

# Dell Security Management Server Virtual

Quick Start and Installation Guide v10.0



## Notes, cautions, and warnings

**NOTE:** A NOTE indicates important information that helps you make better use of your product.

**CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

**WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

© 2012-2018 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

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

### Quick Start and Installation Guide

2018 - 08

Rev. A01

# Contents

<b>1 Quick Start Guide.....</b>	<b>5</b>
Installation.....	5
Configuration.....	5
Open Management Console.....	5
Administrative Tasks.....	5
<b>2 Detailed Installation Guide.....</b>	<b>7</b>
About Security Management Server Virtual.....	7
Contact Dell ProSupport.....	7
Requirements.....	7
Security Management Server Virtual.....	7
Management Console.....	9
Proxy Mode.....	10
Security Management Server Virtual Architecture Design.....	11
Download and Install OVA File.....	12
Open Management Console.....	14
Install and Configure Proxy Mode.....	14
Basic Terminal Configuration Tasks.....	15
Check System Dashboard.....	15
Change Host Name.....	16
Change Network Settings.....	16
Set DMZ Server Support .....	17
Change Time Zone.....	17
Update Security Management Server Virtual.....	17
Change User Passwords.....	21
Set up Secure File Transfer (SFTP) Users.....	22
Enable SSH.....	22
Start or Stop Services.....	22
Reboot the Appliance.....	22
Shut down the Appliance.....	23
Advanced Terminal Configuration Tasks.....	23
Configure Log Rotation.....	23
Backup and Restore.....	23
Configure SMTP Settings.....	24
Import an Existing Certificate or Enroll a New Server Certificate.....	25
Enable Database Access.....	26
Set or Change Terminal Language.....	26
View Logs.....	27
Open the Command Line Interface.....	27
Generate a System Snapshot Log.....	28
<b>3 Maintenance.....</b>	<b>29</b>

<b>4 Troubleshooting.....</b>	<b>30</b>
<b>5 Post-Installation Configuration.....</b>	<b>31</b>
Configuration for Data Guardian.....	31
Validate Manager Trust Chain Check.....	31
<b>6 Management Console Administrator Tasks.....</b>	<b>32</b>
Assign Dell Administrator Role.....	32
Log in with Dell Administrator Role.....	32
Commit Policies.....	33
<b>7 Ports.....</b>	<b>34</b>

# Quick Start Guide

This Quick Start Guide is for more experienced users, to get the Dell Server up and running fast. As a general rule, Dell recommends installing the Dell Server first, followed by installation of clients.

For more detailed instructions, see the [Security Management Server Virtual Installation Guide](#).

For information about Dell Server prerequisites, see [Security Management Server Virtual Prerequisites](#), [Management Console Prerequisites](#), and [Proxy Mode Prerequisites](#).

For information on how to update an existing Dell Server, see [Update Security Management Server Virtual](#).

## Installation

- 1 Browse to the directory where the Dell Data Security files are stored and double-click to import into VMware the Security Management Server Virtual **v10.x.x Build x.ova**.

**NOTE:** OVA is now SHA256 signed and will fail to import within the VMWare thick client. For formation see <https://kb.vmware.com/s/article/2151537>.

- 2 Power on Security Management Server Virtual
- 3 Follow the on-screen instructions.

## Configuration

Before you activate users, it is recommended to complete the following configuration tasks at the Security Management Server Virtual terminal:

- [Configure SMTP Settings](#)
- [Import an Existing Certificate or Enroll a New Server Certificate](#)
- [Update Security Management Server Virtual](#)
- Install an FTP client that supports SFTP on port 22, and [Set up File Transfer \(FTP\) Users](#).

If your organization has external facing devices, see [Install and Configure Proxy Mode](#).

## Open Management Console

Open the Management Console at this address: <https://server.domain.com:8443/webui/>

The default credentials are **superadmin/changeit**.

For a list of supported web browsers, see [Management Console Prerequisites](#).

## Administrative Tasks

If you have not launched the Management Console, do so now. The default credentials are **superadmin/changeit**.

Dell recommends that you assign administrator roles as soon as it is convenient. To complete this task now, see [Assign Dell Administrator Role](#).

Click "?" in the upper right corner of the Management Console to launch *AdminHelp*. The *Get Started* page displays. Click **Add Domains**.

Baseline policies have been set for your organization but should be modified depending on your specific needs, as follows (licensing and entitlements guide all activations):

- Policy Based Encryption will be enabled with Common-Key encryption
- Computers with self-encrypting drives will be encrypted
- BitLocker Management is not enabled
- Advanced Threat Prevention is not enabled
- Threat Protection is disabled
- External media will not be encrypted
- Ports will not be managed by Port Control
- Devices with Full Disk Encryption installed will not be encrypted
- Data Guardian is disabled

See the AdminHelp topic *Manage Policies* to navigate to Technology Groups and policy descriptions.

Quick Start tasks are complete.

# Detailed Installation Guide

This Installation Guide is for less experienced users, to install and configure Security Management Server Virtual. As a general rule, Dell recommends installing the Security Management Server Virtual first, followed by installation of clients.

For information on how to update an existing Security Management Server Virtual, see [Update Security Management Server Virtual](#).

## About Security Management Server Virtual

The Management Console allows administrators to monitor the state of endpoints, policy enforcement, and protection across the enterprise. Proxy mode provides a front-end DMZ mode option for use with Security Management Server Virtual.

Security Management Server Virtual has the following features:

- Centralized management of up to 3,500 devices
- Role-based security policy creation and management
- Administrator-assisted device recovery
- Separation of administrative duties
- Automatic distribution of security policies
- Trusted paths for communication between components
- Unique encryption key generation and automatic secure key escrow
- Centralized compliance auditing and reporting
- Auto-generation of self-signed certificates

## Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product.

Additionally, online support for Dell products is available at [dell.com/support](http://dell.com/support). Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Tag or Express Service Code available when you call.

For phone numbers outside of the United States, see [Dell ProSupport International Phone Numbers](#).

## Requirements

### Security Management Server Virtual

#### Hardware

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

#### Virtualized Environment

Security Management Server Virtual v10.0 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>.

## Management Console

### Internet Browsers

**NOTE:**  
The browser must accept cookies.

The following table details supported Internet browsers.

#### Internet Browsers

- Internet Explorer 11.x or later

- Mozilla Firefox 41.x or later
- Google Chrome 46.x or later

## Proxy Mode

### Hardware

The following table details *minimum* hardware requirements.

#### Processor

Modern Dual-Core CPU (1.5 Ghz +)

#### RAM

2 GB minimum dedicated RAM / 4 GB dedicated RAM recommended

#### Free Disk Space

1.5 GB free disk space (plus virtual paging space)

#### Network Card

10/100/1000 network interface card

#### Miscellaneous

IPv4, IPv6 or a combination of IPv4 and IPv6 are supported

### Software

The following table details the software that must be in place before installing proxy mode server.

