Trend Micro™ TippingPoint™

Virtual Threat Protection System (vTPS) 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/threat-protection-system.aspx

Document Part No.: TPEM69847/230927

Release Date: April 2024

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 Threat Protection 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

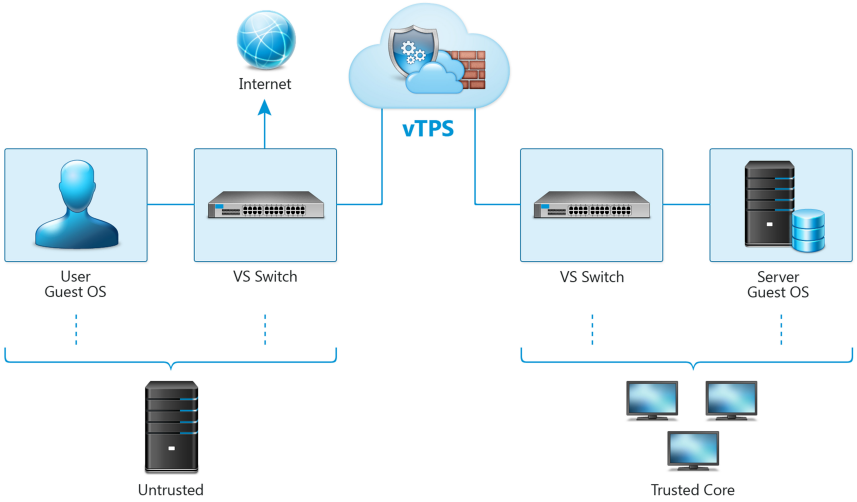
Chapter 1

Deployment overview

Use the configuration steps in these topics to deploy a TippingPoint Virtual Threat Protection System (vTPS) virtual appliance in either a VMware or kernel-based virtual machine (KVM) environment. The vTPS virtual appliance is a software appliance designed to give you the same level of functionality available in the TippingPoint Threat Protection System (TPS), but virtually rather than physically. Just as with a TPS device, the vTPS virtual appliance protects your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings you maintain on the vTPS virtual appliance. You can share the same policies across virtual and physical deployments, and you can centralize the management of your deployments with a Security Management System (SMS) or a virtual SMS (vSMS).

Learn more on page 2-1 about the few differences between vTPS and TPS functionality—for example, command line interface (CLI) operations that control hardware LEDs, and other functions specific to a physical device.

Refer to the following illustration for an example of a basic hypothetical deployment. You must configure your vTPS virtual appliance between L2 broadcast domains (VLANs or switches).



After you deploy the vTPS virtual appliance, access the appliance by using the SMS client. Learn more about these interfaces from the TPS product documentation.

Chapter 2

vTPS functionality

The Virtual Threat Protection System (vTPS) virtual appliance is a software-based security appliance that can inspect traffic in a virtual network between Layer 2 broadcast domains. With few exceptions, the vTPS platform is designed to be functionally identical to a physical TPS device.

The vTPS virtual appliance has most of the same features as the TPS device, including:

- In-line, real-time threat protection for inbound IPv4 traffic that is SSL encrypted
- HTTP response processing to decode URL encodings and numeric character references
- DNS reputation remediation for enabling `NXDOMAIN (name does not exist)` responses to clients that make DNS requests for hosts that are blocked
- Layer 2 Fallback (Intrinsic High Availability)
- Enhanced SNMP support
- The ability to collect a client's true IP address.
- The ability to identify the HTTP URI and hostname information associated with an event.

- Flexibility to upgrade inspection throughput from 500 Mbps to 2 Gbps.

For successful TPS functionality in a virtual environment, the vTPS virtual appliance:

- Supports Layer 2 IPS deployments—The vTPS virtual appliance connects the virtual switches. Traffic between the virtual switches is bridged on these connections using promiscuous mode.
- Provides full protection of North-South traffic.
- Provides limited protection of East-West traffic (according to existing network policy constructs).

For optimal deployment of your vTPS virtual appliance, you should note the specific areas in which your virtual appliance functionality differs from a physical TPS device.

Note

Any unsupported features will not be displayed in the three vTPS interfaces—Local Security Manager (LSM), Command Line Interface (CLI), and Security Management System (SMS).

The following topics highlight the areas where a vTPS virtual appliance diverges functionally from a physical TPS device:

- *Deployment and licensing on page 2-3*
- *Specifications on page 2-4*
- *Unsupported features on page 2-7*
- *Commands on page 2-8*

Deployment and licensing

Because the vTPS virtual appliance is a virtual product, the out-of-box experience (OBE) for vTPS users is described in an email from Trend Micro TippingPoint. This email contains licensing and activation information and directs you to use the license manager on the Threat Management Center (TMC) to create and download vTPS certificate packages.

When setting up your vTPS virtual appliance, note the following:

- The vTPS virtual appliance initially starts up in vTPS Trial Mode. Trial Mode is primarily exploratory and comes with a limited number of security filters in the Digital Vaccine package. In this mode, an SMS can manage only one vTPS virtual appliance at a time. Because Trial Mode has a fixed serial number and entitlement, you cannot use Trial Mode to perform TippingPoint Operating System (TOS) upgrades or distribute Digital Vaccines.
- The vTPS virtual appliance remains in Trial Mode until you install a valid certificate for vTPS Standard Mode. *Learn more on page 4-1* about upgrading to vTPS Standard Mode.
- The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

The following table highlights the ways in which getting set up on a TPS device and vTPS virtual appliance are different:

Deployment	TPS device	vTPS virtual appliance
OBE	After you install the device in a rack, a setup wizard guides you through system checks, initializations, and configurations.	Obtain the license entitlement and certificate using the license manager on the TMC. Initial deployment defaults to a Trial Mode. You cannot perform any updates.

Deployment	TPS device	vTPS virtual appliance
Digital Vaccine	All TPS devices running TOS v6.0 or later use the v4.0.0.*x* Digital Vaccine package. All other TPS devices use the v3.2.0.*x* Digital Vaccine package.	Uses a version of the v4.0.0.*x* Digital Vaccine package that does not include Zero Day Initiative (ZDI) filters.

