TREND MICRO | txOne networks

1.2

TXOne StellarOne™

Installation Guide (for Windows Hyper - V)

Unify your cyber security posture with one centralized console

Endpoint Security

TXOne Networks 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 theapplicable documentation, which are available from the TXOneNetworks website at:

http://docs.trendmicro.com/en-us/enterprise/txone-stellarenforce.aspx and

http://docs.trendmicro.com/en-us/enterprise/txone-stellarprotect.aspx

Document Part No.: SLEM19520/220422
Release Date: April 2022
Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/orprovides 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 productmay be available at the TXOne Online Help Center and/or the TXOne Knowledge Base.

TXOne always seeks to improve its documentation. If you havequestions, comments, or suggestions about this or any TXOnedocument, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site: http://docs.trendmicro.com/en-us/survey.aspx

Privacy and Personal Data Collection Disclosure

Certain features available in TXOne products collect and send feedback regarding product usage and detection information toTXOne. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want TXOne to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TXOne StellarOne 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 TXOne is subject to the conditions stated inthe Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

StellarOne Onboarding to Windows Hyper-V

This chapter describes how to deploy Stellar One 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)
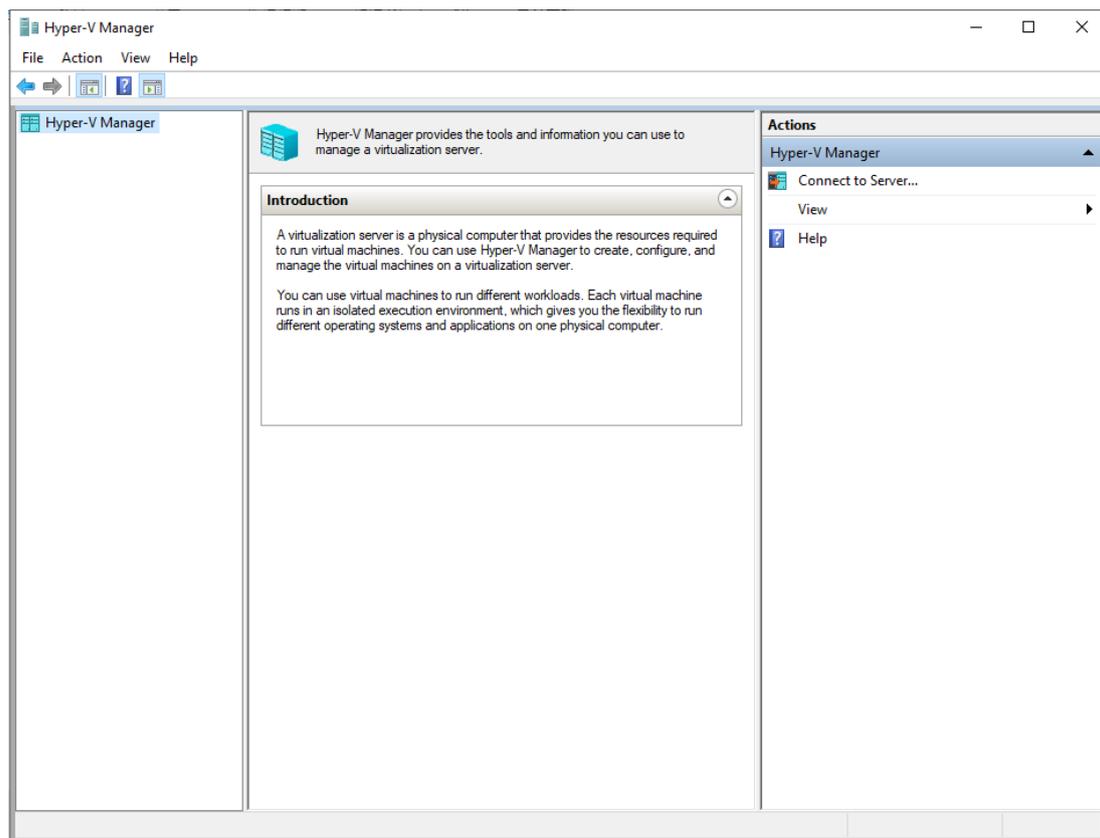
Deploying Stellar One Console

