Virtual Security Management System (vSMS) Getting Started Guide

Version 4.3.0

5998-3350
April 2016

Legal and notice information

Trend Micro makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint®, the TippingPoint logo, and Digital Vaccine® are registered trademarks of Trend Micro. Vertica Copyright © 2016 Hewlett Packard Enterprise Development Company LP. All other company and product names may be trademarks of their respective holders. All rights reserved. This document contains confidential information, trade secrets or both, which are the property of Trend Micro. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro or one of its subsidiaries.

All other company and product names may be trademarks of their respective holders.

TippingPoint Virtual Security Management System (vSMS) Getting Started Guide
Publication Part Number: 5998-3350

Contents

vSMS Getting Started

This information describes the installation and configuration of the TippingPoint Virtual Security Management System (vSMS). This information is for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint vSMS appliances.

The following sections help you get started with the vSMS:

- *Overview* on page 3
- *Installation* on page 6
- *Configuration* on page 9

About This Guide

The *Virtual Security Management System User Guide* provides information to help you quickly get started configuring your TippingPoint system and using the Virtual Security Management System (vSMS) to manage your TippingPoint network devices.

This section includes the following topics:

- *Target audience* on page 1
- *Related documentation* on page 2
- *Conventions* on page 2
- *Customer support* on page 3

Target audience

This guide is intended for security network administrators and specialists that have the responsibility of monitoring, managing, and improving system security. The audience for this material is expected to be familiar with the TippingPoint security systems and associated devices.

Users should be familiar with the following concepts:

- Basic networking
- Network security
- Routing

Related documentation

A complete set of product documentation for the Virtual Security Management System is available online. The product document set generally includes conceptual and deployment information, installation and user guides, CLI command references, safety and compliance information, and release notes.

For information about how to access the online product documentation, refer to the *Read Me First* document in your product shipment.

Conventions

This information uses the following conventions.

Typefaces

TippingPoint publications use the following typographic conventions for structuring information:

Convention	Element
Bold font	- Key names - Text typed into a GUI element, such as into a box - GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click **OK** to accept.
Italics font	Text emphasis, important terms, variables, and publication titles
`Monospace font`	- File and directory names - System output - Code - Text typed at the command-line
`Monospace, italic font`	- Code variables - Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

Messages

Messages are special text that is emphasized by font, format, and icons.

⚠ **Warning!** Alerts you to potential danger of bodily harm or other potential harmful consequences.

△ **Caution:** Provides information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

Note: Provides additional information to explain a concept or complete a task.

Important: Provides significant information or specific instructions.

Tip: Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

Customer support

TippingPoint is committed to providing quality customer support for all of its products. If you need customer support, contact the TippingPoint support center for your product. You can find the customer support contact information for your product in the Read Me First document that is in your product shipment. The Read Me First document is also available on the TippingPoint Threat Management Center (TMC).

If this is your first purchase of a TippingPoint product, contact customer support to register your product and access online support.

Self-service portal

TippingPoint provides an online self-service portal for TippingPoint customers. The Self-Service Portal provides a tool for customers to manage their support cases. After registering for an account, you can submit new technical support cases and manage existing ones. For more information about accessing the online Self-Service Portal, refer to the *Read Me First* document.

Contacting support

To expedite your support request, please take a moment to gather some basic information from your records and from your system before contacting customer support. For example, your support representative may need your device serial number and the versions of your product software to assist you. For additional details about contacting support and gathering needed information before contacting support, refer to the *Read Me First* document.

Overview

The Virtual Security Management System (vSMS) is a software-based, virtualized SMS appliance that operates within a VMware virtual environment. The vSMS platform includes two editions: *vSMS Essential* and *vSMS Enterprise*. With few exceptions, the vSMS platform provides the same functionality, the same user interfaces, and operates the same as a physical SMS appliance.

vSMS Essential is intended for small to medium enterprise businesses. As a small deployment solution, vSMS Essential allows you to manage up to two devices. vSMS Essential can be used to manage Threat Protection System (TPS), Next Generation Firewall (NGFW), and 10, 110, and 330 IPS devices.

vSMS Enterprise can manage a full range of TippingPoint devices. You can upgrade your SMS license to manage more than the 25 devices the SMS allows you to manage by default.

vSMS Essential and vSMS Enterprise are identical except for license information and the number and types of devices you can manage.

Before you install vSMS, see the latest *TippingPoint SMS Release Notes* available on the TMC. After you deploy and configure vSMS, refer to the SMS documentation to operate and administer vSMS.

You must have a supported VMware environment already installed and configured before you deploy vSMS.

System requirements

The vSMS platform uses a VMware Open Virtualization Format (OVF) file to operate. OVF is a packaging and distribution format for virtual machines. You must use the VMware vCenter Server to deploy the .ovf file.