#### Prerequisites

---

- **Windows Installer 4.0 or later**

Windows Installer 4.0 or later must be installed on the server where the installation is taking place.

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

If not installed, the installer will install it for you.

- **Microsoft .NET Framework Version 4.5.2**

Microsoft has published security updates for .NET Framework Version 4.5.2

#### **i** NOTE:

Universal Account Control (UAC) must be disabled when installing in a protected directory. After disabling UAC, the server must be rebooted for this change to take effect.

Registry location for Windows Servers: HKLM\SOFTWARE\Dell.

The following table details the software requirements for the proxy mode server.

## Operating System

---

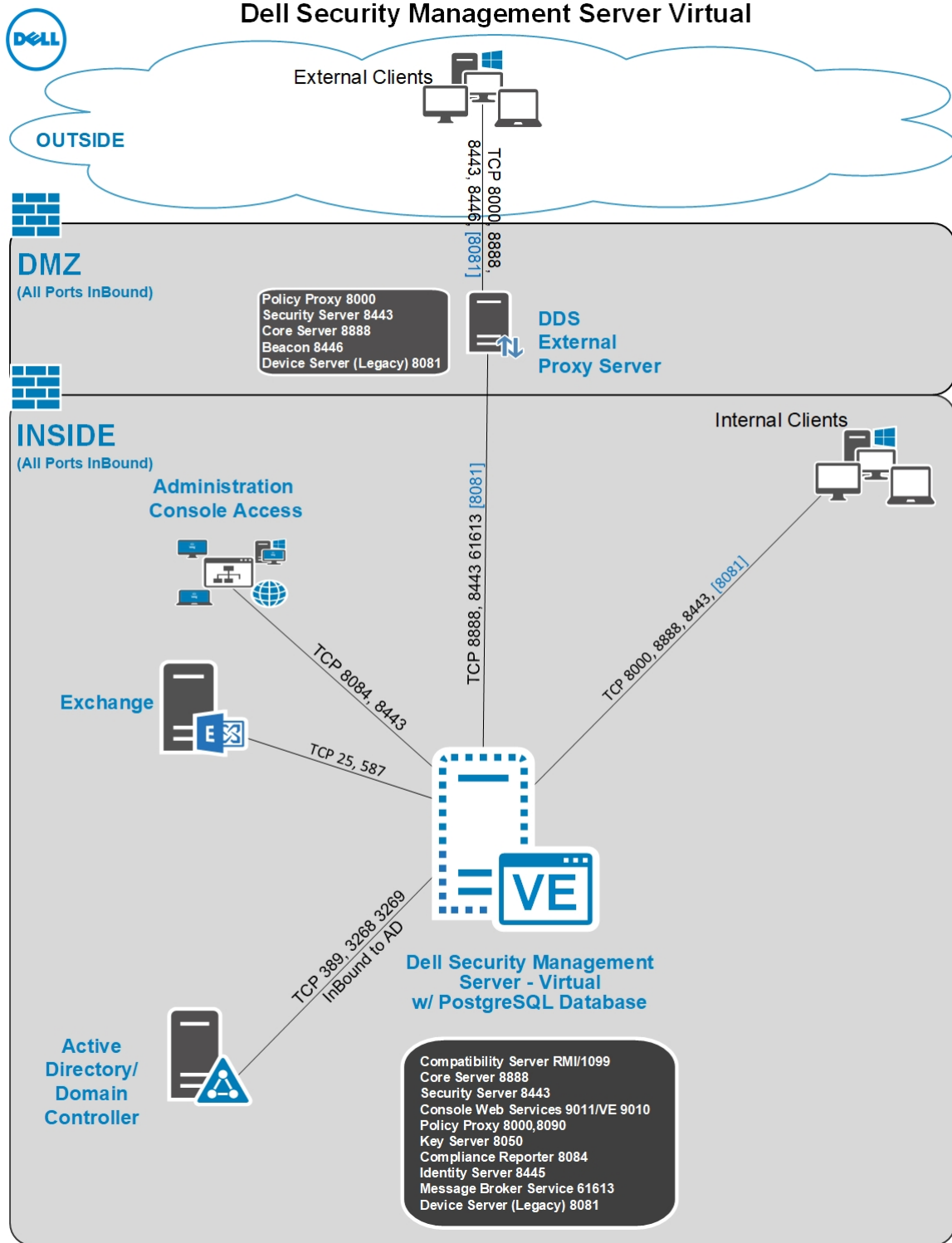
- **Windows Server 2016**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2008 R2 SP0-SP1 64-bit**
  - Standard Edition
  - Enterprise Edition

# Security Management Server Virtual Architecture Design

The Dell Encryption, Endpoint Security Suite Enterprise, and Data Guardian solutions are highly scalable products, based on the number of endpoints targeted for encryption in your organization.

## Architecture Components

Below is a basic deployment for the Dell Security Management Server Virtual.



## Download and Install OVA File

At initial installation, Security Management Server Virtual is delivered as an OVA file, an Open Virtual Application used to deliver software that runs on a virtual machine. The OVA file is available at [www.dell.com/support](http://www.dell.com/support), on the Product Support pages for the following Dell Data Security products:

- [Encryption](#)

- [Endpoint Security Suite Enterprise](#)
- [Data Guardian](#)

To download the OVA file:

- 1 Navigate to the *Drivers and downloads* page for the appropriate product listed above.
- 2 Click **Drivers & downloads**.
- 3 Select the appropriate VMware ESXi version.
- 4 Download the appropriate bundle.

To install the OVA file:

Before you begin, ensure that all system and virtual environment [Requirements](#) are met.

- 1 In the Dell installation media, locate *Security Management Server Virtual v9.x.x Build x.ova* and double-click to import into VMware.

**NOTE:** If using Hyper-V instead of VMware, follow instructions for Windows 10 <https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/>. For Server-based Operating Systems, follow instructions: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server>. If using ESXi instead of VMware, follow instructions: <https://kb.vmware.com/s/article/2109708>.

- 2 Follow the on-screen instructions.

**NOTE:** If the import fails when using VMWare, then the web client is the suggested path for importing the OVA file. For more information, see <https://kb.vmware.com/s/article/2151537>.

- 3 Power on Security Management Server Virtual.
- 4 Select the language for the license agreement, and select **Display EULA**.
- 5 Read the agreement, and select **Accept EULA**.
- 6 If an update is available, select **Accept**.
- 7 Select **Connected Mode** or **Disconnected Mode**.

