



Operational Technology Defense Console – Virtual Appliance 1.5

Quick Setup Guide (for Windows Hyper-V)

2022-07-18



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:

<http://docs.trendmicro.com/en-us/home.aspx>

Trend Micro, the Trend Micro t-ball logo, and TXOne Networks are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

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.

Table of Contents

Table of Contents.....	3
Chapter 1	4
ODC Onboarding to Windows Hyper-V	4
Prerequisites	4
Deploying OT Defense Console.....	4
Accessing the ODC CLI	12
Getting the IP Address of the ODC Instance	12
[Optional] Configure the IP Address Settings	13
System Migration	14
Opening the Management Console.....	15
Appendix A.....	17
Terms and Acronyms.....	17

ODC Onboarding to Windows Hyper-V

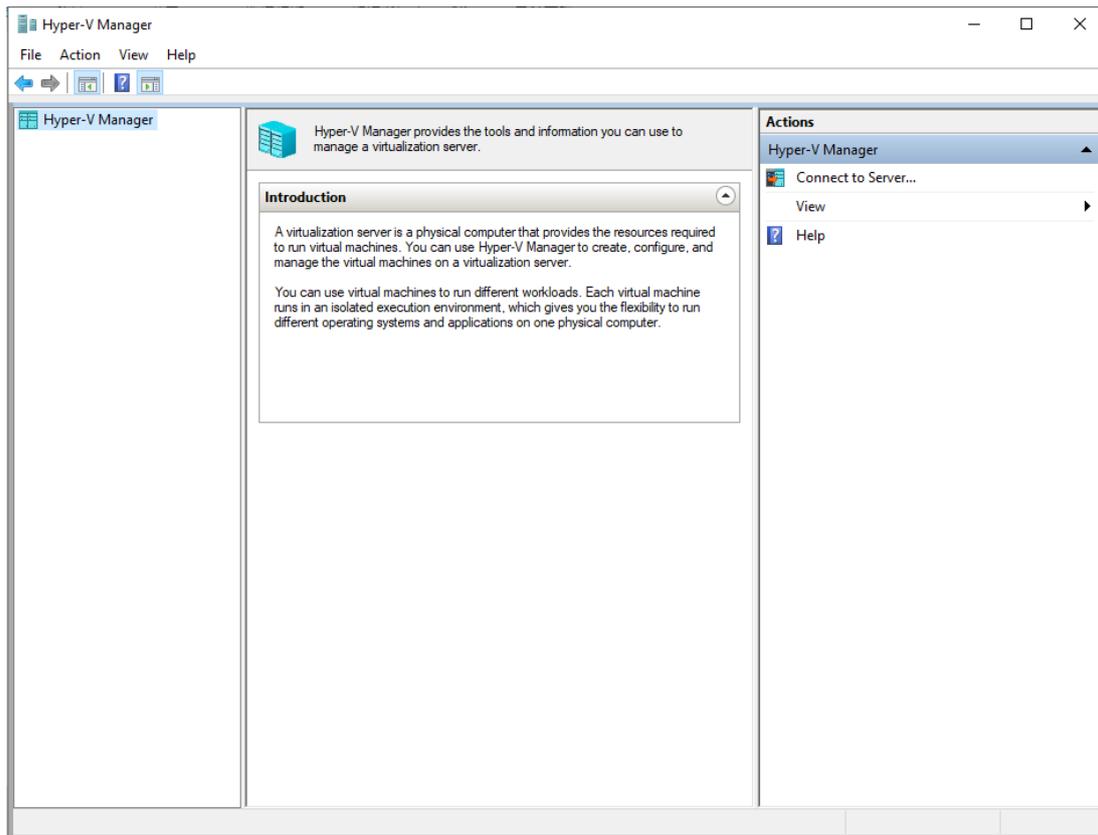
This chapter describes how to deploy OT Defense Console to a Hyper-V system.