1. Launch Hyper-V manager.
2. Under [Actions], click [New] and then click [Virtual Machine].
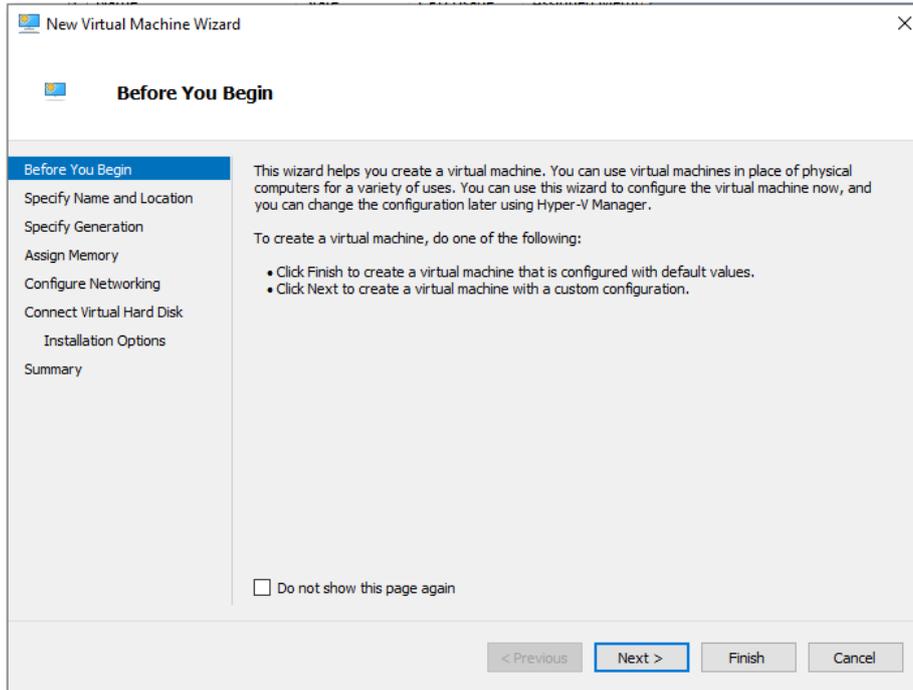
3. Type a name for your new VM.
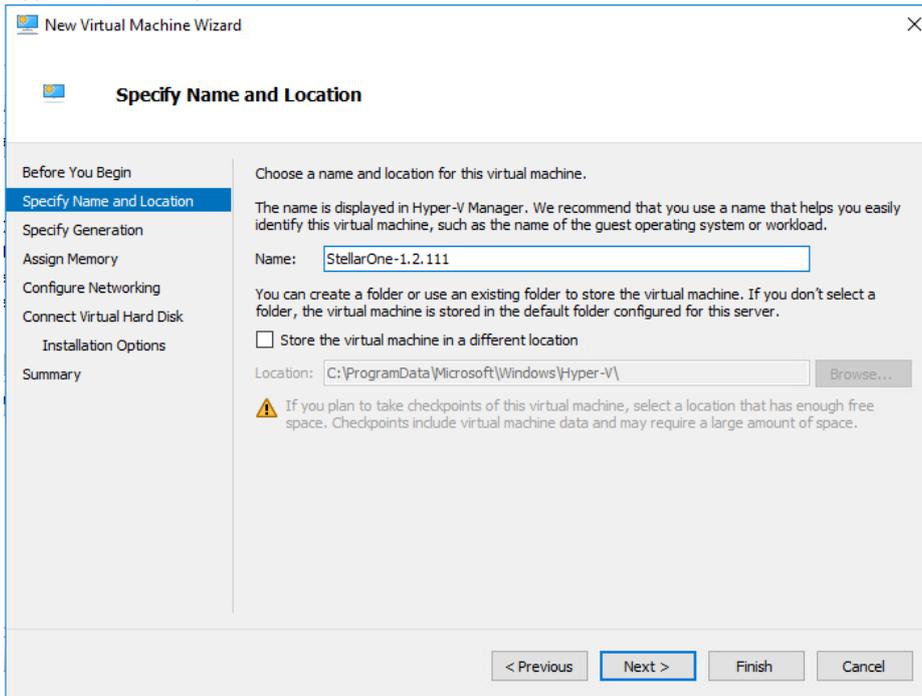
4. Specify the VM's Generation. Current StellarOne only support Hyper-V Generation 1.