**NOTE:** If you select **Disconnected Mode**, it can never be changed to Connected mode.

Disconnected mode isolates the Dell Server from the Internet and an unsecured LAN or other network. All updates must be performed manually. For more information about Disconnected mode and policies, refer to *AdminHelp*.

- 8 In *Set delluser Password*, enter the current (default) password, **delluser**, then enter a unique password, re-enter the unique password, and select **Apply**.

Passwords must include the following:

- At least 8 characters
- At least 1 uppercase letter
- At least 1 digit
- At least 1 special character

**NOTE:** It is possible to retain the default password by selecting **Cancel**, or by pressing **Escape** on the keyboard.

- 9 Select **close** to enter into configure hostname window.
- 10 In *Configure Hostname*, use the backspace key to remove the default hostname. Enter a unique hostname and select **OK**.
- 11 In *Configure Network Settings*, choose either option below, then select **OK**.

- (Default) Use DHCP (IPv4)
- (Recommended) InUse *DHCP*, press the space bar to remove the X and manually enter these addresses, as applicable:

Static IP

Network Mask

Default Gateway

DNS Server 1

DNS Server 2

DNS Server 3

Either IPv6 or IPv4 can be selected for a static configuration.

- **NOTE:** When using a static IP, you must also create a host entry in the DNS server.

- 12 At the time zone confirmation prompt, select **OK**.
- 13 When the message displays to indicate that first boot configuration is completed, select **OK**.
- 14 [Configure SMTP Settings](#).
- 15 [Import an Existing Certificate or Enroll a New Server Certificate](#).
- 16 [Update Security Management Server Virtual](#).
- 17 Install an FTP client that supports SFTP on port 22, and [Set up File Transfer \(FTP\) Users](#).

Security Management Server Virtual installation tasks are complete.

## Open Management Console

Open the Management Console at this address: <https://server.domain.com:8443/webui/>

The default credentials are **superadmin/changeit**.

For a list of supported web browsers, see [Management Console Prerequisites](#).

## Install and Configure Proxy Mode

Proxy mode provides a front end (DMZ mode) option for use with the Dell Server. If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

- NOTE:** The Beacon service is installed as part of this installation to support Data Guardian callback beacon, which inserts a callback beacon into every file protected by Data Guardian when allowing or enforcing Protected Office Documents within the environment. This allows communication between any device in any location and the front end server. Ensure that necessary network security is configured before using the callback beacon.

To perform this installation, you need the fully qualified hostname of the DMZ server.

- 1 In the Dell installation media, navigate to the Security Management Server directory. **Unzip** (DO NOT copy/paste or drag/drop) Security Management Server-x64 to the root directory of the server where you are installing Security Management Server Virtual. **Copying/pasting or dragging/dropping produces errors and an unsuccessful installation.**
- 2 Double-click **setup.exe**.
- 3 Select the language for installation, then click **OK**.
- 4 If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.
- 5 Click **Next** in the Welcome dialog.
- 6 Read the license agreement, accept the terms, then click **Next**.
- 7 Enter the 32-character Product Key and then click **Next**. The Product Key is located in the **EnterpriseServerInstallKey.ini** file.
- 8 Select **Front End Install** and click **Next**.
- 9 To install the front end server to the default location of C:\Program Files\Dell, click **Next**. Otherwise, click **Change** to select another location, then click **Next**.
- 10 You have a choice of digital certificate types to use.

- NOTE:** It is highly recommended that you use a digital certificate from a trusted certificate authority.

Select option "a" or "b" below:

- a To use an existing certificate that was purchased from a CA authority, select **Import an existing certificate** and click **Next**.
- b To create a self-signed certificate, select **Create a self signed certificate and import it to key store and click Next**.

At the *Create Self-Signed Certificate* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organization

Organizational Unit (example: Security)

City

State (full name)

Country: Two-letter country abbreviation

Click **Next**.

**NOTE:** The certificate expires in 10 years, by default.

- 11 In the *Front End Server Setup* dialog, enter the fully qualified hostname or DNS alias of the back end server, select **Dell Security Management Server**, and click **Next**.
- 12 From the *Front End Server Install Setup* dialog, you can view or edit hostnames and ports.
  - To accept the default hostnames and ports, in the *Front End Server Install Setup* dialog, click **Next**.
  - To view or edit hostnames, in the *Front End Server Setup* dialog, click **Edit Hostnames**. Edit hostnames only if necessary. Dell recommends using the defaults.

**NOTE:** A hostname cannot contain an underscore character ("\_").

Deselect a proxy only if certain that you do not want to configure it for installation. If you deselect a proxy in this dialog, it is not installed.

When finished, click **OK**.

- To view or edit Ports, in the *Front End Server Setup* dialog, click either **Edit External Facing Ports** or **Edit Internal Connecting Ports**. Edit ports only if necessary. Dell recommends using the defaults.

If you deselect a proxy in the *Edit Front End Host Names* dialog, its port does not display in the External Ports or Internal Ports dialogs.

When finished, click **OK**.

- 13 In the *Ready to Install the Program* dialog, click **Install**.
- 14 When the installation is completed, click **Finish**.

## Basic Terminal Configuration Tasks

Basic configuration tasks are accessed from the Main Menu.

## Check System Dashboard

To check the status of Dell Server services, in the Main Menu, select **System Dashboard**.

The *System Information* widget displays the current version, hostname, IP address, as well as the usage for CPU, memory and disk.

The *Version History* widget displays versioned database schema changes. Data comes from the 'information' table and is sorted by time, with newest version on top.

The following table describes each service and its function in the *Service Health* widget .

Name	Description
Message Broker	Enterprise Server Bus
Identity Server	Handles domain authentication requests.
Compatibility Server	A service for managing the enterprise architecture.
Security Server	Provides the mechanism for controlling commands and communication with Active Directory.
Compliance Reporter	Provides an extensive view of the environment for auditing and compliance reporting.
Core Server	A service for managing the enterprise architecture. This service also handles all activation, policy and inventory gathering from "Agent" based devices.
Core Server HA (High Availability)	A high-availability service that allows for increased security and performance of HTTPS connections when managing the enterprise architecture.
Inventory Server	Processes the inventory queue.
Forensic Server	Provides web services for forensic API.
Policy Proxy	Provides a network-based communication path to deliver security policy updates and inventory updates.

Services are monitored and restarted automatically if necessary.

**NOTE:** If the `databasecustomizer` process fails, servers move to the **Execution Failed** state. To check the `Databasecustomizer` log, in the Main Menu, select **View Logs**.

## Change Host Name

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

- 1 From the *Basic Configuration* menu, select **Host Name**.
- 2 Use the backspace key to remove the existing hostname then replace it with a new host name and select **OK**.

