Dell Security Management Server Virtual

Quick Start and Installation Guide v10.2.4

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。

2019 - 05

Rev. A01

Contents

1

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、Dell Server 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、デルでは最初に Dell Server 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、Security Management Server Virtual I インストールガイドを参照してください。

Dell Server の前提条件については、「Security Management Server Virtual の前提条件」、「管理コンソールの前提条件」、「プロキシモードの前提条件」を参照してください。

既存の Dell Server をアップデートする情報については、「Security Management Server Virtual のアップデート」を参照してください。

インストール

1 Dell Data Security 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 Security Management Server Virtual **v10.x.x Build x.ova** にインポートします。

> **メモ: OVA は現在 SHA256 署名を使用しており、VMware シッククライアント内へのインポートには失敗します。詳細については、https://kb.vmware.com/s/article/2151537 を参照してください。**

2 Security Management Server Virtual の電源を入れます。

3 画面に表示される手順に従います。

設定

ユーザーをアクティブ化する前に、Security Management Server Virtual 端末で次の設定タスクを完了することをお勧めします。

- 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
- Security Management Server Virtual 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。

管理コンソールを開く

次のアドレスで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。

サポートされるウェブブラウザのリストについては、「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

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。

管理コンソールの右上隅の「?」をクリックして、*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）。

- ポリシーベース暗号化は共通キー暗号化で有効にされます
- 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 Prevention が有効になっていません
- Threat Protection は無効にされます
- 外部メディアは暗号化されません
- ポート制御によるポートの管理は行われません
- フルディスク暗号化がインストールされているデバイスは暗号化されません
- Data Guardian は無効にされます

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。

2

インストール詳細ガイド

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向けに Security Management Server Virtual 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、デルでは最初に Security Management Server Virtual 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 Security Management Server Virtual をアップデートする詳細情報については、「Security Management Server Virtual のアップデート」を参照してください。

Security Management Server Virtual について

管理者は、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、保護の状態を監視します。プロキシモードは、Security Management Server Virtual 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。

Security Management Server Virtual 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

デル製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 4310039）にご連絡ください。

さらに、デル製品のオンラインサポートも dell.com/support から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タグまたはエクスプレス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 の各国の電話番号を記載したページを参照してください。

要件

Security Management Server Virtual

Hardware

The recommended disk space for Security Management Server Virtual is 80 GB.

Virtualized Environment

Security Management Server Virtual v10.2.3 has been validated with the following virtualized environments.

Dell currently supports hosting the Dell Security Management Server or Dell Security Management Server Virtual within a Cloud-hosted Infrastructure as a Service (IaaS) environment, such as Amazon Web Services, Azure, and several other vendors. Support for these environments will only be limited to the functionality of the application server hosted within these Virtual Machines, the administration and security of these Virtual Machines will be up to the administrator of the IaaS solution.

Additional infrastructure requirements (Active Directory, as well as SQL Server for the Dell Security Management Server) are still required for proper functionality.

Virtualized Environments

- VMware Workstation 12.5
  - 64-bit CPU required
  - 8GB RAM required
  - 80 GB Hard Drive Space
  - Host computer with at least two cores
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware Workstation 14.0
  - 64-bit CPU required
  - 8 GB RAM required
  - 80 GB Hard Drive Space
  - Host computer with at least two cores
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware Workstation 14.1
  - 64-bit CPU required
  - 8 GB RAM required
  - 80 GB Hard Drive Space
  - Host computer with at least two cores
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware ESXi 6.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An Operating System is not required
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

Virtualized Environments

- VMware ESXi 6.0
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An Operating System is not required
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware ESXi 5.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An Operating System is not required
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- Hyper-V Server (Full or Core installation)
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An operating system is not required
  - Hardware must conform to minimum Hyper-V requirements
  - Must be run as a Generation 1 Virtual Machine

NOTE: For information on setting up Hyper-V, follow instructions for Endpoint Operating Systems: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v or for Server Operating Systems: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

管理コンソール

インターネットブラウザ

メモ:
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

ハードウェア

次の表は、最小ハードウェア要件の詳細です。

プロセッサ

最新のデュアルコア CPU（1.5 Ghz 以上）

RAM

2 GB の専用 RAM（最小）/ 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容量が必要）

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

IPv4、IPv6、または IPv4 と IPv6 の組み合わせがサポートされている

ソフトウェア

次の表では、プロキシモードサーバ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 4.5.2**

  Microsoft は、.NET Framework バージョン 4.5.2 のセキュリティアップデートを公開しました。

メモ:
保護されたディレクトリにインストールする場合は、ユニバーサルアカウント制御（UAC）を無効にする必要があります。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。