Specifications

Both the TPS device and the vTPS Standard virtual appliance share the following specifications.

Description	Specification
Average IPS latency	Less than 100 microseconds
Security contexts	750,000

For the various licensed throughput options available for physical TPS devices and the vTPS, refer to the *SMS User Guide*.

The specifications of the physical TPS device and the vTPS Standard virtual appliance differ in the following areas.

Description	TPS device	vTPS virtual appliance
Concurrent sessions	440T: 7,500,000 2200T: 10,000,000 1100TX: 15,000,000 5500TX: 30,000,000 8200TX/8400TX: 120,000,000 8600TXE: 300,000,000 9200TXE: 300,000,000	1,000,000

DESCRIPTION	TPS DEVICE	vTPS VIRTUAL APPLIANCE
New connections per second	440T: 70,000 2200T: 115,000 1100TX: 122,000 5500TX: 397,000 8200TX/8400TX: 650,000 8600TXE: 1,000,000 9200TXE: 1,000,000	VMware: Up to 120,000 KVM: Up to 60,000
Ethernet maximum transmission units (MTU)	9050	1500

Note

All virtual machines (VMs) on a shared host compete for resources. To achieve optimal performance numbers for the vTPS virtual appliance, ensure that the hypervisor provides adequate CPU and RAM for the VM. Performance numbers will vary depending on hypervisor configuration and hardware resources available.

The SSL performance of the physical TPS device and the vTPS Standard virtual appliance differ in the following areas.

Note

The TPS 440T, and 1100TX devices do not support SSL inspection.

DESCRIPTION	TPS DEVICE	vTPS VIRTUAL APPLIANCE
Profiles	8096	756
Policies	8096	756
Policy IP Exceptions	1024	128

Description	TPS device	vTPS virtual appliance
Servers	1024	128
Server IPs	8	8
Server Ports	8	8
Certificates	2200T: 256 5500TX: 256 8200TX/8400TX: 256 8600TXE: 1,000 9200TXE: 1,000	32

The following functionality is different in the vTPS Standard virtual appliance.

Specification	TPS device	vTPS Standard virtual appliance
Port configuration	Eight data ports. You can configure physical characteristics of ports (such as speed and duplex). Ports are fixed.	Two virtual data ports. You cannot configure physical characteristics of ports (such as speed and duplex). You can remove and replace a port.
User disk	External 8 GB CFast (440T/ 2200T or SSD (1100TX) card. External 32 GB SSD (5500TX, 8200TX/8400TX) External 240 GB SSD (8600TXE/9200TXE)	No separate user disk. The vTPS Standard virtual appliance has a single-disk architecture with an 8-GB user disk partition.

Specification	TPS device	vTPS Standard virtual appliance
Environmental requirements	For operating, storage, and environmental requirements, refer to the *Threat Protection System Hardware Specification and Installation Guide*.	Not applicable.
External HA interfaces	1 HA port 1 ZPHA port	No HA ports supported.

Unsupported features

You can configure all available features using the vTPS interfaces (LSM, CLI, SMS). Any unsupported features will not be displayed in these interfaces.

The following features supported in the physical TPS devices are not supported in the vTPS Standard virtual appliance:

- Physical characteristics of ports (such as speed and duplex). Ports are virtual instead of copper or fiber.
- Data security (encrypting the removable disk that stores logs)
- Link setting updates when you configure a port
- Transparent High Availability (TRHA) deployments
- Zero Power High Availability (ZPHA) deployments

> **Note**
> This means that the vTPS virtual appliance does not pass traffic at all during a software upgrade or during a reboot of the device.

- VLAN Translation
- Inspection bypass
- sFlow® sampling

- Jumbo frames
- Reputation Enforcement Options
- East-West protocol (such as VXLAN)
- Direct-attach network interface controller (NIC)

Commands

The following commands that a physical TPS device supports are not available for the vTPS virtual appliance:

- Data security
  - `log-storage`
- Health
  - `reports (reset|enable|disable) fan`
  - `reports (reset|enable|disable) temperature`
- Port settings
  - `interface <port_identifier> physical-media`
  - `interface mgmt physical-media`
- High availability – You can use the following high-availability commands, but *only* for Layer 2 Fallback settings:
  - `high-availability`
  - `high-availability force (normal | fallback)`
  - `show high-availability`
- sFlow sampling
  - `sflow`
  - `show sflow`
- Inspection bypass

  - `running-inspection-bypass` context commands
  - `show inspection-bypass`
- VLAN translation
  - `running-vlan-translations` context commands
  - `show vlan-translations`

Chapter 3

Install and configure the vTPS virtual appliance

Use the following topics to configure your vTPS virtual appliance:

Note

All virtual machines (VMs) on a shared host compete for resources. When a hypervisor becomes overloaded with too many VMs or with VMs that are resource-intensive, a system boot can potentially slow down to the point of failure. To prevent delays or timeout errors in the boot process, watch for deviations in system performance and reallocate the appropriate resources as necessary.

Learn more about configuring security policy for your virtual appliance from your SMS and LSM documentation.

General requirements

IPS performance can vary according to the hypervisor setting and use of resources on the host VM. To deploy a vTPS virtual appliance in any software environment, follow these specifications:

- **Memory (RAM)** – 16 GB
- **Number of CPU cores:** 6
- **Disk space** – 16.2 GB

Note

Although the vTPS virtual appliance supports both thin and thick provisioning, use thick provisioning for optimum performance.

- **CPU** – Host CPU must support the AVX2 instruction set. These CPU configurations were tested:
  - Intel Xeon CPU E5-2630v4
  - Intel Xeon CPU E5-2670v3
  - Intel Xeon CPU E5-2695v3
  - Intel Xeon CPU E5-2695v4
  - Intel Xeon CPU E5-2698v3
  - Intel Xeon CPU Silver 4316

Install and deploy a vTPS virtual appliance by using VMware ESXi

Use the information in these topics to configure the vTPS virtual appliance for startup by using the vCenter application:

- *VMware ESXi requirements on page 3-3*
- *Configure the vTPS virtual appliance on VMware on page 3-3*
- *Start your vTPS virtual appliance on page 3-11*

- *Upgrade to Standard Mode on page 3-12*

VMware ESXi requirements

The vTPS virtual appliance supports the following system and software environment for a VMware ESXi deployment.