New Virtual Machine Wizard

Specify Generation

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
    Installation Options
Summary

Choose the generation of this virtual machine.

○ Generation 1
This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

○ Generation 2
This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

< Previous   Next >   Finish   Cancel

5. Allocate memory for the new VM. (StellarOne min Memory need 16GB = 16384MB)

New Virtual Machine Wizard

Assign Memory

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: 16384   MB

☐ Use Dynamic Memory for this virtual machine.

ⓘ 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.

< Previous   Next >   Finish   Cancel

6. Configure the VM's networking settings.

8
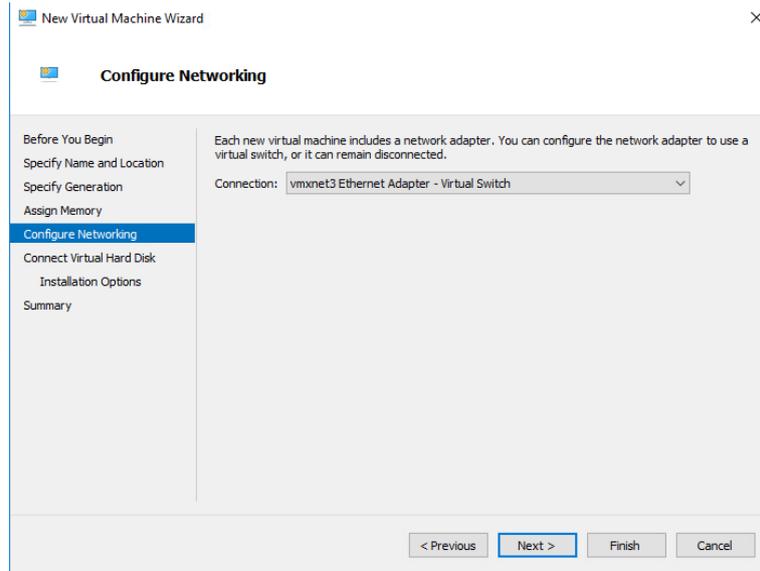
7. Select a virtual hard disk (choose the StellarOne vhdx file provided by Trend Micro).
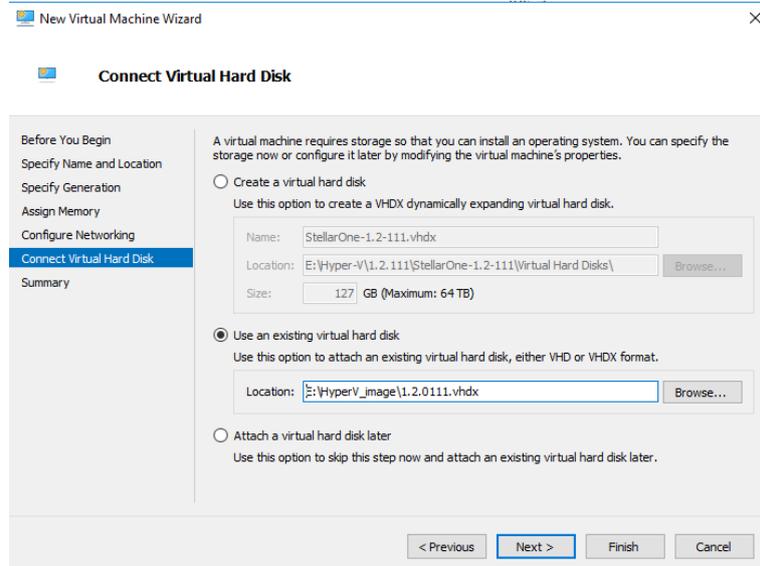
8. Check your settings then click [finish].
