Server バス
Dell Identity Server	ドメイン認証要求を処理します。
Dell Compatibility Server	エンタープライズアーキテクチャを管理するためのサービスです。
Dell Security Server	コマンド、および Active Directory との通信を制御するメカニズムを提供します。Dell Policy Proxy との通信に使用されます。
Dell Compliance Reporter	監査とコンプライアンスのレポートのために、環境の詳細ビューを提供します。
Dell Core Server	エンタープライズアーキテクチャを管理するためのサービスです。
Dell Core Server HA (高可用性)	エンタープライズのアーキテクチャの管理における HTTPS 接続のセキュリティおよびパフォーマンスの強化を可能にする高可用性サービスです。
Dell Inventory Server	インベントリキューを処理します。
Dell Forensic Server	フォレンジック API のためのウェブサービスを提供します。
Dell Policy Proxy	セキュリティポリシーのアップデートとインベントリのアップデートを配信するためのネットワークベースの通信パスを提供します。

DDP Enterprise Server - VE はサービスを監視し、必要に応じてサービスを再起動します。

メモ: データベースカスタマイザプロセスが失敗すると、サーバーが実行失敗状態に移行します。データベースカスタマイザログをチェックするには、メインメニューで ログの表示 を選択します。

ログの表示

次のログをチェックするには、メインメニューで **ログの表示** を選択します。

Syslog ログ メールログ Auth ログ（ SSH ） Postgres ログ 監視ログ

- システムログ

  Syslog ログ

  メールログ

  Auth ログ（ SSH ）

  Postgres ログ

  監視ログ
- サーバーログ

  Compatibility Server

  Security Server

  Message Broker

  Core Server

  Core Server HA

  Compliance Reporter

  Identity Server

  Inventory Server

  Forensic Server

  Policy Proxy
- データベースカスタマイザログ

コマンドラインインタフェ-スを開く

コマンドラインインタフェースを開くには、メインメニューで **シェルの起動** を選択します。

コマンドラインインタフェースを終了するには、**exit** と入力して **Enter** を押します。

システムスナップショットログの生成

Dell ProSupport のシステムスナップショットログを生成するには、メインメニューで **サポートツール** を選択します。

1 サポートツール メニューから、**システムスナップショットログの生成** を選択します。
2 ファイルが作成されたことを示すメッセージが表示されたら、**OK** を選択します。

ddpsupport ユーザーがアクティブ化されている場合、Dell ProSupport は DDP Enterprise Server - VE SFTP サーバーからログを取得できます。ddpsupport ユーザーがアクティブ化されていない場合は、Dell ProSupport にお問い合わせください。詳細については、「Dell ProSupport へのお問い合わせ」を参照してください。

4

DDP Enterprise Server - VE のメンテナンス

不要な DDP Enterprise Server - VE のバックアップを削除する必要があります。

過去 10 件のバックアップのみが保持されます。ディスクパーティション容量が 10 パーセント以下になった場合、それ以上のバックアップは保存されません。この状態が発生すると、ディスク割り当て容量が少なくなっているという電子メール通知が送信されます。

5

DDP Enterprise Server - VE トラブルシューティング

電子メール通知がすでに設定されている時にこの状態が発生すると、電子メール通知を受信することができます。電子メール通知の情報に基づいて、次の手順に従います。

1 適切なログファイルをチェックする。
2 必要に応じてサービスを再起動する。設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。
3 システムスナップショットログの生成
4 Dell ProSupport へのお問い合わせ。詳細については、「Dell ProSupport へのお問い合わせ」を参照してください。

6

インストール後の設定タスク

インストール後、お使いの環境内の一部のコンポーネントを、組織によって使用されている Dell Data Protection ソリューションに応じて設定することが必要になる場合があります。

Data Guardian の VE を設定する

Data Guardian をサポートするように VE を設定するには、VE リモート管理コンソールで Cloud Encryption ポリシーをオンに設定します。Data Guardian 保護 Office ドキュメントモードを有効にするには、保護 Office ドキュメントポリシーをオンに設定します。

Data Guardian クライアントをインストールする手順については、『*Enterprise Edition Advanced* インストールガイド』、『*Enterprise Edition Basic* インストールガイド』、または『*Data Guardian* ユーザーガイド』を参照してください。

Mobile Edition のための EAS 管理のインストールと設定

Mobile Edition を使用するには、EAS 管理をインストールし、設定する必要があります。Mobile Edition を使用する予定ではない場合、本項はスキップしてください。