次の表では、プロキシモードサーバのソフトウェア要件の詳細を説明します。

オペレーティングシステム

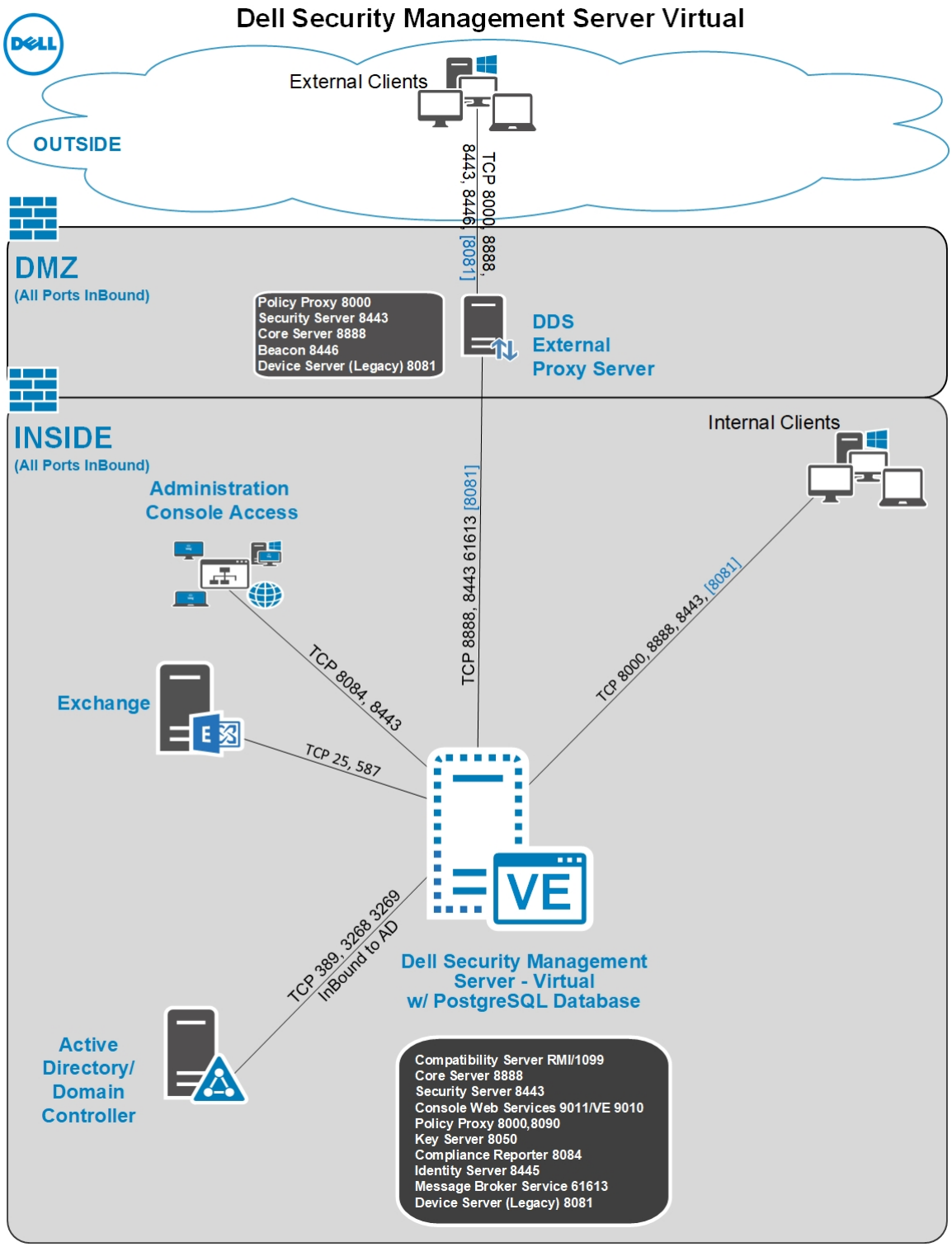
- **Windows Server 2019**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2016**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **LDAP リポジトリ**
  - Active Directory 2008 R2
  - Active Directory 2012 R2
  - Active Directory 2016

Security Management Server Virtual のアーキテクチャの設計

Dell Encryption、Endpoint Security Suite Enterprise、および Data Guardian の各ソリューションは非常に拡張性の高い製品で、組織内の暗号化を目的としたエンドポイントの数に基づいて拡張可能です。

アーキテクチャコンポーネント

以下は、Dell Security Management Server Virtual の基本的な導入です。



OVA ファイルのダウンロードおよびインストール

Security Management Server Virtual 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 Security 製品における 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

- Endpoint Security Suite Enterprise
- Data Guardian

OVA ファイルのダウンロード手順

1 上記の適切な製品の ドライバおよびダウンロード ページにアクセスします。
2 **ドライバおよびダウンロード** をクリックします。
3 適切な VMware ESXi のバージョンを選択します。
4 適切なバンドルをダウンロードします。

OVA ファイルのインストール手順

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 Dell インストールメディアで、*Security Management Server Virtual v9.x.x* ビルド *x.ova* を見つけてダブルクリックし、VMware にインポートします。

メモ: VMware ではなく Hyper-V を使用している場合は、Windows 10 の手順「https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/」に従ってください。サーバベースのオペレーティングシステムの場合は、次の手順「https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server」に従ってください。VMware の代わりに ESXi を使用している場合は、次の手順「https://kb.vmware.com/s/article/2109708」に従ってください。

2 画面に表示される手順に従います。

メモ: VMware の使用時にインポートに失敗する場合は、Web クライアントで OVA ファイルをインポートすることをお勧めします。詳細については、https://kb.vmware.com/s/article/2151537 を参照してください。

3 Security Management Server Virtual の電源投入
4 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。
5 ライセンス契約を読み、**EULA に同意する** を選択します。
6 アップデートが利用可能な場合、**同意する** を選択します。
7 **接続モード** 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、接続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 Dell Server 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。

8 *delluser* パスワードの設定 で、現在（デフォルト）のパスワード **delluser** 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、**適用** 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: キャンセル を選択するか、キーボードの Escape キーを押すと、デフォルトのパスワードをそのまま使用できます。

9 **閉じる** を選択して、ホスト名の設定ウィンドウに入ります。
10 ホスト名の設定 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。
11 ネットワークの設定 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（IPv4）。
- （推奨）*DHCP* を使用する 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

静的な設定では、IPv6 または IPv4 のいずれかを選択します。

- **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。**

12 タイムゾーンの確認プロンプトで、**OK** を選択します。

13 最初の起動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 SMTP 設定の構成。

15 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。

16 Security Management Server Virtual のアップデート。

17 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。

Security Management Server Virtual インストールタスクが完了しています。

管理コンソールを開く

次のアドレスで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。

サポートされるウェブブラウザのリストについては、「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

プロキシモードには、Dell Server を使用するフロントエンド（DMZ モード）オプションがあります。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: このインストールでは、Data Guardian コールバックビーコンをサポートするためのビーコンサービスがインストールされます。これにより、環境内で保護対象 Office ドキュメントを許可または行使する際に、Data Guardian のすべての保護対象ファイルにコールバックビーコンが挿入されます。その結果、任意の場所にある任意のデバイスとフロントエンドサーバの間で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。

このインストールを実行するには、DMZ サーバの完全修飾ホスト名が必要です。

1 Dell インストールメディアで、Security Management Server ディレクトリに移動します。Security Management Server-x64 を、Security Management Server Virtual 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、インストールは失敗します。**

2 **setup.exe** をダブルクリックします。

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 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 32 文字のプロダクトキーを入力し、**次へ** をクリックします。プロダクトキーはファイル「EnterpriseServerInstallKey.ini」にあります。

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** をクリックして別の場所を選択し、**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。

メモ: 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。

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。

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：セキュリティ）

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: デフォルトでは、証明書は 10 年で期限切れになります。

11 フロントエンドサーバセットアップ ダイアログで、バックエンドサーバの完全修飾ホスト名または DNS エイリアスを入力し、**Dell Security Management Server** を選択して、**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。

インストール時にプロキシを設定しない場合にのみ、プロキシの選択を外してください。このダイアログで選択しないと、プロキシは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。

の基本端末設定タスク

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。

システムダッシュボードのチェック

Dell Server の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 **システムダッシュボード** を選択します。

システム情報 ウィジェットには、現在のバージョン、ホスト名、IP アドレスとともに、CPU、メモリ、ディスクの使用状況が表示されます。

バージョン履歴 ウィジェットには、データベーススキーマの変更履歴がバージョンごとに表示されます。データは「情報」テーブルから取得されており、時間順にソートされ、一番上が最新バージョンです。

次の表に、サービス状態 ウィジェットの各サービスとその機能の説明を示します。

名前	説明
Message Broker	Enterprise Server バス
Identity Server	ドメイン認証要求を処理します。
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。
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。
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。
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。また、このサービスは、すべてのアクティベーション、ポリシー、および "エージェント" ベースのデバイスからのインベントリ収集を処理します。
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。
Inventory Server	インベントリキューを処理します。
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。
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。

サービスが監視され、必要に応じて自動的に再起動されます。

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。

ホスト名の変更

このタスクはいつでも完了できます。Security Management Server Virtual を使用して開始することは必須ではありません。

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 ホスト名を削除し、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。Security Management Server Virtual を使用して開始することは必須ではありません。

1 基本設定メニューから、**ネットワーク** 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（IPv4）。
- （推奨）*DHCP* を使用する 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

静的な設定では、IPv6 または IPv4 のいずれかを選択します。

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 サーバサポートの設定

このタスクはいつでも完了できます。Security Management Server Virtual の使用を開始する必要はありません。

1 詳細設定 メニューから、**DMZ サーバサポート** を選択します。
2 スペースバーを使用して、DMZ サーバサポートの有効化 フィールドに **X** を入力します
3 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: DMZ サーバを活用するには、上記の「プロキシモードのインストールと設定」でプロキシサーバのインストール手順を参照してください。

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。Security Management Server Virtual の使用を開始する必要はありません。

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。

Update Security Management Server Virtual

For information about a specific update, see *Security Management Server Virtual Technical Advisories*, located at dell.com/support. To see the version and installation date of an update that is already applied, check the *System Dashboard*.

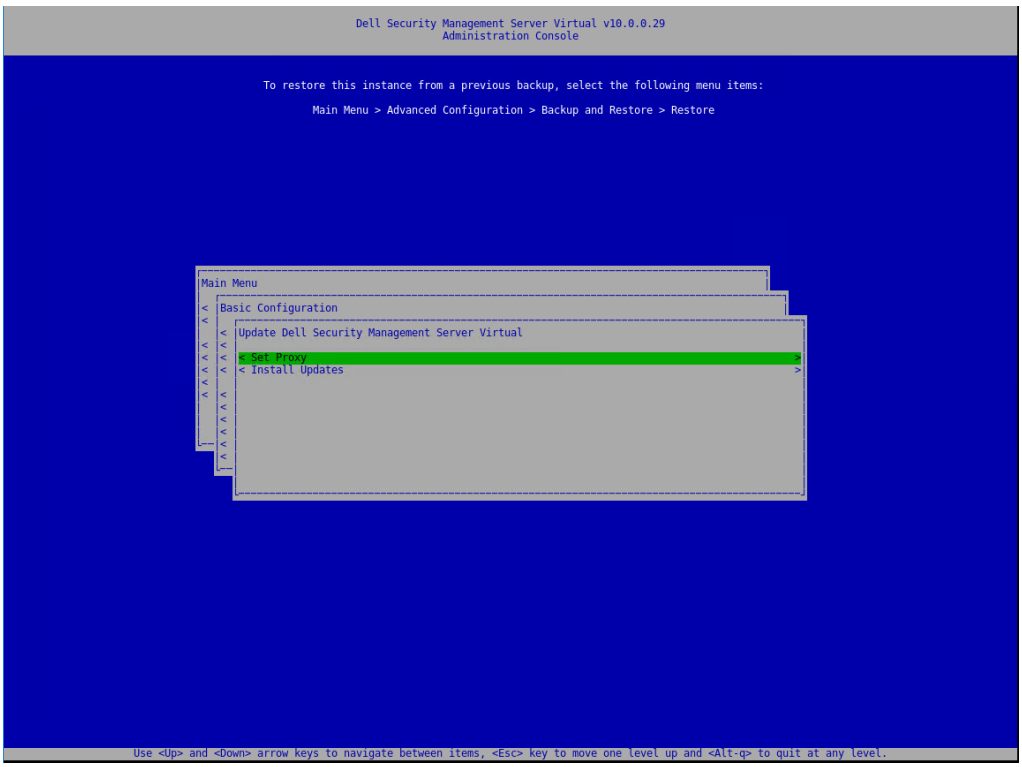
To receive email notifications when Dell Server updates are available, see Configure SMTP Settings.