Important

Before upgrading to the current TOS version, check the ESXi user interface to ensure that these requirements are met. If necessary, log in to vCenter to make the updates.

- **ESXi Hypervisor version**:
  - Versions 7.0 or 8.0 (only paid versions supported)

Note

Install all updates on your hypervisor hosts before deploying virtual devices in your ESXi environment.

- **Virtual Hardware version:** 11
- **Networking requirements**:
  - Three vNICs — one for management and two for data. The vTPS supports both vSwitches and distributed vSwitches (dvSwitches).
  - You must configure the two data vNICs in promiscuous mode for Layer 2 routing. To avoid ARP request flooding, configure the two data ports on separate networks. Ensure that you set any Forged Transmits and MAC Address Changes to ACCEPT so that network packets get forwarded.
  - Layer 3 virtual segments do not require promiscuous mode.

Configure the vTPS virtual appliance on VMware

To configure vTPS virtual appliance on VMware:

Procedure

1. Create three virtual switches on the ESXi host—one for the management port and two for the data ports, and ensure that you connect the three vNICs to the correct virtual switches.

   Learn more about VMware.

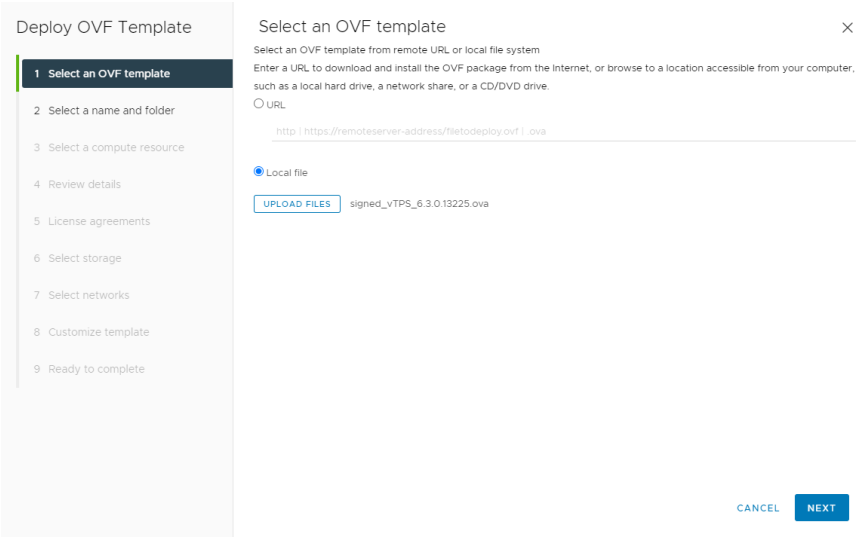
   Note

   Consider the following when configuring your network ports.

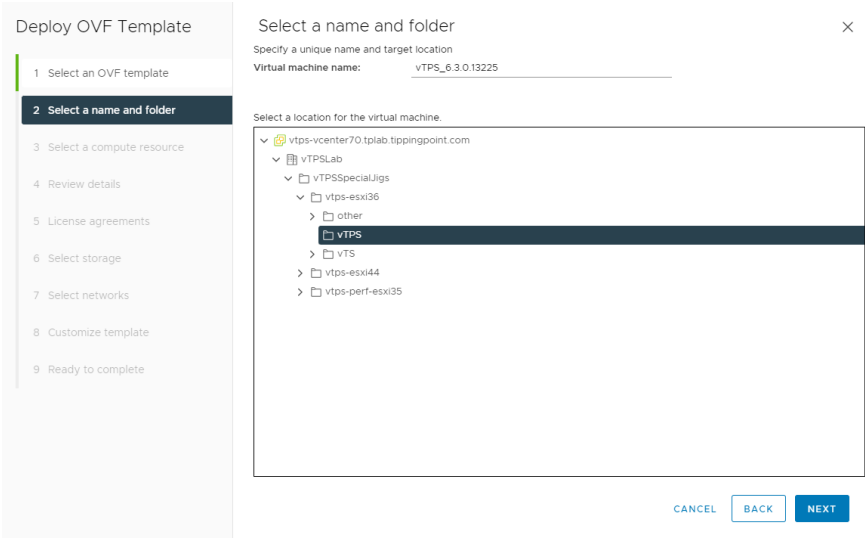
   - In order for the vTPS to function properly for Layer 2 routing, create the ports, map them to their correct interfaces, and enable them in promiscuous mode. (Promiscuous mode is not required for Layer 3 virtual segments.)
   - By default, ESXi attempts to attach all the adapters to the virtual switch that was created first.
   - Make sure that you set any Forged Transmits and MAC Address Changes to ACCEPT for network packets to get forwarded.
   - If you deploy two vTPS devices using the same two networks, traffic loops through both devices.
   - You must configure the VLAN ID field to `All(4095)` for data port virtual switches if you intend to use VLANs for data ports.
   - If your configuration requires traffic to cross multiple VLANs before reaching the vTPS, make sure that your remove the VLAN tags from the ports to prevent the traffic from going through the same network on its way back.

2. Copy the vTPS OVA package to your system. Use VMware ovftool build 4.6.
3. From vSphere, open the package and launch the **Deploy OVF Template** wizard.

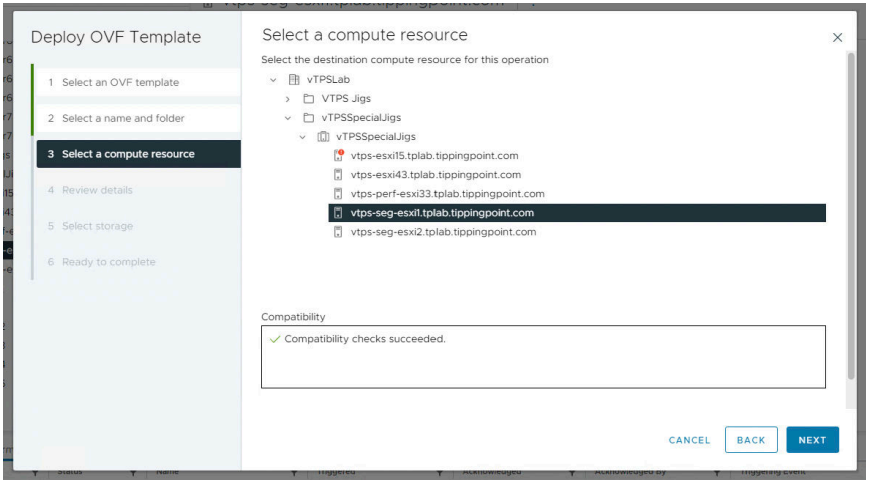
After you have verified that the publisher information and accepted the End User License Agreement (EULA), specify the OVF template to use from a URL or your local system.