Prerequisites

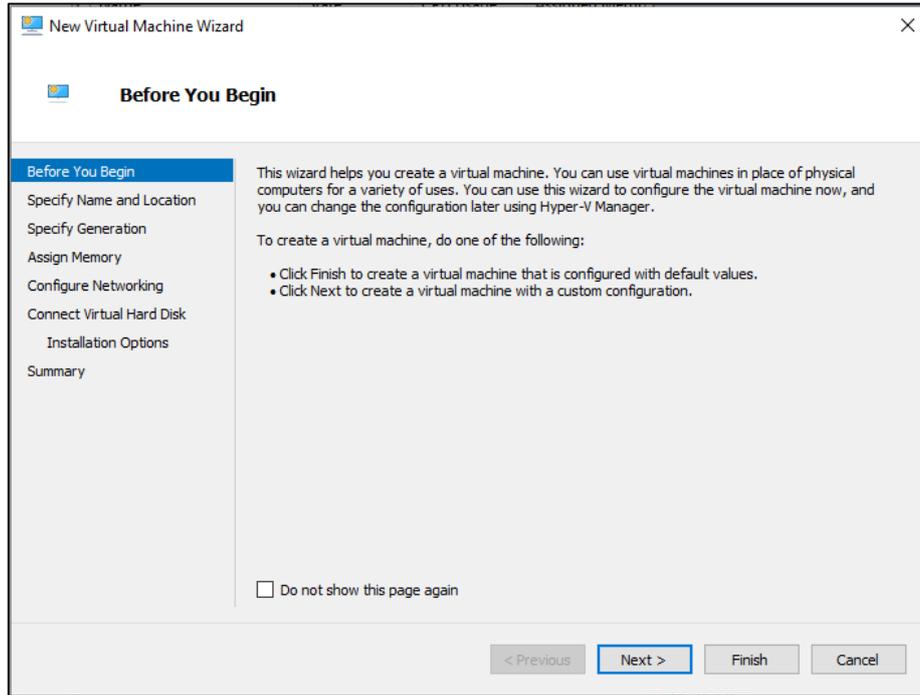
- The vhdx packages provided by Trend Micro must be available and accessible to Windows Hyper-V.
- The necessary networks have been properly created in Windows Hyper-V.
- Extra disk space (50GB or more)

Deploying OT Defense Console

1. Launch Hyper-V manager.



2. Under [Actions], click [New] and then click [Virtual Machine].



New Virtual Machine Wizard

Before You Begin

This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

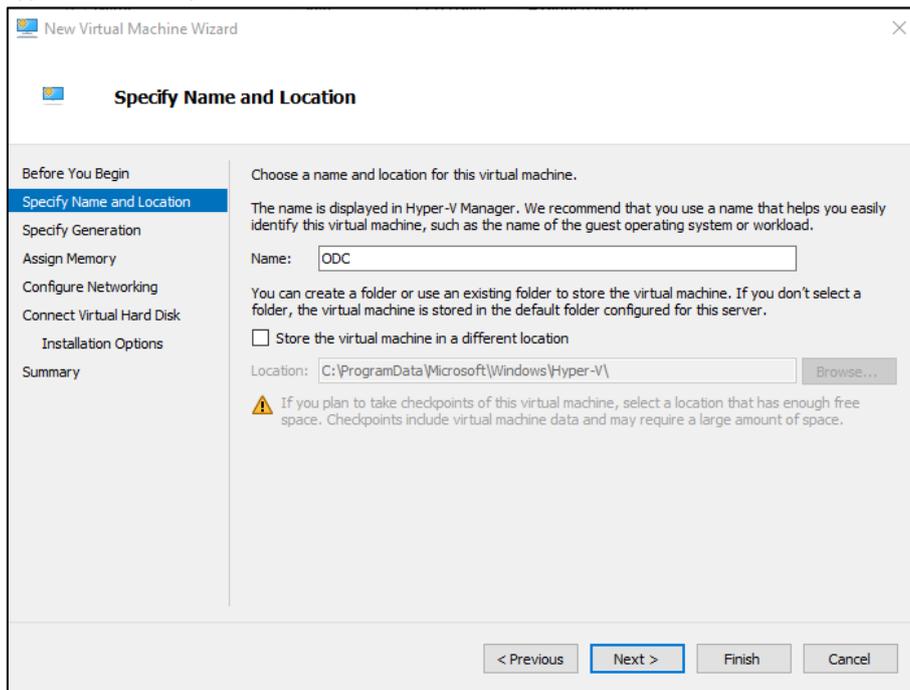
To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

Do not show this page again

< Previous Next > Finish Cancel

3. Type a name for your new VM.



New Virtual Machine Wizard

Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

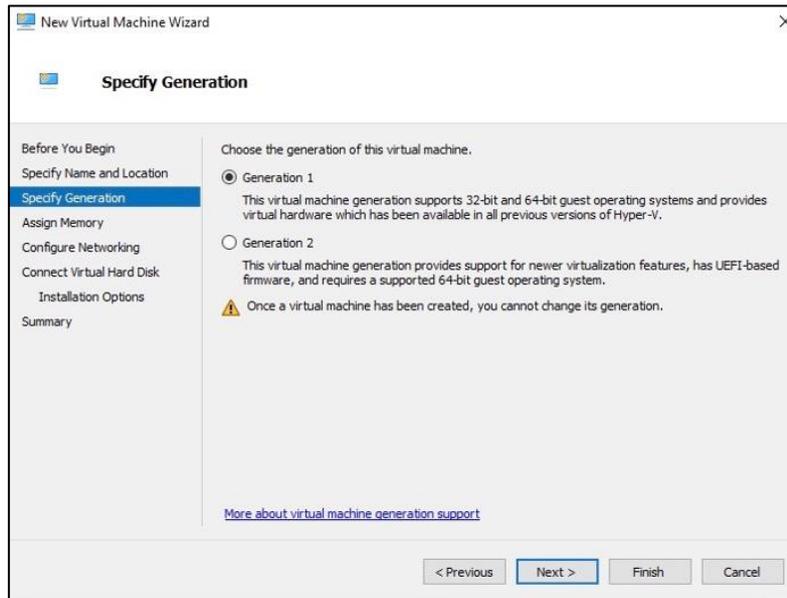
Store the virtual machine in a different location

Location: Browse...