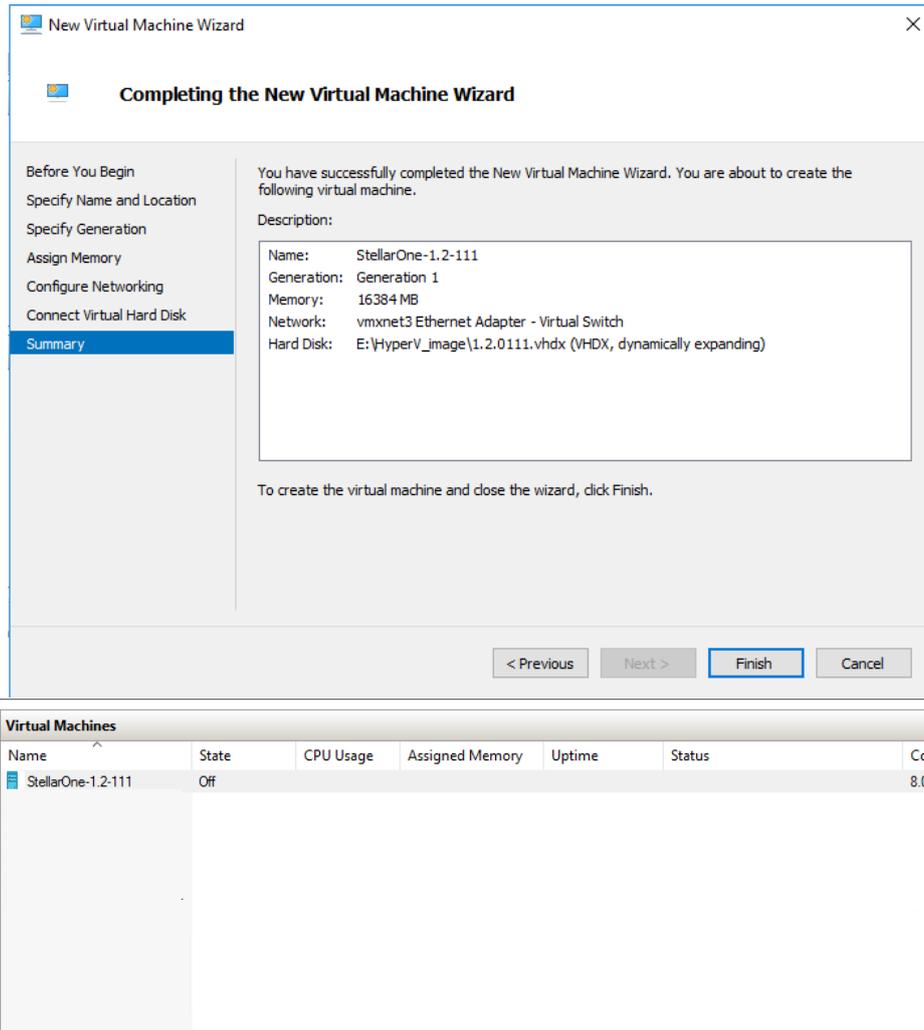
9. Add a new disk.
   a. Select Virtual machine, Right click menu select [Settings].
   b. Select [Hard Disk], then click [Add].
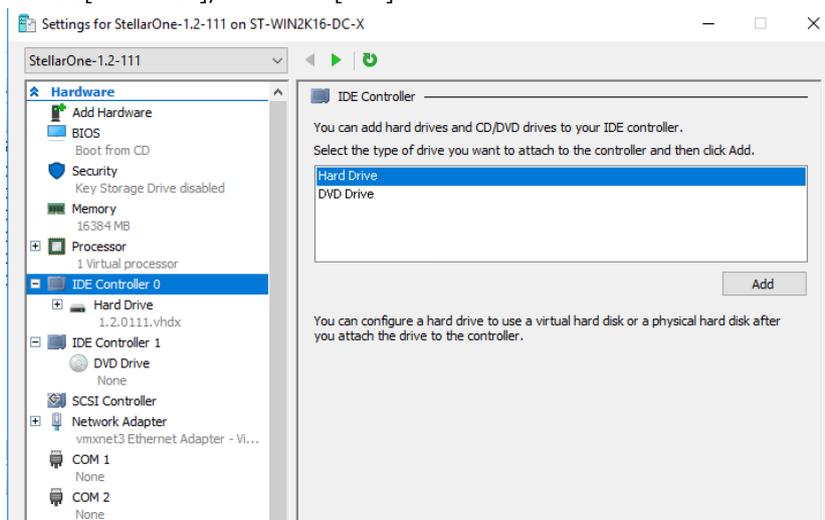
   c. Click [New].
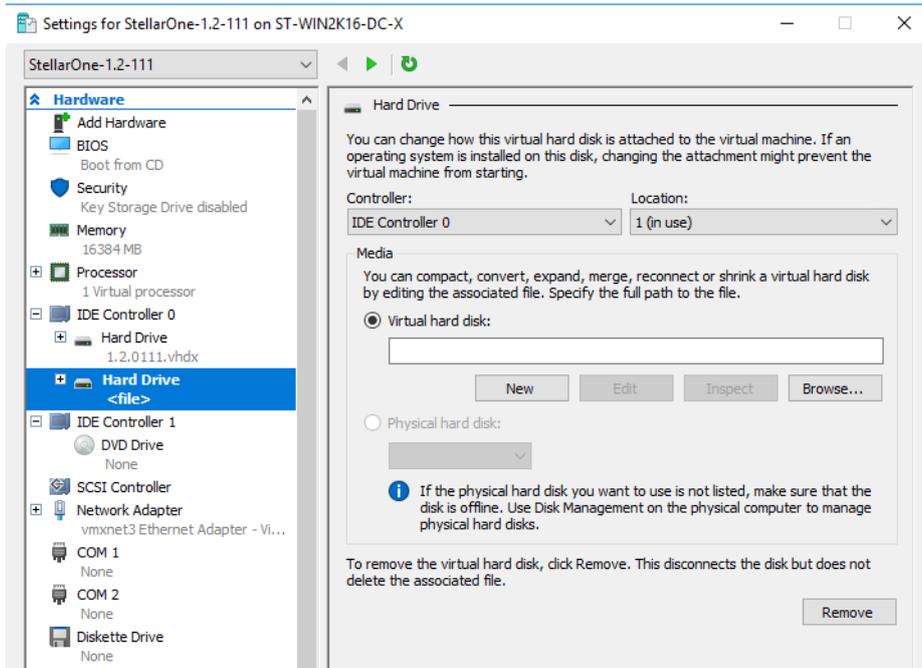
d. Choose the VHDX disk format.
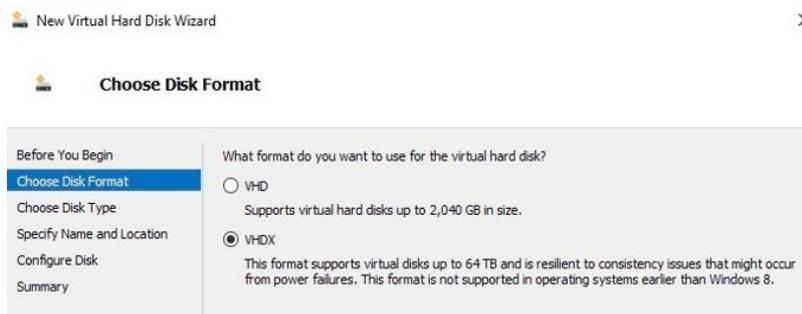
e. Choose the disk type [Dynamically expanding].
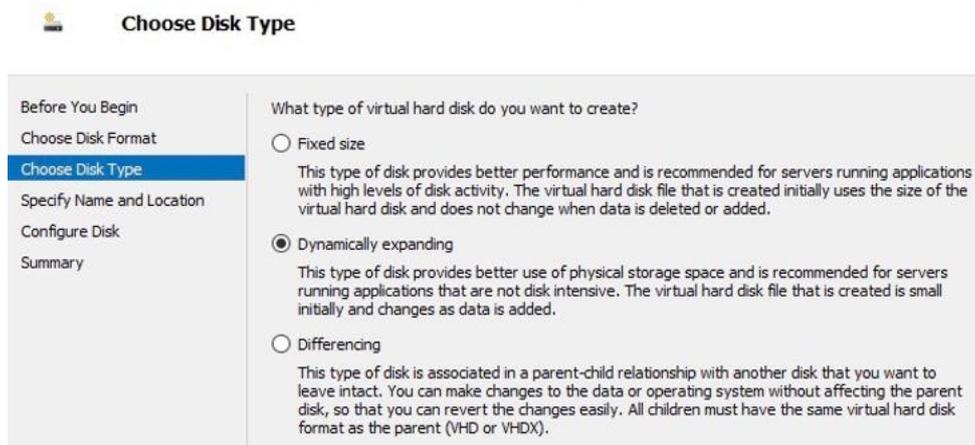
f. Specify name and location.

