



Operational Technology Defense Console – Virtual Appliance 1.5

Quick Setup Guide
(for KVM)

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

Table of Contents.....	3
Chapter 1	4
ODC Onboarding to KVM	4
Prerequisites.....	4
Deploying OT Defense Console	4
Accessing the ODC CLI	9
Getting the IP Address of the ODC Instance	10
[Optional] Configuring the IP Address Settings	10
Opening the Management Console	11
System Migration.....	13
Appendix A.....	14
Terms and Acronyms	14

ODC Onboarding to KVM

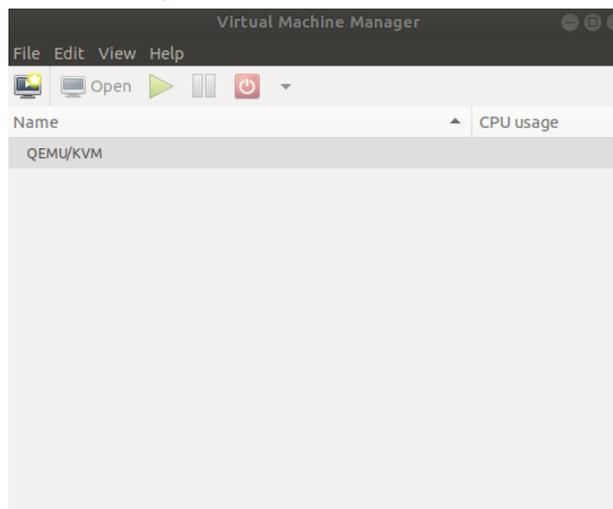
This chapter describes how to deploy OT Defense Console to a KVM.

Prerequisites

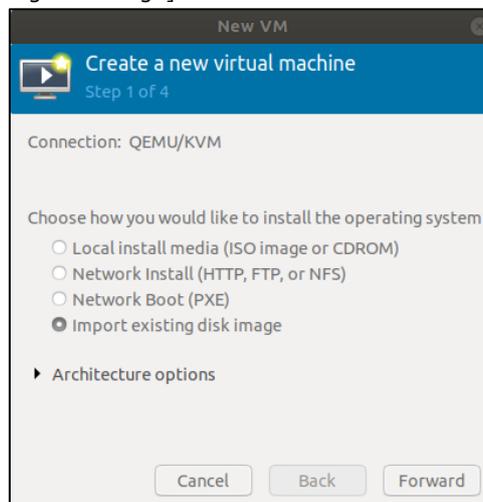
- The qcow2 packages provided by Trend Micro must be available and accessible to KVM 2.0.0.
- The necessary networks have been properly created in KVM.
- An extra disk (with more than 50GB of free disk space)

Deploying OT Defense Console

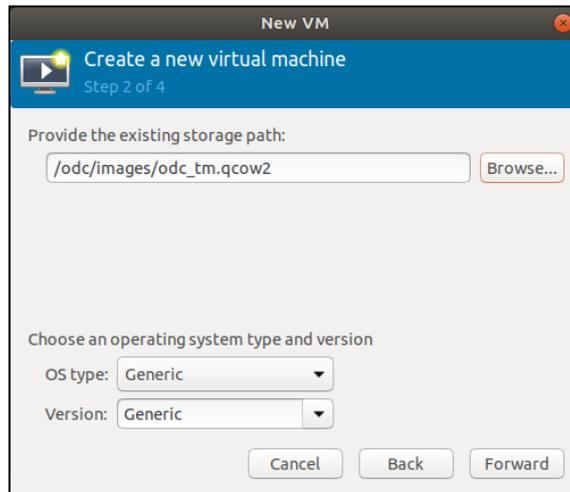
1. Open Virtual Machine Manager.



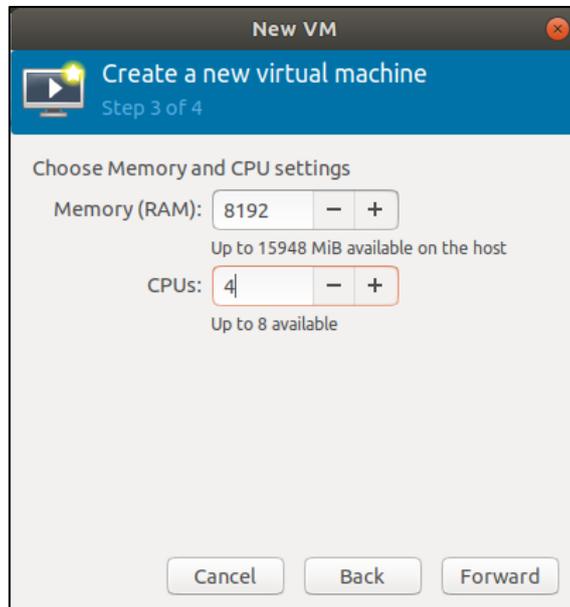
2. Click the [Create a new virtual machine] icon at the top left corner.
3. Select [Import existing disk image].



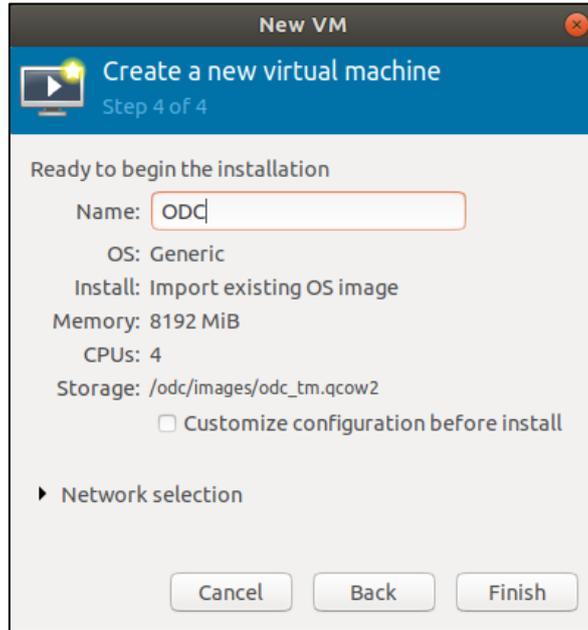
4. Click [Browse] and choose an ODC VM image.



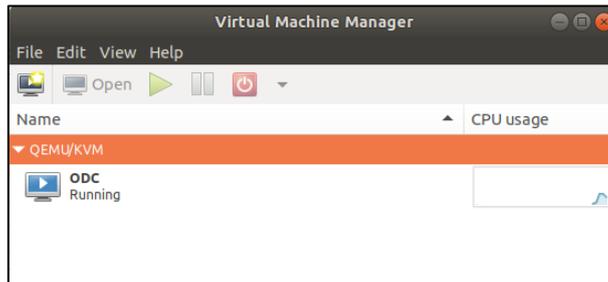
5. Adjust memory allotment and number of CPU cores.



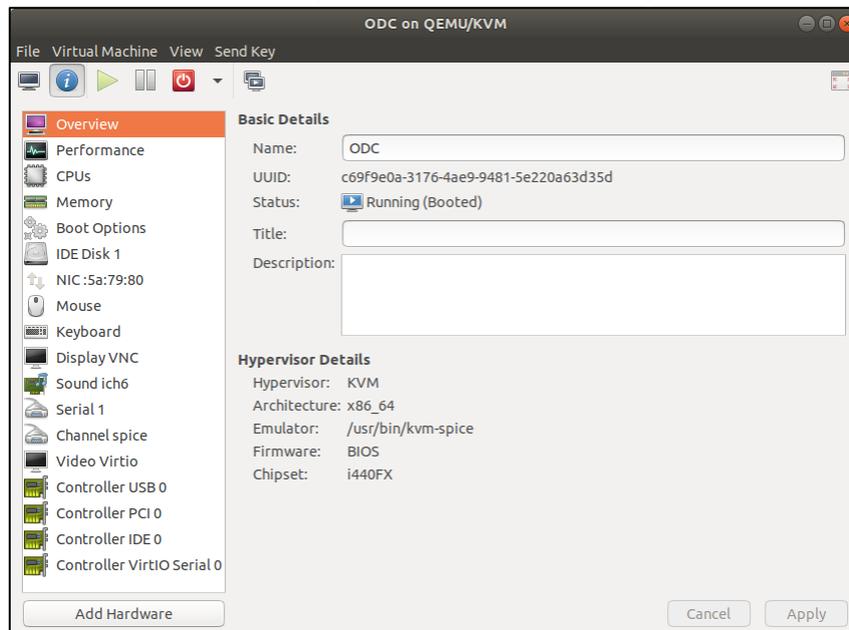
6. Input a virtual machine name, and click [Finish].



