PROTECTED THEATER INSTALL - ADD AND CONFIGURE THE PT VIRTUAL ENVIRONMENT

The initial setup of the Protected Theater can be completed in VMware or Hyper-V. Before adding and configuring the environment, verify the hardware you selected meets **Protected Theater Minimum System Requirements (https://docs.mandiant.com/home/msv-protected-theater--system-requirements)** and you have addressed everything listed in **Before you Begin (https://docs.mandiant.com/home/msv-pt-before-you-begin)**. Then complete the following three steps:

1. **Create the Virtual Environment - VMware**
   or
   Create the Virtual Environment - Hyper-V
2. **Verify Virtualization (https://docs.mandiant.com/home/verify-virtualization)**
3. **Set up Networking**

Create the PT Virtual Environment in VMware

Only complete this step if you are working in VMware.

1. Download the Protected Theater OVA image from the Validation Platform customer portal.
2. Deploy the Protected Theater OVA image into the virtual infrastructure.
   If you need assistance with this, see the **VMware documentation (https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-17BEDA21-43F6-41F4-8FB2-E01D275FE9B4.html)** for your product version.
3. Update the Virtual Hardware settings so they match the Protected Theater Requirements.

   System Requirements are equal to the Protected Theater Requirements **PLUS** the disk image requirements.

   a. Configure the CPU, memory, and hard disk requirements by following the guidance in the **Protected Theater Minimum System Requirements (https://docs.mandiant.com/home/msv-protected-theater--system-requirements)**.
   b. For the Network adapter, select an interface that includes a static IP.
   c. Reserve all guest memory for the host to improve performance.
      i. Expand the **Memory** section.
      ii. Select the **Reserve all guest memory** checkbox.
      If this is not possible, there is a less invasive adjustment that can be made. Information on that adjustment is available at **https://kb.vmware.com/s/article/1002586**.
   d. Enable Nested virtualization / update **Hardware virtualization** settings.

- The Director validates nested virtualization is enabled when the Protected Theater initializes and reviews the image details. You cannot boot the image if this is not enabled.
  More information is available from VMware at **https://communities.vmware.com/t5/Nested-Virtualization-Documents/Running-Nested-VMs/ta-p/2781466**. This can only be done through the web client for ESXi.
- Updating this will increase the efficiency of the Protected Theater as it reduces the amount of virtualization needed within ESXi by giving the Protected Theater more direct access to the hardware.

i. Expand the **CPU** section.
ii. Select the **Expose hardware assisted virtualization to the guest OS** checkbox.

e. Click **OK** to save your changes.

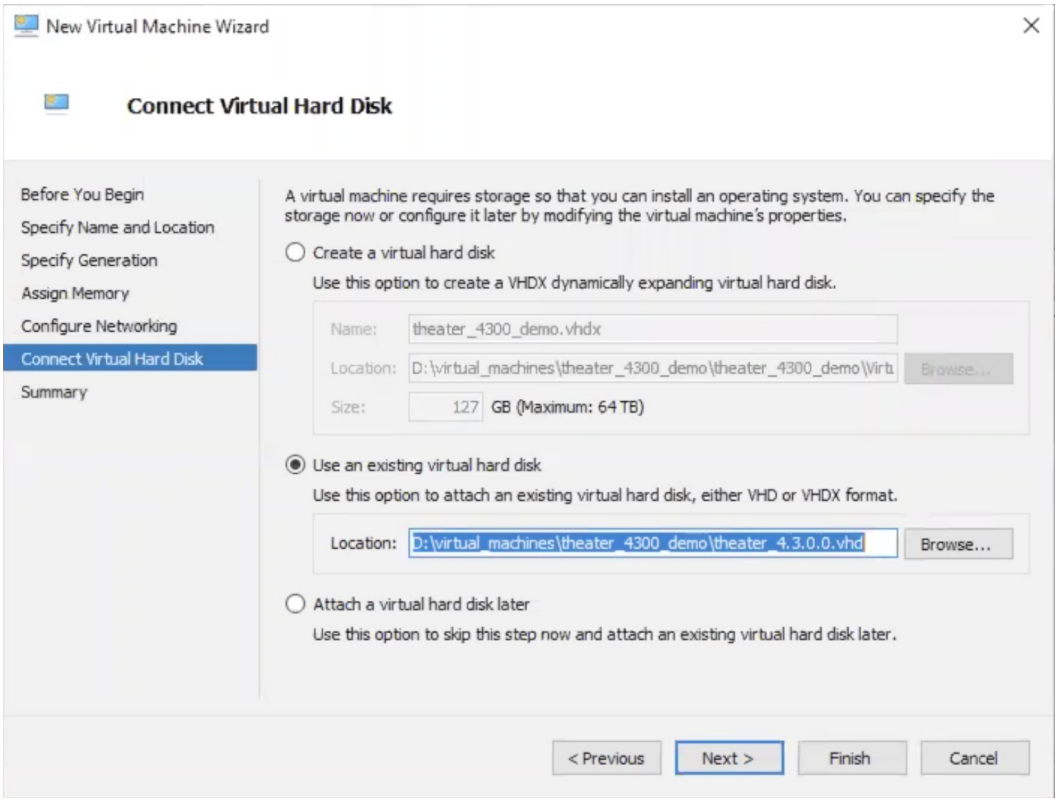
Create the PT Virtual Environment in Hyper-V