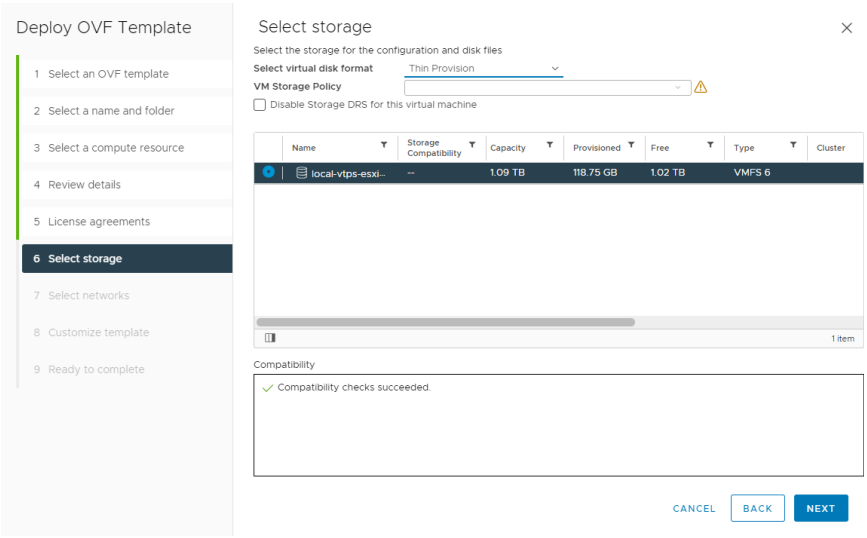
4. On the Select a name and folder screen, you can rename and choose a specific install location for the VM instance, or you can accept the default name and location.



5. Select the destination resource that you want on the Select a compute resource screen.



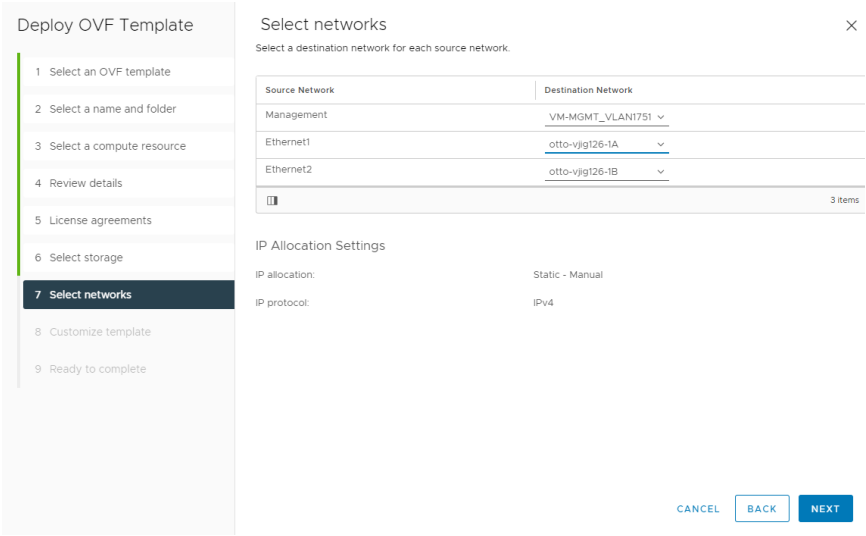
6. Review the template details and click **Next** to verify or **Back** to make changes.
7. Accept the License Agreement and click **Next**.
8. Select where to store the configuration and the format in which to store the virtual disks on the Select storage screen.



Note

The vTPS virtual appliance supports both thin and thick provisioning. For optimum performance, use thick provisioning.

9. On the Select networks screen, map your three source network options to a destination network.



Note

Accepting the default values configures the management port and the data ports on the same network, which can flood the environment with ARP requests. To avoid this, ensure that you configure the two data ports on different networks.

The first interface you provide is your management port. Ensure that your management network can access this port. Then select networks for the two data ports according to your virtual switch/port configuration.

Important

Ensure that you correctly map your network adapters so that you can access your vTPS virtual appliance by using the CLI and SMS client.

10. If you use a vSphere client to deploy directly on a host, you can configure the vTPS parameters only after the vTPS boots using the out-of-box experience (OBE) interface on the console. If you use a vCenter

server to deploy, the Customize template screen prompts you to configure the parameter values:

- IP address
- Netmask value
- Default Gateway
- IPv6 Address (optional)
- IPv6 Prefix Length (optional)
- IPv6 Default Gateway (optional)
- IPv6 Autoconfiguration (optional)
- Hostname (required)
- Host location (optional)
- IP address of DNS servers (optional)—You can add up to two addresses

Note

The VMware deployment screen supports setting up only an IPv4 IP address. If you want to set up an IPv6 address, first install the vTPS virtual appliance with IPv4 by using the OBE interface on the console. Configure an IPv6 address after you boot the device.

- DNS Domain Name (optional)
- Security Level
- Username—The SuperUser user name
- Password for the SuperUser
- Console—Default and recommended value is `vga`; if you specify `serial` as the console, *Learn more on page 5-3* about how to configure it

Note

The vTPS virtual appliance supports only one console type. After you initially select the console type, you would have to redeploy the vTPS virtual appliance to change the console type.