前提条件

- EAS メールボックスマネージャサービスのログインアカウントは、Exchange ActiveSync ポリシーの作成 / 変更、ユーザーメールボックスへのポリシーの割り当て、および ActiveSync デバイスに関する情報をクエリする許可を持つアカウントである必要があります。
- ファイルを変更してサービスを再起動するには、EAS 設定ユーティリティを管理者権限で実行する必要があります。
- DDP Enterprise Server - VE へのネットワーク接続は必須です。
- DDP Enterprise Server - VE のホスト名または IP アドレスを用意します。
- Exchange 環境をホストするサーバーに Microsoft メッセージキュー（MSMQ）がインストール / 設定されている必要があります。まだ設定されていない場合は、MSMQ 4.0 を Windows Server 2008 または Windows Server 2008 R2 にインストールします（Exchange 環境をホストしているサーバー上）– http://msdn.microsoft.com/en-us/library/aa967729.aspx

導入プロセス時

Exchange ActiveSync を使用して、Mobile Edition 経由でモバイルデバイスを管理する予定の場合、Exchange Server 環境を設定する必要があります。

EAS デバイスマネージャのインストール

1 Mobile Edition インストールメディアで EAS 管理フォルダに移動します。EAS デバイスマネージャフォルダで、setup.exe を *Exchange Client Access Server* にコピーします。

2 **setup.exe** をダブルクリックして、インストールを開始します。お使いの環境に複数の *Exchange Client Access Server* がある場合、それぞれの環境でこのインストーラを実行します。

3 インストール用言語を選択して **OK** をクリックします。

4 ようこそ 画面が表示されたら、**次へ** をクリックします。

5 ライセンス契約を読み、条項に同意して、**次へ** をクリックします。

6 **次へ** をクリックして、EAS デバイスマネージャ をデフォルトの場所 C:\Inetpub\wwwroot\Dell\EAS Device Manager\ にインストールします。

7 インストールを開始する準備ができました 画面で、**インストール** をクリックします。

ステータスウィンドウにインストールの進捗状況が表示されます。

8 必要に応じて Windows インストーラログを表示するボックスにチェックを入れ、**終了** をクリックします。

EAS メールボックスマネージャのインストール

1 Mobile Edition インストールメディアで EAS 管理フォルダに移動します。EAS Mailbox Manager フォルダで、setup.exe を *Exchange Mailbox Server* にコピーします。

2 **setup.exe** をダブルクリックして、インストールを開始します。お使いの環境に複数の *Exchange Mailbox Server* がある場合、それぞれの環境でこのインストーラを実行します。

3 インストール用言語を選択して **OK** をクリックします。

4 ようこそ 画面が表示されたら **次へ** をクリックします。

5 ライセンス契約を読み、条項に同意して、**次へ** をクリックします。

6 **次へ** をクリックして、EAS Mailbox Manager をデフォルトの場所 **C:\Program Files\Dell\EAS Mailbox Manager** にインストールします。

7 ログオン情報 画面で、このサービスを使用するためにログオンするユーザーアカウントの資格情報を入力します。

ユーザー名：ドメイン\ユーザー名

パスワード：このユーザー名に関連付けられているパスワード

次へ をクリックします。

8 インストールを開始する準備ができました 画面で、**インストール** をクリックします。

ステータスウィンドウにインストールの進捗状況が表示されます。

9 必要に応じて Windows インストーラログを表示するボックスにチェックを入れ、**終了** をクリックします。

EAS 設定ユーティリティの使用

1 同じコンピュータで、**スタート** > **Dell** > **EAS 設定ユーティリティ** > **EAS 設定** と移動して、EAS 設定ユーティリティを実行します。

2 **セットアップ** をクリックして EAS 管理を設定します。

3 以下の情報を入力します。

DDP Enterprise Server - VE ホスト名

Dell Policy Proxy のポーリング間隔（デフォルトは 1 分）

EAS デバイスマネージャをレポート限定モードで実行するボックスを選択します（導入時の推奨）。

> **メモ:**
> レポート限定モードを使用すると、不明なデバイス / ユーザーによる Exchange ActiveSync へのアクセスが許可されますが、トラフィックは引き続きユーザーに報告されます。導入が完了して稼働しはじめたら、この設定を変更してセキュリティを厳しくすることができます。

OK をクリックします。

4 成功メッセージが表示されます。**はい** をクリックして IIS と EAS メールボックスマネージャサービスを再起動します。

5 終了したら **終了** をクリックします。

導入プロセス後

導入が完了して稼働しはじめ、セキュリティを厳しくする準備が整えば、次の手順に従います。

Exchange メールボックスサーバーで次の手順を実行します。

1 **スタート** > **Dell** > **EAS 設定ユーティリティ** > **EAS 設定** と移動して、EAS 設定ユーティリティを実行します。