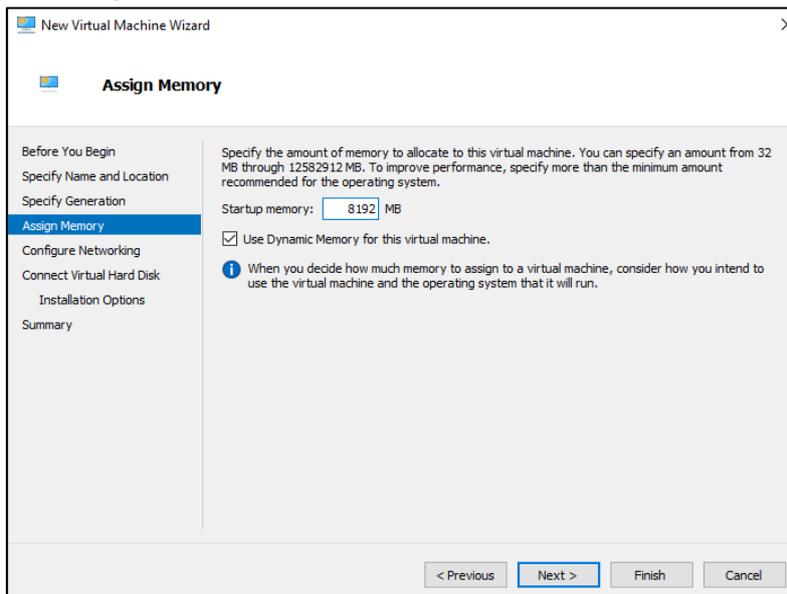
 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

< Previous Next > Finish Cancel

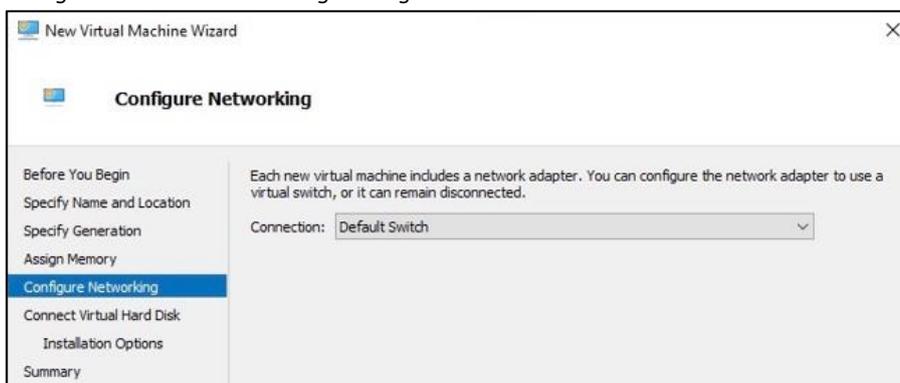
4. Specify the VM's Generation.



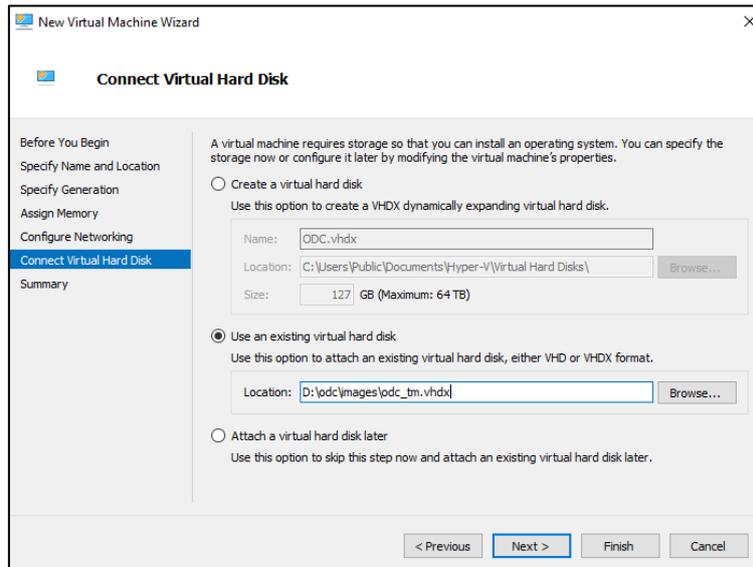
5. Allocate memory for the new VM.



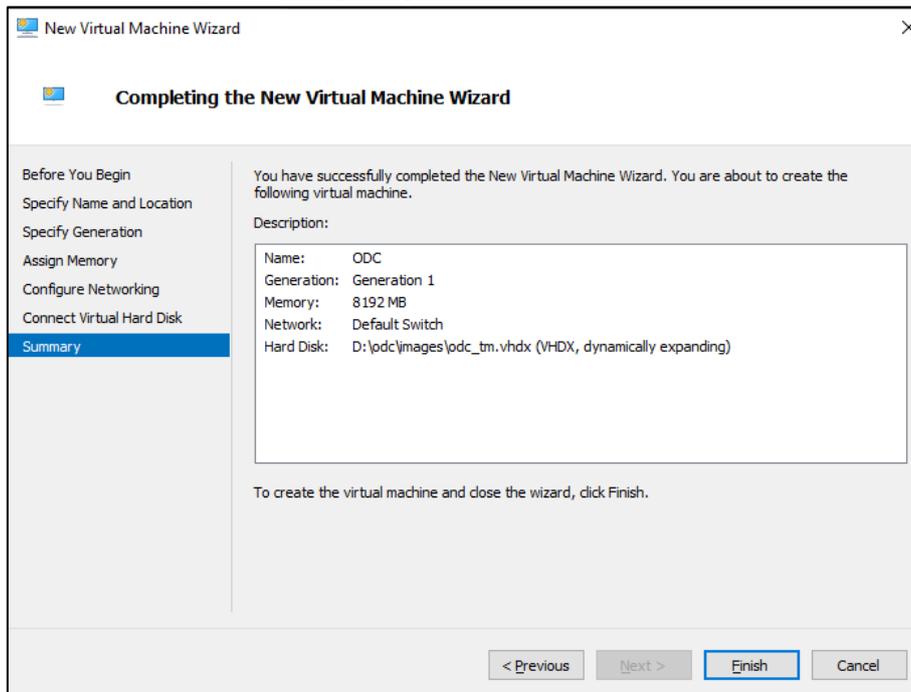
6. Configure the VM's networking settings.



7. Select a virtual hard disk (choose the ODC vdhx package provided by Trend Micro).

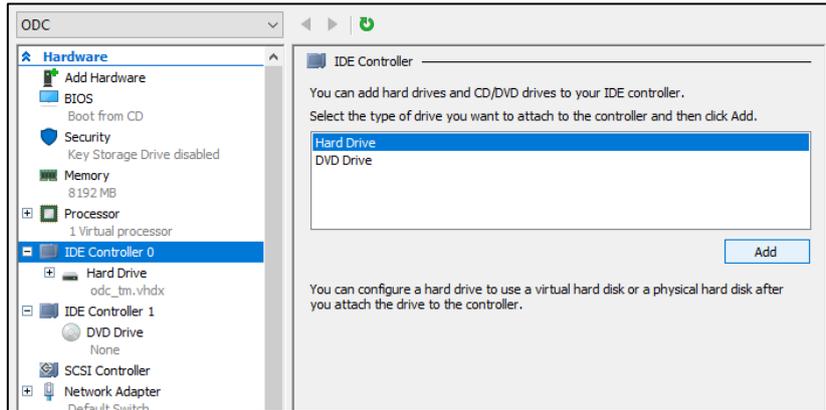


8. Check your settings then click [finish].

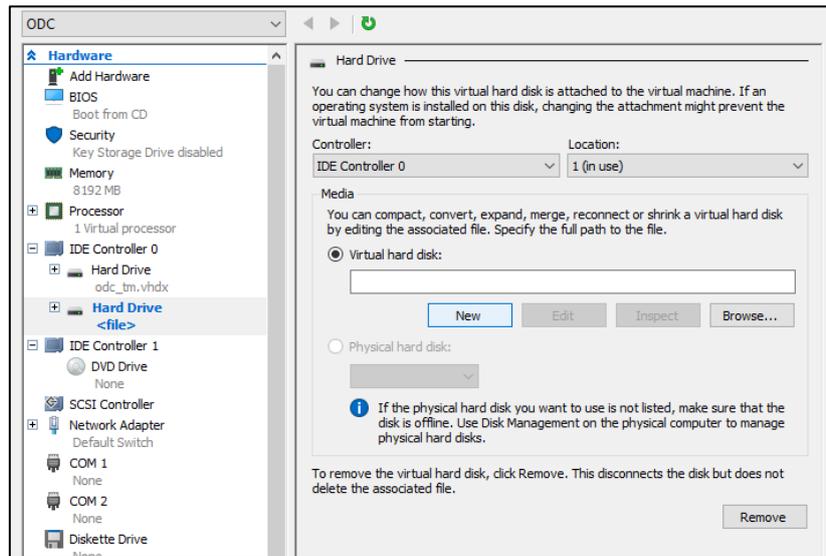


Virtual Machines					
Name	State	CPU Usage	Assigned Memory	Uptime	Status
ODC	Off				

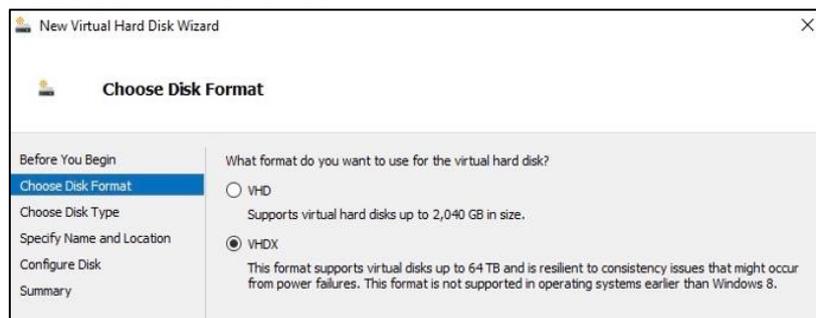
9. Add a new disk.
 - a. Select [Hard Drive], then click [Add].



b. Click [New].



c. Choose the VHDX disk format.



d. Choose the disk type [Dynamically expanding].

Choose Disk Type

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

What type of virtual hard disk do you want to create?

Fixed size

This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

Dynamically expanding

This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.

Differencing

This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

e. Specify name and location.

Specify Name and Location

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

Specify the name and location of the virtual hard disk file.

Name:

Location:

f. Configure disk size (ODC's disk size is based on the sizing table below).

Configure Disk

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

You can create a blank virtual hard disk or copy the contents of an existing physical disk.

Create a new blank virtual hard disk

Size: GB (Maximum: 64 TB)

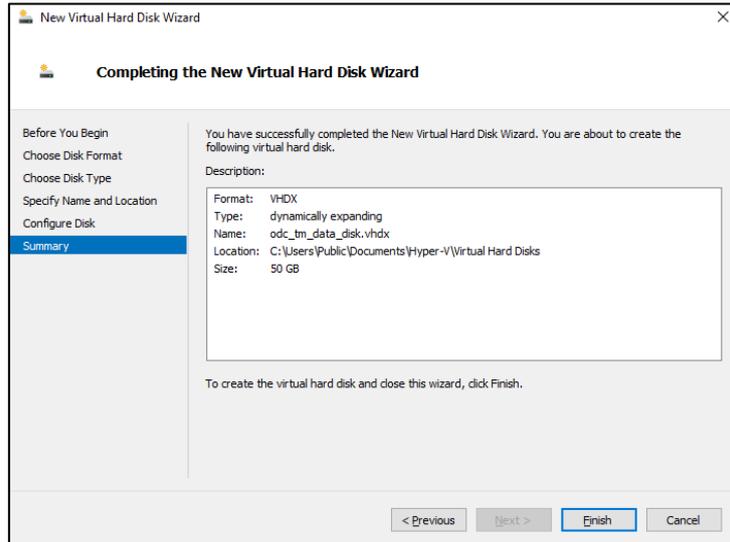
Copy the contents of the specified physical disk:

Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	465 GB
\\.\PHYSICALDRIVE1	119 GB

Copy the contents of the specified virtual hard disk

Path:

g. Click [Finish].



The external disk size can be decided depending on the number of logs to be stored, as shown on the suggestion table below.

Disk space	Maximum event logs	Notes
>= 50 GB	5,000,000 logs	Modified and enlarge size since support more log type
>= 170 GB	10,000,000 logs	Modified and enlarge size since support more log type
>= 330 GB	50,000,000 logs	Modified and enlarge size since support more log type
>= 600 GB	100,000,000 logs	Modified and enlarge size since support more log type

Note: The ODC requires one external disk and the minimum size of the external disk must be more than 50GB; otherwise the ODC will not finish the initialization and will not complete the boot process.

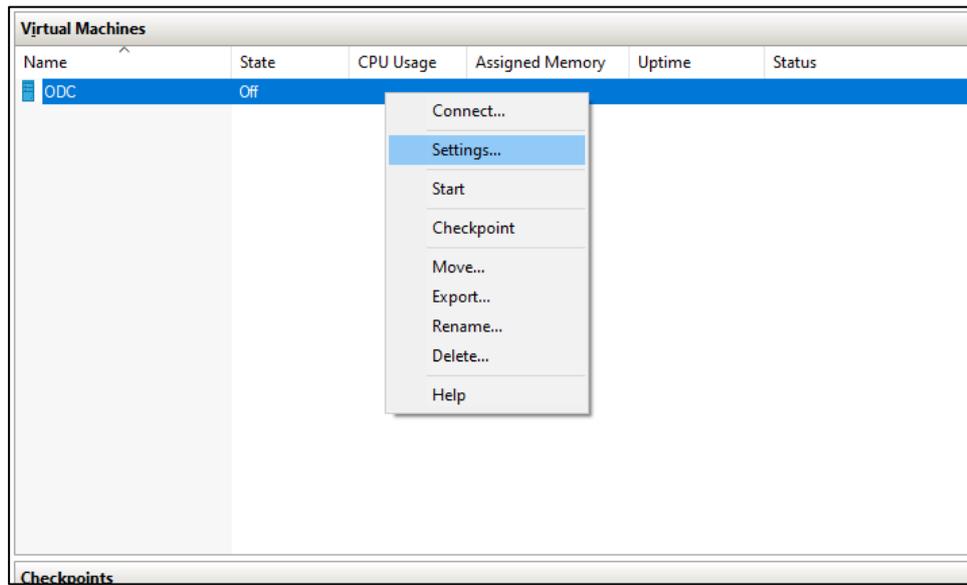
Note: The external disk is used to store the system configurations and event logs. You may attach the external disk of a terminated ODC instance here instead of adding a new disk if you want to migrate the previous configurations and logs to the new ODC instance.