g. Configure disk size (STELLAR ONE's disk size is based on the sizing table below).

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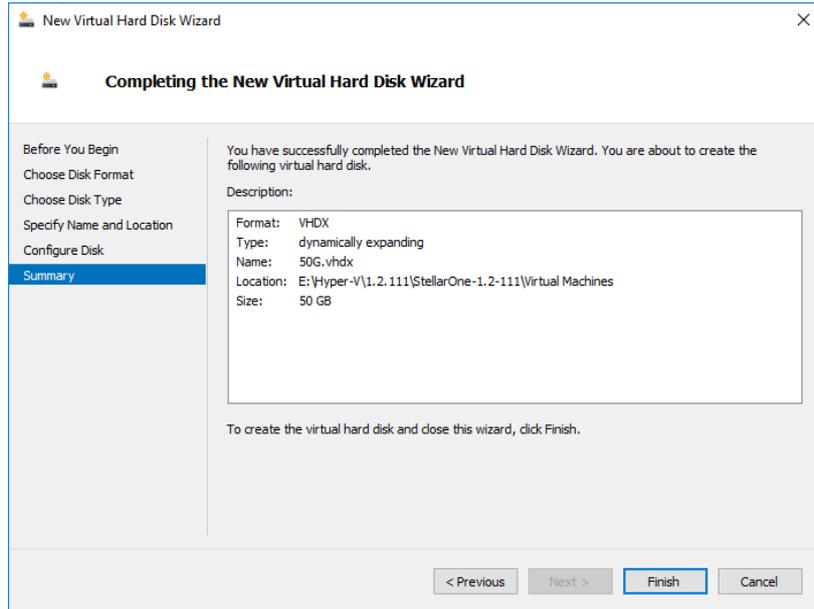
The external disk size can be decided depending on the number of logs to be stored, as shown on the suggestion table below.

#of Logs	Disk
5,000,000	50 GB
10,000,000	150 GB
50,000,000	300 GB
100,000,000	500 GB

Note: The Stellar One requires one external disk and the minimum size of the external disk must be above 50GB, otherwise the STELLAR ONE will not finish 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 STELLAR ONE instance here instead of adding a new disk if you want to migrate the previous configurations and logs to the new Stellar One instance.

10. **(Optional)** Adjust your STELLAR ONE instance to use proper resource configurations based on the following sizing table or at least using default settings (4 CPU cores, 16 GB of memory).