If policy changes have been made but not committed in the Management Console, commit the policy changes before updating the Dell Server:

1 As a Dell administrator, log in to the Management Console.
2 In the left menu, click **Management** > **Commit**.
3 Enter a description of the change in the Comment field.
4 Click **Commit Policies**.
5 When the commit is complete, log off the Management Console.

Update Security Management Server Virtual (Connected Mode)

1 Dell recommends performing a regular backup. Before updating, ensure that the backup process has been functioning properly. See Backup and Restore.
2 From the **Basic Configuration** menu, select **Update Dell Security Management Server Virtual**.



NOTE: The version number may differ from the attached screen capture.

3 Select the desired action:

- Set Proxy Settings - Select this option to set the proxy settings for downloading updates.

  In the *Configure Proxy Settings* screen, press the space bar to enter an **X** in *Use Proxy*. Enter the HTTPS, and HTTP. If firewall authentication is required, press the space bar to enter an **X** in Authentication Required. Enter the user name and password, and select **OK**.

  NOTE: This Set Proxy option also now updates the proxy settings for the various java-based applications for pulling On-The-Box licenses as well as communication to the Endpoint Security Suite Enterprise SaaS and the Dell/Credant back-end infrastructure.

- When selecting **Install Updates**, the Security Management Server Virtual queries the built-in, default Ubuntu repositories and dist.ddspproduction.com, Dell's custom repository containing application updates.

NOTE: Dell queries dist.ddspproduction.com through port 443 and port 80 for all Ubuntu updates. Any available updates are downloaded. The proxy settings defined in Set Proxy are used for port 443 and port 80 connections for download.

Update Security Management Server Virtual (Disconnected Mode)

1 Dell recommends performing a regular backup. Before updating, ensure that the backup process has been functioning properly. See Backup and Restore.

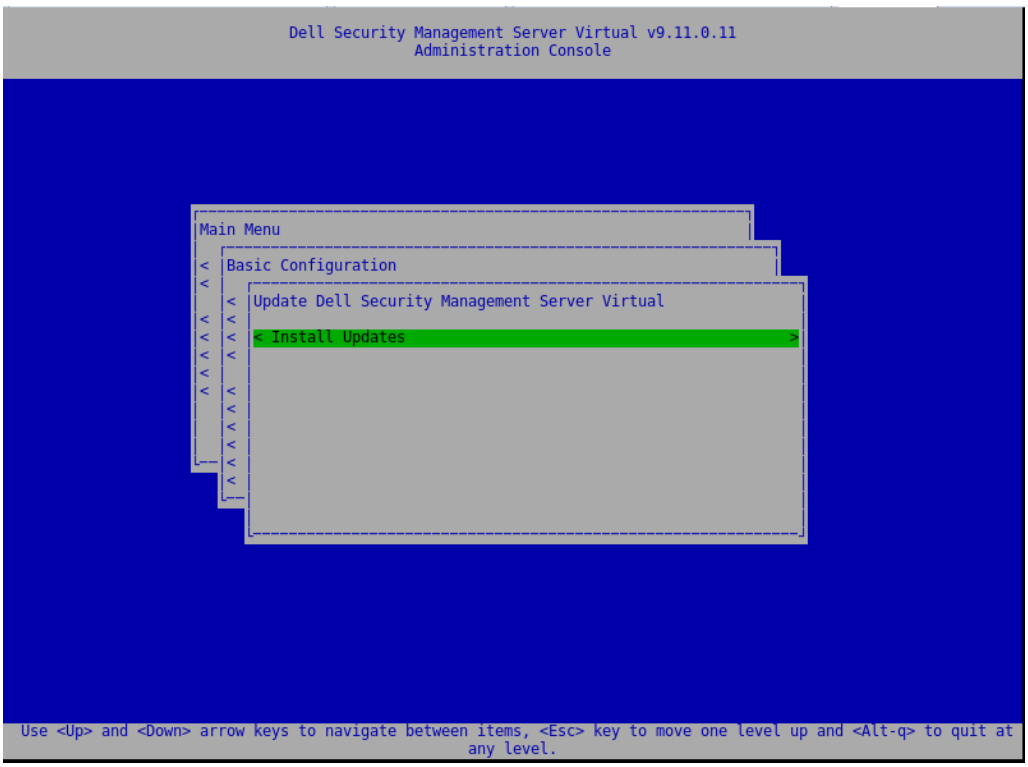
2 Obtain the .deb file that contains the latest Dell Server update from Dell ProSupport.