10. **(Optional)** Adjust your ODC instance to use proper resource configurations based on the following sizing table or using default settings (8 CPU cores, 20 GB of memory).

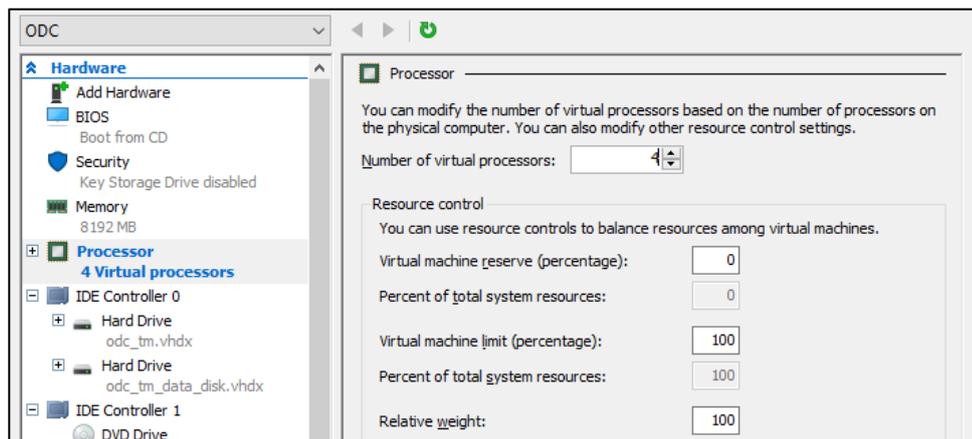
Sizing Table

Nodes	CPU	Memory
50	4 cores	16 GB
100	4 cores	16 GB
150	6 cores	32 GB
200	8 cores	32 GB
300	12 cores	64 GB
500	16 cores	96 GB
1000	32 cores	128 GB

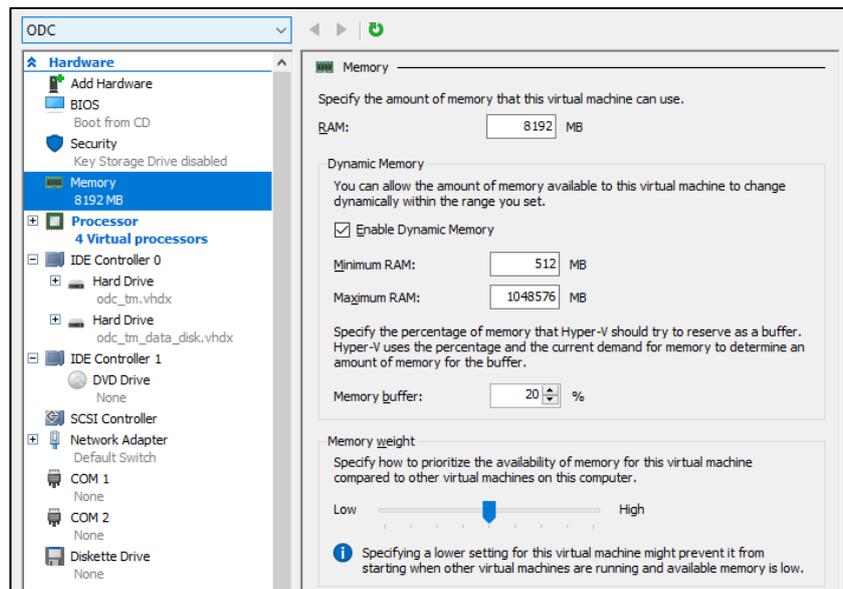
- a. Shut down the instance of ODC and click [Settings].



- b. Configure the number of CPU cores.



- c. Configure the amount of memory.



- d. Boot the ODC instance.