Only complete this step if you are working in Hyper-V.

1. Download the Protected Theater VHD image from **Actor and Protected Theater Downloads (https://docs.mandiant.com/home/msv-actor-installers)**.
2. Extract the VHD and then copy it to your desired location. If you have a standard virtual machines folder, we suggest you use that.
3. Create the Virtual Machine in Hyper-V.
   a. Click **New** > **Virtual Machine**.
   b. Click **Next**.
   c. Enter a **Name** for your Actor virtual machine and (optional) select the **Location** where the virtual machine should be stored. Then click **Next**.
   d. Specify **Generation**. Generation 1 is recommended. Then click **Next**.
   e. Assign Memory. **12288 mb** may be adequate, depending on your baseline OS requirements. For additional details, see **Protected Theater Minimum System Requirements (https://docs.mandiant.com/home/msv-protected-theater--system-requirements)**. Then click **Next**.

      Do NOT select Use Dynamic Memory for this virtual machine.

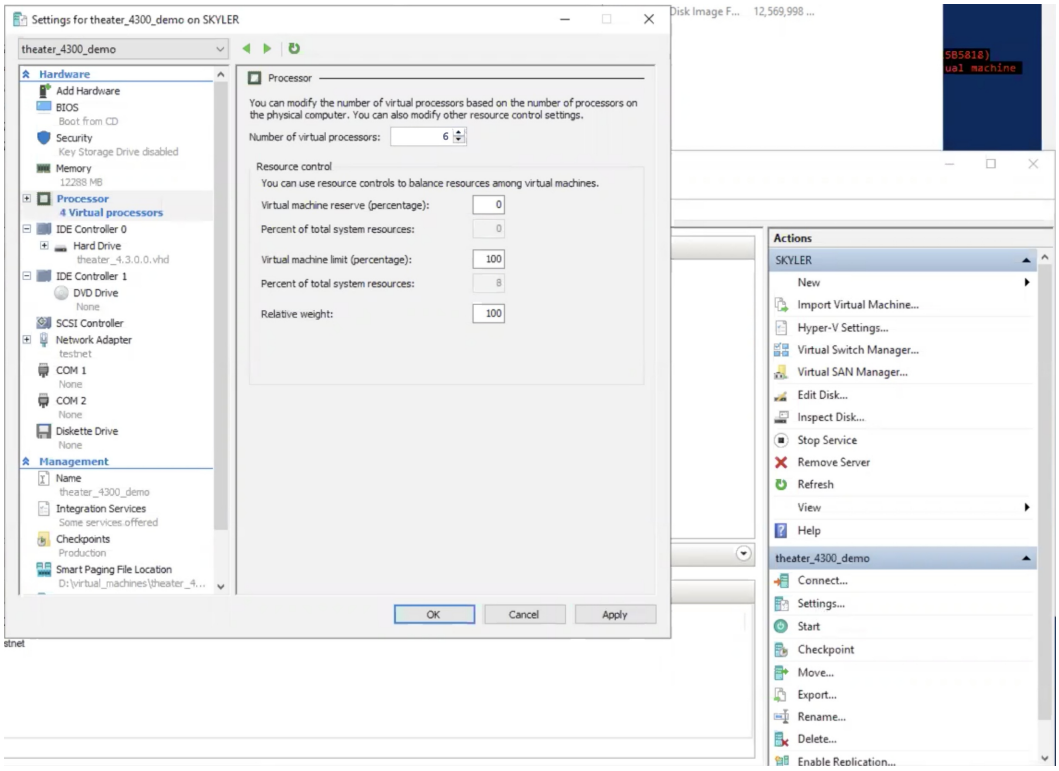
   f. Select your network **Connection**. Then click **Next**.
   g. Choose **Use an existing virtual hard disk**, navigate to the disk's location, and then click **Next**.



