Trend Micro™ TippingPoint™

Virtual Security Management System (vSMS) User Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

https://docs.trendmicro.com/en-us/tippingpoint/security-management-system.aspx

Document Part No.: TPEM69836/230927

Release Date: December 2023

Protected by U.S. Patent No.: Pending

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TippingPoint Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Chapter 1

Overview

The Trend Micro™ TippingPoint™ Virtual Security Management System (vSMS) is a software-based SMS appliance that operates within a virtual environment. The vSMS platform enables you to manage an unlimited number (of any model) of TippingPoint devices. The vSMS platform provides the same functionality, the same user interfaces, and operates the same as a physical SMS appliance.

Before you install vSMS, see the latest *Security Management System Release Notes* . After you deploy and configure vSMS, refer to the SMS documentation to operate and administer vSMS.

To ensure that you have the latest versions of product documentation, visit the Online Help Center.

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.

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

- 300 GB virtual disk size. For a larger disk partition, this size can be dynamically increased. A size of 600 GB is recommended. The maximum supported size is 1800 GB.
- 8 virtual CPUs
- 2.27 GHz CPU speed
- 32 GB memory
- 2 virtual network adapters. 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. For High Availability clusters, both systems must have similar memory, CPU, and disk space.

Note

An upgrade will fail on any system that has a drive that is smaller than 300 GB or less than 12 GB of RAM.

Partitions

Disk partitions are created when you initially deploy a vSMS. The vSMS must run partition version 2 or later in order to upgrade to the latest version of SMS.

Run the `get repos.partition-version` from the SMS CLI to identify which partition version your vSMS is running. If your vSMS is running partition version 0 or 1, you cannot upgrade to the latest version of SMS. You must first perform a full SMS backup, redeploy the vSMS to get the latest partition version, and then restore the backup. You can restore any SMS database backups beginning with SMS 5.4.1 or later on an SMS running the latest TippingPoint Operating System (TOS).

VMware vSphere environment

A supported VMware vSphere environment must already be set up before you can install and use the vSMS. The vSMS platform uses a VMware Open Virtualization Format (OVF) file to operate.

- VMware vSphere Client version 7.0 or 8.0
- VMware ESX/ESXi version 7.0 or 8.0 (only paid versions supported)

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 the vSMS. 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

Important

You can upgrade the vSMS to this release directly from vSMS v5.4.1 or later. If you are running vSMS versions older than v5.4.1, upgrade to v5.4.1 before upgrading to this release, or redeploy the vSMS directly. Learn more about paths for upgrading.

If you are upgrading your vSMS to TOS v6.2.0 or later in a KVM environment, you must ensure that the CPU is reconfigured to support a minimum of x86-64-v2, ARMv8.0-A, POWER9, or z14 processing. To do this, do any of the following:

- Update the CPU details in the virt-manager user interface's Console view (**Edit>Virtual machine details>View details>CPUs** and check the **Copy host CPU configuration** checkbox.
- Edit the CPU details by using `sudo virsh edit NAME` on the KVM server command line. Change the CPU host to `'host-model'`, and remove any existing feature policy entries before saving the file:

```
<cpu mode='host-model' check='partial'>
  <model fallback='allow'/>
  <topology sockets='x' cores='y' threads='z'/>
 </cpu>
```

If you made any changes to the KVM vSMS configuration, shut down and restart the image for them to take effect.

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.

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.

Note

Installation summary

The TippingPoint vSMS installation and configuration involves the following components:

- VMware environment
  - VMware vSphere Client
  - VMware ESX/ESXi (only paid versions supported)
  - VMware Open Virtualization Format (.ovf) file and a .vmdk file
- KVM environment
  - RHEL system
  - Tar package
- vSMS software package
- 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 Software License Key from Trend, and then perform the deployment using the following steps.

STEP	TASK
Step 1	*Validate the virtual environment on page 2-2*
Step 2	*Obtain the vSMS software package on page 2-2*
Step 3	*Download the vSMS certificate package on page 2-3*
Step 4	*Deploy the vSMS software on VMware on page 2-4* OR *Deploy the vSMS software on KVM on page 2-6* OR *Deploy the vSMS software on OpenStack on page 2-8*
Step 5	*Configure the vSMS server on page 3-2*
Step 6	*Install the vSMS certificate package on page 3-3*
Step 7	*Install the SMS client on page 3-3*
Step 8	*Log in to the SMS on page 3-6*

Chapter 2

Installation

Before you begin, see the *Installation summary on page 1-5* 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 2-2*
2. *Download the vSMS certificate package on page 2-3*

Perform the following tasks through your virtual environment:

1. *Deploy the vSMS software on VMware on page 2-4*

   -or- *Deploy the vSMS software on KVM on page 2-6*

   -or- *Deploy the vSMS software on OpenStack on page 2-8*
2. *Configure the vSMS server on page 3-2*
3. *Install the vSMS certificate package on page 3-3*

Validate the virtual environment

Before you deploy vSMS, ensure your virtual environment meets the system requirements described in *System requirements on page 1-2*.

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 software package is 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:

Procedure

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 Package page, select the 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 does not match, make sure you have the right package and download again or contact product 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 separate files, which are needed to deploy the SMS virtual appliance. The file names are similar in format to the following:

   ```
   vsms-6.0.0.205662-signed-disk1.vmdk

   vsms-6.0.0.205662-signed.cert

   vsms-6.0.0.205662-signed.mf

   vsms-6.0.0.205662-signed.ovf
   ```

   Note

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

Download the vSMS certificate package

Download the vSMS certificate package from the license manager after you complete your product purchase order through your regular sales channel. After you download the vSMS certificate package, install the certificate. See *Install the vSMS certificate package on page 3-3* for more information.

To download the vSMS certificate package

Procedure

1. Open the license manager.

To access the license manager, go to the TMC, and navigate to **My Account** > **License Manager**.

2. From the License Management page of the license manager, click **Download Cert**.
3. Select **vSMS Cert** from the drop down options.

   The vSMS Certificate Package page displays on the TMC.
4. Click **Download**.
5. Accept the EULA Agreement.
6. Save the vSMS certificate zip file to a local folder that is accessible from your virtual environment.

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 1-2*.

Important

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

Procedure

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

Procedure

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 1-2*.

Note

If you are deploying the vSMS on OpenStack, go to *Deploy the vSMS software on OpenStack on page 2-8*

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

Procedure

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=32768
--vcpus sockets=2,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 host
--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.

Adding a device

Add one or more devices on the SMS to begin managing your TippingPoint system.

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

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 – 8
3. RAM – 32 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.

Procedure

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.
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.

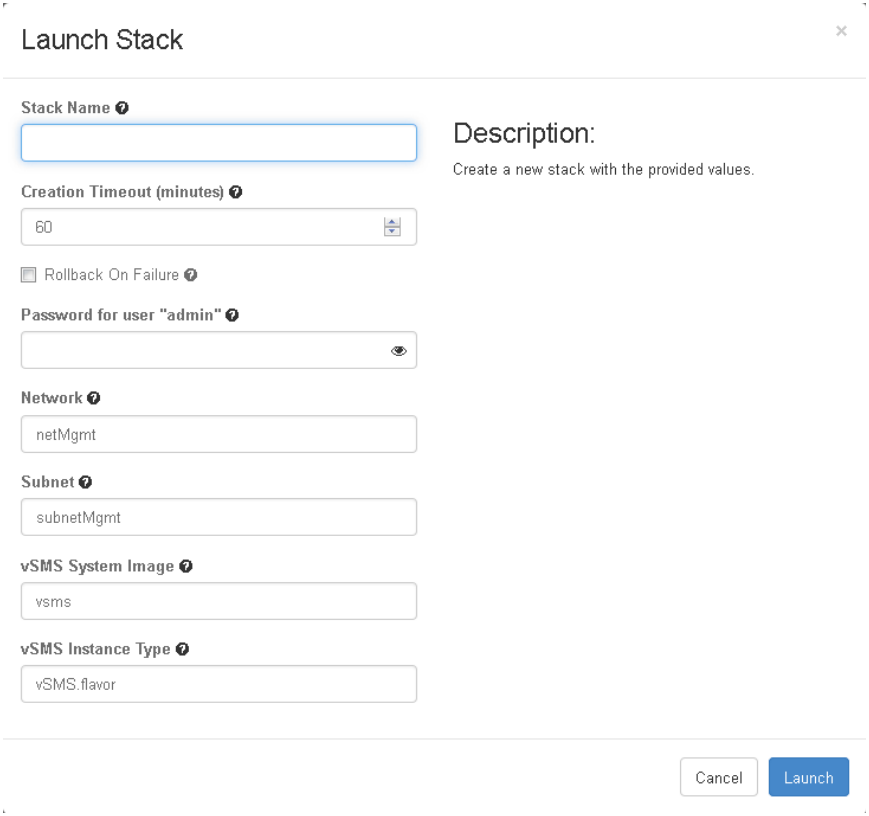
Launch the OpenStack HEAT template using the Horizon web-based user interface

Procedure

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

Procedure

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.

Chapter 3

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:

Procedure

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 – 3) 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, 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 certificate package

Install the vSMS license certificate package after you download the package from the license manager. See *Download the vSMS certificate package on page 2-3* for more information.

Procedure

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 **Select files** and then select the vSMS certificate license package that you downloaded.

   The vSMS displays the license activation code.
3. Click **Install Certificate**, and then click **OK** to restart the vSMS.

   After the vSMS restarts, you can install the SMS client. See *Install the SMS client on page 3-3* for more information.

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 after 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 3-4*.

Procedure

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 during the vSMS Server setup.
4. Click **Client Installation** in the navigation pane.
5. Select the appropriate SMS client installer for your platform and download it.

   Note

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

6. 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.

OS X prerequisites

Important information when using 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 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.

Note

If you have already completed this step in a previous SMS release, you do not need to do this again.

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

- Temporarily make the following changes to the JRE on your local Mac OS X.
- 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 (see above).

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

Procedure

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*.

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 to back up and restore features when migrating from one version of SMS to another. For more information, 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 management console.

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. If you 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.

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.

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: TPEM69836/230927