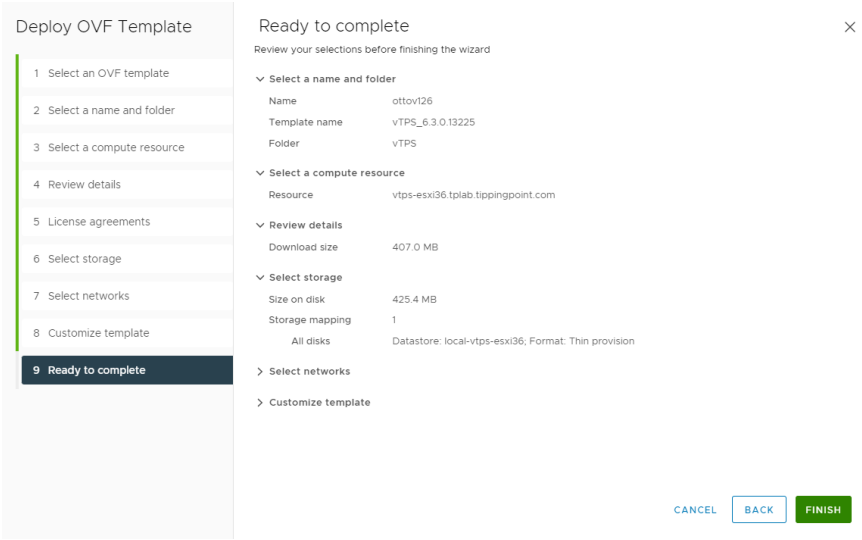
- SSH Public Key for the superuser account (this field is optional)
- Certificate URL (optional)—Your vTPS virtual appliance attempts to get the file from the URL and install the device certificate to convert from Trial Mode to Standard Mode; you can complete this task another time, if needed, by using the SMS client.

When you have entered values for all the properties, click **Next**.

Note

Any properties that you do not assign a value to remain unassigned.

11. Verify that all the properties have been correctly set for your deployment in the Ready to Complete screen.



12. Click **Finish**.

    The initial boot displays your deployment progress and any messages with the VGA console, even if you previously selected `serial` as the console. The interface prompts you to provide values for any deployment questions you previously skipped.

After the OBE boot completes:

- If you provided a certificate URL during the deployment, the vTPS virtual appliance automatically downloads the certificate and reboots to activate it.
- If you selected to use the serial console, the vTPS virtual appliance automatically reboots. The serial console displays all messages from this next boot.

  Note

  The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

- If neither of the preceding bullets apply, a login prompt is displayed. You can now access the device using the console, SSH or SMS client.

Start your vTPS virtual appliance

Follow these steps to complete the initial deployment:

Procedure

1. In vCenter, right-click your new VM and select **Power > Power on** from the menu.
2. If you did not use vCenter to provide network settings, you can access the vCenter VGA console for the vTPS virtual appliance to configure those settings.

What to do next

If you did not use vCenter to provide license key information in the preceding step, the vTPS virtual appliance boots in Trial Mode by default. The following display from the CLI indicates that you are in Trial Mode.

```
docvtps{}show version
              Serial: D-VTPS-TRIAL-0001
            Software: 6.2.0.4803i Build Date: “dep 13 2023 16:09:27”
                                  Production [9ac20f021]
     Digital Vaccine: 4.0.0.1000
       Reputation DV: N/A
               Model: vTPS Standard Trial
           HW Serial: TMTPVT1ABC
         HW Revision: VSA
            Failsafe: 1.3.0.4801
          Throughput: 100 Mbps
    System Boot Time: Fri Sep 15 20:56:55 2023
              Uptime: 00:02:06
```

Upgrade to Standard Mode

If you did not provide a certificate URL during deployment, upgrade to Standard Mode. *Learn More on page 4-1* about upgrading to Standard Mode.

If you did provide a certificate URL during deployment, activation of the certificate occurs automatically.

Install and deploy a vTPS virtual appliance by using KVM

Use the information in these topics to configure the vTPS virtual appliance for startup by using a kernel-based virtual machine (KVM):

- *KVM requirements on page 3-13*
- *Obtain software licensing and certificates on page 3-15*

- *Deploy a vTPS virtual appliance on KVM on page 3-15*
- *Automating vTPS installation on KVM on page 3-18*
- *Upgrade to Standard Mode on page 3-12*

KVM requirements

A KVM deployment of the vTPS virtual appliance that uses the following specifications has been verified:

- **Software environments** – Ensure you have the following minimum requirements:

  Note

  vTPS installation has been verified with RHEL version 8.0 or 9.0 KVM hosts. A six-core configuration requires the following minimum software package versions:

  - libvirt version 1.1.0
  - Quick Emulator (QEMU) version 8.0.3
  - virt-install version 1.1.0

- **Networking environments** – Ensure you have three bridge interfaces: one for management and two for data. Each data bridge should be associated with a KVM network.

```
# nmcli connection add type bridge con-name mgmt ifname mgmt
# nmcli connection add type bridge con-name data-A ifname
       data-A bridge.ageing-time 0 bridge.stp no ipv4.method
       disabled ipv6.method disabled mtu 9000
# nmcli connection add type bridge con-name data-B ifname
       data-B bridge.ageing-time 0 bridge.stp no ipv4.method
       disabled ipv6.method disabled mtu 9000
```

Note

Disabling address learning using `bridge.ageing-time 0` ensures that bridges properly forward all Layer 2 frames to the vTPS. Otherwise, especially in cases where a single data port sees both sides of the network connection (such as in IDS mode), the bridge is prevented from sending the frames to the vTPS appliance by the default address learning mode.

Create KVM networks around the data bridges by defining their properties in XML files, and then importing that XML file into libvirt:

```
# cat data-A.xml
<network>
  <name>data-A</name>
  <forward mode="bridge"/>
  <bridge name="data-A"/>
</network>
# cat data-B.xml
<network>
  <name>data-B</name>
  <forward mode="bridge"/>
  <bridge name="data-B"/>
</network>
# virsh net-define data-A.xml
# virsh net-define data-B.xml
```

- **Console access** – Default and recommended console is a graphical UI, such as virt-manager, virt-viewer, vncviewer, or other VNC client. *Learn more on page 5-3* about configuring the serial console.

Note

The vTPS virtual appliance supports only one console type. After you initially select the console type, you cannot change it later.

