TREND MICRO™

4.4.0

TippingPoint™ Virtual Security Management System (vSMS)

Getting Started Guide

Virtual security management system for centralized global vision and security policy control.

Virtual Security Management System (vSMS) Getting Started Guide

Version 4.4.0

September 2016

Legal and notice information

TippingPoint Virtual Security Management System (vSMS) Getting Started Guide

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 4

Installation on page 8

Configuration on page 18

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 1
- *Conventions* on page 2

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 uses 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.

Contacting support

Contact the TippingPoint Technical Assistance Center (TAC) by using any of the following options.

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *https://tmc.tippingpoint.com*

Overview

The Virtual Security Management System (vSMS) is a software-based, virtualized SMS appliance that operates within a 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 of the following devices:
  - 10/110/330 (IPS)
  - 660N/1400N (IPS)
  - Virtual Threat Protection System (vTPS)
  - Threat Protection System (TPS)
  - Next Generation Firewall (NGFW)
- **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 *Security Management System 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 virtual environment already installed and configured before you deploy the vSMS.

System requirements

This section provides the requirements needed to deploy the vSMS in either a VMware or kernel-based virtual (KVM) environment.

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
- 12 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.

VMware vSphere environment

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

The vSMS platform uses a VMware Open Virtualization Format (OVF) file to operate. OVF is a packaging and distribution format for virtual machines.

- VMware vSphere Client version 5.5 or 6.0
- VMware ESX/ESXi version 5.5 or 6.0

Note: We recommend that you install all updates on your hypervisor hosts before deploying virtual devices in your ESXi environment.

KVM environment

A supported KVM environment must already be set up before you can install and use either vSMS solution. KVM deployment of the vSMS has been successfully tested using the following specifications:

- RHEL version 6 (for three cores); libvirt version 0.10.2; QEMU version 0.12.0.
- RHEL version 7 with the KVM hypervisor (for four cores); libvirt version 1.1.0; Quick Emulator (QEMU) version 1.5.3.

The KVM environment must have the following tar packages installed:

- `qemu-kvm`
- `virt-install`
- `virt-viewer`

Migration

For vSMS version 4.1 or later, you can perform an incremental upgrade to a later version without redeploying the vSMS.

To migrate from versions earlier than 4.1 to the current version, redeploy the vSMS as follows:

1. Back up the vSMS database.

   Note: For added assurance, take a snapshot of the vSMS virtual appliance using the tools in your virtual environment.

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

Note: Alternatively, if you have sufficient resources on your virtual host, you can shut down 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 virtual environment.

Installation summary

The TippingPoint vSMS installation and configuration involves the following components:

- VMware environment
  - VMware vSphere Client
  - VMware ESX/ESXi
  - VMware Open Virtualization Format (.ovf) file and a .vmdk file
- KVM environment
  - RHEL system
  - Tar package
- vSMS software package (Essential or Enterprise)
- vSMS software package MD5 checksum
- Certificate package

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

Step	Task
Step 1	*Validate the virtual environment* on page 8
Step 2	*Obtain the vSMS software package* on page 8
Step 3	*Obtain the vSMS certificate package* on page 9

Step	Task
Step 4	*Deploy the vSMS software on VMware* on page 9 OR *Deploy the vSMS software on KVM* on page 11 OR *Deploy the vSMS software on OpenStack* on page 11
Step 5	*Configure the vSMS server* on page 18
Step 6	*Install the vSMS Software License Key* on page 19
Step 7	*Install the SMS client* on page 19
Step 8	*Log in to the SMS* on page 20

Installation

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

Before you begin, see the *Installation summary* on page 6 and the latest *Security Management System Release Notes* available on the TMC.

Perform the following tasks before you deploy the vSMS software:

1. *Obtain the vSMS software package* on page 8
2. *Obtain the vSMS certificate package* on page 9

Perform the following tasks through your virtual environment:

1. *Deploy the vSMS software on VMware* on page 9

   OR *Deploy the vSMS software on KVM* on page 11

   OR *Deploy the vSMS software on OpenStack* on page 11
2. *Configure the vSMS server* on page 18
3. *Install the vSMS Software License Key* on page 19

Validate the virtual environment

Before you deploy vSMS, ensure your virtual environment meets the system requirements described in *System requirements* on page 4.

Note: If you are deploying the vSMS on VMware, 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 TMC. Download the software from the TMC and store it in a location accessible from your virtual environment.

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 virtual environment.
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.

   To deploy the vSMS on a KVM environment, the software package includes a tar package.

   To deploy the vSMS on a VMware environment, 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 certificate package

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 Entitlements by email to obtain your unique vSMS certificate package. Each certificate package has information associated with it, including whether the license information is for vSMS Essential or vSMS Enterprise. The certificate package information, including the name of the certificate file, should not be changed.
3. TippingPoint sends your certificate package to you by email. When you receive it, you can deploy the vSMS. Save the certificate package to a storage location that is accessible from your virtual environment. For more information, see *Install the vSMS Software License Key* on page 19.

Deploy the vSMS software on VMware

The vSMS is a virtual appliance compressed and packaged according to the VMware Open Virtualization Format (OVF).

A supported VMware vSphere environment must already be set up before you can install and use either vSMS solution. For more information, see *System requirements* on page 4.

Important: VMware vCenter server is not required to deploy the vSMS .ovf file. You can deploy the .ovf file directly through ESX/ESXi utilities.

1. Use the VMware vSphere client to log on to and access 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. Verify the deployment settings on the summary screen, and then click **Finish**.

   The vSMS deployment is complete.
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

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. 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**.

Deploy the vSMS software on KVM

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.

A supported KVM environment must already be set up before you can deploy the vSMS software. For more information, see *System requirements* on page 4.

Note: If you are deploying the vSMS on OpenStack, go to *Deploy the vSMS software on OpenStack* on page 11

Follow these steps to deploy the vSMS software on a kernel-based virtual machine (KVM).

1. Set up two bridge networks on KVM (for example, `br215` and `br216`). Alternatively, you can set up a single bridge network and specify it twice when you deploy the vSMS package.
2. Copy the vSMS tar package to your system.
3. Extract the package with the `#tar -zxf <tar filename>` command.
4. Deploy the vSMS package with the following command:

```
#virt-install
--name=<vsms_name>
--ram=12288
--vcpus sockets=1,cores=4
--boot hd
--disk path=<full_path_to_current_dir>/system_disk.raw
--network bridge=br215,model=e1000
--network bridge=br216,model=e1000
--virt-type=kvm
--cpu qemu64,+ssse3,-svm
--graphics vnc
```

   Note: You cannot reuse the system disk file (`system_disk.raw`) to create another VM. To create another VM, copy the vSMS package to a different directory and then extract the system disk file from the vSMS package.

5. Use the `#virsh console <vsms_name>` to connect to the console.

Deploy the vSMS software on OpenStack

A HEAT template can be used to describe the vSMS infrastructure.

Note: The TippingPoint vSMS has been tested specifically in the DevStack environment. Similar deployments using Kilo and Liberty are also supported.

Note: You must disable security groups and enable the NoopFirewallDriver for Nova and Neutron.

vSMS emulation requirements

The OpenStack HEAT template requires the following emulation configuration:

- Disk driver – ide

vSMS functional requirements

The OpenStack HEAT template requires the following functional configuration:

1. Hypervisor – kvm
2. Virtual processors – 2
3. RAM – 12 GB
4. Disk images – 1 system disk
5. Network ports – 2

Configuring the OpenStack HEAT template

Note: The following commands show values for a sample template. You must provide values appropriate for your environment.

1. Create the networks using neutron command lines:

   ```
   neutron net-create netMgmt --provider:network-type local
   ```

2. Create the subnets using neutron command lines:

   ```
   neutron subnet-create netMgmt 192.168.2.0/24 --name subnetMgmt
   ```

3. Create the vSMS flavor:

   ```
   nova flavor-create --is-public true vSMS.flavor auto 12288 300 2
   ```

4. Import the kvm image.

   a. Untar the files.

      ```
      tar –xvf  <vSMS KVM>.tar.gz
      ```

   b. Create the system disk image.

      ```
      glance image-create
      --name vsms
      --visibility public
      --file system_disk.raw
      ```

```
    --disk-format raw
    --container-format bare
    --property hw_disk_bus=ide
    --property hypervisor_type=qemu
    --progress
```

Template sample

The following template shows values for a sample environment. You must modify the sample template and provide values appropriate for your environment before using the template.

To access a sample HEAT template file, untar the vSMS KVM deployment Tar package and open the vsms_template.yaml template file.

```
heat_template_version: 2015-04-30

description: Simple vSMS instance with 2 ports. The template will require
the user to use a fixed IP address for the ports. The flavor should be based
on the compute host capability. Refer to the vSMS Getting Started Guide.


parameters:
  vsms_image_id:
    type: string
    label: vSMS System Image
    description: The name of the vSMS system disk image
    default: vsms
  vsms_instance_type:
    type: string
    label: vSMS Instance Type
    description: Type of instance (flavor) to be used for vSMS
    default: vSMS.flavor
  private_net:
    type: string
    label: Network
    description: ID of the network into which vSMS is deployed
    default: netMgmt
  private_net_subnetid:
    type: string
    label: Subnet
    description: ID of the subnet into which vSMS is deployed
    default: subnetMgmt

resources:
  vsms_port1:
        type: OS::Neutron::Port
        properties:
          network_id: { get_param: private_net }
```

```
        fixed_ips:
          - subnet_id: { get_param: private_net_subnetid }
vsms_port2:
      type: OS::Neutron::Port
      properties:
        network_id: { get_param: private_net }
        fixed_ips:
          - subnet_id: { get_param: private_net_subnetid }

vtps_simple_instance:
  type: OS::Nova::Server
  properties:
    image: { get_param: vsms_image_id }
    flavor: { get_param: vsms_instance_type }
    networks:
      - port: { get_resource: vsms_port1 }
      - port: { get_resource: vsms_port2 }
```

Launch the template

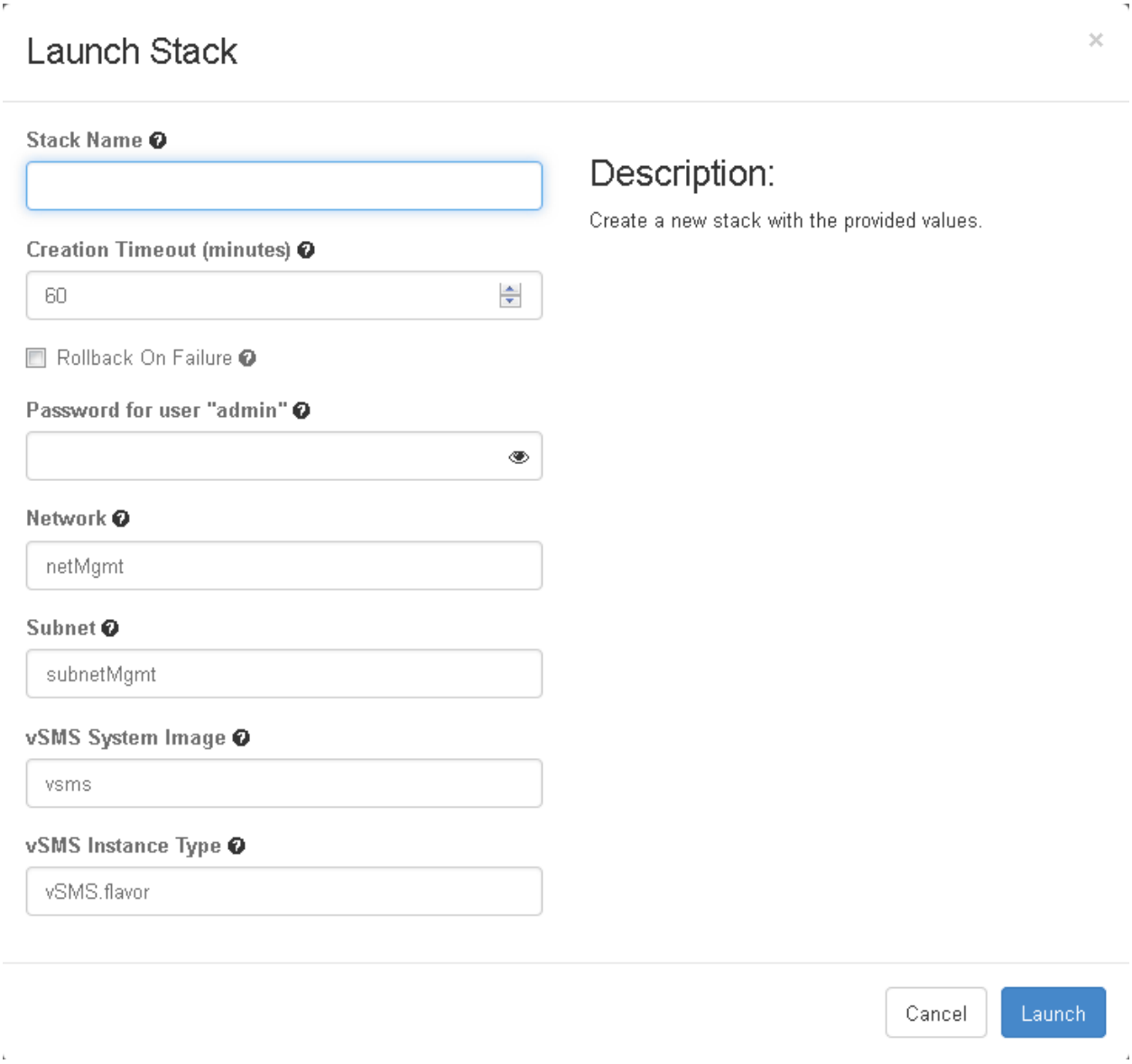
You can launch the OpenStack HEAT template you created using the Horizon web-based user interface or the command line interface.

Launch the OpenStack HEAT template using the Horizon web-based user interface

1. (Optional) Use the following command to validate the template:

   ```
   heat template-validate --template-file <template>.yaml
   ```

2. Select the template.
3. Enter the template parameters, and then click **Launch**.



4. After you launch the vSMS template, review the IP address assigned to the vSMS on OpenStack. You must enter the same IP address and subnet during vSMS OBE.

Launch the OpenStack HEAT template using the command line interface

1. (Optional) Use the following command to validate the template:

   ```
   heat template-validate --template-file <template>.yaml
   ```

2. Use the following command to launch the template:

   ```
   heat -d stack-create vsms --template-file <template>.yaml
   ```

Quick troubleshooting tips

Before contacting support, check to see if any issues you have are addressed in the following troubleshooting tips.

Verifying OpenStack HEAT template properties

Resolution: Use the virsh utility to dump the template xml file and examine your property settings, including the CPU count, the disk adapter type, and the network adapters:

```
localuser@vTPS-Helion1:~/heat_templates$ virsh

Welcome to virsh, the virtualization interactive terminal.

Type:  'help' for help with commands
       'quit' to quit

virsh #
virsh # list --all
 Id    Name                           State
----------------------------------------------------
 3     instance-00000002              running

virsh # dumpxml instance-00000002
  <cpu mode='custom' match='exact'>
   <topology sockets='2' cores='1' threads='1'/>
  </cpu>
    <emulator>/usr/bin/kvm-spice</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' cache='none'/>
      <source file=
'/opt/stack/data/nova/instances/56a5d809-5df5-435d-a665-24885891fff6/disk'/>
      <target dev='hda' bus='ide'/>
      <alias name='ide0-0-0'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <interface type='bridge'>
      <mac address='fa:16:3e:d8:1e:be'/>
      <source bridge='qbr37a85eb2-d0'/>
      <target dev='tap37a85eb2-d0'/>
      <model type='virtio'/>
      <alias name='net1'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </interface>
    <interface type='bridge'>
      <mac address='fa:16:3e:d8:1e:be'/>
```

```
    <source bridge='qbr37a85eb2-d0'/>
    <target dev='tap37a85eb2-d0'/>
    <model type='virtio'/>
    <alias name='net1'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
  </interface>
```

Examining OpenStack HEAT template events

Resolution: Use the `heat event-list <name of stack>` command to see a list of events.

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

After you have configured the server and installed the Software License Key, 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.

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 SuperUser 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 vSMS Software License Key

When you receive the Software License Key from TippingPoint Entitlements, you can install the vSMS license. For more information, see *Obtain the vSMS certificate package* on page 9.

1. Open a Web browser and enter the IP address or host name of your vSMS (for example, `https://123.45.67.89`).
2. Click **Choose File** and then select the Software License Key you received from TippingPoint.

   The vSMS displays the name of the Software License Key.
3. Click **Install Certificate**, and then click **OK** to restart the vSMS.

   After the vSMS restarts, you can *install the SMS client* on page 19.

   Note: If you attempt to refresh the Web browser while the SMS reboots, the page may appear blank. If this happens, use the IP address to reconnect to the SMS when the SMS finishes rebooting.

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
- Linux
- Mac OS X

Note: Before you can install the SMS client on an OS X computer, you must follow the instructions outlined in the *OS X prerequisites* on page 20.

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.

Important information when using a Mac OS X to host an SMS client

When you upgrade the SMS client on OS X with Oracle Java Runtime version 1.8u71 or later, the SMS 4.4.0 client will not be able to connect to an SMS that is still running with a 1k certificate key. To avoid this issue, upgrade the SMS from a 1k certificate key to a 2k key.

If you cannot connect to the SMS using Mac OS X, you have two options:

1. Temporarily make the following changes to the JRE on your local Mac OS X. - OR -
2. Use a Windows SMS client to update the SMS to a 2K certificate key. After you do this, you will no longer need to temporarily change to the JRE on your local Mac OS X.

How to change the JRE on your local Mac OS X

1. Edit the `java.security` file located in the /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security directory.
2. Locate `jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024`, and then delete `MD5` from the line.

   The line should now be `jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024`.
3. Locate `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768`, and then delete `MD5withRSA` from the line.

   The line should now be `jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768`.
4. Open the dmg (disk image) and run the installer application.

Note: If you receive the error message "TippingPoint SMS client Installer is damaged and can't be opened", go to Mac System Preferences > security & privacy settings and change "Allow applications downloaded from" to "Anywhere."

Note: If you receive additional error messages, contact support.

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 *Security Management System User Guide*.

Adding a device

Add one or more devices to the SMS to begin managing your TippingPoint system. Your vSMS software entitlement package 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 *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.

vSMS Essential supports management for the following device models:

- 10/110/330 (IPS)
- 660N/1400N (IPS)
- vTPS
- TPS
- NGFW

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 *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 *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 *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 TPS and IPS devices, the SMS performs most of the tasks that are also available from the Local Security Manager (LSM) application. When a TPS or 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 *Security Management System User 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 *Security Management System Command Line Interface Reference*.

TREND MICRO INCORPORATED
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com
Item Code: APEM47354/160315