

2.2 TXOne StellarOne

Installation Guide

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 the applicable documentation, which are available at:

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

TXOne Networks, StellarOne, StellarProtect, and StellarProtect (Legacy Mode) are trademarks or registered trademarks of TXOne Networks Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2023. TXOne Networks Incorporated. All rights reserved.

Document Part No.: APEM229710/230327

Release Date: April 2023

Protected by U.S. Patent No.: Patents pending.

Privacy and Personal Data Collection Disclosure

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

The following link outlines the types of data that TXOne Networks, StellarOne, StellarProtect, and StellarProtect (Legacy Mode) collect 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 Networks is subject to the conditions stated in the TXOne Networks Privacy Notice:

<https://www.txone.com/privacy-policy/>

Table of Contents

Preface

Preface	vi
About the Documentation	vi
Audience	vii
Document Conventions	vii
Terminology	viii

Chapter 1: Introduction

About TXOne Stellar	1-2
Key Features and Benefits	1-2
What's New	1-3

Chapter 2: Installation Planning

System Requirements	2-2
Hardware Requirements	2-2
Hardware Requirements for VMware System	2-3
Hardware Requirements for Hyper-V System	2-4
Deciding an Instance Type for StellarOne on AWS EC2 Platform	2-6
Planning Network Bandwidth for Agent Deployment	2-7
Ports and FQDN Used	2-8
Supported Agent Versions	2-10

Chapter 3: Installation

StellarOne Installation Flow	3-2
StellarOne Onboarding to VMware ESXi	3-2
Prerequisites	3-2

Deploying StellarOne on the VMware ESXi	3-3
StellarOne Onboarding to VMware Workstation	3-12
Prerequisites	3-12
Deploying StellarOne on the VMware Workstation	3-12
StellarOne Onboarding to Windows Hyper-V	3-17
Prerequisites	3-17
Deploying StellarOne to a Hyper-V System	3-18
StellarOne Onboarding to AWS EC2	3-32
Prerequisites	3-32
Deploying StellarOne on AWS EC2	3-33
Opening StellarOne Management Console	3-46
Getting the License File	3-49
OT Intelligent Trust	3-51

Chapter 4: Configuring StellarOne via Command Line Interface (CLI)

Using the StellarOne Command Line Interface (CLI)	4-2
Configuring the IP Address via CLI	4-3
Configuring the Advertise Address via CLI	4-6
Modifying Communication Ports via CLI	4-9
Changing Language Settings via CLI	4-11
Managing Docker Network via CLI	4-13
Resetting Administrator's Password via CLI	4-13

Chapter 5: Upgrade

Supported Upgrade Paths	5-2
Upgrade Methods	5-3
Firmware Upgrade	5-3
Mount Upgrade (VMware)	5-4
Mount Upgrade (Hyper-V)	5-7

Chapter 6: Technical Support

Troubleshooting Resources	6-2
Using the Support Portal	6-2
Threat Encyclopedia	6-2
Contacting Trend Micro and TXOne	6-3
Speeding Up the Support Call	6-4
Sending Suspicious Content to Trend Micro	6-5
Email Reputation Services	6-5
File Reputation Services	6-5
Web Reputation Services	6-5
Other Resources	6-6
Download Center	6-6

Index

Index	IN-1
-------------	------

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.

TXOne Networks always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any TXOne Networks document, please contact us at docs@txone-networks.com.

Preface

This Installation Guide introduces TXOne StellarOne™ and guides administrators through installation and deployment.

Topics in this chapter include:

- *About the Documentation on page vi*
- *Audience on page vii*
- *Document Conventions on page vii*
- *Terminology on page viii*

About the Documentation

TXOne StellarOne™ documentation includes the following:

DOCUMENTATION	DESCRIPTION
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the other documents.
Installation Guide	A PDF document that discusses requirements and procedures for installing StellarOne
Administrator's Guide	A PDF document that discusses StellarOne agent installation, getting started information, and server and agent management
Online Help	HTML files that provide "how to's", usage advice, and field-specific information

DOCUMENTATION	DESCRIPTION
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following websites: https://kb.txone.com/ http://success.trendmicro.com

Audience

TXOne StellarOne™ documentation is intended for administrators responsible for StellarOne management, including agent installation. These users are expected to have advanced networking and server management knowledge.

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output

CONVENTION	DESCRIPTION
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the TXOne StellarOne™ documentation:

TERMINOLOGY	DESCRIPTION
server	The StellarOne console server program
server endpoint	The host where the StellarOne server is installed
agents	The host running the StellarProtect program
managed agents managed endpoints	The hosts running the StellarProtect program that are known to the StellarOne server program
target endpoints	The hosts where the StellarOne managed agents will be installed

TERMINOLOGY	DESCRIPTION
Administrator (or StellarOne administrator)	The person managing the StellarOne server
StellarOne (management) console	The user interface for configuring and managing StellarOne settings and the agents managed by StellarOne
CLI	Command Line Interface
license activation	Includes the type of StellarOne server installation and the allowed period of usage that you can use the application
agent installation folder	<p>The folder on the host that contains the StellarProtect agent files. If you accept the default settings during installation, you will find the installation folder at one of the following locations:</p> <p>C:\Program Files\TXOne\StellarProtect</p> <p>C:\Program Files\TXOne\StellarProtect (Legacy Mode)</p>

Chapter 1

Introduction

This section introduces TXOne StellarOne™ and provides an overview of its features.

Topics in this chapter include:

- *About TXOne Stellar on page 1-2*
- *Key Features and Benefits on page 1-2*
- *What's New on page 1-3*

About TXOne Stellar

TXOne Stellar is a first-of-its-kind OT endpoint protection platform, which includes:

- StellarOne™, the centralized management console designed to streamline administration of both StellarProtect for modernized systems and StellarProtect (Legacy Mode) for legacy systems.
- StellarProtect™, the unified agent with industrial-grade next-generation antivirus and application lockdown endpoint security deployment for modernized OT/ICS endpoints.
- StellarProtect (Legacy Mode)™, for trust-list based application lockdown of legacy and fixed-use OT/ICS endpoints with anti-malware or on-demand AV scan.

Together, TXOne Stellar allows protection for modernized and legacy systems running side-by-side to be coordinated and maintained from the same management console, helping protect businesses against security threats and increase productivity.

Key Features and Benefits

The TXOne StellarOne™ management console provides following features and benefits.

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Dashboard	The web console dashboard provides summarized information about monitored agents. Administrators can check deployed agent status easily, and can generate security reports (Legacy Mode only) related to specific agent activity for specified periods.

FEATURE	BENEFIT
Centralized Agent Management	<p>StellarOne allows administrators to perform the following tasks:</p> <ul style="list-style-type: none"> • Monitor StellarProtect/StellarProtect (Legacy Mode) agent status • Examine connection status • View configurations • Collect agent logs on-demand or by policy (Legacy Mode only) • Turn agent Application Lockdown on or off • Enable or disable agent Device Control • Configure agent Maintenance Mode settings • Update agent components • Initialize the Approved List • Deploy agent patches • Add trusted files and USB devices • Export agents' information • Import/Export agents' configuration settings or Approved List (Legacy Mode only)
Centralized Event Management	<p>On endpoints protected by StellarProtect/StellarProtect (Legacy Mode) agents, administrators can monitor status and events, as well as respond when files are blocked from running. StellarOne provides event management features that let administrators quickly know about and take action on the blocked-file events.</p>
Server Event Auditing	<p>Operations performed by StellarOne web console accounts are logged. StellarOne records an operating log for each account, tracking who logs on, who deletes event logs, and more.</p>

What's New

TXOne StellarOne™ 2.2 provides following new features and enhancements.

TABLE 1-2. What's New in TXOne StellarOne™ 2.2

FEATURE	BENEFIT
Enhanced dashboard	Adds one type of blocked events, Malware Scan, to be displayed in the Blocked Event History widget on the dashboard.
Adding Lockdown features for StellarProtect	You can now remotely configure the sub-features and trusted hash values settings of Application Lockdown for StellarProtect agents.
Agent's User password management	In addition to existing Agent's Administrator password, you can also manage Agent's User password remotely from StellarOne web console.
New update command button for StellarProtect - Check Connections	This new button for StellarProtect allows you to check connections between the selected endpoints and StellarOne.
New update command button - Apply Policies	This new button allows you to apply policies immediately to the selected endpoints.
Policy refresh interval	You can now set how often you want StellarOne to apply policies to the managed endpoints.
Performance settings for Scheduled Scan and Scan Now	These settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources under different circumstances.
Time sync with NTP	In addition to manually modifying StellarOne system time, the option to configure StellarOne for automatically synchronizing system time with an NTP server is available now.
Enhanced email security	Provides protocol command options such as STARTTLS and SMTPS to secure transmissions of email notifications of warning or outbreak events.
Enhanced CLI command	Add a new vShell command for configuring StellarOne FQDN setting to allow communication with agents or SSO (Single Sign-On) login

Chapter 2

Installation Planning

This section shows how to plan for TXOne StellarOne installation.

Topics in this chapter include:

- *System Requirements on page 2-2*
- *Hardware Requirements on page 2-2*
- *Planning Network Bandwidth for Agent Deployment on page 2-7*
- *Ports and FQDN Used on page 2-8*

System Requirements

TXOne StellarOne™ is packaged in an Open Virtual Appliance (OVA) or Virtual Hard Disk v2 (VHDX) format. The above-mentioned package files respectively apply to different hypervisors.

Supported Hypervisors (OVA file)

- VMware ESXi 6.5 or above
- VMware Workstation 16 Pro or above

Supported Hypervisors (VHDX file)

- Windows Server 2019, Hyper-V Manager Windows 10 or above



Note

For StellarOne deployed from AMI on a AWS EC2 instance, refer to [Deciding an Instance Type for StellarOne on AWS EC2 Platform on page 2-6](#) for more details.

Supported Browser

- Google Chrome 87 or above
- Microsoft Edge 79 or above
- Mozilla Firefox 78 or above

Minimum Supported Resolution

- 1366x768

Hardware Requirements

Hardware requirements vary depending on the number of agents and logs that will be configured and retained. Please refer to the sections below for determining the optimal number of agents that your StellarOne server deployment can manage on different platforms.

Hardware Requirements for VMware System

Refer to the tables below for determining the optimal number of agents that your StellarOne server deployment can manage on the VMware system.

TABLE 2-1. Sizing Table for VMware

MAX. NO. OF AGENTS	MIN NO. OF VCORES	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (RECOMMENDED)
30,000	8	32 GB	25 GB	100 GB
20,000	8	16 GB		100 GB
15,000	4	16 GB		50 GB
10,000	4	16 GB		50 GB
5,000	4	12 GB		50 GB
1,000	4	12 GB		50 GB
500	4	12 GB		50 GB

The external disk space varies depending on the number of logs planned to be stored, as shown in the table below.

TABLE 2-2. No. of Logs versus Disk Space

NO. OF LOGS	DISK SPACE
90,000,000	150 GB
60,000,000	100 GB
30,000,000	50GB

To determine the ideal specifications for your external HDD, please refer to the following formula:

[Output log numbers for a single agent per day] x [Log storage period in days] x [Total number of agents]

Example: External HDD size for 20,000 agents

- Output log numbers for a single agent per day: 100 events
- Log storage period in days: 30 days
- Total number of agents: 20,000 agents

Total number of logs: $100 \times 30 \times 20000 = 60,000,000$ Logs

In this case, it would be required to prepare 100 GB for storage space.



Note

1. The StellarOne requires one external disk with at least 50 GB minimum space for initialization and booting process.
 2. The external disk is used to store the system configurations and event logs. You may reuse the external disk of a terminated StellarOne instance if you want to migrate the previous configurations and logs to a new StellarOne instance.
 3. Please also take the network bandwidth into consideration when planning for agent deployment. Refer to [Planning Network Bandwidth for Agent Deployment on page 2-7](#) for more details.
-

Hardware Requirements for Hyper-V System

Refer to the tables below for determining the optimal number of agents that your StellarOne server deployment can manage on the Hyper-V system.

TABLE 2-3. Sizing Table for Hyper-V

MAX. NO. OF AGENTS	MIN. NO. OF CPU	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (RECOMMENDED)
30,000	10	24 GB	25 GB	100 GB
20,000	8	16 GB		100 GB
15,000	8	16 GB		50 GB
10,000	8	16 GB		50 GB
5,000	8	16 GB		50 GB
1,000	4	16 GB		50 GB
500	4	8 GB		50 GB

TABLE 2-4. No. of Logs versus Disk Space

NO. OF LOGS	DISK SPACE
300,000,000	500 GB
180,000,000	300 GB
90,000,000	150 GB
30,000,000	50GB

**Note**

1. The StellarOne requires one external disk with at least 50 GB minimum space for initialization and booting process.
2. The external disk is used to store the system configurations and event logs. You may reuse the external disk of a terminated StellarOne instance if you want to migrate the previous configurations and logs to a new StellarOne instance.
3. Please also take the network bandwidth into consideration when planning for agent deployment. Refer to [Planning Network Bandwidth for Agent Deployment on page 2-7](#) for more details.

Deciding an Instance Type for StellarOne on AWS EC2 Platform

Refer to the tables below for determining the optimal number of agents that your StellarOne server deployment can manage on the AWS EC2 platform.



Note

Please refer to [Amazon EC2 Instance Types](#) for specifications of the instance types.

TABLE 2-5. Sizing Table for AWS EC2

MAX. NO. OF AGENTS	MIN. NO. OF CPU	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (RECOMMENDED)
30,000	10	24 GB	25 GB	100 GB
20,000	8	16 GB		100 GB
15,000	8	16 GB		50 GB
10,000	8	16 GB		50 GB
5,000	8	16 GB		50 GB
1,000	4	16 GB		50 GB
500	4	8 GB		50 GB

TABLE 2-6. No. of Logs versus Disk Space

NO. OF LOGS	DISK SPACE
300,000,000	500 GB
180,000,000	300 GB
90,000,000	150 GB
30,000,000	50GB

**Note**

1. The StellarOne requires one external disk with at least 50 GB minimum space for initialization and booting process.
2. The external disk is used to store the system configurations and event logs. You may reuse the external disk of a terminated StellarOne instance if you want to migrate the previous configurations and logs to a new StellarOne instance.
3. Please also take the network bandwidth into consideration when planning for agent deployment. Refer to [Planning Network Bandwidth for Agent Deployment on page 2-7](#) for more details.

Planning Network Bandwidth for Agent Deployment

Please take network bandwidth into consideration when planning for agent deployment. See below as an example of calculating the bandwidth required to support the number of agents planned to deploy.

Basic concept:

Total available bandwidth / Deployment task size = How many agents can be deployed at one task

Currently, there are 3 types of StellarOne deployment tasks:

- Incremental Pattern Update: works for agent pattern version no less than server version for two weeks, which requires about less than 5 MB
- Full Pattern Update: works for agent pattern version that's already exceeded two-week duration compared to server/update source, which requires about 80 MB
- Agent Remote Patch: update with the remote agent deployment upgrade package, which requires about 70 MB

The following tables illustrate the number of agents to be deployed on condition that the deployment takes 5 minutes and requires 50% of network

bandwidth, as well as the recommended policy refresh interval regarding the number of agents managed.

TABLE 2-7. Agent Deployment Plan

TOTAL BANDWIDTH / DEPLOYMENT TASK	NO. OF AGENTS DEPLOYED			
	10 MBPS	100 MBPS	1000 MBPS	10 GBPS
Incremental Pattern Update	38	375	3750	37500
Full Pattern Update	2	23	234	2344
Agent Remote Patch	3	27	268	2679

TABLE 2-8. Policy Refresh Interval vs No. of Agents Managed

POLICY REFRESH INTERVAL	NO. OF AGENTS MANAGED
5 minutes	5000
10 minutes	10000
20 minutes	20000
60 minutes	60000

Ports and FQDN Used

The following table shows the ports used by the StellarOne server.

TABLE 2-9. Ports and FQDN Used

FROM	TO	OPEN PORT	FQDN	FUNCTION
StellarProtect	StellarOne	9443, 443	-	StellarOne's listening port for StellarProtect
StellarProtect (Legacy Mode)	StellarOne	8000, 443	-	StellarOne's listening port for StellarProtect (Legacy Mode)
StellarOne	StellarProtect	14336	-	StellarProtect's listening port
StellarOne	StellarProtect (Legacy Mode)	14336	-	StellarProtect (Legacy Mode)'s listening port
StellarOne	License (PR) Server	443	odc.cs.txone-networks.com	StellarOne connects to global server port for license verification and renewal through HTTPS
Browser	StellarOne Web	443	-	StellarOne's listening port for web access through HTTPS
StellarOne	Active Update Server	443	https://ttau.cs.txone.com/protect https://ttau.cs.txone.com/enforce	StellarOne connects to global server port for the Stellar Active Update through HTTPS

**Note**

The following ports are reserved for StellarOne private service usage and are not allowed to use for other purposes.

TABLE 2-10. StellarOne Occupied Ports

STELLARONE OCCUPIED PORT	PORT
StellarProtect (Legacy Mode) Default Port	8000
StellarProtect Default Port	9443
SSH	22
NTP	123
Web	443
StellarOne Internal Service	25
	7590
	8888
	8889
	8999
	9091

Supported Agent Versions

The following table indicates the StellarOne supported agent versions.

**WARNING!**

- Before upgrading, please check the table below to identify the StellarOne supported agent versions.
- Please upgrade the StellarOne server first before you upgrade the agents.

TABLE 2-11. Supported Agent Version

SERVER VERSION		AGENTS VERSION	
STELLARONE	STELLARPROTECT	STELLARPROTECT (LEGACY MODE)	STELLARENFORCE
2.2	2.2 and earlier versions	1.5 and earlier versions	N/A
2.1	2.1 and earlier versions	1.4 and earlier versions	N/A
2.0	2.0 and earlier versions	1.3 and earlier versions	1.3 and earlier versions
1.2	1.2 and earlier versions	N/A	1.2 and earlier versions
1.1	1.1 and earlier version	N/A	1.1 and earlier version
1.0	1.0	N/A	1.0

**Important**

Please try to keep or upgrade the managed agents in or to the corresponding StellarOne major release version as indicated in the table above. Though StellarOne provides backward compatibility to support agents with earlier version, new features or enhanced functionality should not be applicable on some agents with earlier versions.



Note

The StellarEnforce was renamed StellarProtect (Legacy Mode) upon the release of version 1.3.

Chapter 3

Installation

This chapter guides you through TXOne StellarOne installation. StellarOne is packaged in an Open Virtual Appliance (OVA) or Virtual Hard Disk v2 (VHDX) format and supports 4 types of platforms: VMware ESXi, VMware Workstation, Windows Hyper-V systems, and AWS EC2.

Topics in this chapter include:

- *StellarOne Installation Flow on page 3-2*
- *StellarOne Onboarding to VMware ESXi on page 3-2*
- *StellarOne Onboarding to VMware Workstation on page 3-12*
- *StellarOne Onboarding to Windows Hyper-V on page 3-17*
- *StellarOne Onboarding to AWS EC2 on page 3-32*
- *Opening StellarOne Management Console on page 3-46*

StellarOne Installation Flow

Installing StellarOne web console requires performing the following steps:

Procedure

1. Deploy a StellarOne instance on VMware ESXi or Workstation, Windows Hyper-V, or AWS EC2 platform.
 2. Add an external hard disk with at least 50 GB of space to the StellarOne instance.
 3. Log on StellarOne web console to set up the administrator's account.
 4. Log on StellarOne web console to activate the product license and set time properties.
 5. Configure settings such as IP address and communication ports.
-

StellarOne Onboarding to VMware ESXi

This section describes how to deploy StellarOne to the VMware ESXi system.

Prerequisites

- The OVA packages provided by TXOne must be available and accessible to VMwareESXi.
- VMware ESXi 6.5 or above is required.
- The necessary networks have been properly created for ESXi.
- An external disk with at least 50 GB.

Deploying StellarOne on the VMware ESXi

Below section details procedures of deploying StellarOne from an OVA file to the VMware ESXi system.

Procedure

1. Log in to the VMware vSphere web client
2. Under **Navigator**, click **Host > Create/Register VM**.

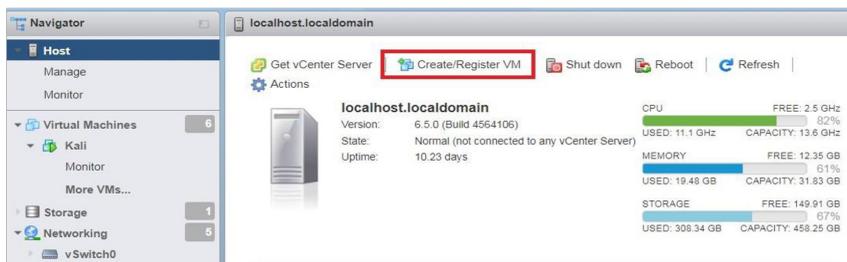


FIGURE 3-1. Navigator

3. Select **Deploy a virtual machine from an OVF or OVA file**.

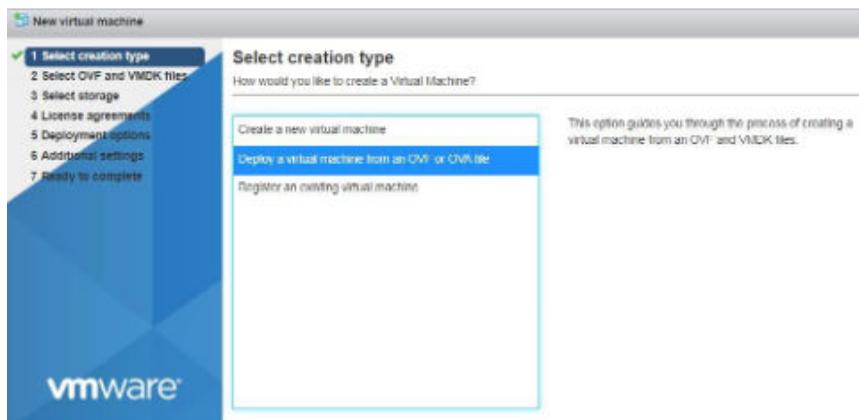


FIGURE 3-2. Select creation type

4. Input a name for your new StellarOne instance and then select the StellarOne disk image to upload.

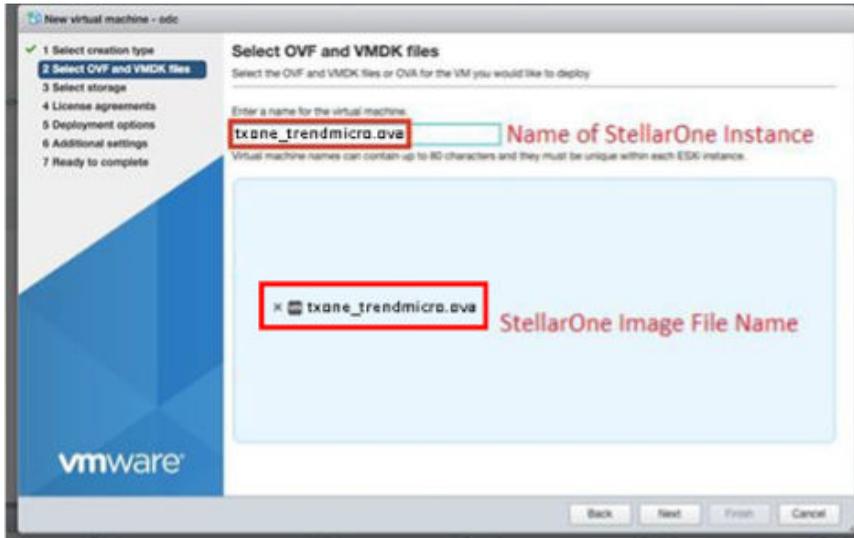


FIGURE 3-3. Select OVF and VMDK files

5. Choose a storage location for the StellarOne instance.

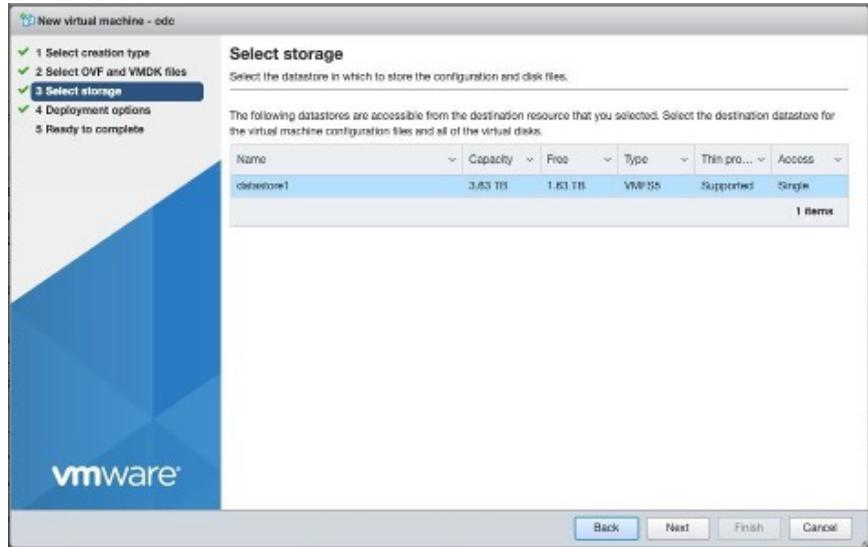


FIGURE 3-4. Select storage

6. Select deployment options.

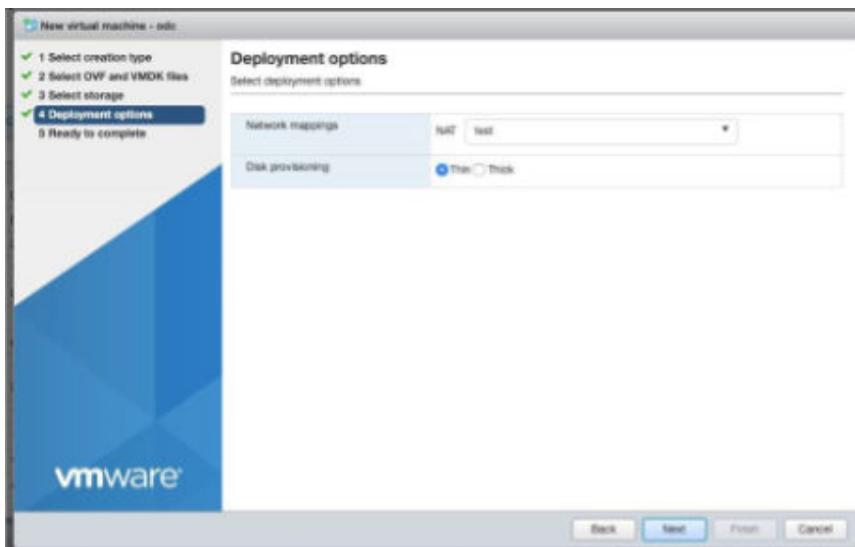


FIGURE 3-5. Deployment options

7. When you see **Ready to complete**, click **Finish** to start the deployment.

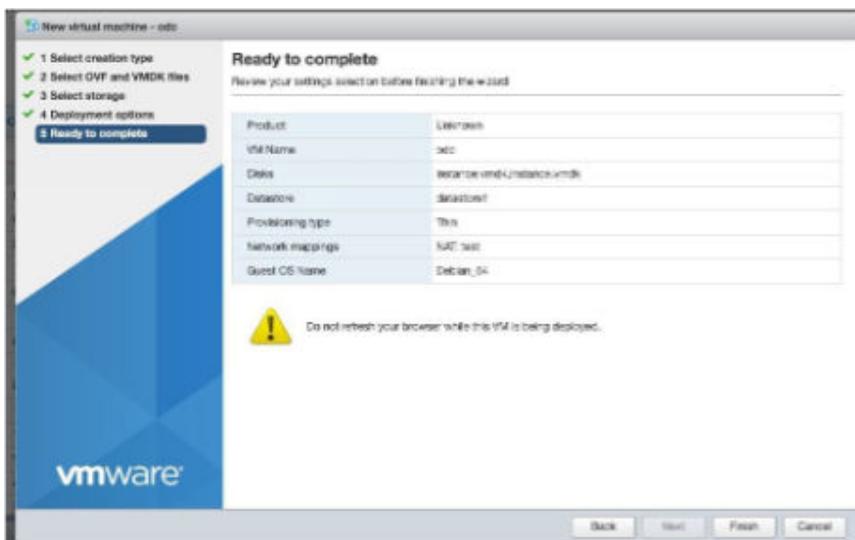


FIGURE 3-6. Ready to complete

8. Under the **Recent Tasks** pane, you will see a progress bar indicating the StellarOne image is being uploaded. Please wait until the upload is finished.
9. Add an external disk with at least 50 GB of capacity to the StellarOne instance.
 - a. Close the StellarOne instance if it is open.
 - b. The external disk capacity is determined by the number of logs to be stored, as shown in the table below.

No. of Logs	Disk Capacity
90,000,000	150 GB
60,000,000	100 GB
30,000,000	50 GB

To determine the ideal specifications for your external HDD, refer to the following formula:

[Output log numbers for a single agent per day] x [Log storage period in days] x [Total number of agents]

For example, to calculate the external HDD capacity required for 20,000 agents on the assumption that:

- Output log number for a single agent per day: 100 events
- Log storage period in days: 30 days
- Total number of agents: 20,000 agents

The total number of logs: $100 \times 30 \times 20,000 = 60,000,000$ logs

In this case, it is required to prepare an external disk with capacity of 100 GB for storage space.

- c. Follow the procedures to add the external disk: **Actions > Edit Settings > Add Hard Disk > New hard disk > Save**

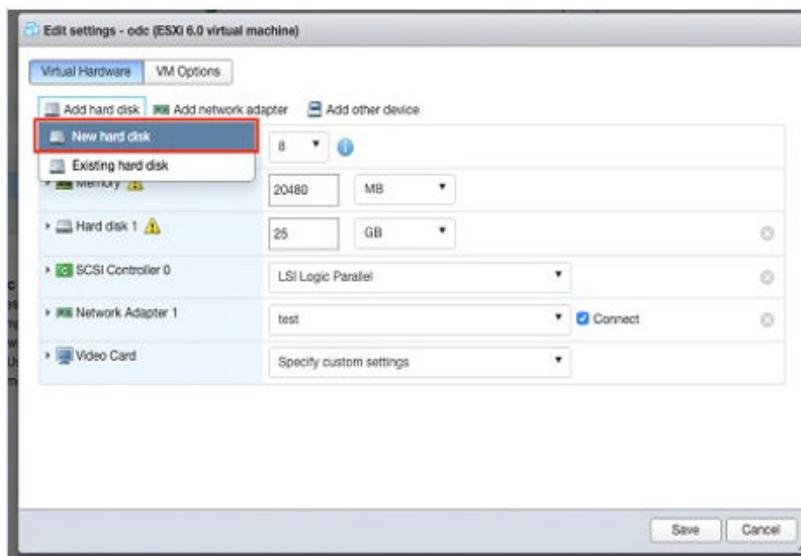


FIGURE 3-7. Edit settings - New hard disk

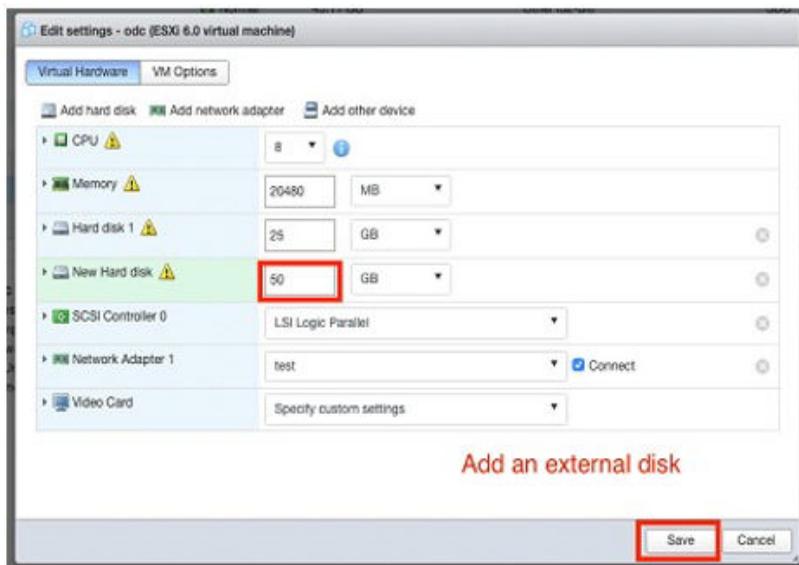


FIGURE 3-8. Edit settings - New hard disk capacity

- d. If you need to increase the number of logs StellarOne can store, follow the procedures.
 - i. Shut down StellarOne
 - ii. Increase the external disk capacity to fit the maximum log requirements
 - iii. Restart the StellarOne instance. After that, the storage space available for StellarOne log files will be expanded.
- e. If you want to migrate the existing StellarOne settings to the newly launched VM, please refer to [System Migration on page 5-4](#).



- Note**
- StellarOne requires one external disk with minimum capacity above 50GB; otherwise, StellarOne will not finish initialization and will not complete the boot process.
 - The external disk is used to store the system configurations and event logs. You may attach the external disk of a terminated StellarOne instance here instead of adding a new disk if you want to migrate the previous configurations and logs to a new instance.

10. Turn on the VM.



FIGURE 3-9. VM turned on

- (Optional) Adjust your StellarOne instance to use proper resource configurations based on the default setting (8-core CPU, 16 GB Memory).
 - Shut down the StellarOne instance and click **Edit**. The **Edit Settings** window will appear.
 - Configure the number of CPU cores.

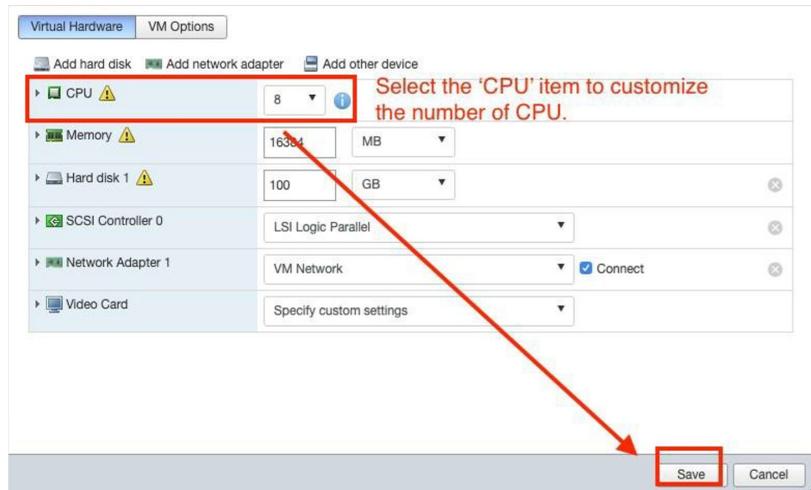


FIGURE 3-10. Select number of CPU

- c. Configure the amount of Memory.

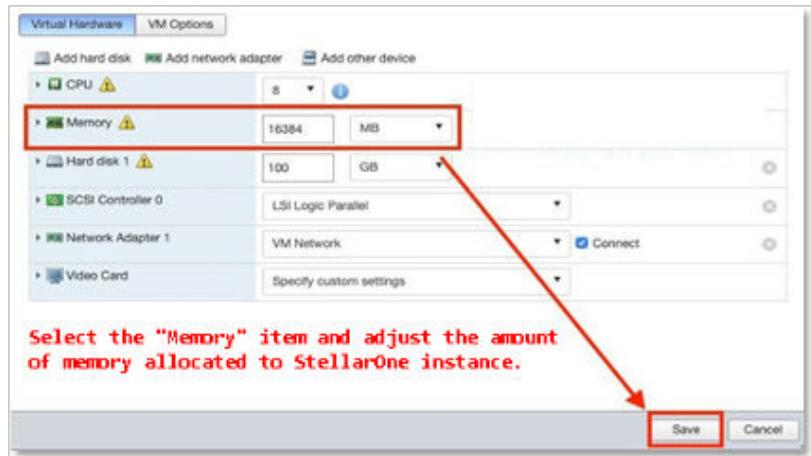


FIGURE 3-11. Configure Memory

**Note**

Refer to the [Hardware Requirements for VMware System on page 2-3](#) to determine CPU and memory requirements for agent deployment.

- d. Boot the StellarOne instance.
-

StellarOne Onboarding to VMware Workstation

This section describes how to deploy StellarOne to the VMware Workstation system.

Prerequisites

- The OVA packages provided by TXOne must be available and accessible to VMware Workstation.
- VMware Workstation 16 Pro or above is required.
- The necessary networks have been properly created for VMware Workstation.
- An external disk with at least 50 GB.

Deploying StellarOne on the VMware Workstation

Below section details procedures of deploying StellarOne from an OVA file to the VMware Workstation.

Procedure

1. Start the VMware Workstation and click **File** on the menu bar.
2. Select **Open** to import the StellarOne VM image file (*.ova).
3. Select the StellarOne VM image file from your localhost file path and click **Import**.

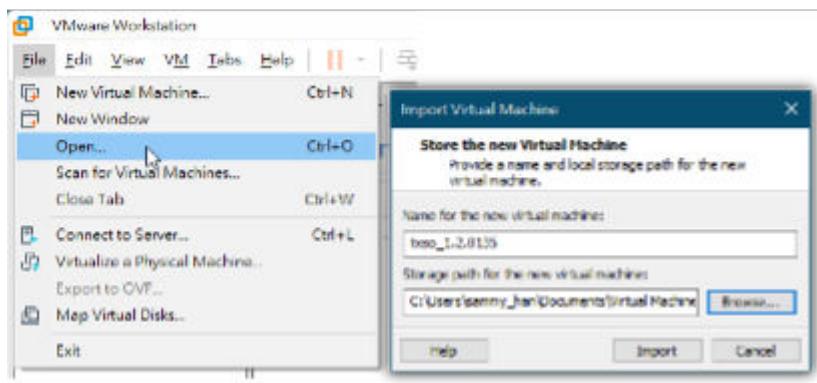


FIGURE 3-12. Import File to VMware Workstation

4. Check the detailed VM information of the imported StellarOne VM.

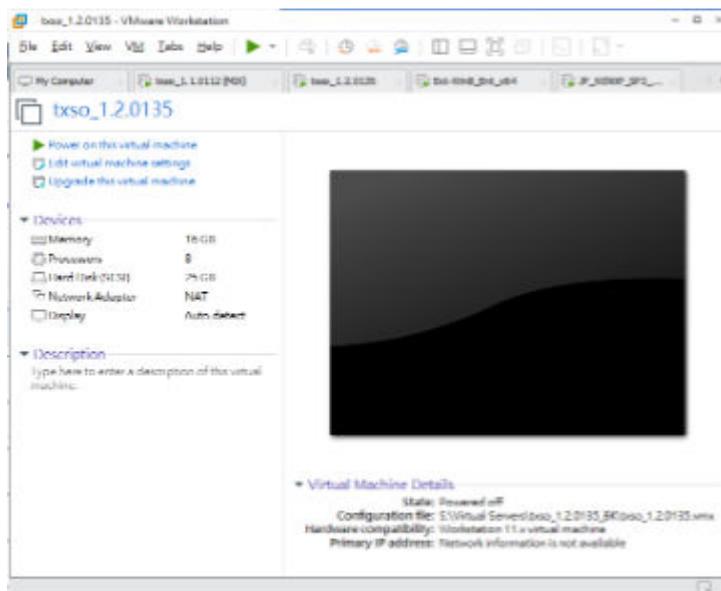
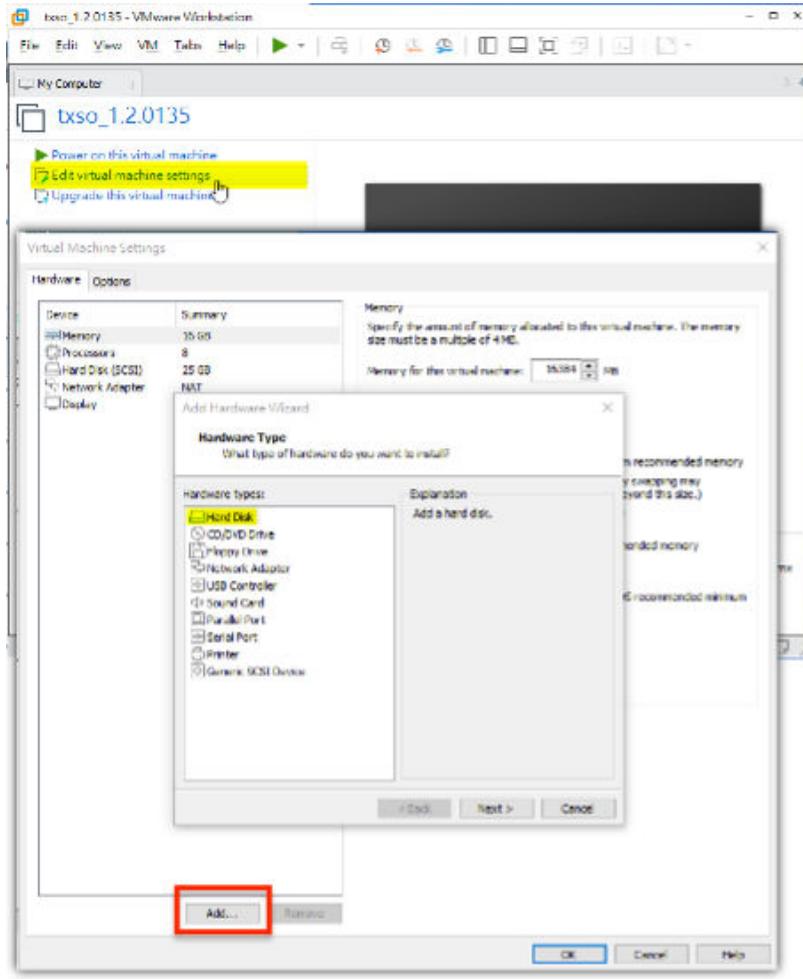


FIGURE 3-13. StellarOne VM Details

5. Add an extra hard disk.
 - a. Click **Edit virtual machine settings**.
 - b. Click **Add... > Hard Disk** for **Hardware Type**

**FIGURE 3-14. Add a Hard Disk**

- c. Select **SCSI (Recommended)** as the disk type.
- d. Select **Create a new virtual disk** as the disk item.
- e. Set **Maximum disk size (GB)** as 50.

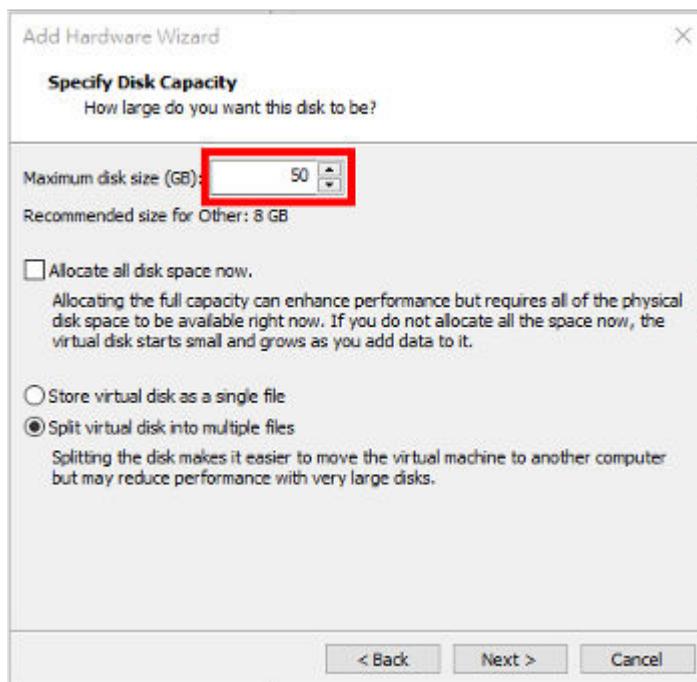


FIGURE 3-15. Add Hardware Wizard

- f. Select path to store the disk and click **Finish**. The new external disk will be created in **Virtual Machine Settings**.

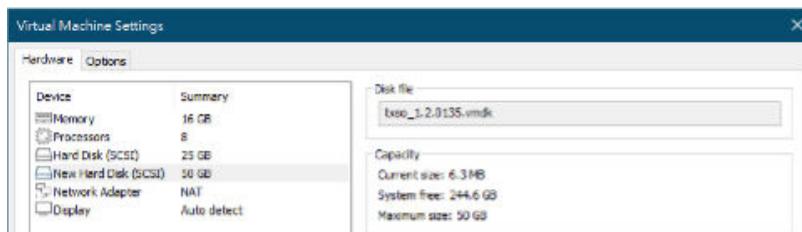


FIGURE 3-16. Hardware Overview in Virtual Machine Settings

6. (Optional) Adjust your StellarOne instance to use proper resource configurations based on the default settings (8 CPU cores, 16 GB memory).
 - a. Click **Edit virtual machine settings**.
 - b. Specify the amount of **Memory** allocated to the StellarOne instance.

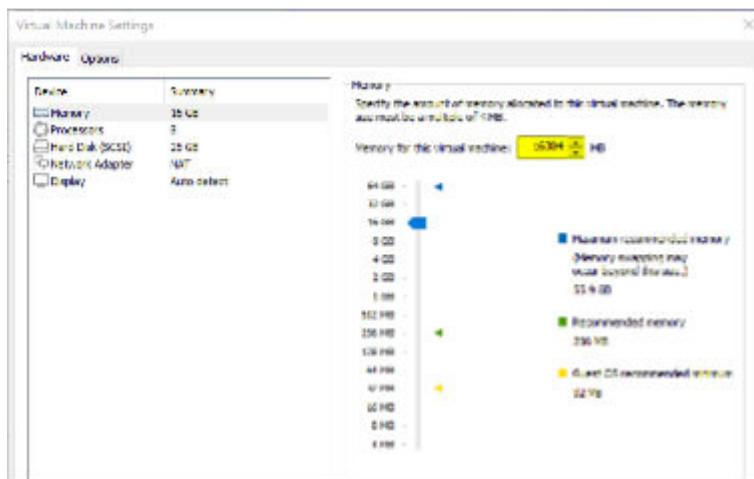


FIGURE 3-17. Memory for Virtual Machine

7. (Optional) Change the network adapter settings from **NAT** to **Bridged**.
 - a. Right-click the StellarOne VM icon and select **Settings**

- b. Select **Network Adapter** and change the default setting from **NAT** to **Bridged** if necessary.

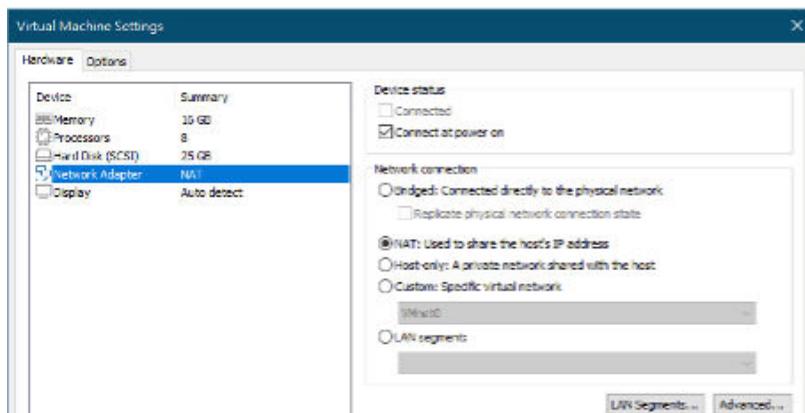


FIGURE 3-18. Network Adapter in Virtual Machine Settings

8. Boot the StellarOne VM, and the StellarOne instance will start.

StellarOne Onboarding to Windows Hyper-V

This section describes how to deploy StellarOne to the Windows Hyper-V system.

Prerequisites

- The VHDX packages provided by TXOne must be available and accessible to Windows Hyper-V.
- Windows Server 2019, Hyper-V Manager Windows 10 or above.
- The necessary networks have been properly created for Windows Hyper-V.

- An external disk with at least 50 GB.

Deploying StellarOne to a Hyper-V System

Below section details procedures of deploying StellarOne from a VHDX File to a Hyper-V system.

Procedure

1. Launch **Hyper-V Manager**

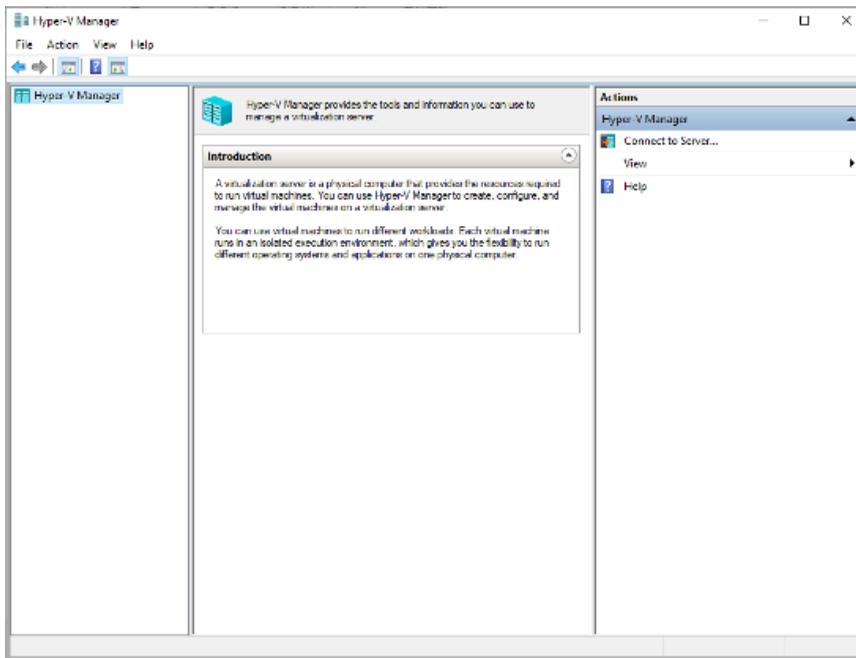


FIGURE 3-19. Hyper-V Manager

2. Under **Actions**, click **New > Virtual Machine**.
3. The **New Virtual Machine Wizard** appears, click **Next**.

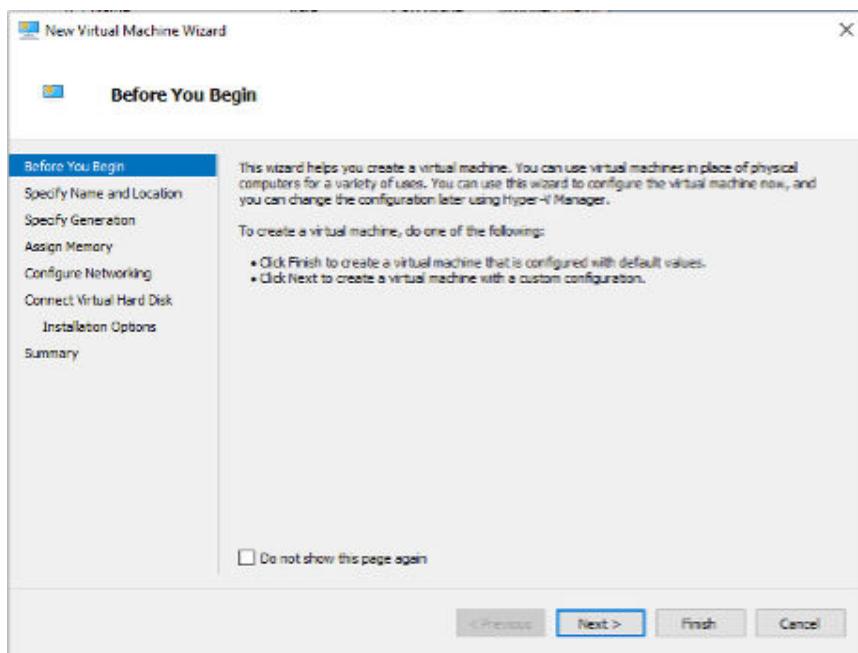


FIGURE 3-20. New Virtual Machine Wizard: Before You Begin

4. Under **Specify Name and Location**, type a name for your new virtual machine.

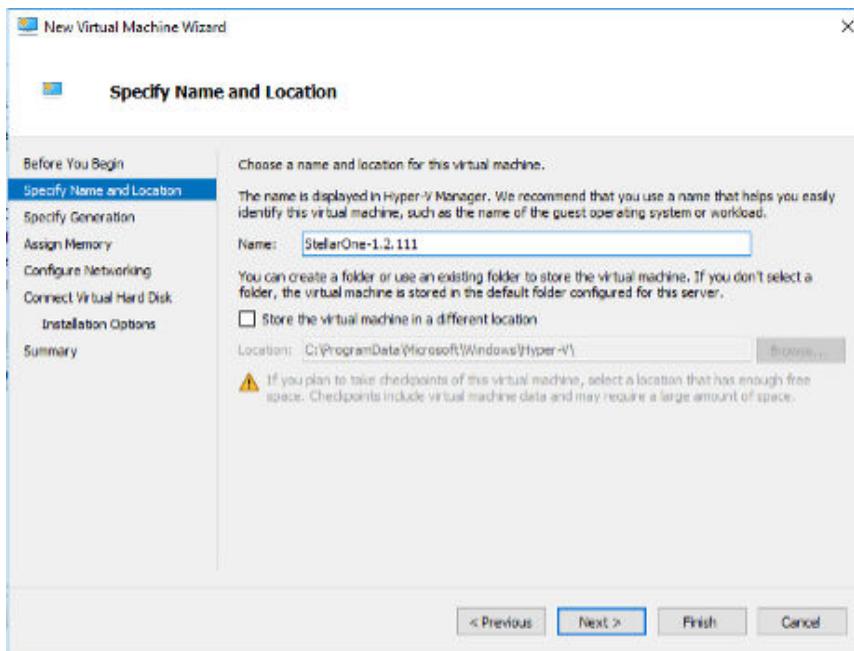


FIGURE 3-21. New Virtual Machine Wizard: Specify Name and Location

5. Under **Specify Generation**, select **Generation 1**.

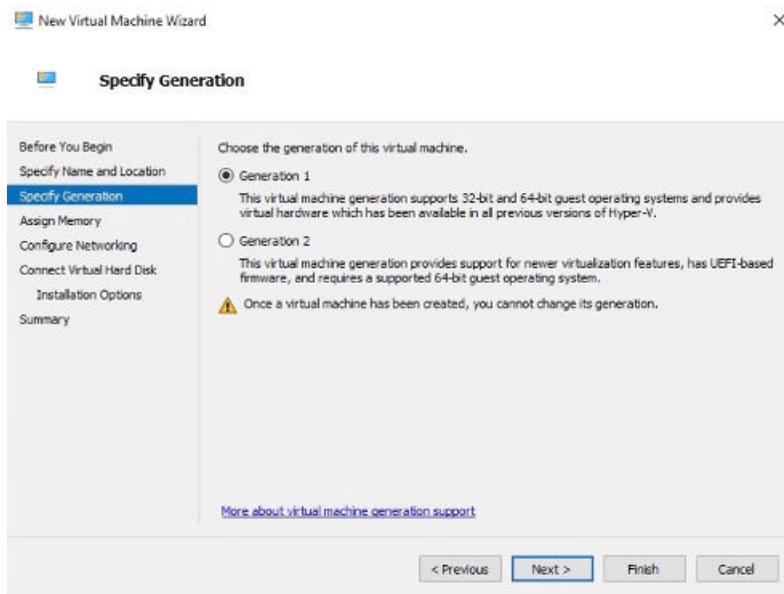


FIGURE 3-22. New Virtual Machine Wizard: Specify Generation

6. Under **Assign Memory**, allocate memory for the new virtual machine.

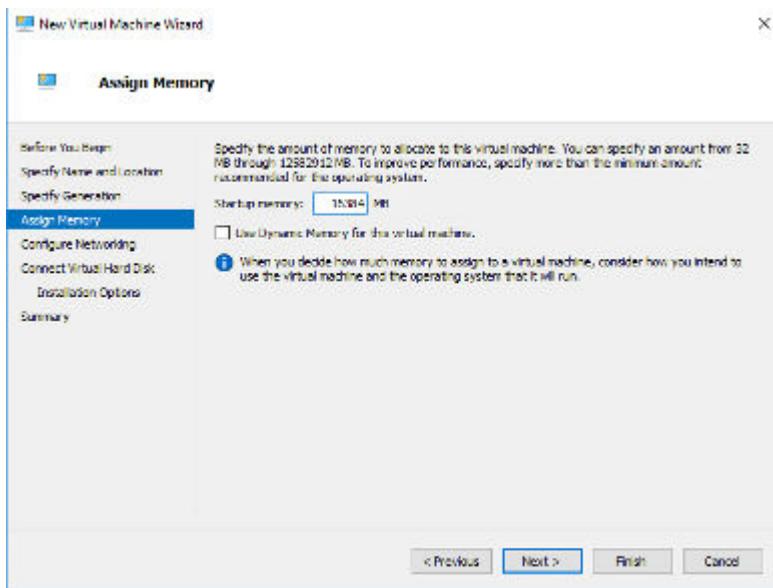


FIGURE 3-23. Assign Memory for Virtual Machine



Note

StellarOne requires minimum memory of 8 GB.

7. Configure the VM's network settings.

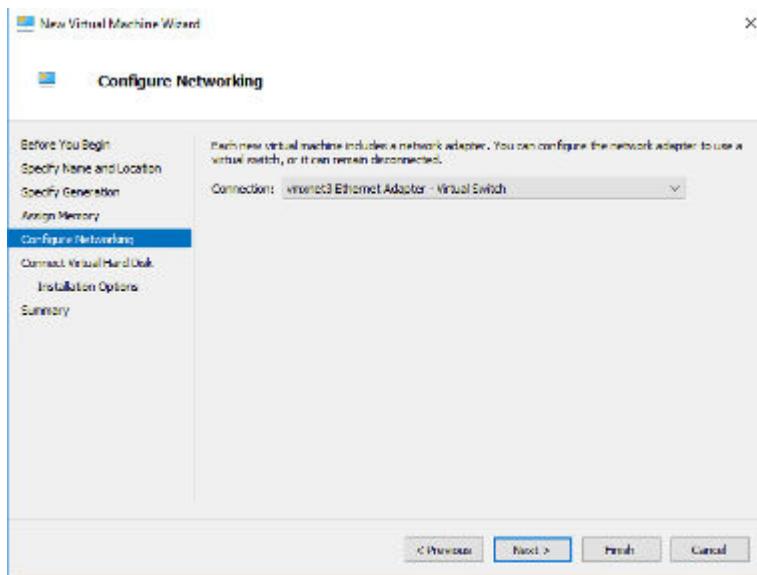


FIGURE 3-24. Configure Networking for Virtual Machine

8. Select a virtual hard disk (select the StellarOne .vhd file)

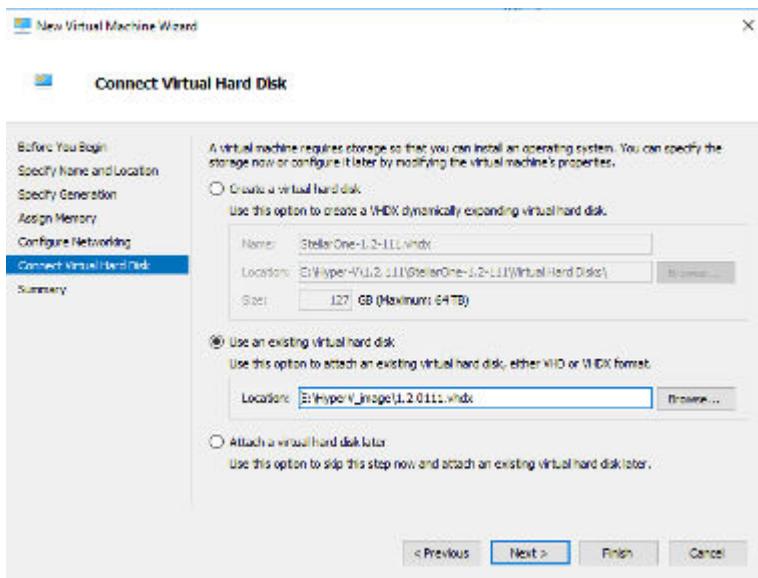


FIGURE 3-25. Connect Virtual Hard Disk

9. Check your settings and then click **Finish**.

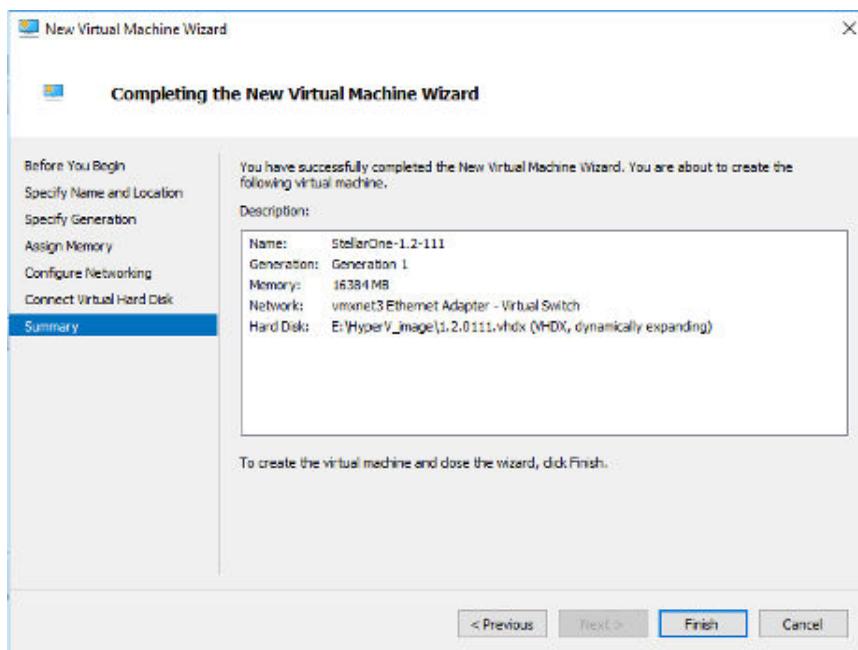


FIGURE 3-26. Completing the New VM Wizard

10. Add a new disk for the virtual machine.



Note

Make sure the previous StellarOne instance is turned off.

Virtual Machines						
Name	State	CPU Usage	Assigned Memory	Uptime	Status	Co
StellarOne-1.2-111	Off					9.0

FIGURE 3-27. State of previous StellarOne is off

- a. Select **Virtual Machine**, right click **Menu** and then select **Settings**.
- b. Select **Hard Drive**, and then click **Add**.

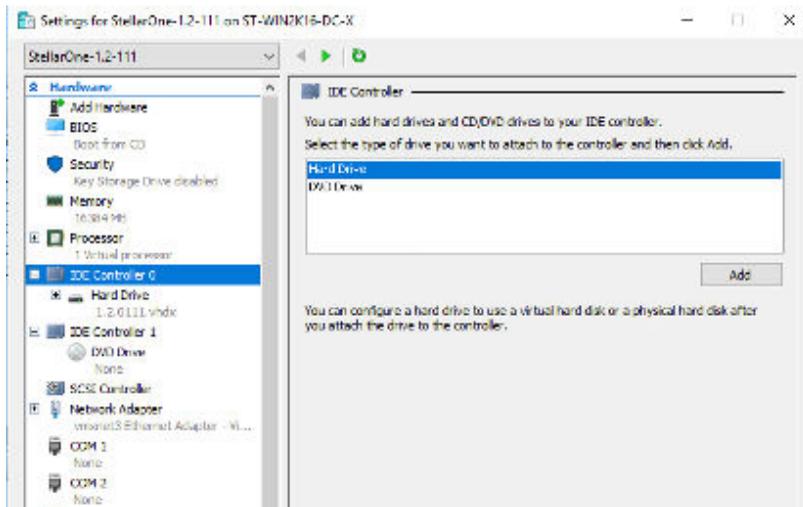


FIGURE 3-28. Settings for StellarOne - 1

- c. Click **New**.

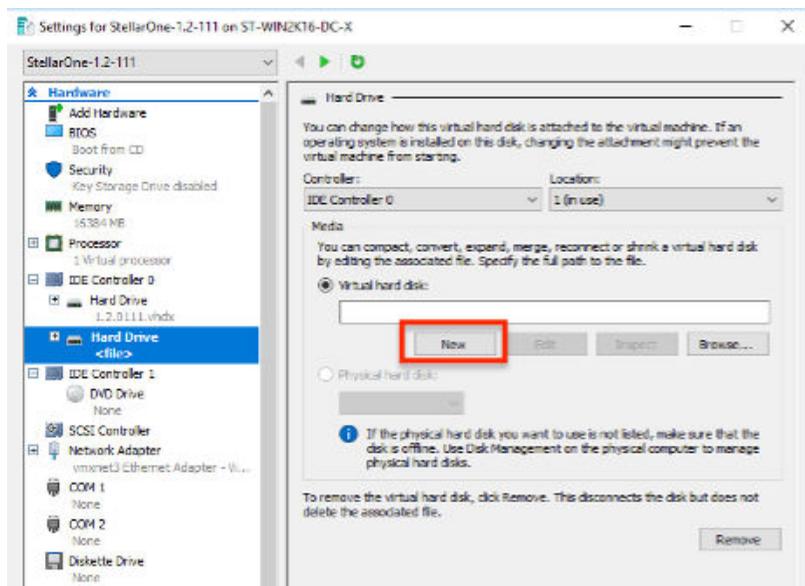


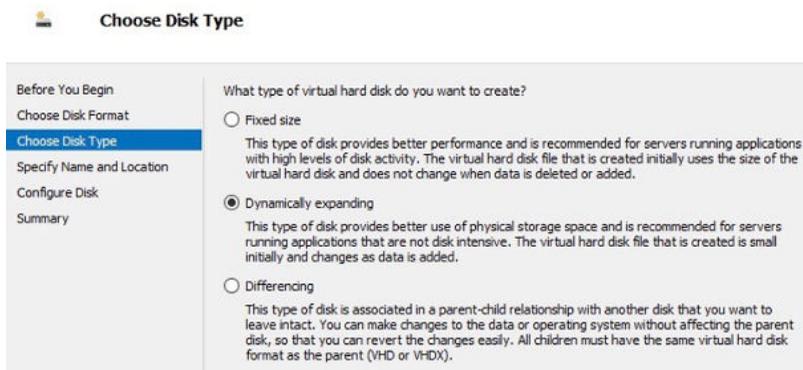
FIGURE 3-29. Settings for StellarOne - 2

- d. Under **Choose Disk Format**, select **VHDX** as the disk format.

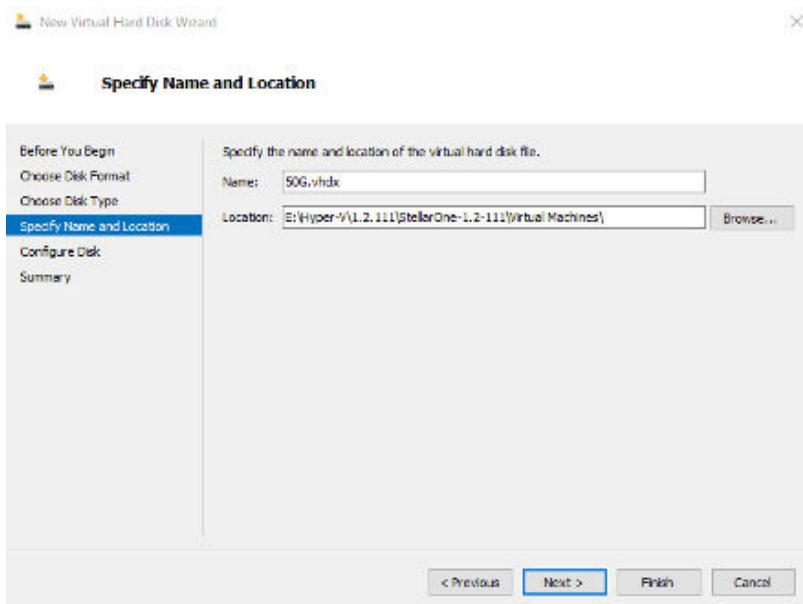


FIGURE 3-30. Choose Disk Format

- e. Under **Choose Disk Type**, select **Dynamically expanding** as the disk type.

**FIGURE 3-31. Choose Disk Type**

- f. Specify name and location for the virtual hard disk file.

**FIGURE 3-32. Specify Name and Location**

- g. Configure disk size.

**Note**

Refer to the *Sizing Table for Hyper-V System on page 2-4* to determine the proper disk size for StellarOne.

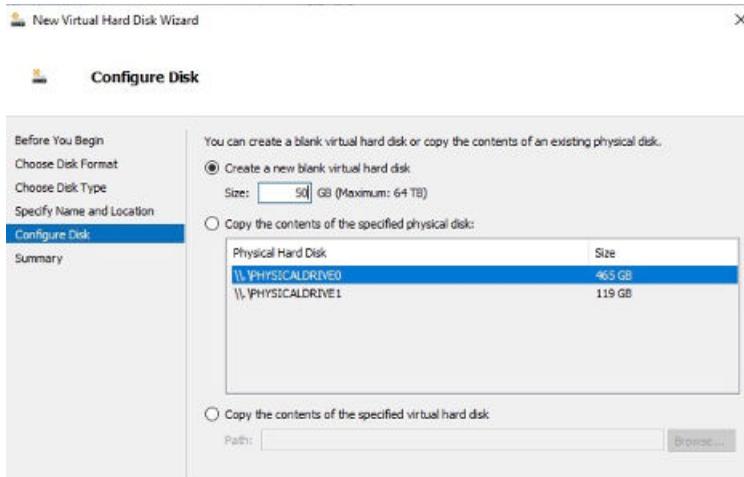


FIGURE 3-33. Configure Disk for StellarOne

- h. Click **Finish**.

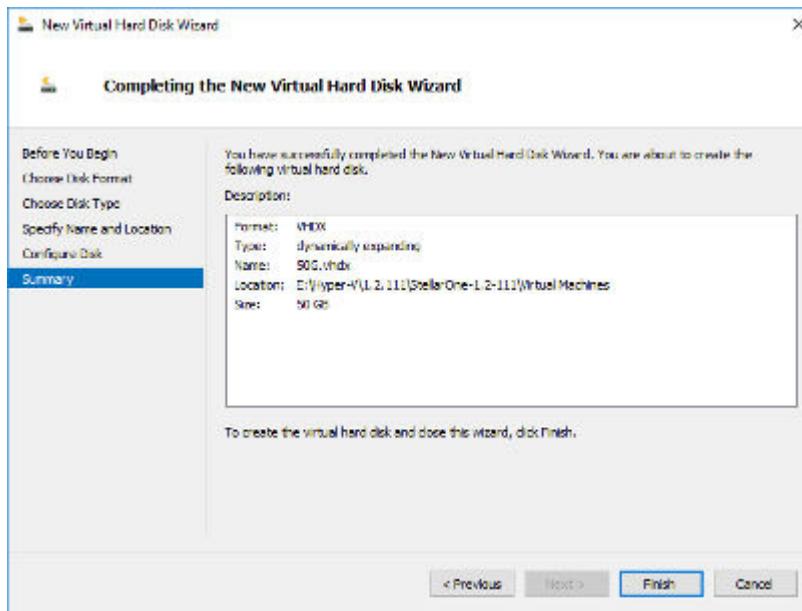


FIGURE 3-34. Completing the New Virtual Hard Disk Wizard

11. (Optional) Refer to [Hardware Requirements for Hyper-V System on page 2-4](#) to determine CPU and memory requirements for agent deployment and corresponding StellarOne configuration and resource allocation. It is advisory to at least adopt the default settings (4 CPU cores, 16 GB Memory).
 - a. Shut down the StellarOne instance. Select and right click the instance, and then click **Settings**.

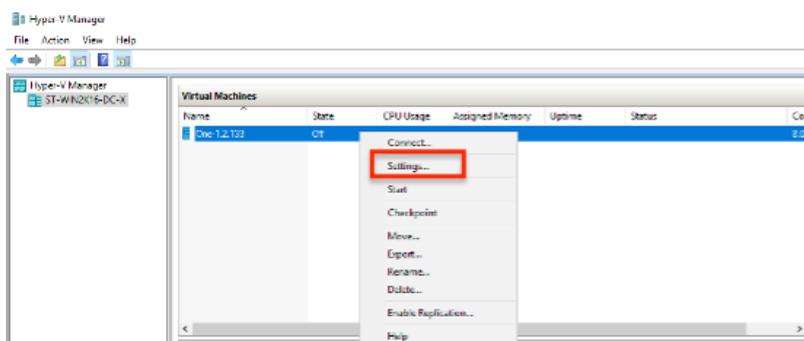


FIGURE 3-35. StellarOne Configuration

- b. Under **Processor**, configure the number of virtual processors and resource control settings.

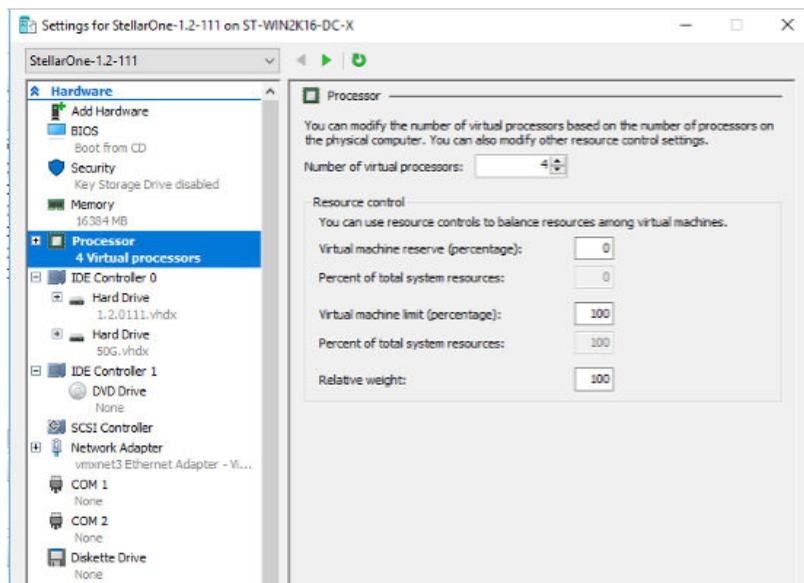


FIGURE 3-36. Processor Settings in StellarOne Configuration

- c. Under **Memory**, configure the amount of memory.

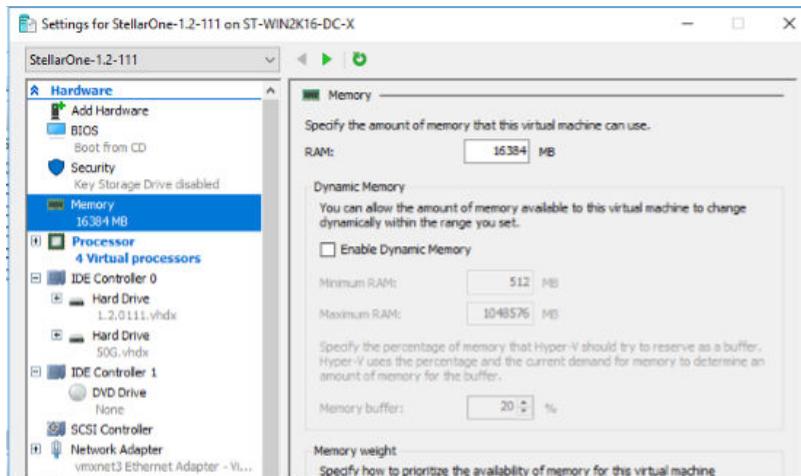


FIGURE 3-37. Memory Settings in StellarOne Configuration

- d. Boot the StellarOne instance.

StellarOne Onboarding to AWS EC2

This section describes how to deploy StellarOne on the AWS EC2 platform.

Prerequisites

- An AWS account is required
- StellarOne for AWS supports only BYOL (Bring Your Own License)
- An external disk (EBS) with at least 50 GB.



Note

Please contact your support provider for the BYOL license.

Deploying StellarOne on AWS EC2

Below section details procedures of deploying StellarOne from BYOL AMI on the AWS EC2 platform.