Obtain software licensing and certificates

For information, see *Upgrade from vTPS Trial to vTPS Standard on page 4-1*.

Deploy a vTPS virtual appliance on KVM

To install a vTPS on KVM:

Procedure

1. Copy the vTPS tar package to your system.
2. Extract the package with the `tar --sparse -zxvf vTPS_performance_kvm_x.x.x_xxxxx.tar.gz` command.
3. Use the `chmod` command to change permissions so that the QEMU user can access the file:

   ```
   chmod a+rwx system_disk.raw
   ```

4. Use the `virt-install` command to deploy the vTPS package according to your RHEL version.

   To deploy a vTPS virtual appliance in the libvirt 1.1.0 environment, use the `virt-install` command as follows.

   ```
   virt-install \
   --name=<name of your VM> --ram=16384 \
   --vcpus sockets=1,cores=6 \
   --boot hd --disk path=<path of your system_disk.raw file> \
   --network bridge=mgmt,model=e1000 \
   --network network=data-A,model=virtio,driver_queues=6 \
   --network network=data-B,model=virtio,driver_queues=6 \
   --graphics vnc,port=59<xy>,listen=<ip_of_kvm_host> \
   --virt-type=kvm --cpu Haswell,+ssse3,+sse4.1,+sse4.2,
     -svm,+aes,+pclmuldq,-hle,-rtm,optional=rdrand \
   --force --wait -1
   ```

   Important:

In order for the VM to incorporate the CPU features, additional configuration might be necessary. *Learn more on page 3-2* about configuring CPU features.

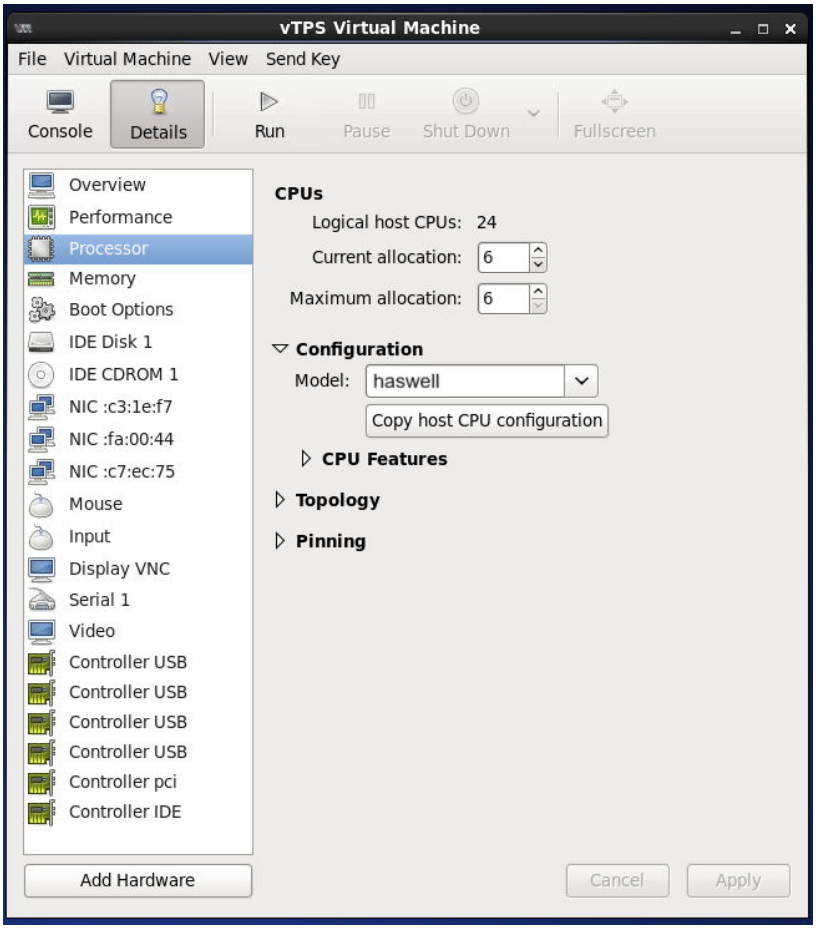
After running the preceding `virt-install` command, shut down the VM. Use `virt-manager` to adjust the CPU parameter to `host`, `Haswell`, or newer:

a. Select **Processor** from the list of hardware.

b. Toggle the **Configuration** triangle and select the appropriate processor model.

c. Either pick a CPU type manually from the list or click **Copy Host CPU Configuration** for the best CPU to match with this host.

d. Click **Apply**.



You can also accomplish this task by using `virsh edit VM-NAME` to edit the VM XML file. Learn more about this option.

Note

The `--wait` option keeps your program running on the shell. After you have installed the vTPS Software License Key and the vTPS virtual appliance is running, you can type Control-C to return to the prompt.

The preceding commands create a vTPS VM with the name <*name of your VM*>. To manage or access the VM, use the `virsh` CLI.

To access the open console of the VM, use `vncviwer` or `virt-viewer` after setting the DISPLAY environment variable as follows:

`vncviewer <ip_of_kvm_host>:59<xy>` (the <*port value*> you supplied for the `graphics` field of the `virt-install` command)

or

```
virt-viewer --connect qemu+ssh://root@ip_of_kvm_host/system
$VM_NAME
```

This completes the vTPS deployment.