3 Store the .deb file in the /updates folder on the secure FTP server of the Dell Server.

Ensure that the FTP client supports SFTP on port 22, and an FTP user is set up. See Set up File Transfer (FTP) Users.

4 From the **Basic Configuration** menu, select **Update Security Management Server Virtual**.

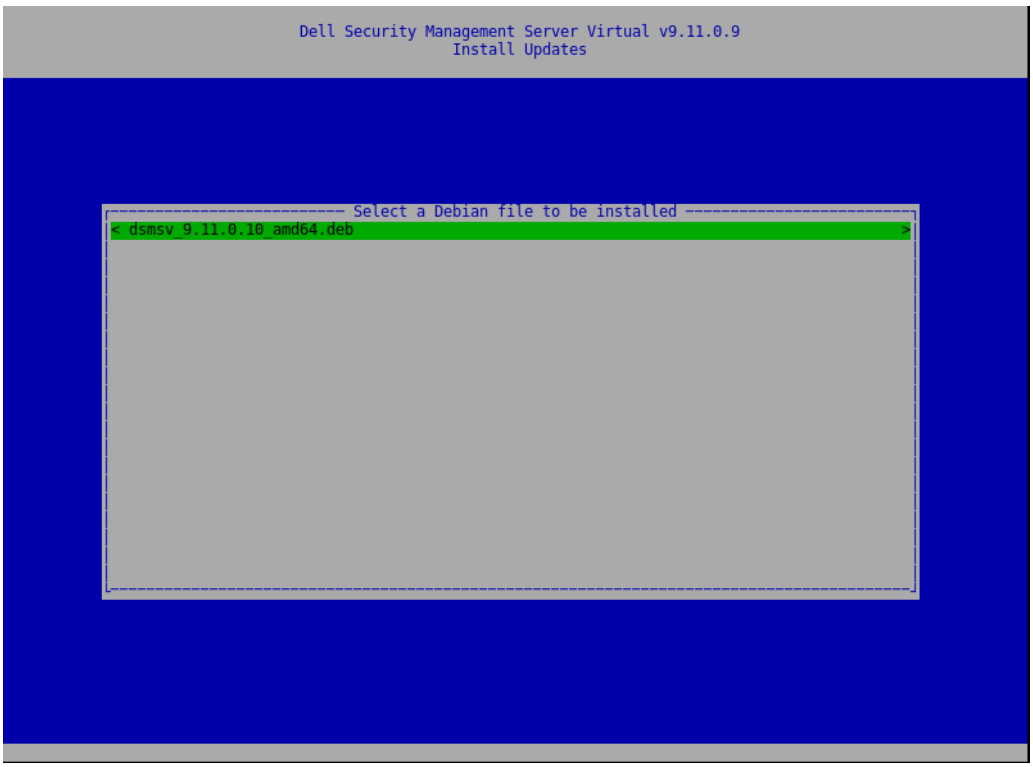
5 Select **Intall Updates** and press **Enter**.



NOTE: The version number may differ from the attached screen capture.

If the .deb file does not display, ensure that the .deb file is stored in the proper location.

6 Select the .deb update file you want to install and press **Enter**.



NOTE: The version number may differ from the attached screen capture.

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。Security Management Server Virtual を使用して開始することは必須ではありません。

次のユーザーのパスワードを変更できます。

- delluser（端末管理者） - このユーザーは、Dell Server の端末とそのメニューにアクセスできます。
- dellconsole（シェルアクセス） - このユーザーは、Dell Server にシェルアクセスできます。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。
- dellsupport（Dell ProSupport 管理者） - このユーザーには「sudo」権限があるため、慎重に使用する必要があります。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

メモ:
別のユーザーアカウントを選択するには、キーボードの "スペースバー" キーを押して、選択リストを表示します。

Secure File Transfer（SFTP）ユーザーの設定

このタスクはいつでも完了できます。Security Management Server Virtual の使用を開始する必要はありません。

1 基本設定 メニューから、**SFTP** を選択します。
2 *SFTP* 画面で、SFTP ユーザーを追加してパスワードを定義するには、ユーザーの ステータス で **Enter** または下矢印キーを押します。スペースバーキーを押すと、既存のユーザーを更新または削除するオプションが表示されます。SFTP ユーザーを無効にするには、ユーザーを選択してから **削除** を選択し、次に SFTP の確認 画面で **はい** を選択します。
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、**適用** 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。Security Management Server Virtual を使用して開始することは必須ではありません。