Accessing the ODC CLI

1. Open the ODC VM console.
2. Log in with "root / txone"
3. After logging in to the ODC, you may optionally type the "help" command to see a list of available commands on the instance.

```
vShell, version v1.5.4
The commands provided in:
access-list  Manage the IP whitelists
dx          Curl the target server.
env        Manage system environment variables
exit      Exit this shell
help      List all command usage
iface     Manage the network interfaces
ping     Test the reachability of a host
poweroff  Shut down the machine immediately
pwd      Change the root user password
reboot   Restart the machine immediately
resolv   Manage the domain name server
scp      Send files via scp
service  Manage the device center services
sftp    Send files via sftp
web     Commands of the device center web

Shortcut table:
Tab      Auto-complete or choose the next suggestion on the list
Ctrl + A Go to the head of the line (Home)
Ctrl + E Go to the tail of the line (End)
Ctrl + D Delete the character located at the cursor
Ctrl + L Clear the screen
```

Getting the IP Address of the ODC Instance

1. Type the following command to get the IP address of the ODC Instance
`$ iface ls`

```

[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "static",
    "Address": "10.7.19.157",
    "Netmask": "255.255.255.0",
    "Gateway": "10.7.19.254"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2f:05:2d brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.157/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:52d/64 scope link
        valid_lft forever preferred_lft forever

```

[Optional] Configure the IP Address Settings

You can choose to configure the IP address manually.

1. Use the "iface update" command to update the settings of an existing network interface. For example, the following command sets the interface "eth0" to a static IP address 10.7.19.187/24 with the Gateway IP address 10.7.19.190:

```
$ iface update eth0 --method static --address 10.7.19.157 --netmask
255.255.255.0 --gateway 10.7.19.254
```

2. Confirm the network interface settings are correct and execute the following command to put the new settings into effect:

```
$ iface restart eth0
```

3. Execute the following command to view the network interface settings:

```
$ iface ls
```

```

[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "static",
    "Address": "10.7.19.157",
    "Netmask": "255.255.255.0",
    "Gateway": "10.7.19.254"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2f:05:2d brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.157/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:52d/64 scope link
        valid_lft forever preferred_lft forever

```

4. Use the "resolv add" command to add a DNS server and "resolv ls" to list the DNS servers you've added. For example, the following command adds "8.8.8.8" to the DNS server list.

```
$ resolv mode custom
$ resolv add 8.8.8.8
```

5. Type the following command to view the DNS server settings.

```
$ resolv ls
```

```
$ resolv mode custom
$ resolv add 8.8.8.8
8.8.8.8 is added
$ resolv ls
Custom Mode
8.8.8.8
```

6. Execute the following command to reboot the VM:

```
$ reboot
```

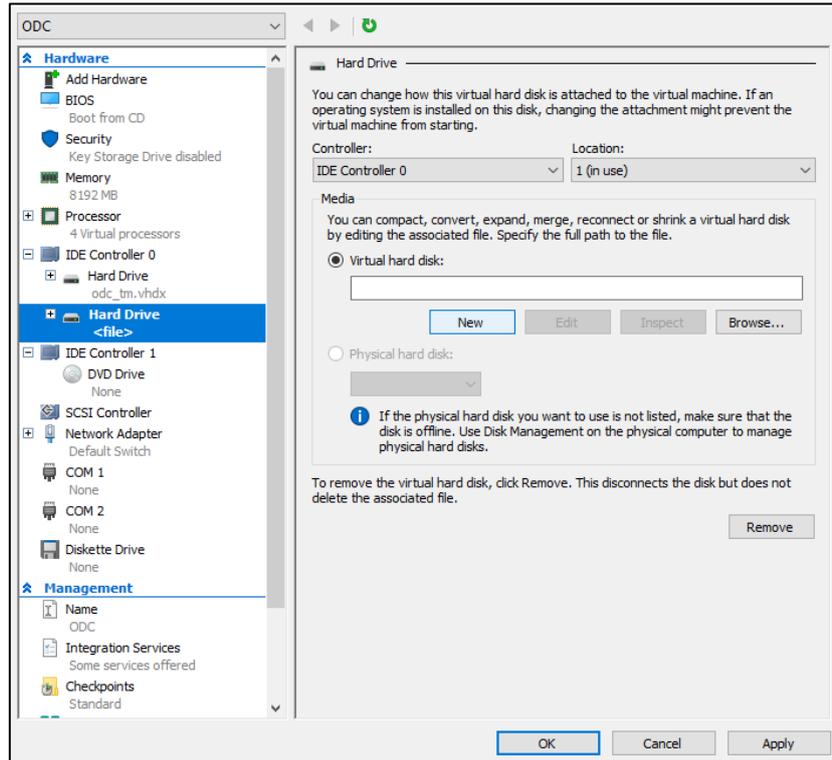
System Migration

When a new version of ODC is released, we can migrate the settings of the old ODC by attaching the external disk of the old ODC to the new ODC VM. The migration of settings can include:

- The UUID of the old ODC
- The pattern and firmware downloaded by the old ODC
- The system configurations of the old ODC, including license, accounting information, security policies and so on.
- The security event logs stored by the old ODC

Procedure

1. Launch the new ODC instance (refer to [Deploying OT Defense Console on page 4](#))
2. Power off the old ODC
3. Click [Browse] and choose an existing disk
4. Attach the external disk of the old ODC to the new ODC
5. The old ODC's information will be migrated into the new ODC



Opening the Management Console

OT Defense Console provides a built-in management console that you can use to configure and manage the product. View the management console using a web browser.