a. Shut down the instance of STELLAR ONE and click [Settings].
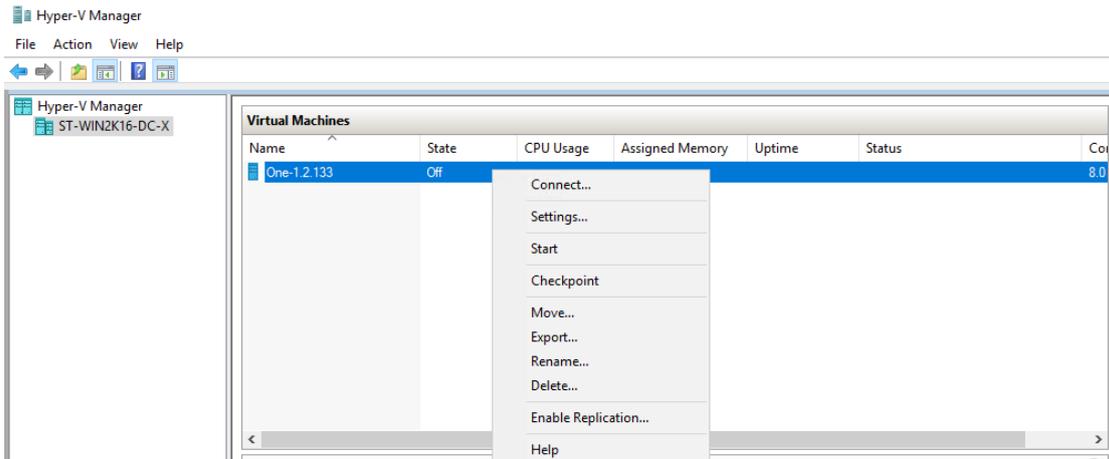
b. Configure the number of CPU cores.
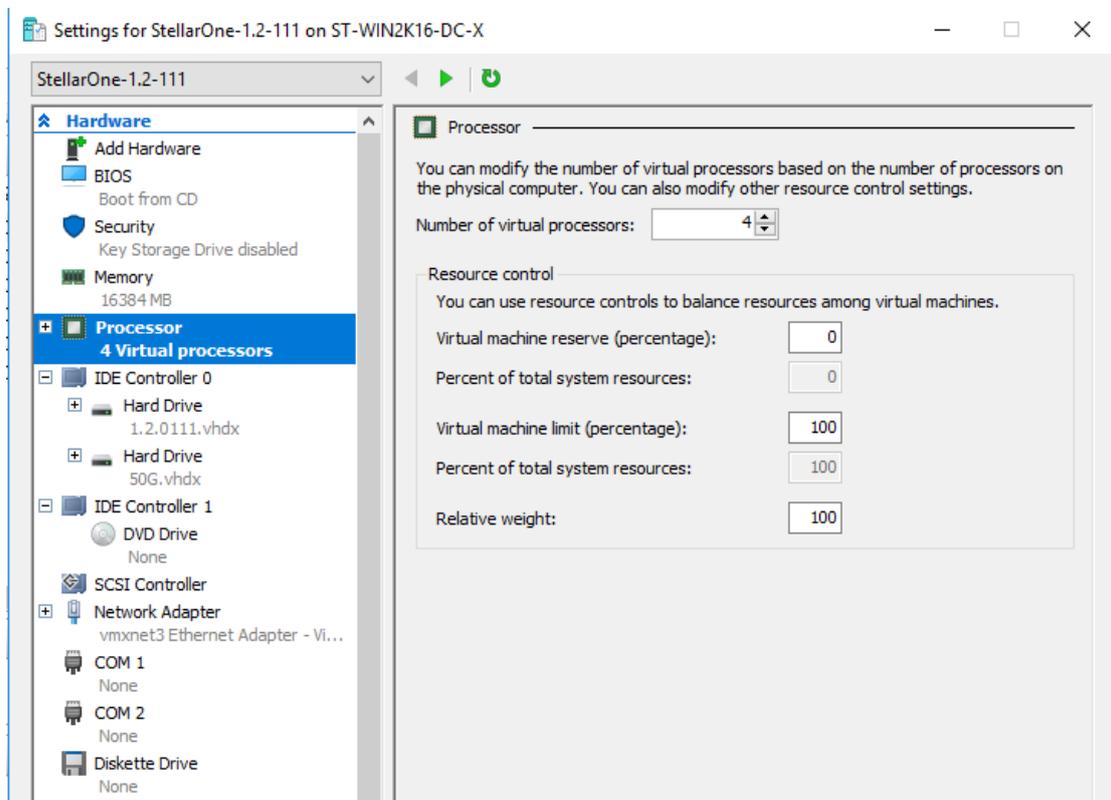
c. Configure the amount of memory.
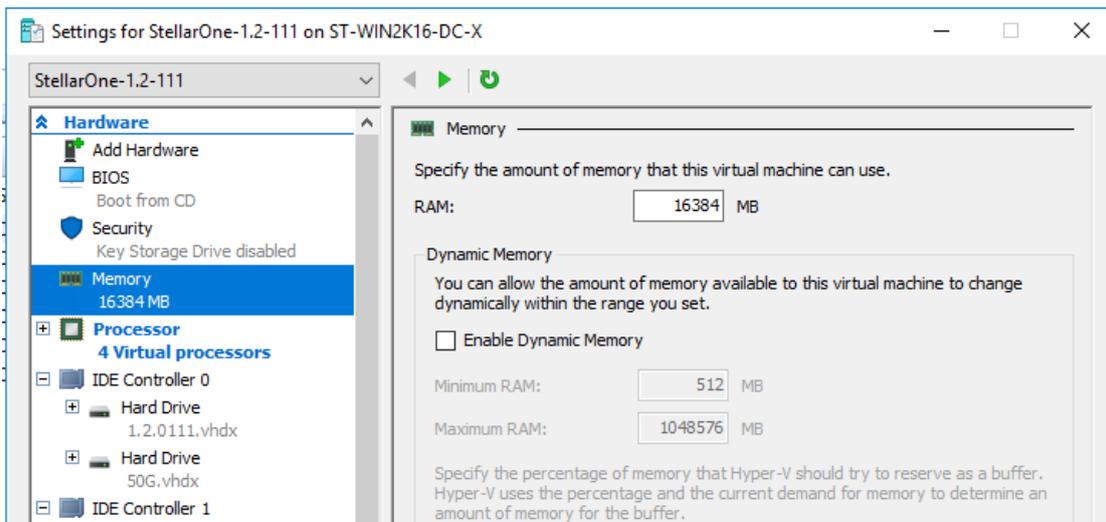
d. Boot the STELLAR ONE instance.