SSH は、サポート管理者のログイン、シェルアクセス、端末のコマンドラインインタフェース用に有効化します。

1 基本設定 メニューから、**SSH** 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 **X** を入力し、**OK** を選択します。

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。

1 すべての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。

アプライアンスの再起動

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、Security Management Server Virtual にログインします。

アプライアンスのシャットダウン

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、Security Management Server Virtual にログインします。

詳細端末設定タスク

詳細設定タスクは、メインメニューからアクセスします。

ログローテーションの設定

メモ: ログローテーションに対応した Dell Security Management Server Virtual のアプリケーションに対するログローテーションの定義は、次の手順に従って行います。

このタスクはいつでも完了できます。Security Management Server Virtual の使用を開始する必要はありません。

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 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。週次のローテーションでは、ドロップダウンメニューを使用して、適切な曜日を選択します。月次のローテーションでは、月の適切な日付を入力します。
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 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、Security Management Server Virtual 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。詳細については、次を参照してください http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

デルサーバ上に保存する場合にディスク使用量が 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。電子メール通知が設定されている場合は、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、ストレージ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、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 に **X** を入力して、**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 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、Dell Server のサービスがすべて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は、サービスを再起動してください。詳細については、「サービスの開始または停止」を参照してください。**すべて**のサービスが実行されている場合に**限り**、復元を開始してください。

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。

バックアップは、再起動後に復元されます。

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:

Dell Server は Linux Debian Ubuntu x64 をベースにしています。

dellsupport として Dell Server 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。

/backup（必須）

/certificates（強く推奨）

/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。

SMTP 設定の構成

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。電子メール通知は、Dell Server のステータスエラー状態、パスワードのアップデート、Dell Server のアップデートの可用性、クライアントのライセンス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 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 SMTP ユーザーを入力します
6 SMTP パスワードを入力します
7 通知送信元 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。
8 サーバステータス送信先 に、サーバステータス通知を送信する電子メールアカウント ID を入力します。受信者はコンマ、またはセミコロンで区切ります。
9 パスワード変更送信先 に、パスワード変更通知を送信する電子メールアカウント ID を入力します。
10 ソフトウェアアップデート送信先 に、ソフトウェアアップデート通知を送信する電子メールアカウント ID を入力します。
11 サービスアラートリマインダ 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 **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。
12 サマリレポート フィールドで通知レポートを有効にするには、必要な間隔（毎日、毎週または毎月）を選択し、スペースバーを押して **X** を入力し、
13 **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

既存の証明書のインポートまたは証明書要求の作成は、Security Management Server Virtual 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: Security Management Server Virtual 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 Dell Server の FTP サーバ上で、証明書を **/certificates** に保存します。
3 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 Dell Server 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。

> **メモ: 詳細については、次を参照してください http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en**

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 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：Dell Server 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 Dell Server の FTP サーバ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 Dell Server 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

メモ: デフォルトで生成される自己署名証明書は、10 年間にわたって生成されます。

1 Dell Server 詳細設定 メニューで、**サーバ証明書** 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。

サービスが自動的に再起動します。

データベースアクセスの有効化

このタスクはいつでも完了できます。Security Management Server Virtual の使用を開始する必要はありません。

メモ: データベースアクセスは必要な場合にのみ有効にし、必要がなくなったら無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 データベースアクセスの有効化 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。

Dell Data Security 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。

端末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。

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。

- 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
  - Message Broker
  - Identity Server
  - Compatibility Server
  - Security Server
  - Compliance Reporter
  - Core Server
  - Core Server HA
  - Inventory Server
  - Forensic Server
  - Policy Proxy
- 管理コンソール
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- データベースカスタマイザログ

メモ: この画面をナビゲーションするには、次の手順を実行します。

- ログの末尾に移動するには、右 Alt キーを押したまま、キーボードの "/" キーを押します。
- ログを終了するには、左のコントロールキーを押したまま、キーボードの "x" を押します。
- 矢印キーを使用すると、ナビゲーションを実行できます。
- Page Up および Page Down を押すと、一度に 1 ページずつ上下に移動します。
- スペースバーを押すと、1 ページずつログを移動します。