Hyper-V example: Connecting a Virtual Hard Disk to a new Virtual Machine

h. Verify everything is configured as expected and then click **Finish**. The virtual machine will display and be selected in the Virtual Machines list.

4. Update the Virtual Machine's Processor info.
   a. Select your Protected Theater Virtual Machine and click **Settings**.
   b. Click **Processor**, adjust the Number of virtual processors to **more than 4**, click **Apply**, and click **OK**.



Hyper-V: Adding processors to a virtual machine

5. Expose the Virtualization Extensions for your VM.
    a. Open a Windows PowerShell Admin window
    b. Run the following command:

    ```
    Set-VMProcessor <VMName> -ExposeVirtualizationExtensions $true
    ```

6. Start the Virtual Machine by selecting the VM in Hyper-V Manager and clicking **Connect**.

Set up networking

After you confirm that virtualization is enabled, you can set up the Protected Theater networking. Choose an option, depending on whether you want to control your OS network settings or have Mandiant control them:

- **Control your OS network settings**: In the `vsetnet` tool, you only select the management interface to use. You are responsible for manually configuring the host's networking settings outside of `vsetnet`.
- **Let Mandiant control your OS network settings**: You select the interface, and then `vsetnet` prompts you for the network settings to use. This is done so the Actor software can make the required changes to the OS networking.

Follow these steps, regardless of the option you chose:

1. Connect to the Protected Theater environment using SSH.
2. Set up the network configuration by running the following command:

    ```
    $ sudo vsetnet
    ```

3. Choose your preferred option:

- We recommend using `ens192` for the (management) interface.
- Remember to use a static IP address.
- Only one IP address is necessary for Protected Theaters.

- **Customer-controlled OS network settings:**
  1. Enter `no` when prompted for Verodin (Mandiant) control of network files, then press Enter.
  2. Select the primary interface (`ens192`) and press Enter.
  3. Enter `no` when prompted for the test data interface and then press Enter. After these steps, Verodin services restart and your network configuration is updated.

The following code output is provided for an example. Also, the network values are for example purposes only and should not be used for your specific network configuration.

```
$ sudo vsetnet

 - Verodin Network Configuration -

Will Verodin control the network configuration files? (yes|no): no


Selecting the primary management interface.
Available Interfaces:
ens192 - IP: MGMT_IP_ADDRESS - MAC: MAC_ADDRESS
Which interface do you want to use for management: ens192

Configure Second Interface for Test Data (yes|no): no

Restarting Verodin services...
```

- **Mandiant-controlled OS network settings**:
  1. Enter `yes` when prompted for Verodin (Mandiant) control of network files, then press Enter.
  2. Select the primary interface (`ens192`) and press Enter.
  3. Enter network values for:
     a. IP Address or DHCP
     b. Network Mask
     c. Gateway
     d. Nameserver IP Address (typically a DNS server)
  4. Enter `no` when prompted for the test data interface and then press Enter. After these steps, Verodin services restart and your network configuration is updated.

The following code output is provided for an example. Also, the network values are for example purposes only and should not be used for your specific network configuration.

```
$ sudo vsetnet

 - Verodin Network Configuration -

Will Verodin control the network configuration files? (yes|no): yes


Selecting the primary management interface.
Available Interfaces:
ens192 - IP: 192.0.2.2 - MAC: 00:00:5E:00:53:00
Which interface do you want to use for management: ens192

Enter IP Address or DHCP: MGMT_IP_ADDRESS

Enter Network Mask: NETWORK_MASK_ADDRESS

Enter Gateway: GATEWAY_ADDRESS

Enter Nameserver IP Address: NAMESERVER_IP_ADDRESS

Configure Second Interface for Test Data (yes|no): no

Restarting Verodin services...
```

4. Once the network settings have been established, confirm the IP settings have been changed by running the following command and noting the `inet` value (in this case, *`MGMT_IP_ADDRESS`*, as used in the preceding examples):

```
$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet MGMT_IP_ADDRESS  netmask NETWORK_MASK_ADDRESS  broadcast GATEWAY_ADDRESS
```