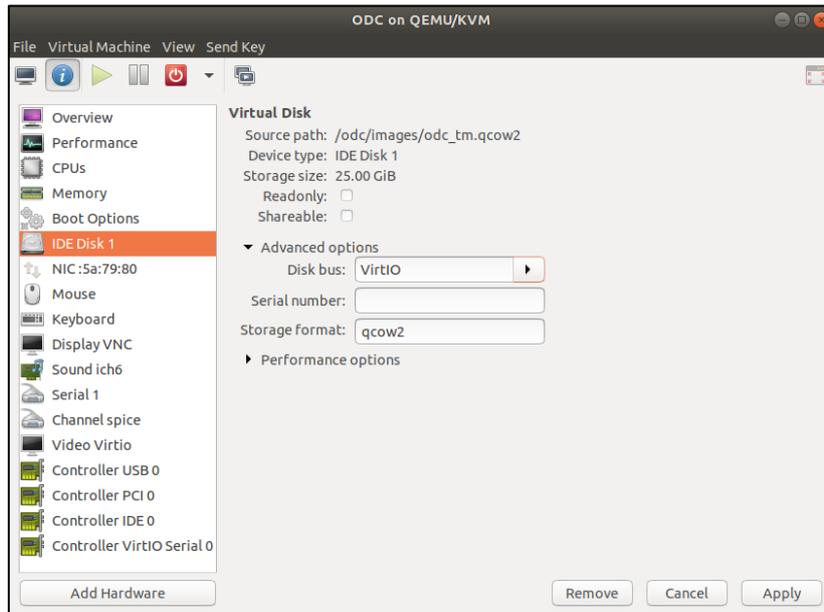
- The new VM will be shown in the virtual machine list.



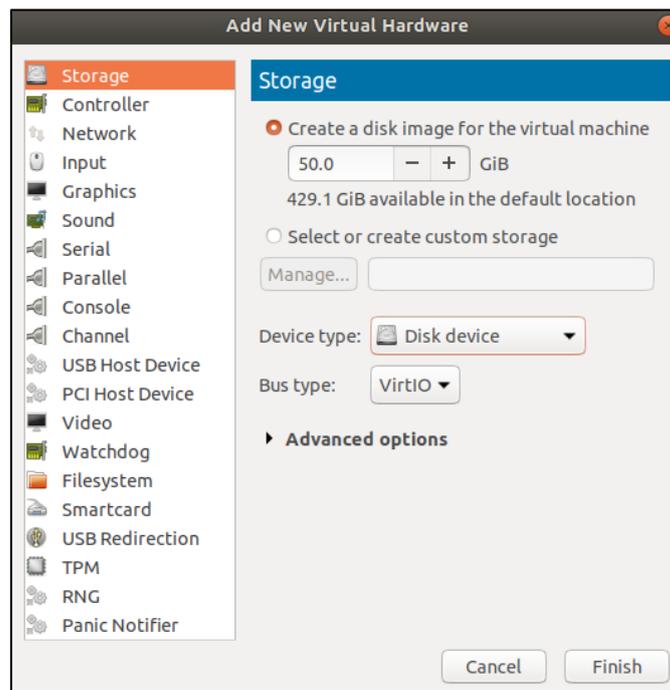
- Click the selected VM and click [Show virtual hardware details].



- At the bottom left corner, click [Add Hardware]. First, select an existing disk, then adjust the disk settings. Under [Disk bus] options, choose [Virtio]. Under [Storage format] options, select [qcow2].



10. Click [Apply] to add a new disk. We can create a new disk image or select another existing storage.



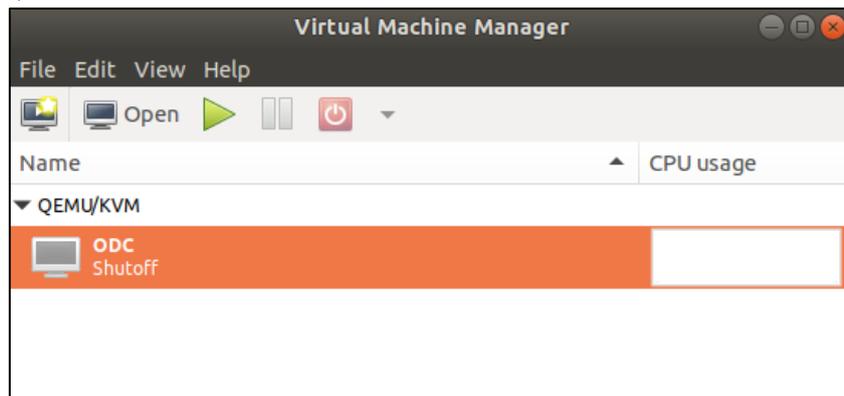
The external disk size can be decided depending on the number of logs to be stored, as shown in the suggestion table below.

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 size of the external disk must be at least 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.

11. Now, the ODC instance will boot.

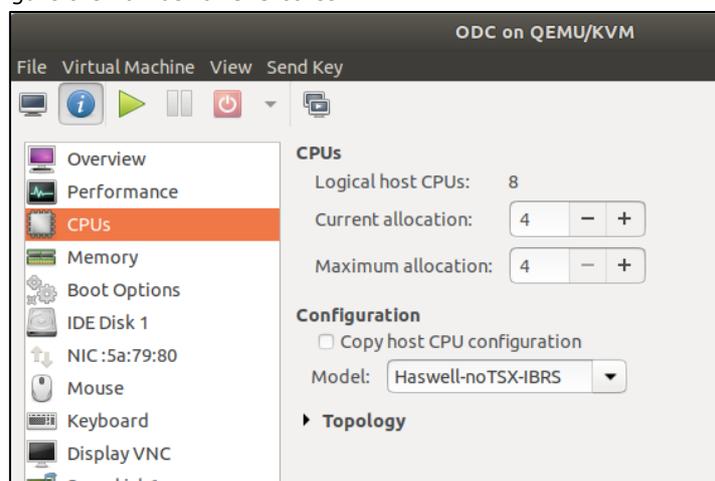


12. **(Optional)** Adjust your ODC instance to use proper resource configurations based on the following sizing table or using default settings (default settings are as follows: 8 CPU cores, 16 GB of memory).

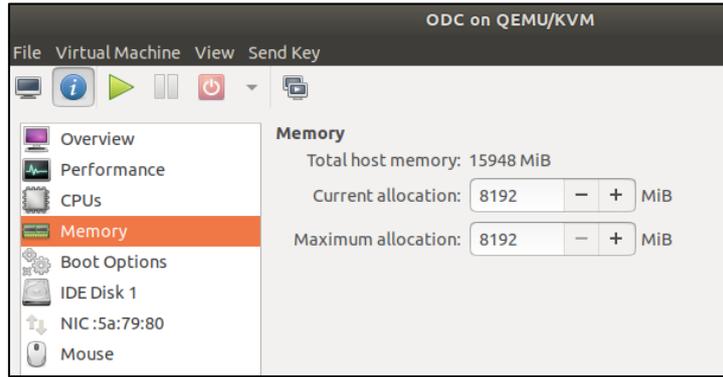
Sizing Table

Nodes	CPUs	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 [Edit].
The [Edit settings] window will appear.
- 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. Change the default password
 - a. Type oobe
 - b. Change the default password
 - c. Re-log in to the ODC with your new password

```
vShell, version v1.0.0
If you want to exit this shell, please type 'exit' or 'Ctrl-D'.
Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
Caution: please type the command ``oobe`` to activate the vShell.
$ oobe
Type current password:
Type the new password:
```

4. 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
resolve    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] Configuring 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. Input 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
```

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 login credentials (user name and password).

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

- User ID: 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 Log On screen will appear again.
- c. Log on again using your new credentials.

OT Defense Console
admin (Admin)

Dashboard
Visibility
Node Management
Logs
Administration
About

Summary +
Tab Settings + Add Widgets

Environment Summary (Group Summary)

All Groups

50
Assets

5
Devices

Asset Types

All Groups

- SCADA 9
- Industrial Network Appliance 4
- Industrial Embedded PC 3
- HMI 6
- Industrial Production Machines 4

Device List

All Groups

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_REL5	1.1.4	IEF-1012_TM	10

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 includes:

- The UUID of the old ODC
- The pattern and firmware downloaded by the old ODC
- The system configuration settings from the old ODC such as its 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 section [Deploying OT Defense Console on page 4](#))
2. Power off the old ODC
3. Click [Browser] 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



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