Automating vTPS installation on KVM

Procedure

1. Use the `yum install genisoimage` command to install `genisoimage` on an RHEL system.
2. Copy the vTPS tar package to your system.
3. Use the `tar --sparse -zxvf vTPS_kvm_x.x.x_xxxxx.tar.gz` command to extract the package.
4. To configure the vTPS parameters from the KVM command line, create a text file named `vtps-env.txt` **(Note: the file *must* be named this)** with this format:

```
com_tippingpoint_IP = <Management IP address of vTPS>
com_tippingpoint_Netmask = <Subnet Mask>
com_tippingpoint_Gateway = <IP Address of Gateway>
com_tippingpoint_Username = <username>
com_tippingpoint_Password = <Password>
com_tippingpoint_DNS = <IP Address of DNS>
com_tippingpoint_DNS2 = <IP Address of DNS2> (optional)
com_tippingpoint_Security_Level = <none/low/medium/high>
```

```
com_tippingpoint_VSSH_Public_Key = SSH KEY (optional)
com_tippingpoint_Cert_URL = <Device Certificate URL> (optional)
com_tippingpoint_Console = serial  (optional; for serial consoles
       only)
```

For example, your file might look like the following sample:

```
com_tippingpoint_IP = 10.11.12.134
com_tippingpoint_Netmask = 255.255.255.0
com_tippingpoint_Gateway = 10.11.12.1
com_tippingpoint_Username = superuser
com_tippingpoint_Password = password
com_tippingpoint_DNS = 15.16.17.18
com_tippingpoint_DNS2 = 0.0.0.0
com_tippingpoint_Security_Level = None
com_tippingpoint_VSSH_Public_Key = SSH KEY
com_tippingpoint_Cert_URL = http://15.16.17.18/certificate.txt
```

5. From the KVM command line, generate an ISO image of the `vtps-env.txt` file with the `genisoimage -r -o vtps_test_metadata.iso vtps-env.txt` command.

   This command generates the following output:

```
root@vtps-kvm06:/# genisoimage -r -o vtps_test_metadata.iso
       vtps-env.txt
I: -input-charset not specified, using utf-8 (detected in
       locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
root@vtps-kvm06:/#
```

Note

The exact output varies depending on the input to the `vtps-env.txt` file.

6. Use the `chmod` command to change permissions so that the QEMU user can access the file:

```
chmod a+rwx system_disk.raw
chmod a+rwx vtps_test_metadata.iso
```

7. Set the following environment variables to the displayed values:

   - `VM_NAME=$VM_NAME`
   - `RAM_SIZE=16384 #8388608 #8GB : 1GB = 1048576`
   - `SYSTEM_DISK_PATH=<location of the image files>/system_disk.raw`
   - `CDROM_IMAGE=<location of the iso file>/vtps_test_metadata.iso`

8. Use the `virt-install` command to deploy the vTPS package according to your RHEL version.

   Attach the generated ISO image (as if it were a CD-ROM) and the bootloader, and deploy the vTPS package in the libvirt 1.1.0 environment with the `virt-install` command.

```
virt-install \
--name=$VM_NAME --ram=16384 --vcpus sockets=1,cores=6 \
--boot hd --disk path=$SYSTEM_DISK_PATH
--cdrom=$CDROM_IMAGE \
--network bridge=<management bridge>,model=e1000 \
--network network=<ingress network name>,model=virtio,
       driver_queues=6 \
--network network=<ingress network name>,model=virtio,
       driver_queues=6 \
--graphics vnc,port=59<xy>,listen=<ip_of_kvm_host> \
--virt-type=kvm --cpu Haswell,+ssse3,+sse4.1,+sse4.2,
```

```
       -svm,+aes,+pclmuldq,-hle,-rtm,optional=rdrand \
--force --wait -1
```

Note

The `--wait` option keeps your program running on the shell. After you have installed the vTPS Software License Key and the vTPS virtual appliance is running, you can type Control-C to return to the prompt.

The preceding commands create a vTPS VM with the name <*name of your VM*>. To manage or access the VM, use the `virsh` CLI.

To access the open console of the VM, use `vncviwer` or `virt-viewer` after setting the DISPLAY environment variable as follows:

`vncviewer <ip_of_kvm_host>:59<xy>` (the <*port value*> you supplied for the `graphics` field of the `virt-install` command)

or

```
virt-viewer --connect qemu+ssh://root@ip_of_kvm_host/system
$VM_NAME
```

This completes the automated KVM vTPS deployment.

Upgrade to Standard Mode

If you did not provide a certificate URL during deployment, upgrade to Standard Mode. *Learn More on page 4-1* about upgrading to Standard Mode.

If you did provide a certificate URL during deployment, activation of the certificate occurs automatically.

Chapter 4

Upgrade from vTPS Trial to vTPS Standard

To upgrade your vTPS virtual appliance from Trial Mode to vTPS Standard Mode, install the license entitlement package and the license certificate package. You can purchase a license through your regular sales channel.

The vTPS virtual appliance remains in Trial Mode until you install a valid certificate. The Trial Mode vTPS comes with limited feature capabilities. After you install a certificate, the vTPS virtual appliance deploys in Standard Mode, and the capabilities purchased with the license package are activated.

When the vTPS virtual appliance upgrades to Standard Mode, you can install your Digital Vaccine package.

Learn more about how to install the license entitlement package, create, download, and install the license certificate package, and install your Digital Vaccine package:

Install your license entitlement package

Note

If your vTPS virtual appliance is managed by an SMS, you can configure the SMS to automatically retrieve and distribute the most current license entitlement package. Learn more from the *SMS User Guide*.

You can retrieve your license entitlement package from the TMC (**My Account > TippingPoint License Package**).

For information on installing your license entitlement package, refer to your LSM and SMS documentation.

Create and download vTPS virtual appliance license certificates

Use the following information to create a vTPS license certificate using the license manager. The license certificate package assigns a purchased inspection throughput license to a vTPS virtual appliance. After you create a vTPS license certificate, install the certificate on the vTPS virtual appliance.

To create a vTPS device license certificate

Procedure

1. Open the license manager.

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

2. From the License Management page of the license manager, click **Create vTPS Licenses**.

3. (Optional) If you want to add SSL inspection to a vTPS device, but SSL is disabled, apply for SSL compliance.

   There are four states of SSL compliancy; Unknown, Pending, Compliant, and Non-Compliant. Before you enable SSL, the SSL compliancy state is set at Unknown.

Complete the following steps to apply for SSL compliance:

a. Next to **Your SSL is disabled**, click **Apply Now**.

b. Fill out the Apply for SSL Compliance page.

c. Click **Apply**.

After you click **Apply**, the SSL compliance state changes to Pending. When the application process is completed, the state changes to either Compliant if SSL is approved or Non-Compliant if SSL is not approved.

If you are SSL Compliant, SSL inspection is enabled on all of your vTPS virtual appliances.

4. Under **Action**, select the number of vTPS certificates that you want to create.
5. Click **Create**.

After the vTPS certificate is created, use the SMS client to install the certificate to a vTPS virtual appliance.