VMware vSphere environment

A supported VMware vSphere environment must already be set up before you can install and use either vSMS solution.

Product	Version
VMware vCenter Server	5.0 or later
VMware vSphere Client	5.0 or later
VMware ESX/ESXi	5.0 or later

Note: Use the vCenter Server to deploy the .ovf file; deploying the file directly through ESX/ESXi utilities is not supported.

Minimum system requirements

The following are the minimum recommended system requirements for the vSMS platform:

- 300 GB virtual disk size

- 2 virtual CPUs
- 2.27 GHz CPU speed
- 6 GB memory
- 2 virtual network adapters

Note: Two virtual network adapters are required to match a physical SMS. One of the virtual network adapters is for management. The second one is required for High Availability out of band replication, even if replication is not in use.

Migration

Automatic migration from vSMS v3.2 or earlier is not supported. In this case, you must redeploy the vSMS to migrate.

For vSMS v3.3 or later, you can perform an incremental upgrade to a later version without redeploying the vSMS.

To migrate from v3.2 to the current version, redeploy the vSMS as follows:

1. Back up the vSMS database.

   Note: For added assurance, use vSphere to take a snapshot of the vSMS virtual appliance.

2. Remove the vSMS virtual appliance from the VMware environment.
3. Deploy the new vSMS virtual appliance into the VMware environment.
4. Restore the vSMS database backup to the new virtual appliance.

Note: Alternatively, if you have sufficient resources on your ESX/ESXi host, you can shutdown the vSMS virtual appliance, turn it off, deploy the new vSMS virtual appliance, and restore the backed up database. After you verify the integrity of the restored database instance, you can then delete the old virtual appliance from the VMware environment.

Installation summary

The TippingPoint vSMS installation and configuration involves the following components:

- VMware vCenter Server
- VMware vSphere Client
- VMware ESX/ESXi
- vSMS software package (Essential or Enterprise), consisting of the vSMS VMware Open Virtualization Format (OVF) file and a .vmdk file

- Certification string
- vSMS software package MD5 checksum

To install the vSMS package, validate the VMware environment where you want to deploy the virtual appliance, obtain the software package and the MD5 checksum from the TMC, obtain the vSMS certification string from TippingPoint, and then perform the deployment using the following steps.

Step	Task
Step 1	*Validate the VMware environment* on page 7
Step 2	*Obtain the vSMS software package* on page 7
Step 3	*Obtain the vSMS certification string* on page 8
Step 4	*Deploy the vSMS software* on page 8
Step 5	*Start the vSMS server* on page 9
Step 6	*Configure the vSMS server* on page 10
Step 7	*Install the SMS client* on page 10
Step 8	*Log in to the SMS* on page 11

Installation

This section provides instructions for installing vSMS Essential or vSMS Enterprise in a VMware environment.

Before you begin, see the *Installation summary* on page 5 and the latest *TippingPoint SMS Release Notes* available on the TMC.

Perform the following tasks before you deploy the vSMS software:

1. *Obtain the vSMS certification string* on page 8
2. *Obtain the vSMS software package* on page 7

Perform the following tasks through your vSphere Client:

1. *Deploy the vSMS software* on page 8
2. *Start the vSMS server* on page 9
3. *Configure the vSMS server* on page 10

Validate the VMware environment

Before you deploy vSMS, ensure your VMware environment is based on vSphere and that it meets the system requirements described in *System requirements* on page 4.

Note: You cannot adjust physical resource settings during initial deployment of the vSMS. To adjust the settings, first deploy vSMS, and then use the vSphere Client to modify the physical resource settings. Note that once disk size is increased it cannot be decreased.

Obtain the vSMS software package

The vSMS Essential and vSMS Enterprise software packages are distributed to customers through the Threat Management Center. Download the software from the TMC and store it in a location accessible from the vSphere Client. Perform the following steps to obtain the software:

1. In a Web browser, open the TMC, and then log in.
2. Select Releases, and then select Software > SMS > Virtual SMS (vSMS).
3. On the vSMS Software Packages page, select the appropriate software package.
4. Note the MD5 checksum displayed in the "Message" area of the Software Details page. You will compare it against the checksum you generate after you download the file to your local system.
5. Click Download.
6. Accept the End User License Agreement, and save the file to a storage location that is accessible from your vSphere Client.
7. Generate an MD5 checksum against your local copy of the .zip file, and then compare it against the MD5 checksum shown on the TMC.

   Note: If the checksum do not match, make sure you have the right package and download again or contact Customer Support.

8. Unzip the vSMS software package.

   The software package expands into two files, both of which are needed to deploy the SMS virtual appliance. The file names are similar in format to the following:

   ```
   vsms-4.0.vSMS.xxxx.ovf
   ```

   ```
   vsms-disk1-4.0.vSMS.xxxx.vmdk
   ```

Note: The .vmdk file must be in the same folder as the .ovf file when you deploy the vSMS software.

Obtain the vSMS certification string

1. After your product purchase order is received, TippingPoint mails you a physical registration card.
2. Use the information on the card to contact TippingPoint by email to obtain your unique vSMS certification string.
3. TippingPoint sends your certification string to you by email. When you receive the certification string, you can deploy the vSMS.

Deploy the vSMS software

The vSMS is a virtual appliance compressed and packaged according to the VMware Open Virtualization Format (OVF). The vSMS contains a ready-to-configure virtual instance of SMS. When the vSMS is deployed, the SMS software running in the virtual appliance operates in the same manner as if it were running on a physical SMS appliance.

△ **Caution:** Deploy the vSMS .ovf file through VMware vCenter Server. Deploying the.ovf file directly through ESX/ESXi utilities is not supported.

1. Use the VMware vSphere Client to log on to the vCenter Server that manages the ESX/ESXi host where you want to deploy the vSMS.
2. Select the host where you want to deploy the vSMS.

   When you deploy the vSMS,be sure to deploy it onto an ESX/ESXi host that has network access to the devices you want the vSMS appliance to manage.
3. Use the following steps to deploy the vSMS .ovf file:
   a. Click File > Deploy OVF Template.
   b. Locate the *.ovf file you obtained when you unzipped the vSMS software package, and then click Next.
   c. Verify the template details, and then click Next.
   d. Specify a name and a location for the vSMS, and then click Next.
   e. Specify a host/cluster where you want to deploy the vSMS, and then click Next.
   f. Select a datastore for the vSMS, and then click Next.

   Note: If the storage page of the OVF deployment wizard indicates the host where you are installing the vSMS appliance does not provide sufficient disk space, you should deploy the vSMS appliance to a different host that has sufficient disk capacity. If you do not have another host where you can deploy the vSMS appliance, select Thin Provision format in the next step.

   g. Choose a format for storing the virtual disks:

- ◦ **Thick Provision Lazy Zeroed** – Storage is immediately allocated, data remaining on the physical device is zeroed out on demand)
- ◦ **Thick Provision Eager Zeroed** – Storage is immediately allocated, data remaining on the physical device is zeroed out when the virtual disk is created)
- ◦ **Thin Provision** – Storage is allocated on demand)

h. Select a Destination Network to which to map the source network in the OVF template.

i. Enter the SMS certification string; cut and paste the certification string from the email you received from TippingPoint into the field in the deployment wizard, and then click Next.

> **Note:** In some cases the certification string you copy into this field will not be displayed. When you click **Next**, be sure to verify the string that appears on the summary screen.

The vSMS requires a valid certification string during the startup procedure; the certification string must match the string from TippingPoint. If you open the string in an application before you copy and paste it into the OVF deployment wizard, make sure the application does not insert carriage returns, new line characters, or other unseen characters.

j. Verify the deployment settings on the summary screen, and then click Finish.

4. After the OVF deployment process completes, right-click the vSMS virtual machine, and then select Edit Settings.
5. Confirm that the first network interface is assigned to the virtual network with access to the security devices you want the vSMS to manage, and then click OK.

Start the vSMS server

While logged in to the VMware vCenter Server, perform the following steps to launch the vSMS and open a console.

1. Expand the datacenter and datastore folders until you see the virtual machine where you installed vSMS.
2. Right-click the vSMS and select Power > Power On.
3. As the virtual machine starts, monitor the vCenter Recent Tasks pane to ensure it completes the power-on process.
4. When the virtual machine is powered on, you can open a console to monitor the booting of the guest operating system. To do this, right-click the virtual machine and select Open Console.

Configuration

This section provides instructions for configuring the SMS server, installing an SMS client, connecting to the server, and performing basic tasks to configure your TippingPoint system.

- *Connecting to the server* on page 10

- *Adding a device* on page 11
- *Distributing a Digital Vaccine* on page 12
- *Backing up and restoring the SMS database* on page 12
- *Resetting the SMS to factory default* on page 12
- *Where to go next* on page 13

Connecting to the server

After you have configured the server, you can install the SMS client and log in to the SMS or connect to the SMS by command line interface (CLI).

Note: Do not change the vSMS vNIC settings. The virtual network interface controller (vNIC) settings configured during the deployment of vSMS are required for the application to operate successfully. For best results, do not change the vNIC settings.

Configure the vSMS server

After powering on the server, the SMS Out-of-Box (OBE) Setup Wizard prompts you to perform basic tasks to configure the system. Perform the following steps:

1. Log on to the SMS server as SuperUser (no password).
2. Read and accept the end-user license agreement to continue.
3. If needed, select a language for a different keyboard layout.
4. Specify a security level (0 – 2) and create a new Super User administrator account and password.
5. Specify the network type, SMS management IP address, network mask, and optional default gateway.
6. Specify a host name to describe the SMS. If desired, enter the optional host location and system contact information.
7. Modify the timekeeping option by enabling NTP Client for your time zone.
8. Modify server options for SSH, HTTPS, HTTP, and SNMP.
9. As an optional step, you can configure a Network Management System to monitor and receive SNMP traps.
10. Configure email contact information.

Install the SMS client

The SMS client can be installed on a physical machine or on a virtual machine.

The client software runs on the following operating systems:

- Windows: Vista, Windows 7, and Windows 8

- Linux
- Mac OS X

1. On your computer, start your web browser.
2. In your browser Address bar, enter the IP address or host name of your SMS appliance. For example: `https://123.45.67.89`.
3. Log in with the SuperUser account created when you configured during the vSMS Server setup.
4. On the SMS Welcome page, select the client that is compatible with your computer software or click the Client Installation link in the navigation pane.
5. Run the installation wizard.

   The installation wizard checks for previous installations and guides you through the options for installing or updating the client software. When installation is complete, the installer prompts you to end or open the client upon completion.

Log in to the SMS

1. Launch the TippingPoint SMS client.
2. Specify the IP address or fully qualified host name of the vSMS server.
3. Provide the user name and password for the SuperUser account created when you configured the vSMS server.
4. Click Login.

   For additional information, see SMS Client in the *TippingPoint Security Management System User Guide*.

Adding a device

Add one or more devices to the SMS to begin managing your TippingPoint system. Your SMS license key determines the number and type of devices that your vSMS is allowed to manage.

For information on adding devices to the SMS, see "Manage Your System" in the *TippingPoint Security Management System User Guide*.

By default, vSMS Enterprise allows you to manage up to 25 devices (any model), and vSMS Essential allows you to manage two devices (TPS, NGFW, and 10/110/330 IPS devices).

Note: vSMS Essential displays a warning message if you manage an unsupported device model or exceed the maximum number of devices allowed in your current license.

Distributing a Digital Vaccine

Digital Vaccines (DVs) contain newly developed filters as well as improvements to existing filters and new filter options investigated and distributed by the TMC. These packages are continually updated to fortify your system against new malicious attacks threatening hosts and network services.

You can download, distribute, activate, and manage Digital Vaccines (DVs), Auxiliary DVs, and DV Toolkit packages from the Profiles workspace in the SMS client.

For information on downloading, activating, and distributing Digital Vaccines, see "Download, Activate, and Distribute Digital Vaccines" in the *TippingPoint Security Management System User Guide*.

Backing up and restoring the SMS database

The SMS database contains data from current and historical events and operations as well as devices the SMS manages.

We strongly recommend that you back up the SMS database periodically to facilitate recovery from an unexpected behavior.

You can use the SMS backup and restore features when migrating from one version of SMS to another, or when promoting from vSMS Essential to vSMS Enterprise.

For details on backing up and restoring the SMS database, see "Backup and Restore" in the *TippingPoint Security Management System User Guide*.

Note: Before you initiate the restore process, ensure there are no active client connections to the SMS server through the SMS client, command line interface, or Web browser.

Resetting the SMS to factory default

The SMS command line interface accepts the `factoryreset` command to reset the system to factory defaults. For the vSMS platform, this command resets the system to factory default settings for the current version of vSMS, unless you choose to reset the device license key.

For example, if you issue the `factoryreset` command on a vSMS instance that was promoted from Essential Edition to the Enterprise Edition, the system will be reset to factory default settings for vSMS Enterprise unless you choose to reset the device license key.

If you choose to reset the device license key during the factory reset, the system will revert to the factory settings for the original configuration.

For additional information about the SMS command line interface, see the *TippingPoint Security Management System CLI Reference*.

Note: Another CLI command, `set license.reset`, removes any new device license keys that have been set. If you run this command on a vSMS Enterprise instance that was promoted from vSMS Essential, the virtual appliance remains vSMS Enterprise.

Where to go next

The SMS is a central console where you can manage multiple TippingPoint devices, products, and services. After the initial setup, you can begin monitoring and managing your TippingPoint systems.

Make sure all TippingPoint devices that you add to the SMS are configured or enabled to accept SMS management. Refer to device product documentation for information about preparing a device for SMS management.

For IPS devices, the SMS performs most of the tasks that are also available from the IPS Local Security Manager (LSM) application. When an IPS device is enabled for SMS control, the device is exclusively controlled by the SMS. You can unmanage devices in the SMS.

For complete information about managing TippingPoint systems, see the *TippingPoint SMS User Interface Guide*, or the SMS online Help.

Note: To access the SMS command line interface (CLI) you must log in with a SuperUser account. The SuperUser account used to access the CLI must have the following authorization: SMS_ACCESS_CLI. For more information about using the CLI, see the *TippingPoint Security Management System Command Line Interface Reference*.