



Operational Technology Defense Console – Virtual Appliance 1.5

Quick Setup Guide (for Windows Hyper-V)

2022-07-18

Copyright © 2022 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.





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







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.

Hyper-V Manager			-	×
File Action View Help				
🔚 Hyper-V Manager	Hyper-V Manager provides the tools and information you can use to	Actions		
	manage a virtualization server.	Hyper-V Manager		•
	Introduction	Connect to Server		
		View		
	A vitualization server is a physical computer that provides the resources required to run vitual machines. You can use Hyper-V Manager to create, configure, and manage the virtual machines on a virtualization server. You can use virtual machines to run different workloads. Each virtual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer.	P Help		

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





Х

🖳 New Virtual Machine Wizard

📕 🛛 Before You I	Begin
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	 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 Wiza	rd	\times
📒 Specify Nam	e and Location	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking	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: ODC 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.	у
Connect Virtual Hard Disk Installation Options	Store the virtual machine is solved in the default folder compared for this server. Store the virtual machine in a different location Oration: Cr/ProgramData/Wircosoft/Windows/Hyper-V/	
Summer y	▲ 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.

New Virtual Machine Wizar	3	×
🔤 Assign Memo	ry	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Startup memory: 8192 MB Image: Specify more than the minimum amount form 32 memory: 8192 MB Image: Use Dynamic Memory for this virtual machine. Image: Specify more than the virtual machine. Image: When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.	1
	< Previous Next > Finish Cancel	

6. Configure the VM's networking settings.

📃 New Virtual Machine Wizard	I		×
Configure Ne	tworking		
Before You Begin Specify Name and Location Specify Generation Assign Memory	Each new virt virtual switch Connection:	ual machine includes a network adapter. You can configure the network adapter to use , or it can remain disconnected. Default Switch	a
Configure Networking			
Connect Virtual Hard Disk Installation Options Summary			

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





8. Check your settings then click [finish].

🖳 New Virtual Machine W	zard					×
🧾 Completin	g the New \	/irtual Machi	ne Wizard			
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Summary	You have following Descriptic Rame: General Memory Networl Hard Dis	successfully comp virtual machine. on: ODC tion: Generation :: 8192 MB :: Default Swi sk: D:\odc\imag	Neted the New Virtual M	achine Wizard. Yo , dynamically expa click Finish.	u are about to creat	te the
			< Previous	Next >	Ejnish	Cancel
Virtual Machines						
Name	State	CPU Usage	Assigned Memory	Uptime	Status	
DC DC	Off					

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





ODC	~	⊲ ▶ ঊ
Hardware Add Hardware BtOS Boot from CD Security Key Storage Drive disabled Memory	^	IDE Controller You can add hard drives and CD/DVD drives to your IDE controller. Select the type of drive you want to attach to the controller and then click Add. Hard Drive DVD Drive
S192 MB Processor 1 Virtual processor IDE Controller 0	4	Add
Hard Drive		You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.
SCSI Controller Network Adapter		

b. Click [New].



c. Choose the VHDX disk format.

🚔 New Virtual Hard Disk Wiz	ard X
Left Choose Disk	Format
Before You Begin	What format do you want to use for the virtual hard disk?
Choose Disk Format	O VHD
Choose Disk Type	Supports virtual hard disks up to 2,040 GB in size.
Specify Name and Location	VHDX
Configure Disk	This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur
Summary	from power failures. This format is not supported in operating systems earlier than Windows 8.

d. Choose the disk type [Dynamically expanding].





🚢 Choose Disk	стуре
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.

🏝 New Virtual Hard Disk Wiza	rd		×
🚢 Specify Name	e 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: odc_tm_data_disk Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\	Browse	
	< Previous Next > Finish	Cancel	

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

监 New Virtual Hard Disk Wi:	ard)
📥 Configure D	isk	
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location	You can create a blank virtual hard disk or copy the c Create a new blank virtual hard disk Size: 50() GB (Maximum: 64 TB) Copy the contents of the specified physical disk:	contents of an existing physical disk.
Summary	Physical Hard Disk _\PHYSICALDRIVE0 _\PHYSICALDRIVE1	Size -465 G8 119 G8
	Copy the contents of the specified virtual hard di Path:	isk Browse

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.

< Previous Next > Einish Cancel

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).

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	

Sizing Table





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

Virtual Machines					
Name	State	CPU Usage	Assigned Memory	Uptime	Status
	Off	Con Setti Che Mov Expo	Assigned Memory nect ngs ckpoint e ort	Uptime	Status
		Ren Dele Help	ime		

b. Configure the number of CPU cores.

ODC	\sim	ব ⊨ ∣ ব
Add Hardware	^	Processor You can modify the number of virtual processors based on the number of processors on
Boot from CD Security Key Storage Drive disabled		the physical computer. You can also modify other resource control settings. Number of virtual processors: 4 💼
Memory 8192 MB		Resource control You can use resource controls to balance resources among virtual machines.
Processor 4 Virtual processors		Virtual machine <u>r</u> eserve (percentage): 0
IDE Controller 0 Hard Drive Adds tm vbdv		Percent of total system resources: 0 Victual machine limit (percentage): 100
Hard Drive odc_tm_data_disk.vhdx		Percent of total system resources: 100
E III IDE Controller 1		Relative weight: 100





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			
<u>C</u> trl + 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





	4 194
	Nome : Lo ,
	ramily: inet,
	Method : Loopback
	"Nome"· "eth@"
	"Family": "inet".
	"Method": "static".
	"Address": "10.7.19.157".
	"Netmask": "255.255.255.0",
	"Gateway": "10.7.19.254"
]	
1: 1	lo: <loopback,up,lower_up> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1</loopback,up,lower_up>
	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</broadcast,multicast,up,lower_up>
	Link/ether 00:00:29:27:05:20 brd ff:ff:ff:ff:ff
	thet 10.7.19.15/724 brd 10.7.19.255 scope global etho
	valid_ift forever preferred_ift forever
	valid 16 forward 16 forward
	valia_lit forever preterrea_lit forever

[Optional] Configure the IP Address Settings

You can choose to configure the IP address manually.

 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
```

- 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



- 4. Use the "resolv add" command to add a DNS server and "resolv Is" 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



- 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





ODC	ŭ 4 ▶ .
A Hardware	A Hard Drive
Add Hardware BIOS Boot from CD	You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.
Security Key Storage Drive disabled	Controller: Location:
Memory	IDE Controller 0 \checkmark 1 (in use) \checkmark
8192 MB	Media
Processor 4 Virtual processors	You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.
IDE Controller 0	Virtual hard disk:
Hard Drive odc_tm.vhdx	
Hard Drive <file></file>	New Edit Inspect Browse
IDE Controller 1 OVD Drive None	Physical hard disk:
SCSI Controller Controller Default Switch	(i) If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.
COM 1 None	To remove the virtual hard disk, dick Remove. This disconnects the disk but does not delete the associated file.
None	Remove
Diskette Drive	
* Management	
I Name ODC	
Integration Services Some services offered	
Checkpoints Standard	v
	OK Cancel Apply

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

- 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-insensititive).

- 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.





	Secured by LXONE networks
A	ppendix A

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