Important

If you do not use an SMS or if your SMS is not connected to the TMC, you must manually download and install the vTPS certificate package. After you download the vTPS certificate package, you can manually install the package from the SMS client.

To download the vTPS certificate package

Procedure

1. In the license manager, click **Download Cert**.
2. Select **vTPS Cert** from the drop down options.

   The vTPS Certificate Package page is displayed on the TMC.

3. Click **Download**.
4. Accept the EULA Agreement.
5. Save the vTPS certificate file to a local folder.

Install the vTPS license certificate using the SMS client

To install a license entitlement package for a managed vTPS appliance using the SMS client, consult the "To manually import a device license entitlement package" topic in the *SMS User Guide*.

Install a Digital Vaccine package

Note

If you use an SMS to manage your vTPS virtual appliance, you can configure the SMS to automatically retrieve and distribute the most current Digital Vaccine package each week. Learn more about how to configure this from the *SMS User Guide*.

While in Trial Mode, your vTPS virtual appliance has a base Digital Vaccine installed with a limited number of security filters that cannot be changed. After you upgrade your device to Standard Mode, you can then install a full Digital Vaccine package.

Learn more about installing your Digital Vaccine package from your SMS documentation.

Chapter 5

Troubleshooting tips

Before contacting support, check to see if the following troubleshooting tips address your issues.

Configuring a distributed switch environment in promiscuous mode

Resolution: You must configure a vTPS virtual appliance in promiscuous (port-mirroring) mode for Layer 2 routing. If a vTPS virtual appliance is connected to a distributed switch, ensure that any Forged Transmits and MAC Address Changes are set to ACCEPT so that network packets can be forwarded to each host in the port group.

Resolution: Although the vTPS virtual appliance does not support VMware vMotion, you can emulate a vMotion configuration by connecting two or more different hosts with two or more vTPS virtual appliances that are actively connected to the distributed vSwitch. The vTPS virtual appliance that is connected to the active VM acts as an IPS, and the vTPS virtual appliance that is not connected to the VM acts as an IDS. If you connect your SMS to both vTPS instances, the SMS will also receive any blocks and alerts.

KVM deployment does not boot

Resolution: Ensure that you have all of the Ethernet ports configured. If you install your VM without the correct number of inspection ports, you must either delete the VM and reinstall it or perform a `debug factory-reset`. If you delete and reinstall the VM, you must be sure to also delete the

`system_disk.raw` file. You can then re-extract the file from the KVM `tar.gz` image file.

CPU usage always displays as 100% in hypervisor

Resolution: To see the actual CPU usage, enter the `show health cpu` command for the device.

Resolution: To manage the CPU usage, create a resource pool in the vSphere Web Client. Learn more about resource pools.

Errors after Suspend and Resume operation

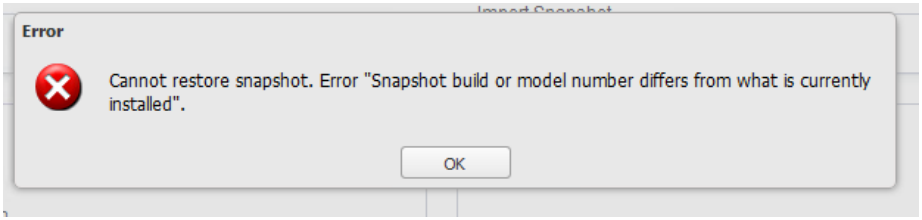
Resolution: Ignore HEALTH-ALERT errors generated after a Suspend and Resume operation.

Resetting OBE parameters after a factory reset

Resolution: A factory reset does not reset the initial deployment parameter values—including IP address, username, and password. To change these values, you must redeploy the vTPS virtual appliance.

Snapshot cannot be restored

Resolution: Only vTPS to vTPS snapshots are supported. Restoring snapshots from other TippingPoint devices is not supported. Attempts will fail with the following error.



Time synchronization issues in KVM environment

Resolution: If, after an extended Suspend and Resume operation, the device time does not sync with the server time, shut down and restart the system.

vTPS virtual appliance experiencing data port performance problems

Example: `ID HEALTHCHECKD Device is still experiencing performance problems (loss=<xx>%, threshold=<x>%). 0 alerts not logged.`

Resolution: Make sure that you properly configure three standard vSwitches or distributed vSwitches on the ESXi or vCenter with multiple port groups for data and vTPS management traffic.

Resolution: Avoid large iptable entries. Larger iptable entries can reduce vTPS virtual appliance performance as much as 20 percent in a KVM deployment.

Resolution: Make sure you enable port groups in promiscuous mode for Layer 2 routing. Ensure that you set any Forged Transmits and MAC Address Changes to ACCEPT so that network packets can get forwarded.

Resolution: Confirm that you have configured each vTPS device with its own data port group. Using the same vSwitches across multiple vTPS virtual appliances can cause performance issues.

Configuring a serial console

ESXi Resolution: If you specified a serial console for your VM, add a serial port by editing the properties of the VM:

1. Right-click your new VM and click **Add**.
2. Select **Serial port** and click then **Next**.
3. Select **Connect via Network** and click then **Next**.
4. Select **Server** and provide a port for the Port URI (for example, `telnet://:1239`).
5. Click **Next**, and then click **Finish**.
6. Reboot the vTPS virtual appliance. Before the console completes the change from VGA to Serial, the appliance reboots a second time automatically.

Note

The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

7. Enter the following command from a Linux shell to access the serial console:

```
telnet <esxi host> <port number>
```

For example:

```
telnet esxi01 1239
```

KVM Resolution: Follow the procedure in *Automating vTPS installation on KVM on page 3-18*. Specify the `com_tippingpoint_Console = serial` option in the `vtps-env.txt` file.

After you specify the serial console, enter the following to access the console from the KVM host:

```
virsh console <VM_NAME>
```

KVM also supports several alternative serial console modes, including TCP, UDP, and UNIX. For these options, use `virt-manager` to delete the existing serial device and add a different type. Learn more from the virtualization administrative guides for KVM or RedHat.

TREND MICRO

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: TPEM69847/230927