## Change Network Settings

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

- 1 From the *Basic Configuration* menu, select **Network**.
- 2 In the *Configure Network Settings* screen, choose either option below then select **OK**.
  - (Default) Use DHCP (IPv4).
  - (Recommended) In *Use DHCP*, press the space bar to remove the X and manually enter these addresses, as applicable:



Static IP

Network Mask

Default Gateway

DNS Server 1

DNS Server 2

DNS Server 3

Either IPv6 or IPv4 can be selected for a static configuration.

**NOTE:**

When using a static IP, you must create a host entry in the DNS server.

## Set DMZ Server Support

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

- 1 From the *Basic Configuration* menu, select **DMZ Server Support**.
- 2 Use the space bar to enter an **X** in the Enable DMZ Server Support field
- 3 Enter the fully qualified domain name of the DMZ server and select **OK**.

**NOTE:** To leverage a DMZ server, please reference the installation instructions for a proxy server above [Install and Configure Proxy Mode](#).

## Change Time Zone

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

- 1 From the *Basic Configuration* menu, select **Time Zone**.
- 2 In the *Time Zone* screen, use the arrow keys to highlight your time zone and select **Enter**.

## Update Security Management Server Virtual

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

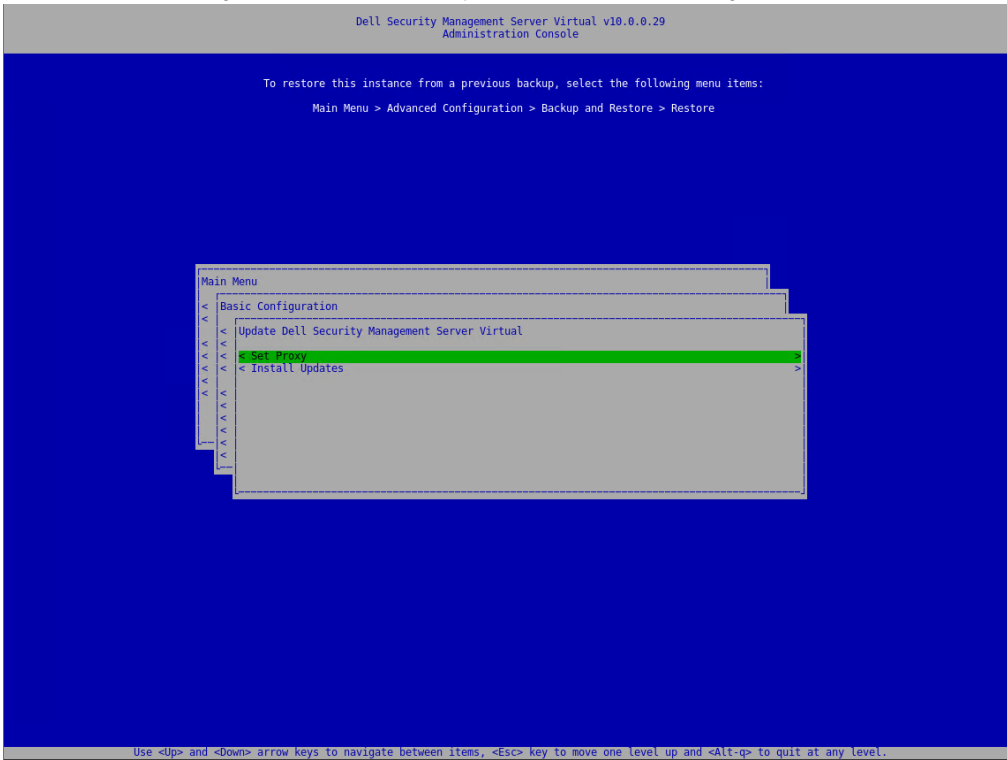
To receive email notifications when Dell Server updates are available, see [Configure SMTP Settings](#).

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)

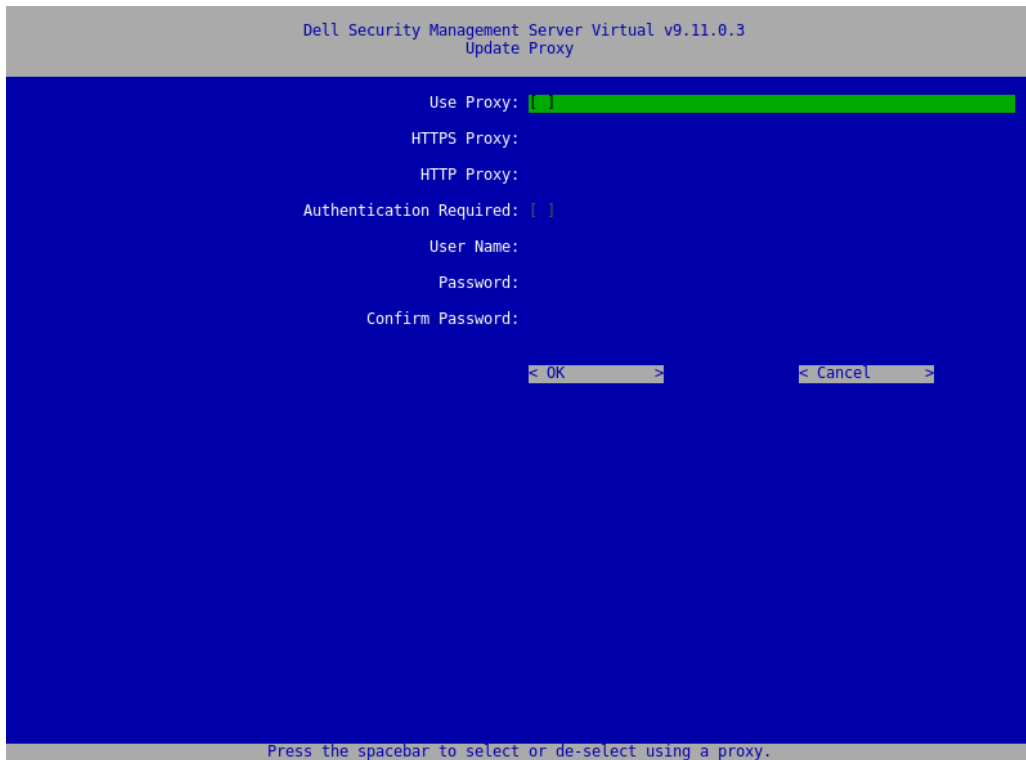
- 1 Dell recommends performing a regular backup. Before updating, ensure that the backup process has been functioning properly. See [Backup and Restore](#).
- 2 From the **Basic Configuration** menu, select **Update Dell Security Management Server Virtual**.



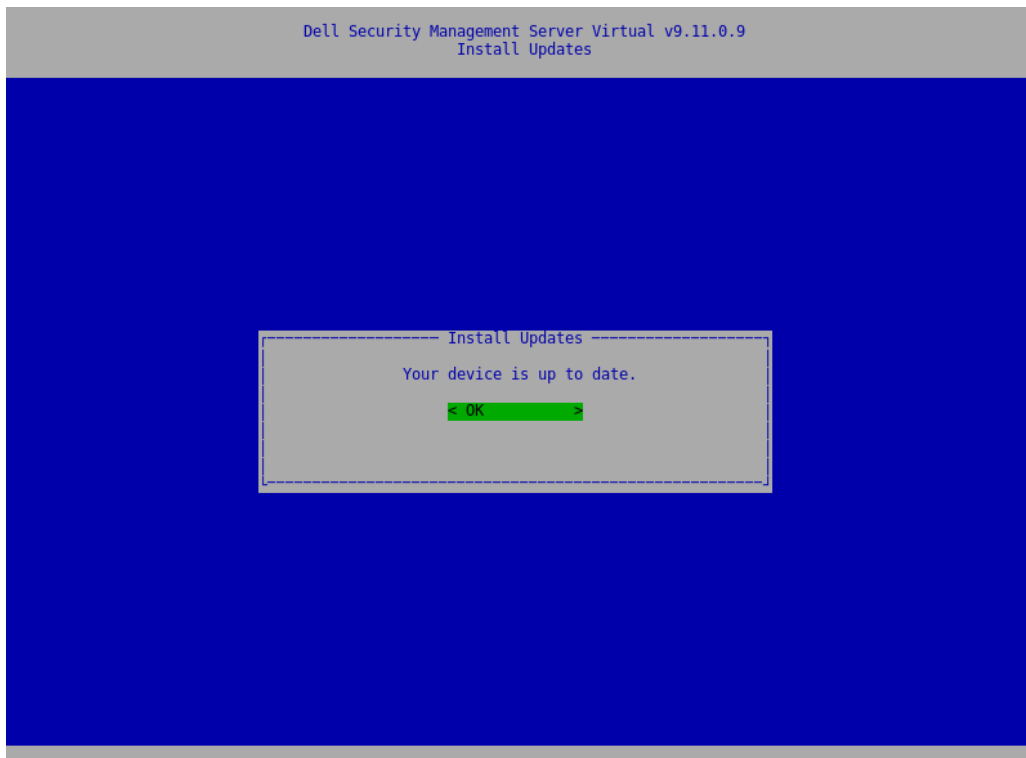
- 3 Select the desired action:
  - Set Proxy Settings - Select this option to set the proxy settings for downloading updates.

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.

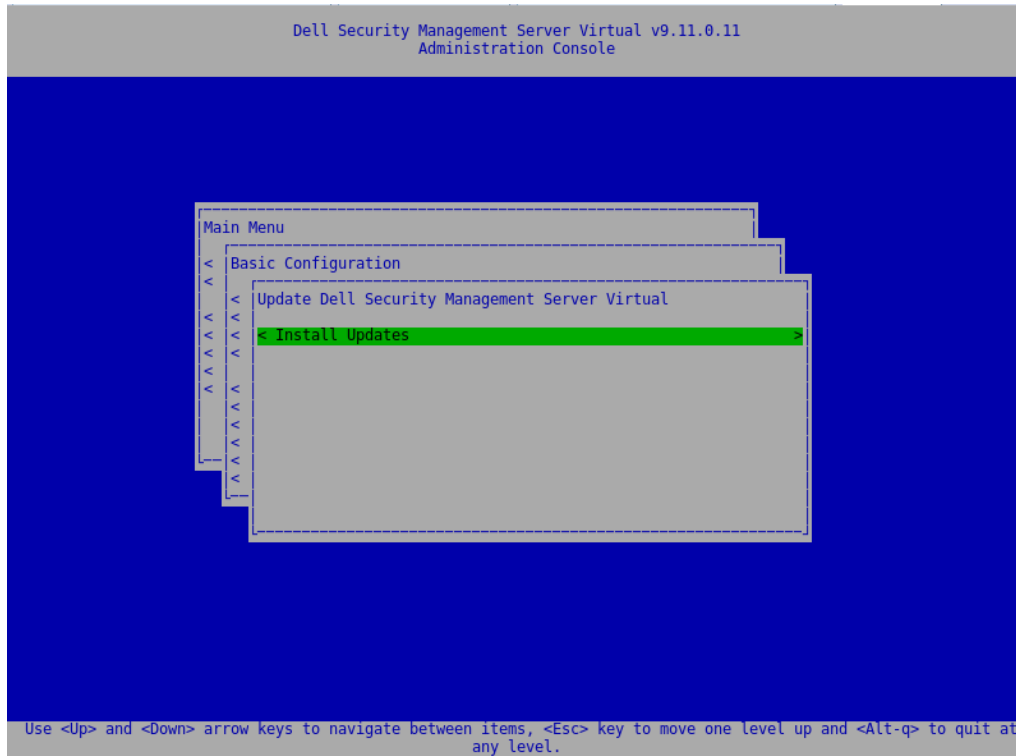


- Install Updates - In v9.11 and later, when selecting **Install Updates**, several generic Ubuntu repositories are queried, along with dist.ddspproduction.com. The dist.ddspproduction.com is Dell's custom repository that contains the application updates for the Dell Security Management Server. These repositories are queried through DNS with port 53 to the defined DNS servers in *Network Configuration* or are pulled through DHCP. Once the server has resolved these connections, Dell reaches out through port 443 to dist.ddspproduction.com and port 80 for all Ubuntu updates. Dell downloads any updates that are available. The proxy settings defined in *Set Proxy* are used for the port 443 and port 80 connections for download.



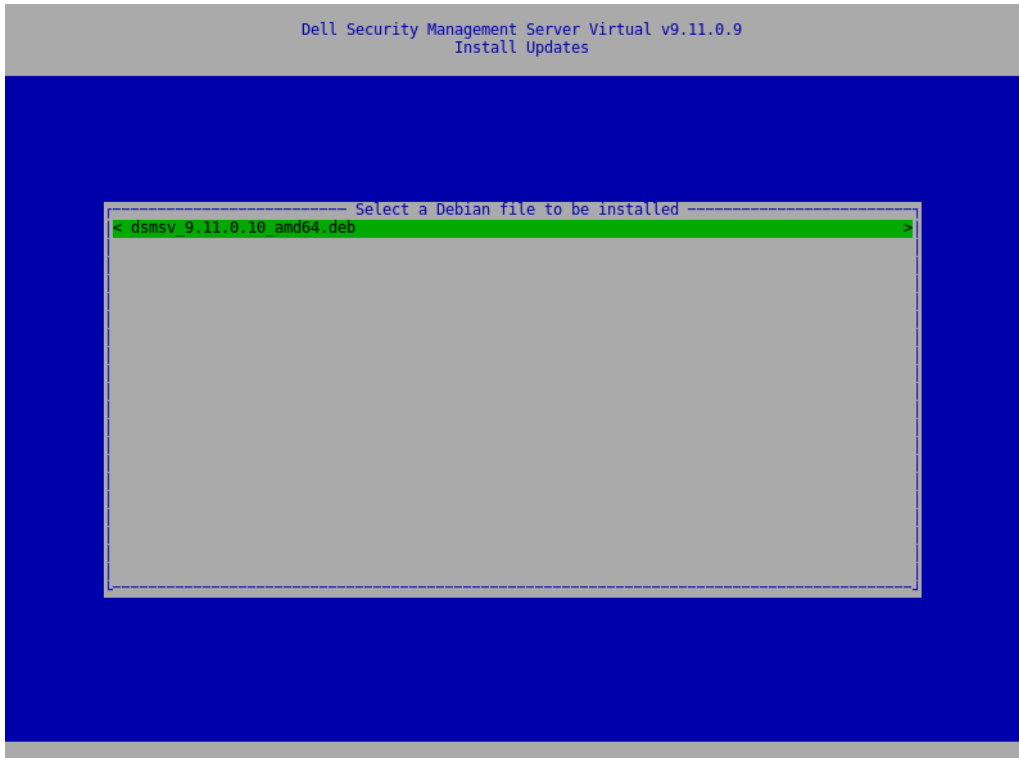
## Update Security Management Server Virtual (Disconnected Mode)

- 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**.



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**.



## Change User Passwords

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

You can change passwords for these users:

- delluser (Terminal administrator) - This user has access to the Dell Server terminal and its menus.
- dellconsole (shell access) - This user has Dell Server shell access. Shell access is available for a network administrator to check and troubleshoot network connectivity.
- dellsupport (Dell ProSupport administrator) - This user has "sudo" rights and should be used sparingly. For security purposes, you control the password for this account.

- 1 From the *Basic Configuration* menu, select **Change User Passwords**.
- 2 In the *Change User Passwords* screen, select user password to change and select **Enter**.
- 3 In the *Set Password* screen, enter the current password, enter the new password, re-enter the new password, and select **OK**.  
Passwords must include the following:

- At least 8 characters
- At least 1 uppercase letter
- At least 1 digit
- At least 1 special character

**NOTE:**

To select different user accounts, use the "spacebar" key on the keyboard to display the selection list.

## Set up Secure File Transfer (SFTP) Users

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

- 1 From the *Basic Configuration* menu, select **SFTP**.
- 2 In the *SFTP* screen, to add an SFTP user and define a password, press **Enter** or the down key in *Status* for the user. Pressing the space bar key offers the option update or delete an existing user. To disable an SFTP user, select **Delete** after selecting user and then select **Yes** on the SFTP confirmation screen .
- 3 Enter a user name and password for the SFTP user.  
Passwords must include the following:
  - At least 8 characters
  - At least 1 uppercase letter
  - At least 1 digit
  - At least 1 special character
- 4 When you are finished entering SFTP users, select **Apply**.

## Enable SSH

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

You can enable SSH for the support administrator login, shell access, and the terminal command-line interface.

- 1 From the *Basic Configuration* menu, select **SSH**.
- 2 Highlight the user for which you want to enable SSH, press the space bar to enter an **X**, and select **OK**.

## Start or Stop Services

Perform this task only if needed.

- 1 To simultaneously start or stop all services, from the *Basic Configuration* menu, select either **Start Application** or **Stop Application**.
- 2 At the confirmation prompt, select **Yes**.

### NOTE:

Server state changes may require up to two minutes to complete.

## Reboot the Appliance

Perform this task only if needed.

- 1 From the *Basic Configuration* menu, select **Reboot Appliance**.
- 2 At the confirmation prompt, select **Yes**.
- 3 After restart, log in to Security Management Server Virtual.

# Shut down the Appliance

Perform this task only if needed.

- 1 From the *Basic Configuration* menu, scroll down and select **Shutdown Appliance**.
- 2 At the confirmation prompt, select **Yes**.
- 3 After restart, log in to Security Management Server Virtual.

# Advanced Terminal Configuration Tasks

Advanced configuration tasks are accessed from the Main Menu.

## Configure Log Rotation

**NOTE:** The instructions below define log rotate for applications on the Dell Security Management Server Virtual that support log rotation.

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

Daily log rotation is enabled by default. To change the default log rotation, from the *Advanced Configuration* menu, select **Logrotate Configuration**.

To disable log rotation, use the space bar to enter an **X** in *No rotation* and select **OK**.

To enable log rotation, follow these steps:

- 1 To enable daily, weekly, or monthly rotation, use the Spacebar to enter an **X** in the appropriate field. For weekly rotation, use the dropdown menu to select the appropriate day of the week. For monthly rotation, input the appropriate day of the month.
- 2 Enter a time for rotation in *Logrotate Time*.
- 3 Select **OK**.

## Backup and Restore

Backups can be configured or performed at any time and are not required to begin using Security Management Server Virtual. Dell recommends that you configure a regular backup process. For more information see <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>

When stored on the Dell Server and the disk is at 90 percent capacity, no new backups are stored. If email notifications have been configured, you will receive an email notification that disk allocation space is low.

**NOTE:**

To preserve disk partition space and prevent automatic deletion of backups, remove unnecessary backups from storage.

Backups are run daily, by default. Dell recommends storing backups to an external secure FTP server at a frequency that meets requirements of the organization for backups and appropriate use of storage space.

To configure a backup schedule, from the *Advanced Configuration* menu, select **Backup and Restore > Configuration** and follow these steps:

- 1 To enable daily, weekly, or monthly backups, use the space bar to enter an **X** in the appropriate field. For weekly or monthly backups, enter the appropriate day of the week or month as a numeral, where Monday=1. To disable backups, use the space bar to enter an **X** in *No backups* and select **OK**.

- 2 Enter a time for backup in *Backup Time*.
- 3 Select **OK**.

To perform an immediate backup, from the *Advanced Configuration* menu, select **Backup and Restore > Backup now**. When the backup confirmation displays, select **OK**.

**NOTE:**

Before beginning a restore operation, all Dell Server services must be running. [Check Server Status](#). If all services are not running, restart the services. For more information, see [Start or Stop Services](#). Begin to restore *only* when *all* services are running.

To restore from a backup, from the *Advanced Configuration* menu, select **Backup and Restore > Restore** then select the backup file to be restored. At the confirmation screen select **Yes**.

The backup is restored after reboot.

### Store backups to a secure FTP server

To store backups to an FTP server, the FTP client must support SFTP on port 22.

According to backup requirements of the organization, backups can be downloaded in the following ways:

- Manually
- Through automated script
- Through the organization's approved backup solution

To download backups using the organization's backup solution, obtain detailed instructions from your backup solution vendor.

**NOTE:**

The Dell Server is based on Linux Debian Ubuntu x64.

Log on to the Dell Server as `dellsupport`, and use the `sudo` command to configure your backup solution:

```
sudo <instructions from backup solution vendor>
```

Back up contents of the following folders:

`/backup` (required)

`/certificates` (strongly recommended)

`/support` (optional)

When the `sudo` process is complete, type **exit** and press **Enter** until the login prompt displays.

## Configure SMTP Settings

To receive email notifications **or** to use Data Guardian, follow the steps in this section to configure SMTP settings. Email notifications inform recipients of Dell Server status error states, password updates, availability of Dell Server updates, and client license issues.

It is a best practice to restart the services any time a settings change is made.

To configure SMTP settings, follow these steps:

- 1 From the *Advanced Configuration* menu, select **E-mail Notifications**.
- 2 In the E-mail Notifications screen, to enable email alerts, press the space bar to enter an **X** in *Enable -Email Alerts*.
- 3 Enter the SMTP Server fully qualified domain name.



- 4 Enter the SMTP Port.
- 5 Enter the SMTP User
- 6 Enter the SMTP Password
- 7 In *Send Notifications From*, enter the email account ID to send email notifications.
- 8 In *Send Server Status to*, enter an email account ID to send server status notifications. Recipients are separated with commas or semicolons.
- 9 In *Send Password Changes to*, enter an email account ID to send password change notifications.
- 10 In *Send Software Updates to*, enter an email account ID to send software update notifications.
- 11 In *Service alert reminder*, to enable reminders, press the space bar to enter an **X** then set the reminder interval in minutes. A Service alert reminder is triggered when the reminder interval has passed after a notification is sent about a system health issue and the host or service remains in the same state.
- 12 In the *Summary Report* field, to enable reports of notifications, select the desired interval (Daily, Weekly, or Monthly) and then press the space bar to enter an **X**.
- 13 Select **OK**.

## Import an Existing Certificate or Enroll a New Server Certificate

You can import an existing certificate or create a certificate request through Security Management Server Virtual.

It is a best practice to restart the services any time a settings change is made.

### Import an Existing Server Certificate

- 1 Export the existing certificate and its full chain of trust from its keystore.

**NOTE:** Keep the export password because you will enter it when you import the certificate into Security Management Server Virtual.

- 2 On the FTP Server of the Dell Server, store the certificate to **/certificates**.
- 3 From the *Advanced Configuration* menu, select **Server Certificates**.
- 4 Select **Import Existing Certificate**.
- 5 Select a certificate file to be installed on the Dell Server.
- 6 When prompted, enter the certificate export password and select **OK**.
- 7 When the import is complete, select **OK**.

**NOTE:** For further information, refer to <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>

### Enroll a New Server Certificate

- 1 From the *Advanced Configuration* menu, select **Server Certificates**.
- 2 Select **New Server Certificate**.
- 3 Select **Create Certificate Request**.
- 4 Complete the fields *Generate Certificate Request*:
  - *Country Name*: Two-letter country code.
  - *State/Province*: Enter the unabbreviated state or province name (example, Texas).
  - *Locality Name/City*: Enter the appropriate value (example, Dallas).
  - *Organization*: Enter the appropriate value (example, Dell).
  - *Organizational Unit*: Enter the appropriate value (example, Security).
  - *Common Name*: Enter the fully qualified domain name of the the Dell Server. This fully qualified name includes the hostname and the domain name (example, server.domain.com).

- *Email ID*: Enter the email address to which your CSR will be sent.
- 5 Follow your organizational process for acquiring an SSL server certificate from a Certificate Authority. Send the contents of the CSR file for signing.
  - 6 When you receive the signed certificate, export the certificate as a .p7b file, and download the full chain of trust in .der format.
  - 7 Make backup copies of the certificate and chain of trust.
  - 8 Upload the certificate file and its full chain of trust to the FTP Server of the Dell Server.
  - 9 From the *Advanced Configuration* menu, select **Server Certificates**.
  - 10 Select **New Server Certificate**.
  - 11 Select `Complete Certificate Enrollment`.
  - 12 Select the certificate file to be installed on the Dell Server.
  - 13 If prompted, enter the Certificate Password: **changeit**.

To enable trust validation on Windows-based Encryption clients, see [Enable Manager Trust Chain Check](#).

### Create and Install a Self-signed Certificate

**NOTE:** The default generated self-signed certificates are generated for 10 years.

- 1 From the Dell Server *Advanced Configuration* menu, select **Server Certificates**.
- 2 Select **Create and Install Self-signed Certificate**.
- 3 To confirm that you want to replace the pre-installed certificate with a new certificate, click **Yes**.
- 4 Enter the Certificate Password: **changeit**.
- 5 After the new certificate is installed, select **OK** and wait for services to restart.

The services automatically restart.

## Enable Database Access

This task can be completed at any time. It is not required to begin using Security Management Server Virtual.

**NOTE:** Dell recommends that you enable database access only if necessary and disable after the necessity has been completed.

- 1 From the *Advanced Configuration* menu, select **Database Access**.
- 2 Use the space bar to enter an **X** in *Enable Database Access* and select **OK**. If the database password has not yet been configured, a prompt for the database password displays.
- 3 Enter the database password.
- 4 Re-enter the database password.  
Dell Data Security application components stop automatically.

## Set or Change Terminal Language

It is a best practice to restart the services any time a settings change is made.

- 1 In the Main Menu, select **Set Language**.
- 2 Use the arrow keys to select the preferred language.

## View Logs

To check the following logs, in the Main Menu, select **View Logs**.

- System Logs
  - Syslog Log
  - Mail Log
  - Auth Log (SSH)
  - Postgres Log
  - Monitor Log
- Server Logs
  - Message Broker
  - Identity Server
  - Compatibility Server
  - Security Server
  - Compliance Reporter
  - Core Server
  - Core Server HA
  - Inventory Server
  - Forensic Server
  - Policy Proxy
- Administration Console
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- Databasecustomizer Log

**NOTE:** To navigate through this screen, use the following:

- To go to the end of the log you can hold the right alt key and then press the "/" key on the keyboard
- To exit the log, hold left control and press "x" on the keyboard.
- arrow keys allow for navigation.
- page up and page down go up and down pages one at a time.
- space bar progresses the logs by one page.

## Open the Command Line Interface

To open the command line interface, in the Main Menu, select **Launch Shell**.

To exit the command-line interface, type **exit** and press **Enter**.

# Generate a System Snapshot Log

To generate a System Snapshot Log for Dell ProSupport, in the Main Menu, select **Support Tools**.

- 1 From the *Support Tools* menu, select **Generate System Snapshot Log**.
- 2 At the indication that the file is created, select **OK**.

## Maintenance

Remove unneeded Security Management Server Virtual backups.

Only the ten most recent backups are retained. If disk partition space is at ten percent or less, no more backups are stored. If this condition occurs, you will receive an email notification that disk allocation space is low.

# Troubleshooting

If an error occurs, and you have configured email notifications, you will receive an email notification. Based on the information in the email notification, follow these steps:

- 1 Check applicable log files.
- 2 Restart services, as needed. It is a best practice to restart the services any time a settings change is made.
- 3 [Generate a System Snapshot Log](#).
- 4 Contact Dell ProSupport. For more information, see [Contact Dell ProSupport](#).

# Post-Installation Configuration

After installation, some components of your environment may need to be configured, based on the Dell Data Security solution used by your organization.

## Configuration for Data Guardian

To configure the Dell Server to support Data Guardian, in the Management Console, set one or both of these policies to **On**: *Protected Office Documents* and *Cloud Encryption*.

For instructions to install the Data Guardian client, refer to the *Data Guardian Administrator Guide* or *Data Guardian User Guide*. It is recommended for Administrators to enable SMTP to allow Dell Data Guardian to send emails to external users, and to allow for easier key management for creators.

## Validate Manager Trust Chain Check

If a self-signed certificate is used on the Security Management Server Virtual for SED or BitLocker Manager, SSL/TLS trust validation must remain **disabled** on the client computer. Before enabling SSL/TLS trust validation on the client computer, the following requirements must be met:

- A certificate signed by a root authority (for example, Entrust or Verisign) must be imported into the Dell Server. See [Import an Existing Certificate or Enroll a New Server Certificate](#).
- The full chain of trust of the certificate must be stored in the Microsoft keystore on the client computer.

To disable SSL/TLS trust validation, on the client computer, change the value of the following registry entry to 1:

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

```
DisableSSLCertTrust=REG_DWORD (32-bit):1
```

# Management Console Administrator Tasks

## Assign Dell Administrator Role

- 1 As a Security Management Server Virtual administrator, log in to the Management Console: <https://server.domain.com:8443/webui/>. The default credentials are **superadmin/changeit**.
- 2 In the left pane, click **Populations > Domains**.
- 3 Click a domain to add a user to.
- 4 On the Domain Detail page, click the **Members** tab.
- 5 Click **Add User**.
- 6 Enter a filter to search the user name by Common Name, Universal Principal Name, or sAMAccountName. The wild card character is **\***.  
A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not display in the Domain or Group Members list in the Management, ensure that all three names are properly defined for the user in the enterprise directory server.  
  
The query will automatically search by common name, then UPN, and then sAMAccount name until a match is found.
- 7 Select users from the *Directory User List* to add to the Domain. Use <Shift><click> or <Ctrl><click> to select multiple users.
- 8 Click **Add**.
- 9 From the menu bar, click the **Details & Actions** tab of the specified user.
- 10 Scroll across the menu bar, and select the **Admin** tab.
- 11 Select the administrator roles to add to this user.
- 12 Click **Save**.

## Log in with Dell Administrator Role

- 1 Log out of the Management Console.
- 2 Log in to the Management Console and login with Domain user credentials.  
Click "?" in the upper right corner of the Management Console to launch *AdminHelp*. The *Get Started* page displays. Click **Add Domains**.

Baseline polices have been set for your organization but should be modified to your specific needs, as follows (licensing and entitlements guide all activations):

- Policy Based Encryption will be enabled with Common-Key encryption
- Computers with self-encrypting drives will be encrypted
- BitLocker Management is not enabled
- Advanced Threat Prevention is not enabled
- Threat Protection is disabled
- External media will not be encrypted
- Ports will not be managed by Port Control
- Devices with Full Disk Encryption installed will not be encrypted
- Data Guardian is disabled

See the AdminHelp topic *Manage Policies* for policy descriptions.



# Commit Policies

Commit policies when installation is completed.

To commit policies after installation or, later, after policy modifications are saved, follow these steps:

- 1 In the left pane, click **Management > Commit**.
- 2 In *Comment*, enter a description of the change.
- 3 Click **Commit Policies**.

## Ports

The following table describes each component and its function.

Name	Default Port	Description
Compliance Reporter	HTTP(S)/ 8084	Provides an extensive view of the environment for auditing and compliance reporting.
Management Console	HTTPS/ 8443	Administration console and control center for the entire enterprise deployment.
Core Server	HTTPS/ 8887 (closed)	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Prevention. Processes inventory data for use by Compliance Reporter and the Management Console. Collects and stores authentication data. Controls role-based access.
Core Server HA (High Availability)	HTTPS/ 8888	A high-availability service that allows for increased security and performance of HTTPS connections with the Management Console, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection, and Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, Data Guardian products, and SED-PBA communication.
Compatibility Server	TCP/ 1099 (closed)	A service for managing the enterprise architecture. Collects and stores initial inventory data during activation and policy data during migrations. Processes data based on user groups.
Message Broker Service	TCP/ 61616 (closed)  and STOMP/  61613 (closed or, if configured for DMZ, 61613 is open)	Handles communication between services of the Dell Server. Stages policy information created by the Compatibility Server for Policy Proxy queuing.
Identity Server	8445 (closed)	Handles domain authentication requests, including authentication for SED Management.
Forensic Server	HTTPS/ 8448	Allows administrators that have appropriate privileges to get encryption keys from the Management Console for use in data unlocks or decryption tasks.  Required for Forensic API.
Inventory Server	8887	Processes the inventory queue.

Name	Default Port	Description
Policy Proxy	TCP/ 8000	Provides a network-based communication path to deliver security policy updates and inventory updates.  Required for Encryption Enterprise (Windows and Mac)
LDAP	389/636, 3268/3269  RPC - 135, 49125+	Port 389 - This port is used for requesting information from the local domain controller. LDAP requests sent to port 389 can be used to search for objects only within the global catalog's home domain. However, the requesting application can obtain all of the attributes for those objects. For example, a request to port 389 could be used to obtain a user's department.  Port 3268 - This port is used for queries specifically targeted for the global catalog. LDAP requests sent to port 3268 can be used to search for objects in the entire forest. However, only the attributes marked for replication to the global catalog can be returned. For example, a user's department could not be returned using port 3268 since this attribute is not replicated to the global catalog.
Client Authentication	HTTPS/ 8449	Allows client servers to authenticate against Dell Server.  Required for Server Encryption
Callback beacon	HTTP/TCP 8446	On a front-end server, this allows a callback beacon to be inserted into each protected Office file, when running Data Guardian Protected Office mode.