Sizing Table

Agents	CPU	Memory
500	4 cores	8 GB
1,000	4 cores	16 GB
5,000	8 cores	16 GB
10,00	8 cores	16 GB
15,000	8 cores	16 GB
20,000	8 cores	16 GB
30,000	10 cores	24 GB

Accessing the STELLAR ONE CLI

1. Open the STELLAR ONE VM console.
2. Login with "root / txone"
3. After logging into the STELLAR ONE, 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 STELLAR ONE Instance

1. Type the following command to get the IP address of the STELLAR ONE 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
```


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
```


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; or 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 log on, the Login Information Setup frame will appear.

|	
Note:	You must change the default login name and password at first log on before you can access the management console.
Note:	New login name can not 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 Log On screen will appear again.

c. Log on again using your new credentials.
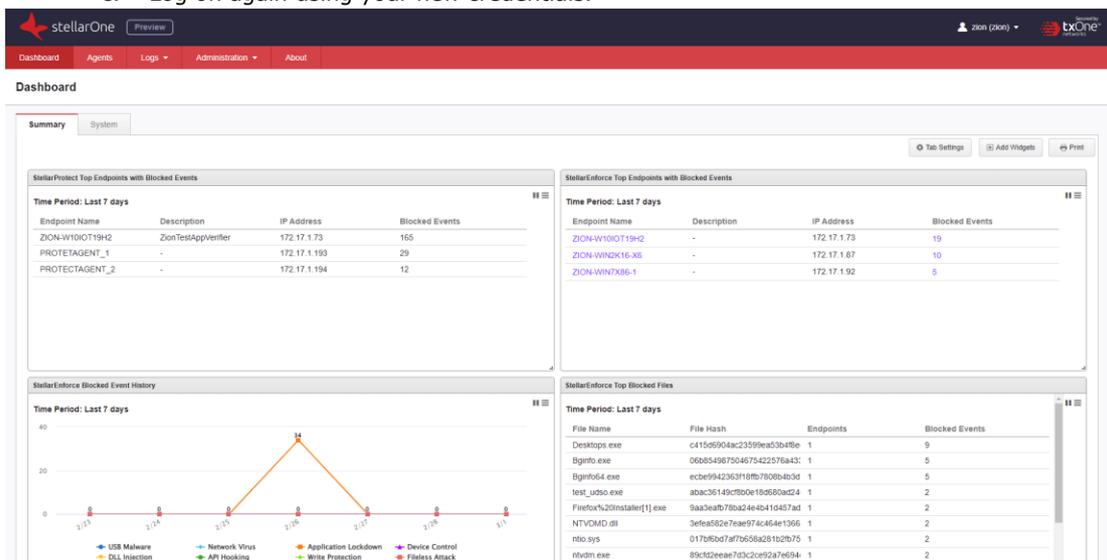
Terms and Acronyms

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

Term/Acronym	Definition
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
IT	Informational Technology
STELLAR ONE	Operational Technology Defense Console
OT	Operational Technology
OT Defense Console	Operational Technology Defense Console
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition