

TXOne StellarOne[™] Installation Guide (for Windows Hyper - v)

Unify your cyber security posture with one centralized console







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/txonestellarenforce.aspx and

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

© 2022 TXOne Networks Incorporated. All rights reserved. TXOne, and TXOne StellarOne are trademarks or registered trademarks of TXOne Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

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 in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy





Table of Contents

Table of Contents	5
Chapter 1	6
StellarOne Onboarding to Windows Hyper-V	6
Prerequisites	6
Deploying Stellar One Console	6
Accessing the STELLAR ONE CLI	
Getting the IP Address of the STELLAR ONE Instance	
[Optional] Configure the IP Address Settings	16
Opening the Management Console	
Appendix A	19
Terms and Acronyms	19
•	







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)

File Action View Help Hyper-V Manager Hyper-V Manager Hyper-V Manager Introduction Avitualization server is a physical computer that provides the resources reguled to run vitual machines. You can use typer-V Manager to create, configure, and memage the vitual machines on or avitualization server. You can use vitual machines revice on avitualization server. You can use vitual machines revices and applications on one physical computer. Help Help Help	Hyper-V Manager		-	×
Hyper-V Manager Hyper-V Manager Hyper-V Manager Introduction A virtualization server is aphysical computer that provides the resources equired to run virtual machines on a virtualization server. You can use hyper-V Manager to create, configure, and manage the virtual machines on a virtualization server. You can use hyper-V Manager to create, configure, and manage the virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on a virtualization server. You can use virtual machines on one physical computer. Weiler Help	File Action View Help			
Hyper-V Manager Hyper-V Manager provides the tools and information you can use to manage a virtualization server. Actions Introduction Introduct				
Image a vitualization server. Introduction A vitualization server is a physical computer that provides the resources required to manage the vitual machines on a vitualization server. You can use vitual machines to an use Hyper-V Manager to create, corrigrey, and manage the vitual machines on a vitualization server. You can use vitual machines to an use Hyper-V Manager to create, corrigrey, and manage the vitual machines on a vitualization server. You can use vitual machines to an undifferent workloads. Each vitual machine manage the vitual machine on an en physical computer. Ifferent operating systems and applications on one physical computer.	Hyper-V Manager	Actions		
Introduction A vitualization server is a physical computer that provides the resource required to run vitual machines. You can use Hyper-V Manager to create, configure, and manage the vitual machines on a vitualization server. You can use vitual machines on a vitualization server. You can use vitual machines on a vitualization server. You can use vitual machines on a vitualization server. You can use vitual machines on a vitualization server. You can use vitual machines on a vitualization server. You can use vitual machines on a vitualization server. You can use vitual machines on a physical computer. different operating systems and applications on one physical computer.	manage a virtualization server.	Hyper-V Manager		•
A vitualization sever 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 vitual machines on a vitualization sever. You can use vitual machines to run different workloads. Each vitual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer. Image: Witual machines to run different workloads. Each vitual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer. Image: Witual machines to run different workloads. Each vitual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer. Image: Witual machines to run different workloads. Each vitual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer. Image: Witual machines to run different workloads. Each vitual machine runs in a mole runs in the runs in	Introduction	E Connect to Server		
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 vitual machines to run different workloads. Each vitual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer.		View		<u> </u>
	A virtualization server is a physical computer that provides the resources required to run virtual machines. You can use Hyper-V Managerto 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.	Help		

Deploying Stellar One Console

- 1. Launch Hyper-V manager.
- 2. Under [Actions], click [New] and then click [Virtual Machine].





×

🖳 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 Wizard	L	×
💴 Specify Name	and Location	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk	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 yo identify this virtual machine, such as the name of the guest operating system or workload. Name: StellarOne-1.2.111 You can create a folder or use an existing folder to store the virtual machine. If you don't seleve folder, the virtual machine is stored in the default folder configured for this server.	iu easily ct a
Installation Options	Store the virtual machine in a different location	
Summary	Location: C:\ProgramData\Microsoft\Windows\Hyper-V\ Bro	wse
	▲ If you plan to take checkpoints of this virtual machine, select a location that has enough f space. Checkpoints include virtual machine data and may require a large amount of space	ree
	< Previous Next > Finish C	ancel

4. Specify the VM's Generation. Current StellarOne only support Hyper-V Generation 1.





🖳 New Virtual Machine Wizard

Before You Begin Specify Name and Location	Choose the generation of this virtual machine. © Generation 1 This with all machine appropriate a property 23 bit and 54 bit quest possible a puttern and equides	
Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	 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	<

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

🖳 New Virtual Machine Wizar	d	×
🛄 🛛 Assign Memo	ry	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Diak Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 1258/2912 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.



7. Select a virtual hard disk (choose the StellarOne vhdx file provided by Trend Micro).

🖳 New Virtual Machine Wiz	ard	×
Connect Vi	tual Hard Disk	
Before You Begin Specify Name and Location Specify Generation Assign Memory	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties. Create a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk.	
Configure Networking Connect Virtual Hard Disk Summary	Name: StellarOne-1.2-111.vhdx Location: E:\Hyper-V\1.2.111\StellarOne-1.2-111\Virtual Hard Disks\ Size: 127 GB (Maximum: 64 TB) (Ise an existing virtual hard disk (Be this option to attach an existing virtual hard disk, either VHD or VHDX format.	
	Location: E: HyperV_image \1.2.0111.vhdx Browse O Attach a virtual hard disk later Use this option to skip this step now and attach an existing virtual hard disk later.	
	< Previous Next > Finish Cancel	

8. Check your settings then click [finish].



•	Secured by
	EXONE networks

 \times

🖳 New Virtual Machine Wizard

Somplet 2	ing the Nev	w Virtual Ma	achine Wizard					
Before You Begin Specify Name and Location Specify Generation	You h follow Descr	ave successfully ing virtual mach iption:	r completed the New Vi ine.	rtual Machin	e Wizard. You a	are about to cre	ate the	
Assign Memory	Nam	ne: Stellar	One-1.2-111					
Configure Networking	Men	nory: 16384	MB					
Connect Virtual Hard Disk	Net	work: vmxn	et3 Ethernet Adapter -	Virtual Swite	ch			
	To cre	eate the virtual r	machine and close the v	wizard, click	Finish.			
			< Pre	evious	Next >	Finish	Cancel	
Virtual Machines								_
Name	State	CPU Usage	Assigned Memory	Uptime	Status	5		Co
StellarOne-1.2-111	Off							8.0

- 9. Add a new disk.
 - a. Select Virtual machine, Right click menu select [Settings].
 - b. Select [Hard Disk], then click [Add].



c. Click [New].





s 🖻	ettings for StellarOne-1.2-111 on ST	T-WIN	V2K16-D	IC-X				_		×
Ste	larOne-1.2-111	\sim		G						
× [] ⊡	Hardware Add Hardware BIOS Boot from CD Security Key Storage Drive disabled Memory 15384 MB Processor I Virtual processor I DE Controller 0 Hard Drive 1.2.0111.vhdx Hard Drive <file></file>	^	You operative the second secon	Hard Drive can change ating systen al machine f roller: Controller 0 dia yu can comp r editing the) Virtual har	how this virtua m is installed or from starting. Deact, convert, e e associated file rd disk: New	I hard disk is a this disk, cha expand, merge . Specify the t	ttached to the vir nging the attachm Location: 1 (in use) e, reconnect or sh full path to the file dit Insp	tual machin ient might p rink a virtua t.	e. If an revent the al hard disk Browse	~
□ 	IDE Controller 1 DVD Drive None SCSI Controller Network Adapter vmmet3 Ethernet Adapter - Vi COM 1 None COM 2 None Diskette Drive None		To re delet	Physical h i If the disk i phys emove the v te the assoc	e physical hard is offline. Use f sical hard disks. /irtual hard disk jated file.	l disk you wan Disk Managem , dick Remove	t to use is not liste ent on the physica . This disconnects	ed, make su al computer the disk bu	re that the to manage ut does not Remove	

d. Choose the VHDX disk format.

L New Virtual Hard Disk Wizard

×

🚢 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.

e. Choose the disk type [Dynamically expanding].

🔓 Choose Disk Type

Before You Begin Choose Disk Format	What type of virtual hard disk do you want to create?
Choose Disk Type	This type of disk provides better performance and is recommended for servers running applications
Specify Name and Location Configure Disk Summary	 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).

f. Specify name and location.



Secured by EXONE networks ×

🏝 New Virtual Hard Disk Wizard

Specify Name and Location

Before You Begin Choose Disk Format	Specify the name and location of the virtual hard disk file. Name: 50G.vhdx	
Choose Disk Type	Location: E:\Hyper-V\1.2.111\StellarOne-1.2-111\Virtual Machines\ Brow	se
Configure Disk Summary		
	< Previous Next > Finish Car	ncel

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

sk	
You can create a blank virtual hard disk or copy the co © Create a new blank virtual hard disk Size: 50 GB (Maximum: 64 TB) O Copy the contents of the specified physical disk:	ntents of an existing physical disk.
Physical Hard Disk	Size
\\. \PHYSICALDRIVE0	465 GB
\ \PHYSICALDRIVE1	119 GB
O Copy the contents of the specified virtual hard dis	*
Path:	Browse
	Sk You can create a blank virtual hard disk or copy the co © Create a new blank virtual hard disk or copy the contents of the specified physical disk: Physical Hard Disk NVPHYSICALDRIVED NVPHYSICALDRIVE1 C Copy the contents of the specified virtual hard dis Path:

h. Click [Finish].





🏝 New Virtual Hard Disk Wizard

Long the New Virtual Hard Disk Wizard

Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location Configure Disk	You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Description: Format: VHDX Type: dynamically expanding
Summary	To create the virtual hard disk and close this wizard, dick Finish.
	< Previous Next > Finish Cancel

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].

Hyper-V Manager							
File Action View Help							
🗢 🔿 🞽 📰 👔							
Hyper-V Manager ST-WIN2K16-DC-X	Virtual Machines						
	Name	State	CPU Usage	Assigned Memory	Uptime	Status	Cor
	One-1.2.133	Off	Connect				8.0
			Settings				
			Start				
			Checkpoint				
			Move				
			Export				
			Rename				
			Delete				
			Enable Replic	ation			
	<		Help				>

b. Configure the number of CPU cores.

StellarOne-1.2-111	v < ▶ 0
A Hardware	Processor
Add Hardware	
BIOS	You can modify the number of virtual processors based on the number of processors
Boot from CD	the physical computer. You can also modify other resource control settings.
Security	Number of virtual processors: 4
Key Storage Drive disabled	
Memory	Resource control
16384 MB	You can use resource controls to balance resources among virtual machines.
+ 🔲 Processor	Virtual machine reserve (percentage): 0
4 Virtual processors	
IDE Controller 0	Percent of total system resources: 0
🛨 🚃 Hard Drive	
1.2.0111.vhdx	Virtual machine limit (percentage): 100
🗄 🚃 Hard Drive	Percent of total system resources: 100
50G.Vndx	
E IDE Controller 1	Relative weight: 100
OVD Drive	
INETWORK Adapter vmvpet3 Ethernet Adapter - Vi	
None	
None	
Diskette Drive	
None	

c. Configure the amount of memory.

StellarOne-1.2-111	✓ ▲ ► Ŭ		
A Hardware	▲ Memory —		
📑 Add Hardware			
BIOS	Specify the amount of memory that this virtual machine can use.		
Boot from CD	RAM: 16384 MB		
Security			
Key Storage Drive disabled	Dynamic Memory		
Memory 16384 MB	You can allow the amount of memory available to this virtual machine to change dynamically within the range you set.		
Processor 4 Virtual processors	Enable Dynamic Memory		
🖃 🧾 IDE Controller 0	Minimum RAM: 512 MB		
Hard Drive 1.2.0111.vhdx	Maximum RAM: 1048576 MB		
Hard Drive 50G.vhdx	Specify the percentage of memory that Hyper-V should try to reserve as a buffer.		
🖃 🌉 IDE Controller 1	amount of memory for the buffer.		





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 prov	vided 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 STELLAR ONE Instance

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



[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
```

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 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.



- 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

 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		
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.

Log on again using your new credentials. c. **tx**One Dashboard Su System e Print ect Top End ce Top En = 11 ≡ Time Period: Last 7 days Time Period: Last 7 days Endpoint Name ZION-W10IOT19H2 PROTETAGENT_1 PROTECTAGENT_2 Endpoint Name IP Address 172.17.1.73 172.17.1.193 172.17.1.194 IP Address 172.17.1.73 172.17.1.87 172.17.1.92 165 29 12 = Time Period: Last 7 days od: Last 7 days File Name
Desktops.exe
Bginfo.exe
Bginfo64.exe
test_udso.exe
Firefox%2000 ad24 Firefox%20in NTVDMD.dll 9aa3eafb78ba24e4b41d457ad lefea582e7eae974c464e1366 ntio.sys ntvdm.exe + USB Ma + DLL Inj + Applie + Write + Device Contro Fileless Attack + Ne



Secured by EXONE networks
Appendix A

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