Procedure

1. Go to the **AWS Marketplace** homepage.
2. Enter the search string such as TXOne or StellarOne in the search bar and then run the search.
3. Click the search result and read the product information carefully before proceeding to the subscription process.
4. After accepting the terms and conditions for using StellarOne, choose the **Fulfillment option**, **Software version**, and **Region** to launch StellarOne.
5. Select **Launch through EC2** as the launch action.

The screenshot shows the AWS Marketplace interface for the product 'TxOne StellarOne Management Console'. The page title is 'Launch this software'. Below the title, there is a section for 'Configuration details' which includes the following information:

Configuration details	
Fulfillment option	64-bit (x86) Amazon Machine Image (AMI) TxOne StellarOne Management Console <i>running on m3.medium</i>
Software version	2.0.9128
Region	US East (N. Virginia)

Below the configuration details, there is a 'Usage instructions' button. Further down, there is a 'Select a launch action' dropdown menu with two options: 'Launch through EC2' (which is selected and highlighted with a red box) and 'Launch from Website'. To the right of this dropdown, there is a text prompt: 'Choose this action to launch from this website'. At the bottom, there is an 'EC2 Instance Type' dropdown menu set to 'm3.medium', with associated specifications: Memory: 3.75 GiB, CPU: 3 EC2 Compute Units (1 virtual core), Storage: 1 x 4 GiB SSD, and Network Performance: Moderate.

FIGURE 3-38. Select a Launch Action

6. Log on the AWS EC2 console.
7. Go to **Images > AMIs**.
8. Select the region you chose in step 4.
9. Find the target AMI from the list of **AMI ID**.
10. Select the target AMI and click **Launch Instance from AMI**.
11. Select a supported instance type.

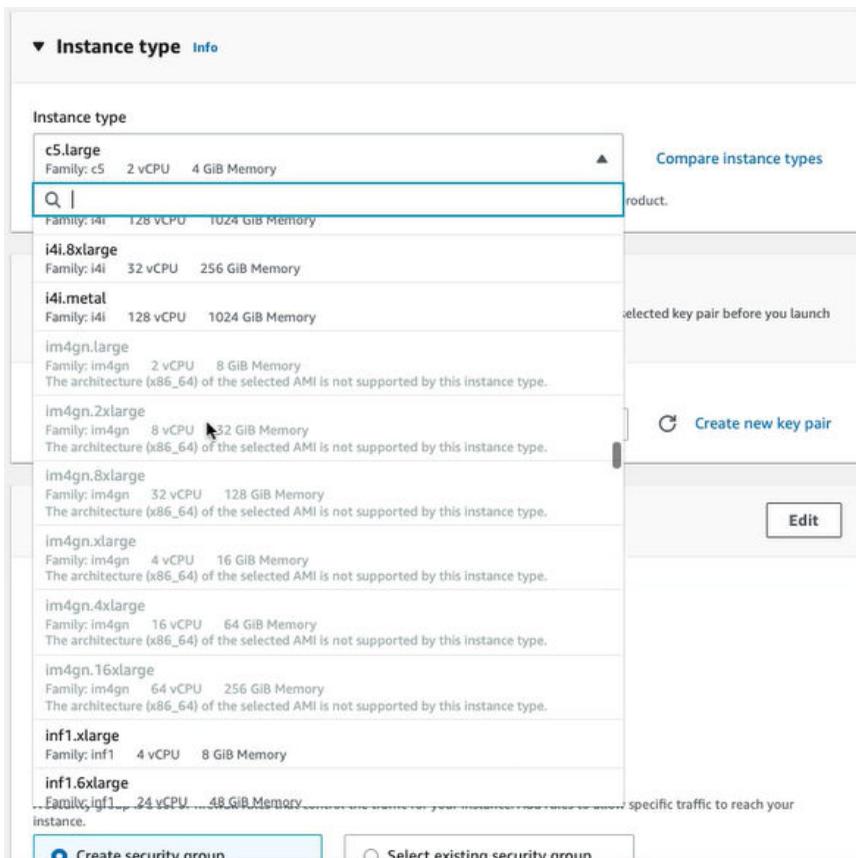


FIGURE 3-39. Select an Instance Type

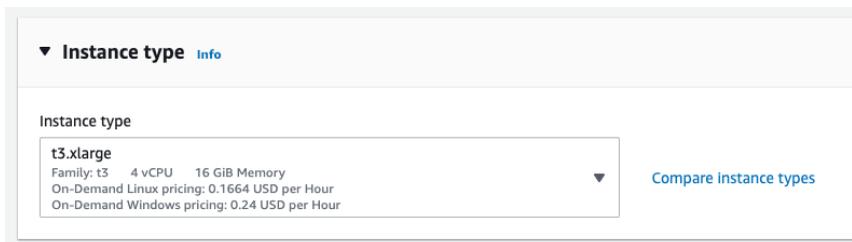


FIGURE 3-40. Information of the Selected Instance Type



Note

- The instance types that do not meet StellarOne's deployment requirements will be unavailable for selection.
- Refer to *Deciding an Instance Type for StellarOne on AWS EC2 Platform on page 2-6* for determining which instance type to use.

12. Configure the instance settings:

- a. Select or create the **Key pair (login)**

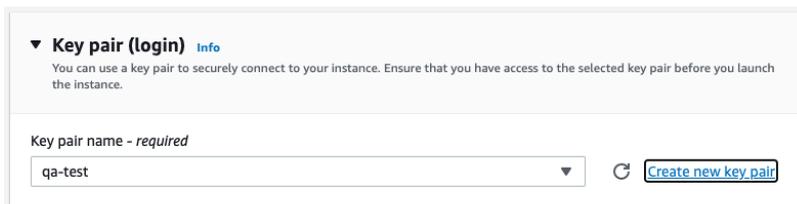


FIGURE 3-41. Key pair (login)

- b. Configure the **Network settings**:

- Be sure to create security group for allowing specific data exchanges to access your instance. It is required to enable the **HTTPS traffic from the Internet** to allow StellarOne to manage endpoints on the network.

- (Optional) If you have the need for SSH login, you can also enable the **Allow SSH traffic from** and select **Anywhere** or specify the IP address.

**Note**

Refer to *Ports and FQDN Used on page 2-8* for configuring the ports that should have access to StellarOne.

- Be sure to grant 8000 or 9443, the dedicated port for StellarProtect or StellarProtect (Legacy Mode), access to your instance.
- For security reasons, it is advisory to allow 443 or 22, the web port or SSH port for StellarOne, to be accessible from trusted IP address.

▼ **Network settings** [Info](#) Edit

Network [Info](#)
vpc-57becc2a

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)
Enable

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-67' with the following rules:

Allow SSH traffic from Anywhere
Helps you connect to your instance
0.0.0.0/0

Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ×

FIGURE 3-42. Network settings

- c. Add an EBS with at least 50 GB of space to the StellarOne instance in **Configure storage**.

▼ **Configure storage** [Info](#) [Advanced](#)

1x GiB ▼ Root volume (Not encrypted)

1x GiB ▼ EBS volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

0 x File systems [Edit](#)

FIGURE 3-43. Configure Storage

- d. Click **Launch Instance**.



Note

It may take 5 to 10 minutes to complete the deployment.

- 13.** Find the StellarOne instance and copy its assigned IP address.

The screenshot shows the AWS Management Console interface. On the left, there is a navigation menu with options like 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', and 'Instances'. The 'Instances' section is expanded, showing a list of instances. One instance named 'qa-test' with ID 'i-026...' is selected and its details are shown on the right. The instance state is 'Running'. Under the 'Instance: i-026...' section, the 'Auto-assigned IP address' is displayed as '3.94...' with a green checkmark and the text 'Auto-assigned IP address' and 's copied'. A red rectangular box highlights this IP address field.

FIGURE 3-44. Auto-assigned IP address



Note

The auto-assigned IP address may change if the instance has been rebooted. Please refer to [Associating the Elastic IP Address with an Instance on page 3-42](#) for assigning a static IPv4 address to your instance.

14. Refer to [Opening StellarOne Management Console on page 3-46](#) for logging on StellarOne via a web browser, or [Accessing StellarOne via SSH on page 3-40](#) for accessing StellarOne via SSH.

Accessing StellarOne via SSH

This section describes how to access StellarOne via Ssh.

Procedure

1. Find the StellarOne instance on the AWS EC2 and copy its auto-assigned IP address.

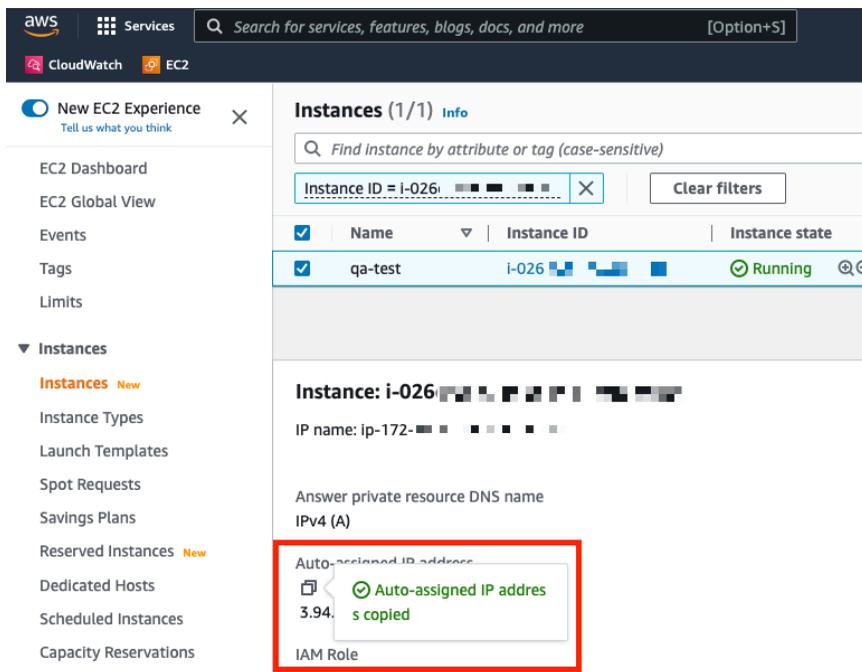


FIGURE 3-45. Auto-assigned IP address

2. Open the SSH terminal on your device and run the following command:


```
ssh -i <private key>.pem admin@<auto-assigned IP address>
```



Note

The auto-assigned IP address may change if the instance has been rebooted. Please refer to [Associating the Elastic IP Address with an Instance on page 3-42](#) for assigning a static IPv4 address to your instance.

3. For **Resource type**, select **Instance**.
4. Choose the target instance.

**Note**

You can search for a specific instance by typing relevant strings in the search bar.

5. (Optional) For **Private IP address**, specify a private IP address with which to associate the Elastic IP address.
6. Click **Associate**.

aws Services Search for services, features, blogs, docs, and more [Option+S]

CloudWatch EC2

EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address

Choose the Instance or network interface to associate to this Elastic IP address (35.168.1.10)

Elastic IP address: 35.168.1.10

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance

Network interface

⚠ If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. [Learn more](#)

Instance

i-026c...

Private IP address
The private IP address with which to associate the Elastic IP address.

Choose a private IP address

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassociated

Cancel Associate

FIGURE 3-47. Associate the Elastic IP Address with an Instance

7. A message appears indicating the Elastic IP address has been associated to the target instance.

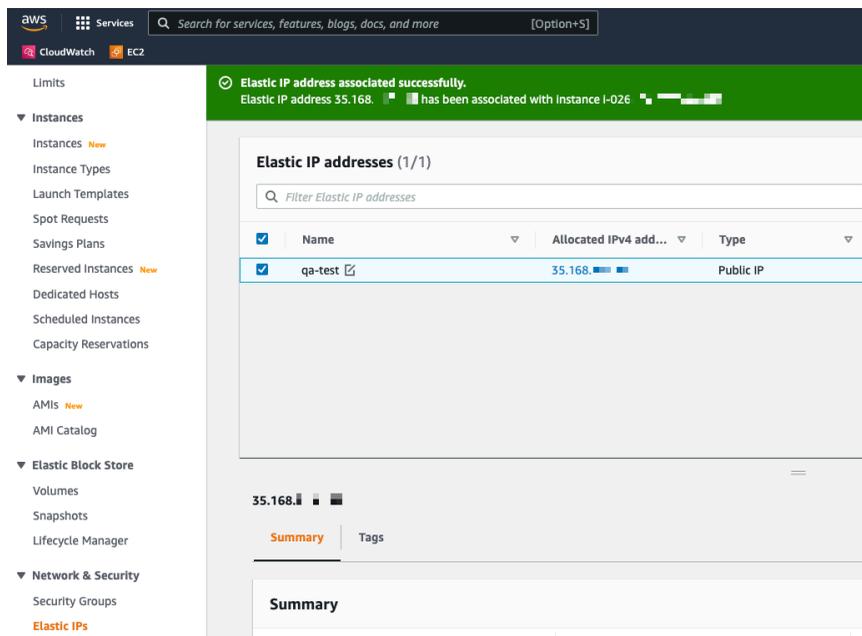


FIGURE 3-48. Associate Elastic IP Address

8. You can use the Elastic IP address to log on StellarOne via a web browser or via SSH now.
9. (Optional) Choose one of the methods below to access StellarOne via SSH with the Elastic IP address:
 - Replace the advertise address with the Elastic IP address by typing:


```
env advertise <the elastic IP address>
```
 - Replace the advertise address with the Elastic Load Balancer address by typing:


```
env advertise <the ELB address>
```

Opening StellarOne Management Console

Procedure

1. In a web browser, type the address of the StellarOne in the following format: `https://<targetserver IP address>`. The log on screen appears.
2. Enter your credentials (user ID and password).
Use the default credentials of administrator when logging on for the first time:
 - User ID: `admin`
 - Password: `txone`
3. Click **Log On**.
4. If this is the first time the StellarOne instance being logged on, follow below procedures to complete the initial settings.
 - a. The **Login Information Setup** window appears and prompts you to change password. Confirm your password settings by:
 - specifying your new password in the **New Password** text field.
 - specifying the password again in the **Confirm Password** text field.



Note

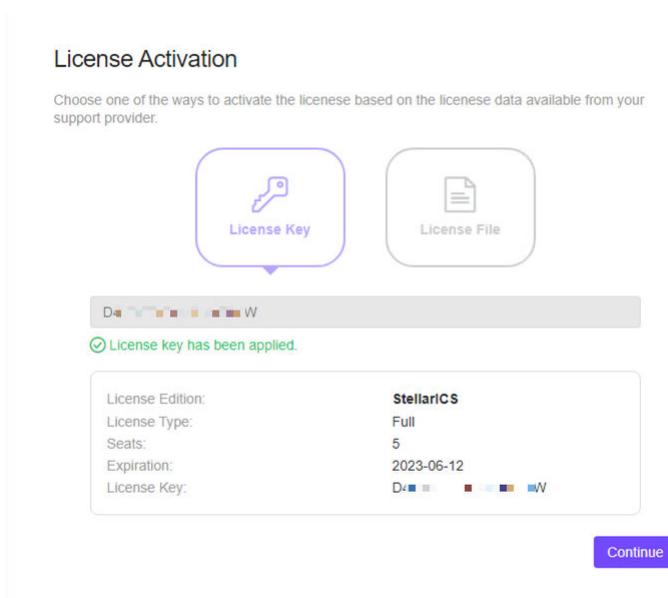
- For StellarOne 1.2 or above, the default login name is always `admin` and can not be changed by the user.
 - For StellarOne 1.0/1.1, in addition to changing the password, the user is also required to change the default login name in this step. The new login name can not be `admin`, `administrator`, `auditor` or `root`.
-
- b. Click **Confirm**. You will be automatically logged out. The **Log On** screen will appear again.

-
- c. Log on again using your new credentials. The **License Activation** window appears.
 - d. Choose one of the ways to activate the license based on the license data available from your support provider:
 - **License Key**
 - i. Click **License Key**.
 - ii. Specify your license key in the text field.
 - **License File:**
 - i. Click **License File**.
 - ii. Select the license file (a .txt file) to import.

**Note**

If you don't have the license file on hand, refer to [Getting the License File on page 3-49](#).

- e. Click **Apply**.
- f. The **License key is valid** message appears. Click **Continue**.



- g. A success message appears. License information also appears at the bottom of the **License Activation** window. Check if it matches the license data provided by your support provider.
- h. Click **Continue**.
- i. The **End User License Agreement and TXOne OT Intelligent Trust** window appears. Click the links to read the documents carefully and click the checkboxes to proceed to next step.



Note

It is advisory to enable **TXOne OT Intelligent Trust** to enhance security deployment. Please refer to [OT Intelligent Trust on page 3-51](#) for more details.

- j. Specify the time settings such as the **Date and Time** as well as the **Time Zone**, and then click **Continue**.
- k. The StellarOne console is ready for use now.

**Note**

After the initial settings are completed, the StellarOne allows various user accounts to log on remotely via a web browser.

5. (Optional) You can change your password by clicking the ID icon at the top right corner of the screen, and then selecting **Change Password**.
 6. (Optional) For security reasons, you can manually log off by clicking the ID icon at the top right corner of the screen.
 - a. A pop-up **Log Off** window appears. Click **Yes** to log out of StellarOne.
-

**Note**

You will be automatically logged off the console if no operations are performed within 30 minutes.

Getting the License File

Depending on the license data available from your support provider, you may need a license file to activate license for StellarOne.

**Note**

The license file can be used for license activation if the StellarOne has no Internet connection.

Procedure

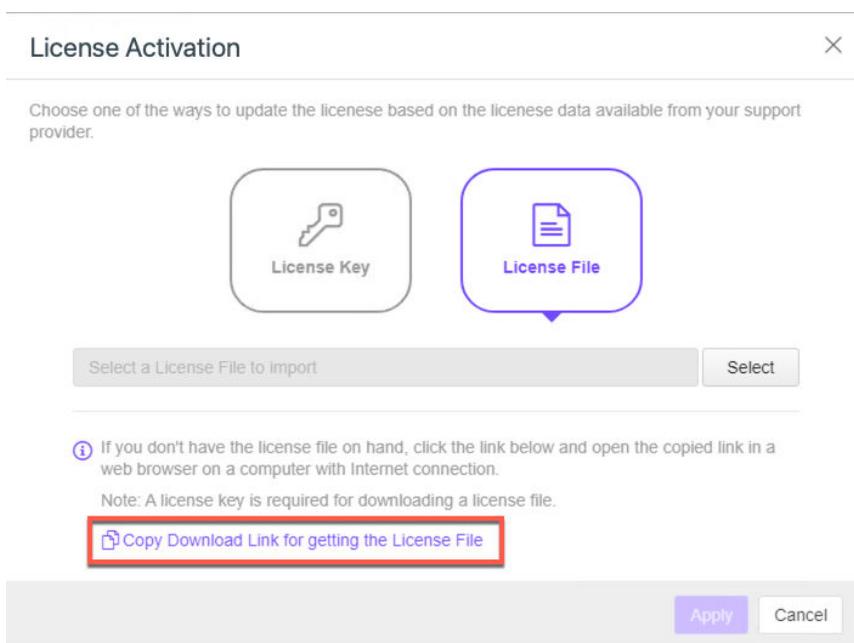
1. Go to **Administration > License**
2. Click the **New License Key / File** button.
3. The **New License** window appears.
4. When you log on StellarOne using your new credentials after the **Login Information Setup** procedure, the **License Activation** window appears.

5. Click **License File**.
6. Click **Copy Download Link for getting the License File** at the bottom of the **License ActivationNew License** window.

**Important**

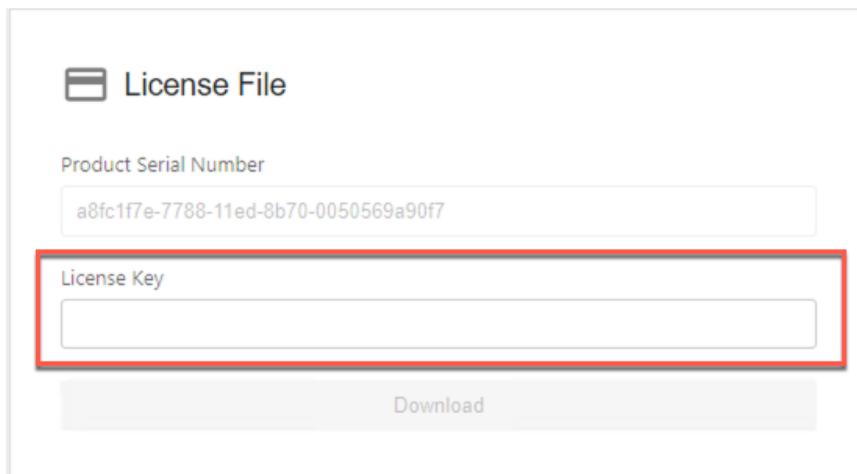
A license key is required for downloading a license file.

FIGURE 3-49. Copy Download Link for License File



7. **The Download Link has been copied** toast message appears.
8. Open the copied link in a web browser on a computer with Internet connection.

9. You will be directed to the TXOne **License File Management** screen. Specify your license key in the **License Key** field, and then click **Download**.



The screenshot displays the 'License File Management' interface. At the top, there is a header 'License File' with a menu icon. Below it, the 'Product Serial Number' is shown as 'a8fc1f7e-7788-11ed-8b70-0050569a90f7'. The 'License Key' field is empty and highlighted with a red border. A 'Download' button is located at the bottom of the form.

FIGURE 3-50. TXOne License File Management

10. A pop-up window appears showing the license information. Read it carefully and click **Yes** for downloading the license file.



Tip

You can send the license file to StellarOne that has no Internet connection via the internal secured network or a trusted portable device.

OT Intelligent Trust

When enabled, TXOne OT Intelligent Trust shares anonymous threat information with the Smart Protection Network, allowing TXOne to rapidly identify and address new threats. You can disable TXOne OT Intelligent Trust anytime on this console.

Chapter 4

Configuring StellarOne via Command Line Interface (CLI)

This chapter describes how to configure some settings for StellarOne via command line interface (CLI).

Topics in this chapter include:

- *Using the StellarOne Command Line Interface (CLI) on page 4-2*
- *Configuring the IP Address via CLI on page 4-3*
- *Modifying Communication Ports via CLI on page 4-9*
 - *Configuring the Advertise Address via CLI on page 4-6*
- *Changing Language Settings via CLI on page 4-11*
- *Managing Docker Network via CLI on page 4-13*
- *Resetting Administrator's Password via CLI on page 4-13*

Using the StellarOne Command Line Interface (CLI)

The following section describes how to log on StellarOne and get a list of available commands via command line interface (CLI).

Procedure

1. Open the StellarOne VM console.
2. Log on by typing `root` as the user name, `txone` as the password.



Note

If the StellarOne instance is deployed from AMI on AWS EC2 platform, type `admin` as the user name and no password is needed.

3. After logging on the StellarOne console, type `help` command for a list of available commands.

```
$ help
vShell, version
The commands provided in:
  access-list  Manage the IP whitelists
  dx           Connection test for 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
  ssh         SSH to a device
  service     Manage the StellarOne service
  sftp        Send files via sftp
  web         Commands of the web management console
  stellar     Commands of the Stellar products
  locale      Locale setting
  network     Manage network for the StellarOne service

Shortcut table:
  Tab         Auto-complete or switch among options available
  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
$ █
```

FIGURE 4-1. Command list

Configuring the IP Address via CLI

The following section describes procedures of configuring the IP address settings for StellarOne instance via CLI.

Procedure

1. Type `iface ls` to get the IP address of the StellarOne instance.

```

clear the screen
$ iface ls
{
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  }
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "dhcp"
  }
}
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 odisc nqueue 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 odisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:fc:65:af brd ff:ff:ff:ff:ff:ff
    inet 192.168.68.147/24 brd 192.168.68.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe65:af64 scope link
        valid_lft forever preferred_lft forever
$

```

FIGURE 4-2. Getting the IP Address of StellarOne

2. Type `iface update` command for updating the settings of current network interface. For example, the following command sets the interface **eth0** to a static IP address `10.7.19.157/24` with the Gateway IP address `10.7.19.254`.

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

3. Check if the network interface settings are correct, and then type the following command to execute the change.

```
iface restart eth0
```

4. Type following command again for viewing the new 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 adisc naqueue 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 adisc 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

```

FIGURE 4-3. Viewing New Network Settings

5. Use the `resolv add` command to add a DNS server and `resolv ls` to view the DNS server list. For example, the following command adds 8.8.8.8 to the DNS server list

```
resolv mode custom
```

```
resolv add 8.8.8.8
```

6. Type 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

```

FIGURE 4-4. Viewing DNS Server Settings

7. Type following command to reboot the VM.

`reboot`

Configuring the Advertise Address via CLI

The following section describes how to configure the IP address or FQDN as the StellarOne advertise address via CLI.

Procedure

1. Type `help` command for a list of available commands.
2. Type `env` and find the `advertise-addr` command.

```

$ help
vShell, version ab2e3bc
The commands provided in:
access-list  Manage the IP whitelists
dk          Connection test for 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
ssh        SSH to a device
service    Manage the StellarOne service
sftp       Send files via sftp
web        Commands of the web management console
stellar    Commands of the Stellar products
locale     Locale setting
network    Manage network for the StellarOne service

Shortcut table:
Tab        Auto-complete or switch among options available
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
$ env
ls          List the OS and Service environment variables
hostname    Edit the variable in /etc/hostname
advertise-addr Set the IP address or FQDN to advertise, or type "default" to use the default IP of the host
logseverity Set the debug log level [default into verbose]

```

FIGURE 4-5. The advertise-addr command

3. Specify the advertise address for StellarOne after the `advertise-addr` command. The following example uses the FQDN as the advertise address:

```
env advertise-addr S1.txone.com
```



```

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-07-25T08:08:00.844Z" entityID="https://10.8.150.84/rest/admin/saml/spmeta">
  <SPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-07-25T08:08:00.84400991Z" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protoco
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://10.8.150.84/saml/slo" ResponseLocation="https://10.8.150.84/saml/slo">
    <NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/NameIDFormat>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://10.8.150.84/saml/acs" Index="1"></AssertionConsumerService>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://10.8.150.84/saml/acs" Index="2"></AssertionConsumerService>
  </SPSSODescriptor>
</EntityDescriptor>

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-07-25T08:10:08.332Z" entityID="https://s1.txone.com/rest/admin/saml/spmeta">
  <SPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-07-25T08:10:08.331700266Z" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protoco
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://s1.txone.com/saml/slo" ResponseLocation="https://s1.txone.com/saml/slo">
    <NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/NameIDFormat>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://s1.txone.com/saml/acs" Index="1"></AssertionConsumerService>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://s1.txone.com/saml/acs" Index="2"></AssertionConsumerService>
  </SPSSODescriptor>
</EntityDescriptor>

```

FIGURE 4-9. Use IP address or FQDN as the advertise address in SAML SSO metadata file

Modifying Communication Ports via CLI

Below section describes how to modify the communication ports for StellarOne instance via CLI.

Procedure

1. Type `env ls` command for the list of current communication ports.

```

$ env ls
Hostname:          ODC
Status:           RUNNING
Product Serial Number: 7e
Version:          2.2.1148
Advertise Address: Not Set
DPI Engine Version:
DPI Pattern Version:
StellarProtect (Legacy Mode) Agent Up Port:8000
StellarProtect (Legacy Mode) Agent Down Port:14336
StellarProtect Agent Up Port: 9443
StellarProtect Agent Down Port:14336
Locale:          en

```

FIGURE 4-10. List of Current Communication Ports

2. Type `stellar` command for available agents to appear for selection.

```
$ stellar
  set-enforce-ports Edit the communication ports for Stellar Enforce agents
  set-protect-ports Edit the communication ports for Stellar Protect agents
```

FIGURE 4-11. Available Agents for Selection

3. Select one of the agents to edit its communication port.

```
$ stellar set-enforce-ports
  set-enforce-ports Edit the communication ports for Stellar Enforce agents
  set-protect-ports Edit the communication ports for Stellar Protect agents
```

FIGURE 4-12. Select the Agent for Editing Communication Port

4. Input the valid value for <up-port> and <down-port>.
 - <up-port>: Port for receiving data from agents.
 - <down-port>: Port for sending command to agents



Note

Make sure not to use StellarOne's service port. Please refer to **Table 2-7. StellarOne Occupied Ports** in *Ports and FQDN Used on page 2-8*.

```
$ stellar set-enforce-ports 8000 14336
Port for receiving data from Stellar Enforce agents: 8000
Port to send commands to Stellar Enforce agents: 14336

Successfully set up ports for Stellar Enforce.
Please reload services to take effect.
```

FIGURE 4-13. Agent's Communication Ports

5. Reboot.



Important

Please note the previously installed package does not contain the new port setting. Be sure to do either of the following actions after changing the communication ports for StellarOne via CLI.

- Download the agent's installer package containing the new port setting from StellarOne, and install it on the agent.
 - Modify the port setting accordingly in the `StellarSetup.ini` file in the agent's existing installer package, and reinstall it on the agent.
-

Changing Language Settings via CLI

Below section describes how to change language settings for StellarOne via CLI. The default language for StellarOne web console is English. You can change the language to Japanese following below procedures.

Procedure

1. Type `locale ja` command to switch the language to Japanese.
2. Reload the StellarOne web console

```
$ help
vShell, version ab2e3bc
The commands provided in:
  access-list  Manage the IP whitelists
  dx           Connection test for 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
  ssh         SSH to a device
  service     Manage the StellarOne service
  sftp        Send files via sftp
  web         Commands of the web management console
  stellar     Commands of the Stellar products
  locale      Locale setting
  network     Manage network for the StellarOne service

Shortcut table:
  Tab        Auto-complete or switch among options available
  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

$ locale ja
Successfully language setting for locale.
Please reload StellarOne console to take effect.
```

FIGURE 4-14. Reload StellarOne console

3. Type `env ls` command to check current language settings.

```

$ env ls
Hostname:                ODC
Status:                  RUNNING
Product Serial Number:  7...
Version:                 2.2.1148
Advertise Address:      Not Set
DPI Engine Version:     2.0.11.33e2e1+turbo
DPI Pattern Version:    SDP_230228_08
StellarProtect (Legacy Mode) Agent Up Port:8000
StellarProtect (Legacy Mode) Agent Down Port:14336
StellarProtect Agent Up Port: 9443
StellarProtect Agent Down Port:14336
Locale:                  ja

```

FIGURE 4-15. Check Language Settings

Managing Docker Network via CLI

The following section describes how to manage docker network on vShell for StellarOne via CLI.

Procedure

1. If 169.254.0.0/16 IP range is used in your network setting, please type `network internal-service-update <New IP>` command to set a new IP address for converting IP/16 subnet mask for docker daemon.
 2. If you want to restore docker daemon back to the default-address-pools (169.254.0.0/16), type `network internal-service-reset` command.
 3. Type `network internal-service-list` command to display the address pools of docker daemon configuration.
-

Resetting Administrator's Password via CLI

The following section describes how to reset administrator's password for StellarOne via CLI.

Procedure

1. Type `web reset admin` command to reset administrator's password.
2. The `reset OK!` message appears. The administrator's password has been reset.
3. Use the default credentials (user ID: `admin` / password: `txone`) to log on the StellarOne web console.



Note

For StellarOne 1.0/1.1, the default login name (user ID) is required to be changed by users. Be sure to use the changed default login name for accessing StellarOne 1.0 or 1.1.

4. The **Login Information Setup** window appears and prompts you to change password. Confirm your password settings by:
 - a. specifying your new password in the **New Password** text field.
 - b. specifying the password again in the **Confirm Password** text field.
 5. Click **Confirm**. You will be automatically logged out. The **Log On** screen will appear again.
 6. Log on again using your new credentials.
-

Chapter 5

Upgrade

This chapter describes the supported upgrade paths and methods for TXOne StellarOne.

Topics in this chapter include:

- *Supported Upgrade Paths on page 5-2*
- *Upgrade Methods on page 5-3*

Supported Upgrade Paths

The following table illustrates the supported upgrade paths for StellarOne installed in VMware or Windows Hyper-V system..

TABLE 5-1. Supported Upgrade Paths

PLATFORM	CURRENT VERSION	SUPPORTED TARGET UPGRADE VERSION	FIRMWARE UPGRADE*	MOUNT UPGRADE
VMWare Hyper-V	2.1	2.2	√	√
	2.0	2.1 / 2.2	√	√
	1.2 Patch 1	2.0 / 2.1 / 2.2	N/A	√
	1.2	2.0 / 2.1	N/A	√
	1.2	1.2 Patch 1	√	√
VMWare	1.1	1.2 / 1.2 Patch 1	√	√
	1.0	1.1	N/A	√



Important

- Do not use firmware upgrade to update StellarOne 1.0, 1.2, or 1.2 Patch1 to a newer version (except for upgrading 1.2 to 1.2 patch 1). Please use mount upgrade instead, which requires importing a new virtual image (.ova or .vhdx file) to a new instance and then mounting the 2nd external disk from the previous StellarOne instance. See [Mount Upgrade \(VMware\) on page 5-4](#) or [Mount Upgrade \(Hyper-V\) on page 5-7](#) for more details.
- StellarOne 1.2 patch1 equals to StellarOne1.2.2114
- TXOne Networks recommends always using firmware upgrade to update StellarOne if both upgrade options are available.

Upgrade Methods

This section describes two methods to upgrade StellarOne installed in VMware or Windows Hyper-V system.

Topics in this section include:

- *Firmware Upgrade on page 5-3*
- *Mount Upgrade (VMware) on page 5-4*
- *Mount Upgrade (Hyper-V) on page 5-7*

Firmware Upgrade

This section describes how to perform firmware upgrade via the StellarOne web console.

Procedure

1. Download the .acf upgrade patch file (e.g., TXOne-S1-acus.fw-2.x.xxxx.acf) from the [Download Center](#).
2. Log on the StellarOne web console and go to **Administration > Firmware**.
3. Click **Import** and select the .acf file downloaded in *Step 1*, and then click **Apply**.
4. Wait until the following window appears and read the upgrade notice carefully.

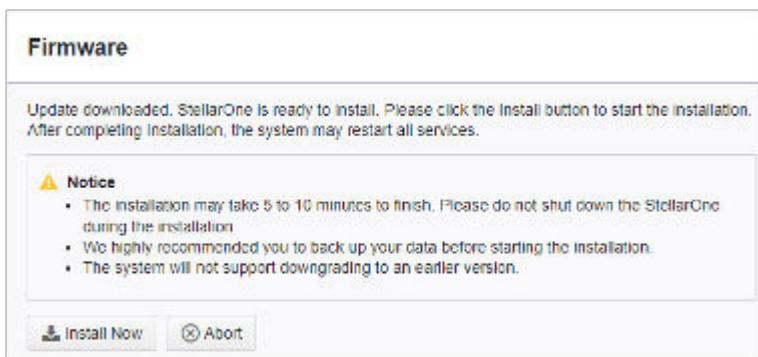


FIGURE 5-1. Firmware Install

5. Click **Install Now** to start the upgrade.

Mount Upgrade (VMware)

This section describes how to perform mount upgrade for StellarOne on VMware ESXi or Workstation. The mount upgrade is performed by attaching the external disk of previous StellarOne instance to the StellarOne instance running new firmware version. The previously configured settings will be transferred to the new StellarOne instance, including:

- The UUID
- The pattern and firmware
- The agent list, policy settings, and StellarOne certificates
- The system configuration, including license, account information, security policies, and proxy/SSO settings
- Security event logs

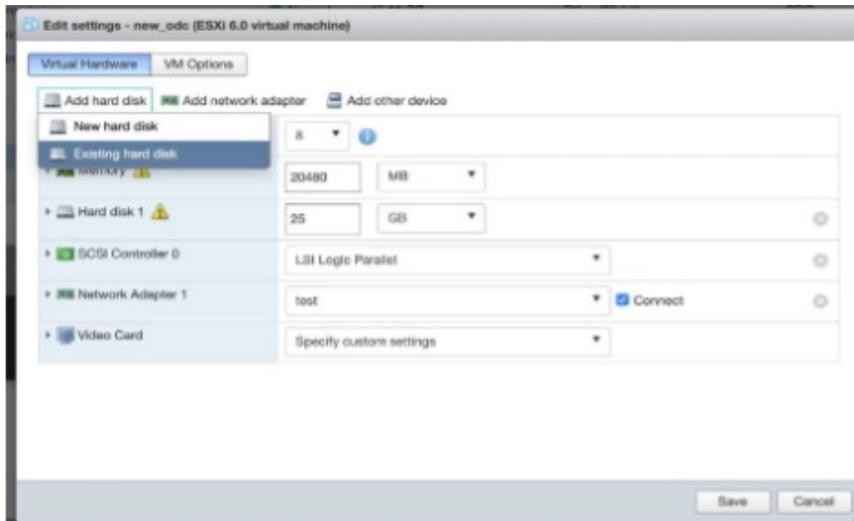


FIGURE 5-3. Select Existing (Previous) Hard Disk

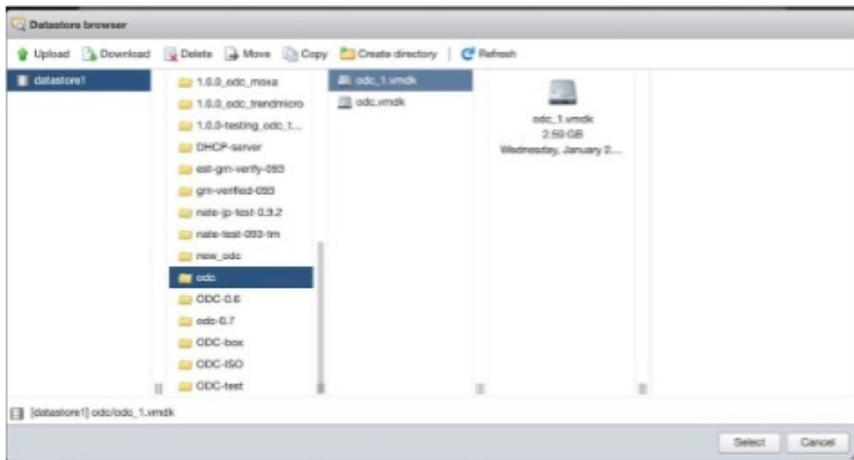


FIGURE 5-4. Attach to New VM

4. The data of the previous StellarOne instance will be migrated to new StellarOne instance.

5. The IP address of the new StellarOne instance must be the same as that of the previous StellarOne instance. If not, manually configure the IP address so the new StellarOne instance and agents can be connected to each other. Next time when the agents synchronize their status with the server, they will connect to the new StellarOne. By default, the agents synchronize with the server every 20 minutes.
 6. If the proxy or scan component update source has already been defined in the previous StellarOne instance, please define it again via the web GUI of the new StellarOne instance.
 7. If you want to change the language setting to Japanese for the new StellarOne instance, see [Changing Language Settings via CLI on page 4-11](#).
-

Mount Upgrade (Hyper-V)

This section describes how to perform mount upgrade for StellarOne in Windows Hyper-V system. The mount upgrade is performed by attaching the external disk of previous StellarOne instance to the StellarOne instance running new firmware version. The previously configured settings will be transferred to the new StellarOne instance, including:

- The UUID
- The pattern and firmware
- The agent list, policy settings, and StellarOne certificates
- The system configuration, including license, account information, security policies, and proxy/SSO settings
- Security event logs



Important

- Before executing a mount upgrade, please create a back up of the VM files first.
 - StellarOne 2.0 ONLY supports mount upgrade from version 1.2 or 1.2 Patch 1.
-

Procedure

1. Launch the new StellarOne instance. See [Deploying StellarOne to a Hyper-V System on page 3-18](#) for deployment details.
2. Close the previous StellarOne instance.
3. Click **Browse** and choose the existing disk.
4. Attach the external disk of previous StellarOne to the new StellarOne instance.

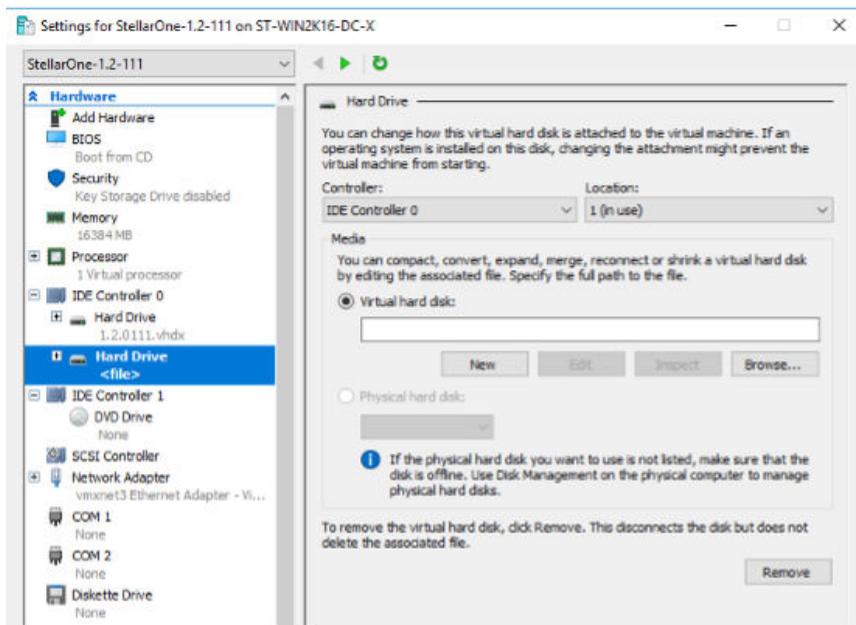


FIGURE 5-5. Shut Down the Previous VM

5. The data of the previous StellarOne instance will be migrated to new StellarOne instance.
6. The IP address of the new StellarOne instance must be the same as that of the previous StellarOne instance. If not, manually configure the IP

address so the new StellarOne instance and agents can be connected to each other. Next time when the agents synchronize their status with the server, they will connect to the new StellarOne. By default, the agents synchronize with the server every 20 minutes.

7. If the proxy or scan component update source has already been defined in the previous StellarOne instance, please define it again via the web GUI of the new StellarOne instance.
 8. If you want to change the language setting to Japanese for the new StellarOne instance, see [Changing Language Settings via CLI on page 4-11](#).
-

Chapter 6

Technical Support

Support for TXOne Networks products is provided mutually by TXOne Networks and Trend Micro. All technical support goes through TXone and Trend Micro engineers.

Learn about the following topics:

- *Troubleshooting Resources on page 6-2*
- *Contacting Trend Micro and TXOne on page 6-3*
- *Sending Suspicious Content to Trend Micro on page 6-5*
- *Other Resources on page 6-6*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <https://success.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



Tip

To submit a support case online, visit the following URL:

<https://success.trendmicro.com/smb-new-request>

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro and TXOne combats this complex malware with products that create a custom

defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware> and <https://www.encyclopedia.txone.com/> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro and TXOne

In the United States, Trend Micro and TXOne representatives are available by below contact information:

TABLE 6-1. Trend Micro Contact Information

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

TABLE 6-2. TXOne Contact Information

Address	TXOne Networks, Incorporated 222 West Las Colinas Boulevard, Suite 1650 Irving, TX 75039 U.S.A
Website	https://www.txone.com
Email address	support@txone.com

- Worldwide support offices:
<https://www.trendmicro.com/us/about-us/contact/index.html>
<https://www.txone.com/contact/>
- Trend Micro product documentation:
<https://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://ers.trendmicro.com/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<http://esupport.trendmicro.com/solution/en-US/1112106.aspx>

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

<https://success.trendmicro.com/solution/1059565>

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

<https://global.sitesafety.trendmicro.com/>

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, TXOne Networks may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

<https://www.trendmicro.com/download/>

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Index

A

- agent deployment plan, 2-7
 - No. of Agents Deployed, 2-8
 - Total Bandwidth / Deployment Task, 2-8

C

- command line interface, 4-2
 - change language settings, 4-11
 - configure advertise address, 4-6
 - configure IP address, 4-3
 - manage docker network, 4-13
 - modify communication ports, 4-9
 - reset administrator's password, 4-13

F

- Firmware upgrade, 5-3

H

- hardware requirements for AWS EC2, 2-6
- hardware requirements for Hyper-V, 2-4
 - 1st HDD Space, 2-5, 2-6
 - 2nd HDD Space, 2-5, 2-6
 - Disk Space, 2-5, 2-6
 - Max. No. of Agents, 2-5, 2-6
 - memory size, 2-5, 2-6
 - Min. No. of CPU, 2-5, 2-6
 - No. of Logs, 2-5, 2-6
- hardware requirements for VMware, 2-3
 - 1st HDD Space, 2-3
 - 2nd HDD Space, 2-3

- Disk Space, 2-3
- Max. No. of Agents, 2-3
- memory size, 2-3
- Min. No. of vCores, 2-3
- No. of Logs, 2-3

I

- installation, 3-2, 3-17, 3-32
 - Deploy on AWS EC2, 3-33
 - Deploy on Hyper-V, 3-18
 - Deploy on VMware ESXi, 3-3
- Installation, 3-12
 - Deploy on VMware Workstation, 3-12
- installation flow, 3-2

M

- Mount upgrade
 - Hyper-V, 5-7
 - VMware, 5-4

P

- Ports and FQDN, 2-8
 - FQDN, 2-9
 - function, 2-9
 - open port, 2-9

R

- reference table
 - Agent Remote Patch, 2-8
 - Full Pattern Update, 2-8
 - Incremental Pattern Update, 2-8
- requirements, 2-2

S

- StellarOne Occupied Ports, 2-10

NTP, 2-10

SSH, 2-10

StellarOne internal service, 2-10

StellarProtect (Legacy Mode)

default port, 2-10

StellarProtect default port, 2-10

Web, 2-10

support

resolve issues faster, 6-4

Supported agent version, 2-10

system requirements, 2-2

U

Upgrade paths, 5-2



TXONE NETWORKS INCORPORATED

222 West Las Colinas Boulevard, Suite 1650
Irving, TX 75039 U.S.A
Email: support@txone.com
www.txone.com

www.txone.com

Item Code: APEM229710/230327