2 **セットアップ** をクリックして EAS 管理を設定します。

3 以下の情報を入力します。

DDP Enterprise Server - VE ホスト名

Dell Policy Proxy のポーリング間隔（デフォルトは 1 分）

EAS デバイスマネージャをレポート限定モードで実行するボックスをクリアします。

OK をクリックします。

4 成功メッセージが表示されます。**はい** をクリックして IIS と EAS メールボックスマネージャサービスを再起動します。

5 終了したら **終了** をクリックします。

マネージャの信頼チェーンチェックの有効化

自己署名証明書が SED または Bitlocker Manager 向けの VE Server で使用されている場合は、クライアントコンピュータで SSL/TLS 信頼検証を無効のままにしておく必要があります。クライアントコンピューターで SSL/TLS 信頼検証を有効にする場合は、次の要件を満たしている必要があります。

- ルート証明機関（Entrust や Verisign など）によって署名された証明書が VE Server にインポートされている必要があります。「既存の証明書のインポートまたは新規サーバー証明書の登録」を参照してください。
- 証明書の完全な信頼チェーンがクライアントコンピュータの Microsoft キーストアに格納されている。

SSL/TLS 信頼検証を有効にするには、クライアントコンピュータで、以下のレジストリエントリを 0 に変更します。

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

DisableSSLCertTrust=REG_DWORD (32-bit):0

7

VE リモート管理コンソールの管理者タスク

Dell 管理者役割の割り当て

1 Dell 管理者として、このアドレスにてリモート管理コンソールにログインします : https://server.domain.com:8443/webui/ 。デフォルトの資格情報は **superadmin/changeit** です。
2 左ペインで **ポピュレーション** > **ドメイン** をクリックします。
3 ユーザーを追加する対象であるドメインをクリックします。
4 ドメイン詳細 ページで、**メンバー** タブをクリックします。
5 **ユーザーの追加** をクリックします。
6 ユーザー名を共通名、UPN (Universal Principal Name)、または sAMAccountName で検索するためのフィルタを入力します。ワイルドカード文字は * です。

   共通名、UPN (Universal Principal Name)、および sAMAccountName は、各ユーザーのエンタープライズディレクトリサーバーで定義されている必要があります。ユーザーがドメインまたはグループのメンバーであるにもかかわらず、管理のドメインまたはグループのメンバーリストに表示されない場合は、エンタープライズディレクトリサーバーでそのユーザーの 3 つの名前がすべて正しく定義されていることを確認してください。

   クエリでは、一致が見つかるまで、共通名、UPN、sAMAccountName の順に自動的に検索します。
7 ディレクトリユーザーリストから、ドメインに追加するユーザーを選択します。複数のユーザーを選択するには、<Shift><click> または <Ctrl><click> を使用します。
8 **追加** をクリックします。
9 メニューバーから、指定したユーザーの **詳細とアクション** タブをクリックします。
10 メニューバーをスクロールして、**管理者** タブを選択します。
11 管理者の役割を選択して、このユーザーに追加します。
12 **保存** をクリックします。

Dell 管理者役割でのログイン

1 リモート管理コンソール Enterprise Server からログアウトします。
2 リモート管理コンソール Enterprise Server にログインし、ドメインユーザー証明書でログインします。
   リモート管理コンソールの右上隅の「?」をクリックして、*Dell Data Protection AdminHelp* を起動します。はじめに ページが表示されます。**ドメインの追加** をクリックします。

   組織にはベースラインポリシーが設定されていますが、次のように、特定のニーズに応じて変更する必要が生じる場合があります (すべてのアクティブ化はライセンスおよび資格によって決まります)。

   - Windows コンピュータは暗号化されます
   - 自己暗号化ドライブが搭載されたコンピュータは暗号化されます
   - Hardware Crypto Accelerator が搭載された Windows コンピュータは暗号化されます
   - BitLocker 管理は無効です
   - Advanced Threat Protection が有効になっていません
   - Threat Protection は有効です
   - 外部メディアは暗号化されません
   - ポートに接続されているデバイスは暗号化されません

- Data Guardian が有効になります
- Mobile Edition は無効です

Technology Group とポリシーの説明については、AdminHelp トピックの「ポリシーの管理」を参照してください。

ポリシーのコミット

インストールが完了したらポリシーをコミットします。

ポリシーの変更を保存し、ポリシーのインストール後、またはそれ以後にポリシーをコミットするには、次の手順に従います。

1 左側のペインで、**管理** > **コミット** をクリックします。
2 コメント フィールドで変更の説明を入力します。
3 **ポリシーのコミット** をクリックします。

8

ソリューションポート

以下の表は、各コンポーネントとその機能について説明しています。

名前	デフォルトポート	説明	必須とされる機能
Compliance Reporter	HTTP (HTTPS) / 8084	監査とコンプライアンスのレポートのために、環境の詳細ビューを提供します。 DDP Enterprise Server - VE のコンポーネントです。	レポート
リモート管理コンソール	HTTPS/8443	企業全体での導入に対応する管理コンソールとコントロールセンター。 DDP Enterprise Server - VE のコンポーネントです。	すべて
Core Server	HTTPS/8888	ポリシーフロー、ライセンス、起動前認証の登録、SED Management、BitLocker Manager、Threat Protection、Advanced Threat Protection を管理します。Compliance Reporter およびリモート管理コンソールが使用するインベントリデータを処理します。認証データを収集し、保管します。役割に基づいたアクセスを制御します。 DDP Enterprise Server - VE のコンポーネントです。	すべて
Core Server HA (高可用性)	HTTPS/8888	Remote Management Console、Preboot Authentication、SED Management、BitLocker Manager、Threat Protection および Advanced Threat Protection による HTTPS 接続のセキュリティおよびパフォーマンスの強化を可能にする高可用性サービスです。 DDP Enterprise Server - VE のコンポーネントです。	すべて
Security Server	HTTPS/8443	Policy Proxy との通信を行います。また、フォレンジッククキーの取得、クライアントのアクティベーション、Data Guardian 製品、および SED-PBA 通信を管理します。 DDP Enterprise Server - VE のコンポーネントです。	すべて
Compatibility Server	TCP/1099 (閉鎖)	エンタープライズアーキテクチャを管理するためのサービスです。アクティベーション中の初期インベントリデータおよび移行時のポリシーデータを収集、保管します。このサービスのユーザーグループに基づいてデータを処理します。 DDP Enterprise Server - VE のコンポーネントです。	すべて
Message Broker サービス	TCP/61616 および STOMP/ 61613(閉鎖、または DMZ 用に設定済	DDP Enterprise Server - VE のサービス間の通信を処理します。ポリシープロキシのキュー操作のために Compatibility Server によって作成されるポリシー情報をステージします。	すべて

名前	デフォルトポート	説明	必須とされる機能
	みの場合は 61613 開放)	DDP Enterprise Server - VE のコンポーネントです。	
Identity Server	HTTPS/8445	SED Manager の認証を含むドメイン認証要求を処理します。 Active Directory アカウントが必要です。 DDP Enterprise Server - VE のコンポーネントです。	すべて
Forensic Server	HTTPS/8448	適切な権限を持った管理者にデータのロック解除または復号化のタスクに使用される暗号化キーを Remote Management Console から取得することを可能にします。 DDP Enterprise Server - VE のコンポーネントです。	フォレンジック API
Inventory Server	8887	インベントリキューを処理します。 DDP Enterprise Server - VE のコンポーネントです。	すべて
Policy Proxy	TCP/ 8000/8090	セキュリティポリシーのアップデートとインベントリのアップデートを配信するためのネットワークベースの通信パスを提供します。 DDP Enterprise Server - VE のコンポーネントです。	Mac 用の Enterprise Edition Windows 用の Enterprise Edition Mobile Edition
LDAP	389/636、3268/3269 RPC - 135、49125+	**ポート 3268** - このポートは、特にグローバルカタログをターゲットとするクエリ用に使用されます。ポート 3268 に送信される LDAP 要求は、フォレスト全体でのオブジェクトの検索に使用することができます。ただし、返されるのはグローバルカタログへのリプリケーション用にマークされた属性のみです。たとえば、ポート 3268 を使用してユーザーの部門は返すことはできません。これは、この属性がグローバルカタログに複製されないためです。 **ポート 389** - このポートはローカルドメインコントローラからの情報の要求に使用されます。ポート 389 に送信される LDAP 要求は、グローバルカタログのホームドメイン内にあるオブジェクトの検索にのみ使用できます。ただし、要求側のアプリケーションは、これらのオブジェクトに対するすべての属性を取得できます。たとえば、ポート 389 への要求は、ユーザーの部門を取得するために使用することができます。	すべて
クライアント認証	HTTPS/8449	クライアントサーバーが DDP Enterprise Server - VE に対して認証することを許可します。	サーバー暗号化
コールバックビーコン	HTTP/8446	Data Guardian 保護 Office モードを実行すると、コールバックビーコンを保護された各 Office ファイルに挿入することができます。	Data Guardian
Advanced Threat Prevention	HTTPS/TCP/443	Advanced Threat Protection を使用する場合のクライアント通信	Advanced Threat Prevention
EAS Device Manager	該当なし	無線機能を有効にします。Exchange クライアントアクセスサーバーにインストールされています。	モバイルデバイスの Exchange ActiveSync 管理。

名前	デフォルトポート	説明	必須とされる機能
EAS メールボックスマネージャ	該当なし	Exchange メールボックスサーバーにインストールされたメールボックスエージェント。	モバイルデバイスの Exchange ActiveSync 管理。

NTP 時刻の同期：TCP および UDP/123（詳細については、次のリンクを参照してください。https://help.ubuntu.com/lts/serverguide/NTP.html）