コマンドラインインタフェースを開く

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。

3

メンテナンス

不要な Security Management Server Virtual バックアップを削除します。

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。

4

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。

5

インストール後の設定

インストール後、組織が使用している Dell Data Security ソリューションに応じて、環境のコンポーネントの一部を設定する必要がある場合があります。

Security Management Server Virtual のインストール後に、次のデフォルトを変更する必要があります。

- 次の場所にあるバック エンド サーバーのパスワードを変更します。

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`
- 次の場所にある環境内のすべてのフロント エンド サーバーのパスワードを変更します。

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

パスワードは次のように表示されます：`proxy-server.password=ENC(<texthere>)`

パスワードを変更するには、次の手順を実行します。

1 次を選択します：`ENC(<texthere>)`

2 選択したテキストを次に変更します：`CLR(<newpasswordhere>)`

サービスが再開されると、変更した行が `CLR` から `ENC` に変わり、パスワードが暗号化されます。

メモ：proxy-server.username も変更できますが、メッセージ ブローカーの application.properties ファイルおよびアクティブなすべてのフロント エンド サーバー内で一致している必要があります。

Data Guardian の設定

Data Guardian をサポートするように Dell Server を設定するには、管理コンソールで、*Protected Office Documents* および *Cloud Encryption* のいずれか、または両方のポリシーを **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、*Data Guardian* 管理者ガイドまたは *Data Guardian* ユーザーガイドを参照してください。管理者は、作成者がより簡単にキー管理をできるよう、SMTP を有効にして、Dell Data Guardian から外部ユーザーへの電子メール送信を許可することをお勧めします。

マネージャの信頼チェーンチェックの妥当性検査

自己署名証明書が SED または BitLocker Manager 向けの Security Management Server Virtual 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 Dell 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 信頼検証を無効にするには、クライアントコンピュータで次のレジストリエントリを 1 に変更します。

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

DisableSSLCertTrust=REG_DWORD (32-bit):1

6

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 Security Management Server Virtual 管理者として、管理コンソール（https://server.domain.com:8443/webui/）にログインします。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 共通名、UPN（Universal Principal Name）、または sAMAccountName によるユーザー名の検索に使用するフィルターを入力します。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 管理コンソールからログアウトします。

2 管理コンソールにログインし、ドメインユーザーの資格情報でログインします。
管理コンソールの右上隅の「?」をクリックして、*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）。

- ポリシーベース暗号化は共通キー暗号化で有効にされます
- 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 Prevention が有効になっていません
- Threat Protection は無効にされます
- 外部メディアは暗号化されません
- ポート制御によるポートの管理は行われません
- フルディスク暗号化がインストールされているデバイスは暗号化されません
- Data Guardian は無効にされます

ポリシーの説明については、AdminHelp のトピック「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 に、変更内容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。

7

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
Compliance Reporter	HTTP(S)/ 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。
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。
Core Server	HTTPS/ 8887（クローズ）	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 Prevention を管理します。Compliance Reporter および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。
Core Server HA (高可用性)	HTTPS/ 8888	管理コンソール、Preboot Authentication、SED Management、FDE、BitLocker Manager、Threat Protection、Advanced Threat Prevention 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。
Security Server	HTTPS/ 8443	Policy Proxy との通信を行います。また、フォレンジックキーの取得、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。
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。ユーザーグループに基づいてデータを処理します。
Message Broker サービス	TCP/ 61616（クローズ） および STOMP/ 61613（閉鎖、または DMZ 用に設定済みの場合は 61613 が開放）	デルサーバ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。
Identity Server	8445（クローズ）	SED Management の認証などのドメイン認証要求を処理します。
Forensic Server	HTTPS/ 8448	適切な権限を持った管理者が、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管理コンソールから取得できるようにします。 Forensic API に必要です。

名前	デフォルトポート	説明
Inventory Server	8887	インベントリキューを処理します。
Policy Proxy	TCP/ 8000	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。 Encryption Enterprise（Windows および Mac）に必要です。
LDAP	389/636、3268/3269 RPC - 135、49125+	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。 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。
クライアント認証	HTTPS/ 8449	クライアントサーバがデルサーバを認証できるようにします。 Server Encryption に必要です。
コールバックビーコン	HTTP/TCP 8446	フロントエンドサーバで、Data Guardian の保護 Office モードを実行するときに、コールバックビーコンが保護された各 Office ファイルに挿入されることを許可します。