Note: View the management console using Google Chrome version 63 or later; Firefox version 53 or later; Safari version 10.1 or later; Edge version 15 or later.

Procedure

1. In a web browser, type the address of the OT Defense Console in the following format:
<https://<target server IP address or FQDN>>
 The login screen will appear.
2. Enter your credentials (user name and password).

Use the default administrator credentials when logging on for the first time:

- User name: admin
- Password: txone

3. Click Log On.

If this is your first login, the Login Information Setup frame will appear.

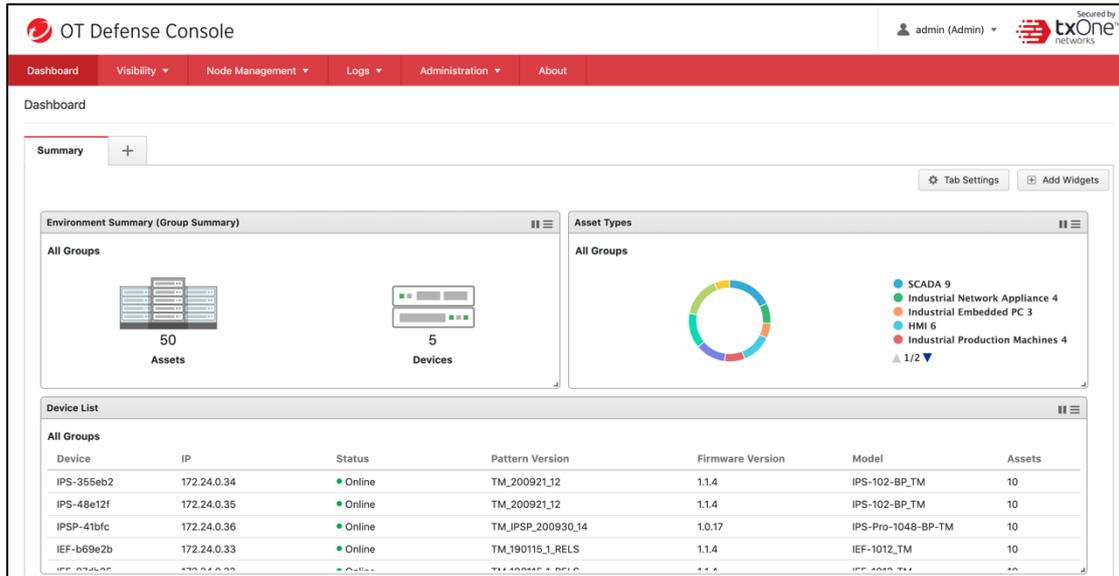
Note: You must change the default login name and password at your first login before you can access the management console.

Note: New login name cannot be "root", "admin", "administrator" or "auditor" (case-insensitive).

- a. Confirm your password settings.
 - New Login Name
 - New Password
 - Retype Password
- b. Click Confirm.

You will be automatically logged out of the system. The Logon screen will appear again.

c. Log on again using your new credentials.



The screenshot shows the OT Defense Console interface. At the top, there is a navigation bar with 'Dashboard', 'Visibility', 'Node Management', 'Logs', 'Administration', and 'About'. The user is logged in as 'admin (Admin)'. The main content area is titled 'Dashboard' and contains several widgets:

- Environment Summary (Group Summary):** Shows 50 Assets and 5 Devices.
- Asset Types:** A donut chart showing the distribution of asset types: SCADA 9, Industrial Network Appliance 4, Industrial Embedded PC 3, HMI 6, and Industrial Production Machines 4.
- Device List:** A table listing individual devices with their IP addresses, status, pattern versions, firmware versions, models, and asset counts.

Device	IP	Status	Pattern Version	Firmware Version	Model	Assets
IPS-355eb2	172.24.0.34	Online	TM_200921_12	1.1.4	IPS-102-BP_TM	10
IPS-48e12f	172.24.0.35	Online	TM_200921_12	1.1.4	IPS-102-BP_TM	10
IPSP-41bfc	172.24.0.36	Online	TM_IPSP_200930_14	1.0.17	IPS-Pro-1048-BP-TM	10
IEF-b69e2b	172.24.0.33	Online	TM_190115_1_RELS	1.1.4	IEF-1012_TM	10

Terms and Acronyms

The following table lists the terms and acronyms used in this document.

Terms/Acronyms	Definitions
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
IT	Informational Technology
ODC	Operational Technology Defense Console
OT	Operational Technology
OT Defense Console	Operational Technology Defense Console
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition