

3.1 TXOne StellarOne

Installation Guide

Patch 1

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:

<https://my.txone.com/>

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 © 2024. TXOne Networks Incorporated. All rights reserved.

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.

Data collected by TXOne Networks is subject to the conditions stated in the TXOne Networks Global Privacy Notice:

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

Table of Contents

Preface

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

Chapter 1: Introduction

About TXOne Stellar	1-2
Key Features and Benefits	1-3
What's New	1-5

Chapter 2: Installation Planning

System Requirements	2-2
Hardware Requirements	2-2
Hardware Requirements for Deploying StellarOne on VMware/Hyper-V/AWS EC2	2-3
Planning Network Bandwidth for Agent Deployment	2-4
Ports and FQDN Used	2-6
Supported Agent Versions	2-8
Instance Data Encryption	2-9

Chapter 3: Installation

StellarOne Installation Flow	3-2
StellarOne Onboarding to VMware ESXi	3-2
Prerequisites	3-2
Deploying StellarOne on the VMware ESXi	3-2

StellarOne Onboarding to Windows Hyper-V	3-12
Prerequisites	3-12
Deploying StellarOne to a Hyper-V System	3-12
StellarOne Onboarding to AWS EC2	3-29
Prerequisites	3-29
Deploying StellarOne on AWS EC2	3-30
Accessing StellarOne via SSH	3-37
Associating the Elastic IP Address with an Instance .	3-39
Opening StellarOne Management Console	3-43
Comparison of License Formats	3-46
Getting the License File	3-46
OT Intelligent Trust	3-48

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	5-4
Mount Upgrade (VMware)	5-5
Mount Upgrade (Hyper-V)	5-7

Chapter 6: Getting Help and Troubleshooting

Troubleshooting Resources	6-2
Self-Diagnosis	6-2
Resolving Low Disk Space Issues	6-2
Resolving Licensing Issues	6-4
Using the Support Portal	6-5
Threat Encyclopedia	6-6
Contacting TXOne Networks	6-6
Speeding Up the Support Call	6-7
Other Resources	6-7
Download Center	6-8

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.

Preface

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

Topics in this chapter include:

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

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
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/




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
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

CONVENTION	DESCRIPTION
 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
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

TERMINOLOGY	DESCRIPTION
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 1-3*
- *What's New on page 1-5*

About TXOne Stellar

TXOne Stellar provides a context-focused security solution for OT endpoints and cyber-physical systems (CPS), aiming to defend operation stability with continuous detection and response aligned to the specific requirements of the OT domain.

TXOne Stellar platform is composed of the centralized management console server and unified agents apt for legacy OT devices and modern cyber-physical systems.

- StellarOne™, designed to streamline administration of the agents installed on modernized systems and legacy systems, along with its intuitive centralized management, consistent policy enforcement, and action-oriented alerts that empower security teams of all sizes and skill levels to successfully mature their organization's security posture.
- StellarProtect™ / StellarProtect (Legacy Mode), using the single-agent design that delivers seamless asset-centric protection and ensures coverage for modern CPS and legacy OT devices throughout their entire asset lifecycle. The lightweight unified agent simplifies security by combining CPS Detection and Response (CPSDR), threat prevention, operations lockdown, and device control.
 - CPSDR: Embodied within the advanced Operations Behavior Anomaly Detection feature, which establishes a unique baseline fingerprint of each agent-device during practicable operating states and performs fingerprint deviation analysis by means of an expansive industrial application repository and ransomware detection engine to defend against unexpected changes that may impact stability.

Moreover, TXOne Stellar brings the contextualization of security into an operation-led view to allow both the operation and security teams to achieve their goals without needing to compromise. To illustrate, if a device suddenly tried to start launching different applications, it would be blocked from doing so.

From the operation view, this may be an unplanned auto-update that, if run, would take the device offline to reboot. From a security

view, this could be an attempt to access an encryption library that is about to be used to execute ransomware. By applying the operation context, both security and operation-initiated changes can be detected, and appropriate responses are taken.

In both cases, CPSDR stopped the incident before it could occur. The security team followed up and resolved the ransomware infection in a different part of the environment. The operation team could schedule the required update to run during planned maintenance period.

- **Multi-Method Threat Prevention:** Provides advanced threat scan on the basis of ICS root of trust and operations-focused machine learning to secure the agent-devices against known and unknown malware threats without compromising operational availability.
- **Operations Lockdown:** For fixed-function and devices with limited patching availability, operations lockdown enforcement prohibits unauthorized changes, including alterations to registry and function parameters.
- **Trusted Peripheral Control:** Unauthorized access from external sources, such as USB devices, is configurable and controlled to reduce physical access threats.

Leveraging an expansive OT application and certificate library and exclusive ransomware detection engine, TXOne Stellar maintains CPS operational integrity through behavioral anomaly detection and eliminates configuration drift for legacy and fixed-use assets with device lockdown. Security teams can confidently deliver detection and response outcomes across the OT terrain, with TXOne Stellar effectively strengthen organization's security posture while maintaining its business operations stability.

Key Features and Benefits

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

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Cyber-Physical System Detection and Response (CPSDR)	The CPSDR requires a deep understanding of what the expected behaviors for each device are. Embodied within the advanced Operations Behavior Anomaly Detection feature, which primarily defends against unexpected changes that may impact operational stability by comparing daily operation processes and behaviors with a unique baseline of each agent-device and performing comprehensive behavioral analysis not only via identifying baseline deviation but also using TXOne Networks' exclusive industrial application repository and ransomware detection engine.
Dashboard	The Dashboard provides an overview of the CPS situational awareness and agent deployment status at the centralized control level, along with the monitored asset status and StellarOne console's system status. Administrators can check deployed agent status easily, have quick access to the detected events for further investigation or actions if needed, and generate security reports 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 (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 and import agent Approved list (Legacy Mode only) • Export agents Approved List
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™ 3.1 Patch 1 provides following new features and enhancements.

TABLE 1-2. What's New in TXOne StellarOne™ 3.1 Patch 1

FEATURE	BENEFIT
Enhanced licensing errors handling	Identifies and displays licensing related errors that help facilitate license activation or renewal process when certain issues occur.
Integration with SageOne management console	Integrates with SageOne, the central management console for managing multiple StellarOne servers.

Chapter 2

Installation Planning

This chapter 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 2-4*
- *Ports and FQDN Used on page 2-6*
- *Supported Agent Versions on page 2-8*
- *Instance Data Encryption on page 2-9*

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, see [Hardware Requirements for Deploying StellarOne on VMware/Hyper-V/AWS EC2 on page 2-3](#) 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 that will be configured and retained, as well as features enabled. See the sections below for determining the optimal number of agents that your StellarOne server deployment can manage on different platforms.

Hardware Requirements for Deploying StellarOne on VMware/ Hyper-V/AWS EC2

See the following table for determining the optimal number of agents that your StellarOne instance can manage on the VMware, Hyper-V, or AWS EC2 platform.



Note

To deploy StellarOne on AWS EC2, please also refer to [Amazon EC2 Instance Types](#) for specifications of the instance types.

TABLE 2-1. Sizing Table for Deploying StellarOne

MAX. NO. OF AGENTS	MIN No. OF VCORES	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (MINIMUM)	2ND HDD SPACE (RECOMMENDED)
30,000	10	32 GB	25 GB	100 GB	500 GB
20,000	8	16 GB		100 GB	400 GB
15,000	8	16 GB		50 GB	300 GB
10,000	8	16 GB		50 GB	200 GB
5,000	8	16 GB		50 GB	150 GB
1,000	4	16 GB		50 GB	100 GB
500	4	12 GB		50 GB	100 GB

**Important**

The StellarOne requires one external disk with at least 50 GB minimum space for initialization and booting process.

- The minimum required 2nd HDD space is used to store the system configurations and event logs.
- The recommended required 2nd HDD space is used to store the system configurations and event logs, as well as executing the **Operations Behavior Anomaly Detection** feature.

For example, if you want to deploy 25,000 agents **without** running the **Operations Behavior Anomaly Detection** feature, you'll need to prepare a 2nd HDD of 100 GB capacity. However, if you want to deploy 25,000 agents and run **Operations Behavior Anomaly Detection**, you'll need to prepare a 2nd HDD of 500 GB capacity

**Note**

1. 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.
 2. Please also take the network bandwidth into consideration when planning for agent deployment. See [Planning Network Bandwidth for Agent Deployment on page 2-4](#) 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 2-2. 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 2-3. Policy Refresh Interval vs No. of Agents Managed

POLICY REFRESH INTERVAL	NO. OF AGENTS MANAGED
5 minutes	5000
10 minutes	10000

POLICY REFRESH INTERVAL	NO. OF AGENTS MANAGED
20 minutes	20000
60 minutes	60000

Ports and FQDN Used

The following table shows the ports used by the StellarOne server. Please keep them opened in your firewall settings for StellarOne's use.

TABLE 2-4. Ports and FQDN Used

FROM	TO	OPEN PORT	FQDN	FUNCTION
StellarProtect	StellarOne	9443, 8000, 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

FROM	TO	OPEN PORT	FQDN	FUNCTION
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 2-5. StellarOne Occupied Ports

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

STELLARONE OCCUPIED PORT	PORT
	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 2-6. Supported Agent Version

SERVER VERSION	AGENTS VERSION		
	STELLARPROTECT	STELLARPROTECT (LEGACY MODE)	STELLARENFORCE
3.1 Patch 1	3.1 Patch 1 and earlier versions	3.1 Patch 1 and earlier versions	N/A
3.1	3.1 and earlier versions	3.1 and earlier versions	N/A
3.0 Service Pack 1	3.0 Service Pack 1 and earlier versions	3.0 Service Pack 1 and earlier versions	N/A
3.0	3.0 and earlier versions	3.0 and earlier versions	N/A
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

SERVER VERSION	AGENTS VERSION		
	STELLARPROTECT	STELLARPROTECT (LEGACY MODE)	STELLARENFORCE
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 versions, new features or enhanced functionalities may not be applicable on some agents with earlier versions.



Note

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

Instance Data Encryption

You can encrypt the data associated with your StellarOne instance deployed on VMware ESXi or AWS EC2 platform. Refer to [VMware ESXi Encryption Options](#) or [Amazon EBS Encryption](#) for more detailed procedures.



Note

Since Microsoft has yet to support the encryption of Linux virtual machine run on Windows Hyper-V system, the StellarOne instance deployed on Hyper-V cannot be encrypted.

Before you begin the encryption configuration for StellarOne, verify the following requirements are met.

- Ensure that the virtual machine is powered off.
 - Ensure that you have the administrator or cryptographic operations privilege.
-



Important

If the encrypted StellarOne instance requires technical support from TXOne Networks, ensure that you decrypt it for problem investigation.

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 Windows Hyper-V on page 3-12*
- *StellarOne Onboarding to AWS EC2 on page 3-29*
- *Opening StellarOne Management Console on page 3-43*

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. For VMware or Hyper-V system, launch the StellarOne instance, and then run the OOB process and configure settings such as IP address and communication ports in the setup CLI.
 4. Log on StellarOne web console to set up the administrator's account.
 5. Log on StellarOne web console to activate the product license and set time properties.
-

StellarOne Onboarding to VMware ESXi

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

Prerequisites

- The OVA packages provided by TXOne must be available and accessible to VMware ESXi.
- 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

The following section describes the procedures of deploying StellarOne from an OVA file to the VMware ESXi system.

Procedure

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

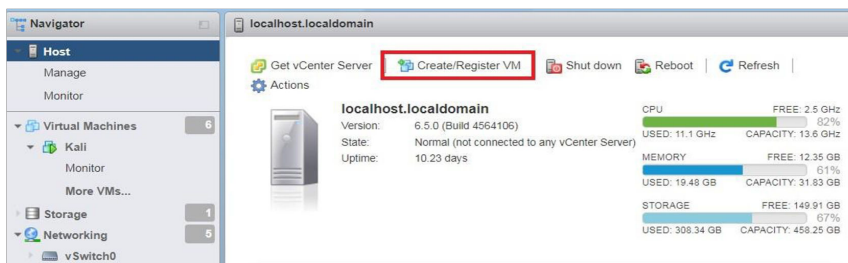


FIGURE 3-1. Navigator

3. In **Select creation type**, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

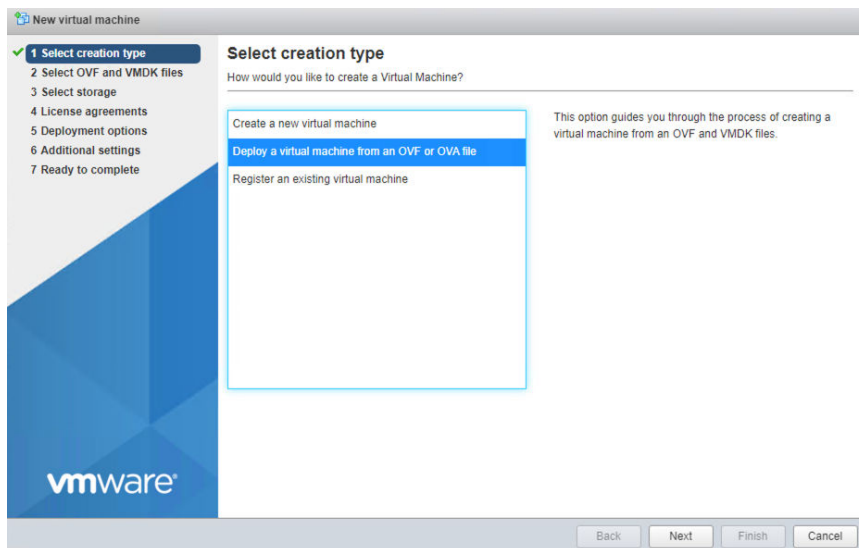


FIGURE 3-2. Select creation type

- Specify a name for your new StellarOne instance and select the StellarOne disk image to upload.

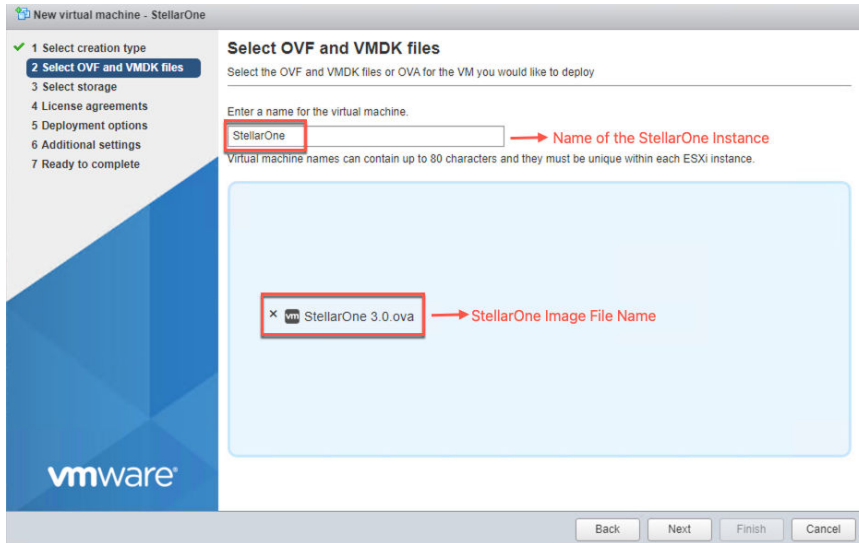


FIGURE 3-3. Select OVF and VMDK files

- Choose a storage location for the StellarOne instance and click **Next**.

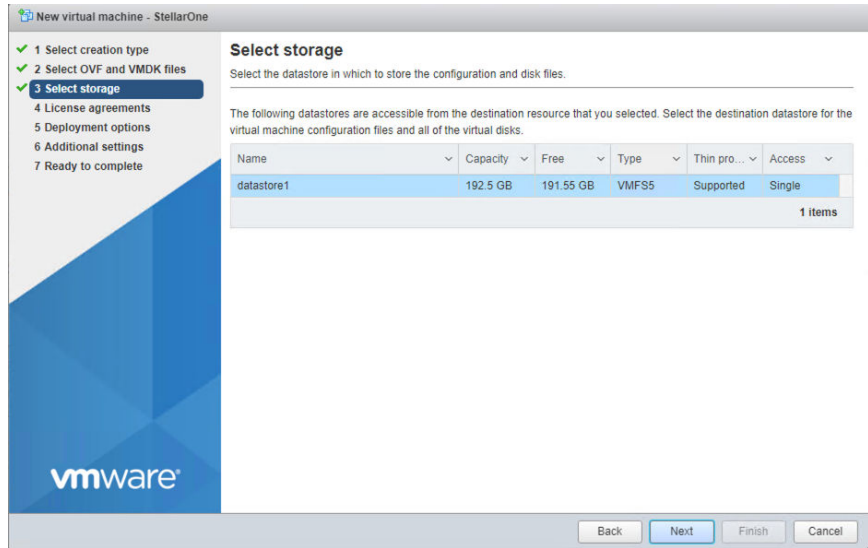


FIGURE 3-4. Select storage

6. Select deployment options and click **Next**.

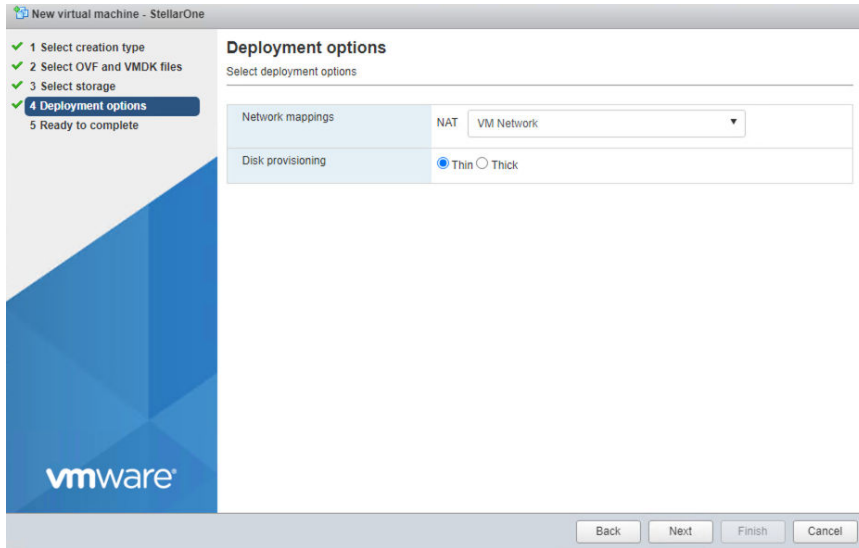


FIGURE 3-5. Deployment options

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

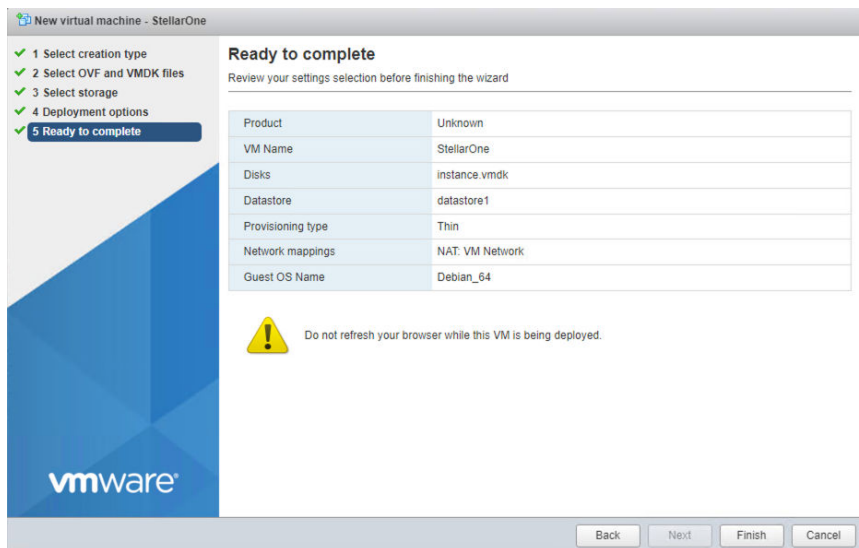


FIGURE 3-6. Ready to complete

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.



Note

See [Hardware Requirements for Deploying StellarOne on VMware/Hyper-V/AWS EC2 on page 2-3](#) for the recommended 2nd disk size for StellarOne.

- b. Follow the procedures to add the external disk: **Actions > Edit settings > Add hard disk > New hard disk**

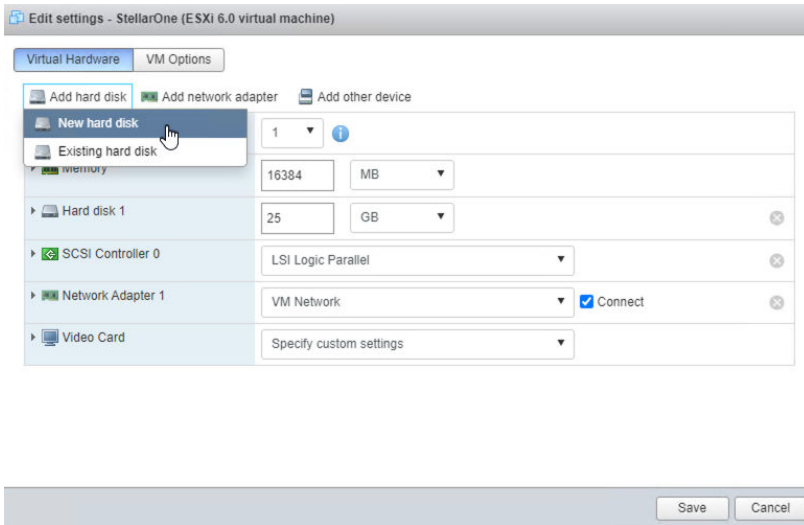


FIGURE 3-7. Edit settings - New hard disk

- c. Set the new hard disk space to 50 GB.

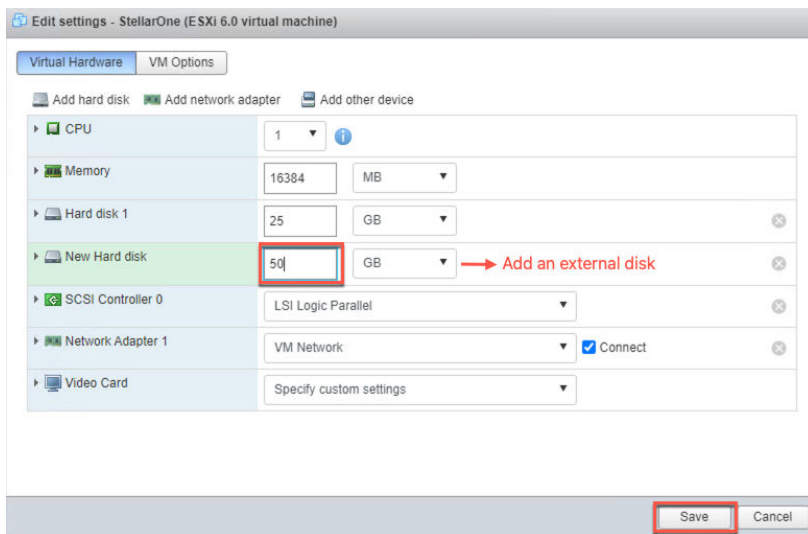
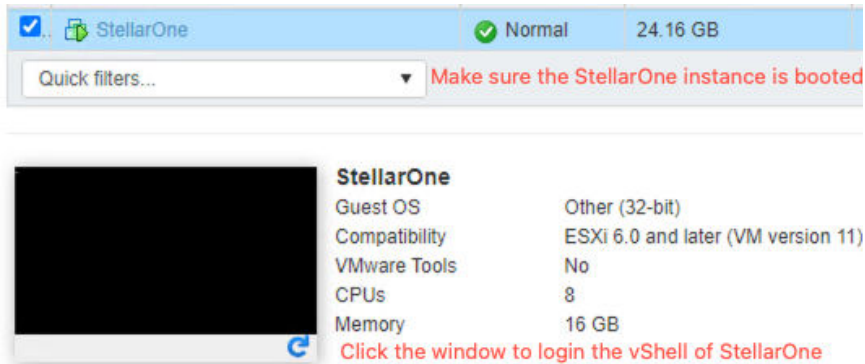


FIGURE 3-8. Edit settings - New hard disk capacity

- a. If you need to increase the number of logs StellarOne can store, follow the procedures.
 1. Shut down StellarOne
 2. Increase the external disk capacity to fit the maximum log requirements
 3. Restart the StellarOne instance. After that, the storage space available for StellarOne log files will be expanded.
- b. If you want to migrate the existing StellarOne settings to the newly launched virtual machine, see [System Migration on page 5-5](#).

**Note**

- a. StellarOne requires one external disk with minimum capacity of 50GB; otherwise, StellarOne will not finish initialization and will not complete the boot process.
- b. 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 virtual machine.**FIGURE 3-9. VM turned on**

11. (Optional) Adjust your StellarOne instance to use the proper resource configurations based on the default setting of 8 CPU cores and 16 GB Memory.
 - a. Shut down the StellarOne instance and click **Actions > Edit settings**. The **Edit settings** window appears.
 - b. Configure the number of CPU cores.

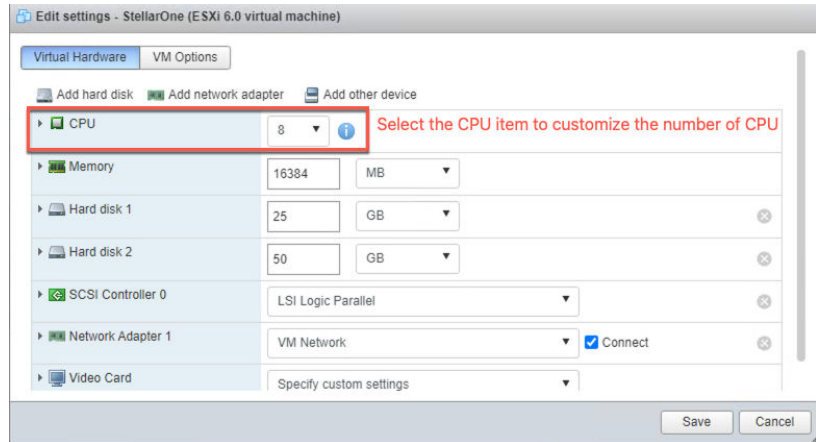


FIGURE 3-10. Select number of CPU

- c. Configure the amount of Memory.

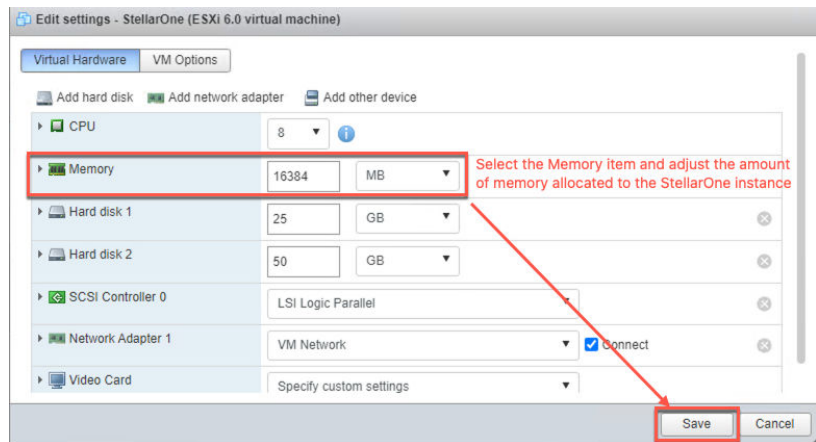


FIGURE 3-11. Configure Memory



Note

See the [Hardware Requirements for Deploying StellarOne on VMware/Hyper-V/AWS EC2 on page 2-3](#) for the CPU and memory requirements for agent deployment and corresponding StellarOne configuration and resource allocation.

- d. Boot the StellarOne instance.
-

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

The following section describes the procedures of deploying StellarOne from a VHDX File to a Hyper-V system.

Procedure

1. Launch **Hyper-V Manager**

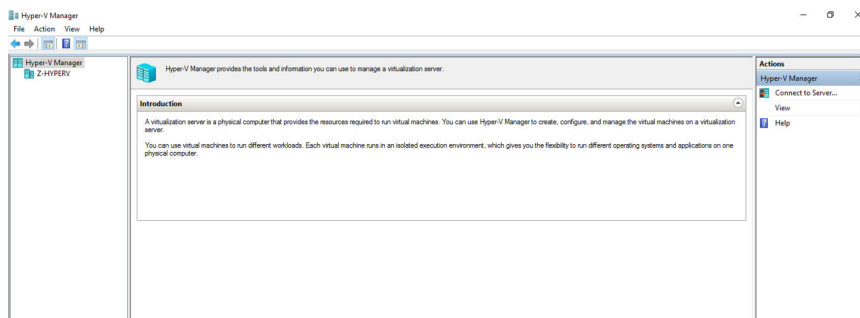


FIGURE 3-12. Hyper-V Manager

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

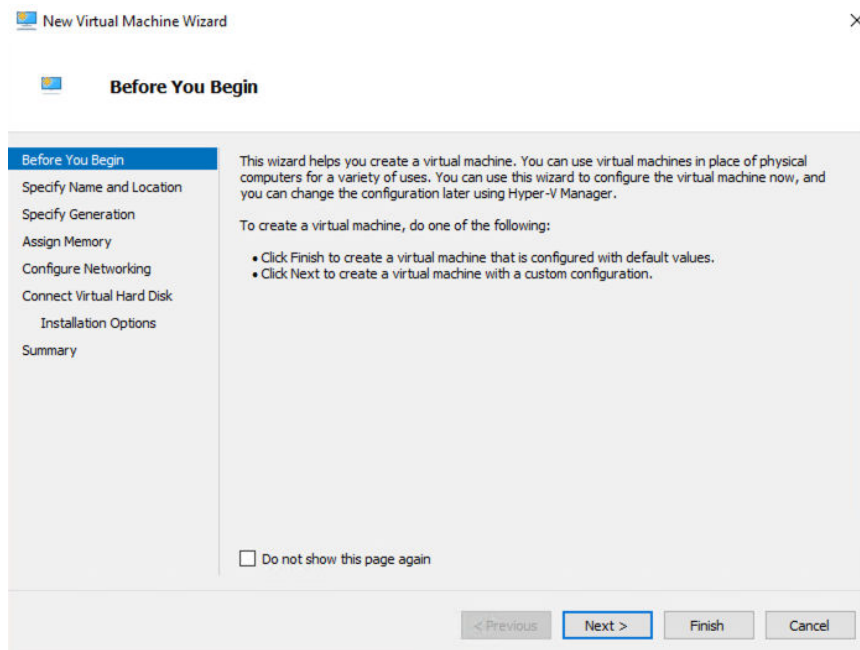


FIGURE 3-13. New Virtual Machine Wizard: Before You Begin

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

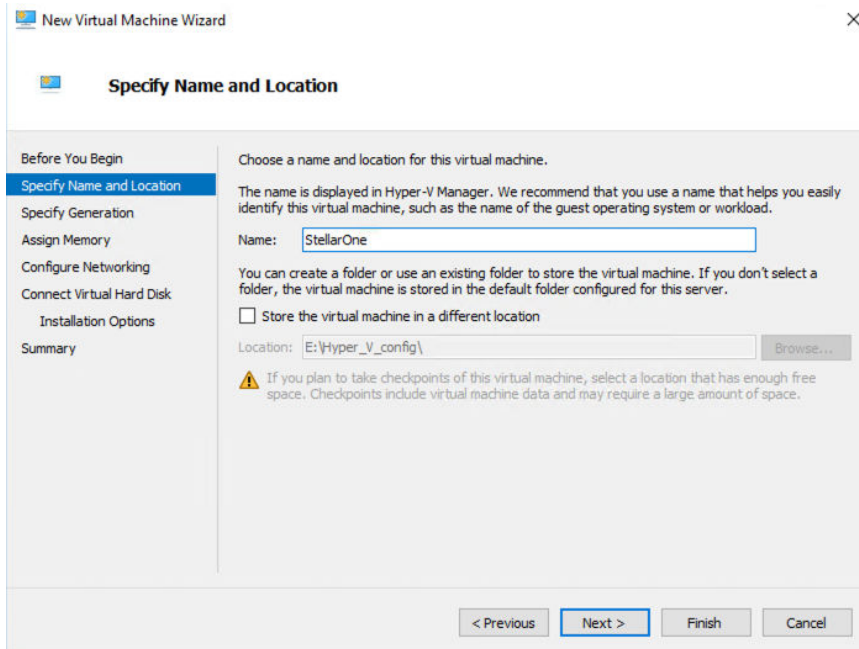


FIGURE 3-14. New Virtual Machine Wizard: Specify Name and Location

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

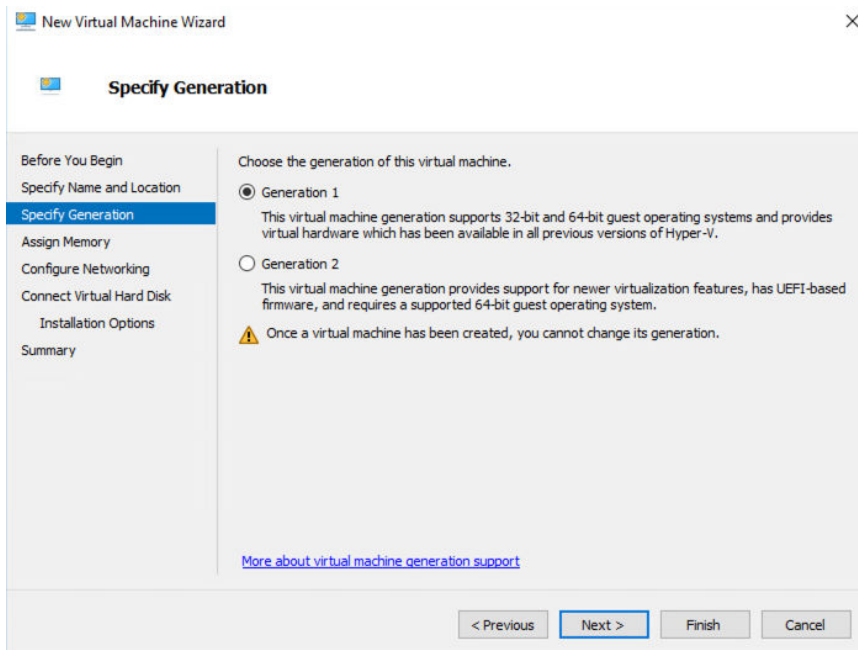


FIGURE 3-15. New Virtual Machine Wizard: Specify Generation

6. In **Assign Memory**, allocate memory for the new virtual machine and click **Next**.

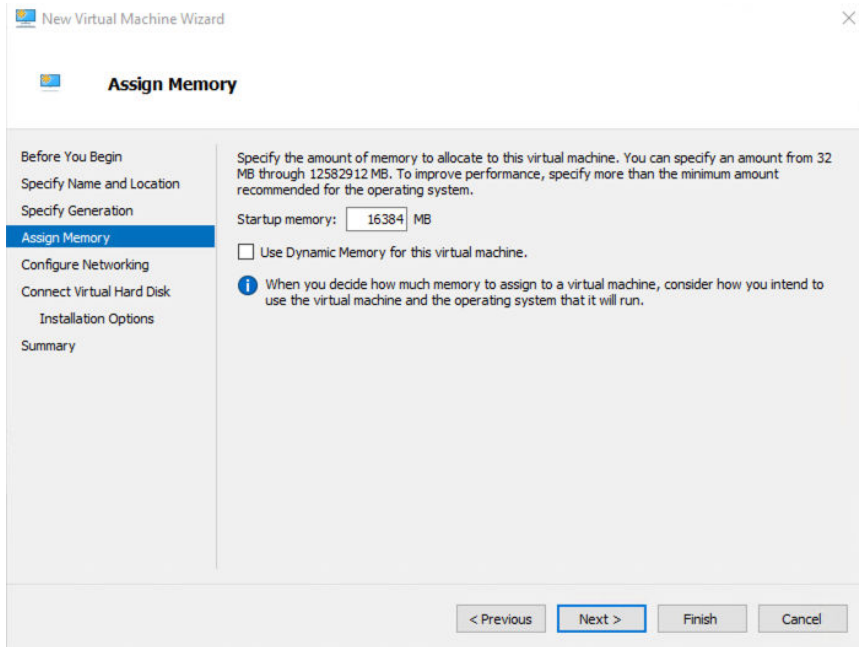


FIGURE 3-16. Assign Memory for Virtual Machine



Note

For further agent deployment and configurations, it is recommended to at least meet the hardware requirements: 8 CPU cores and 16 GB Memory.

7. Configure the network settings for the new virtual machine, and then click **Next**.

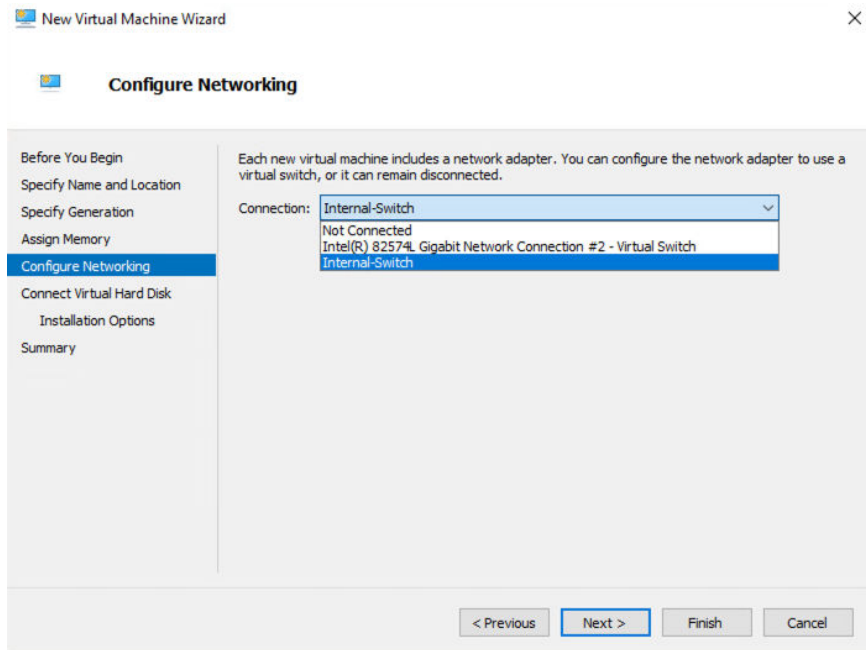


FIGURE 3-17. Configure Networking for Virtual Machine

8. Select a virtual hard disk (the StellarOne .vhdx file) and click **Next**.

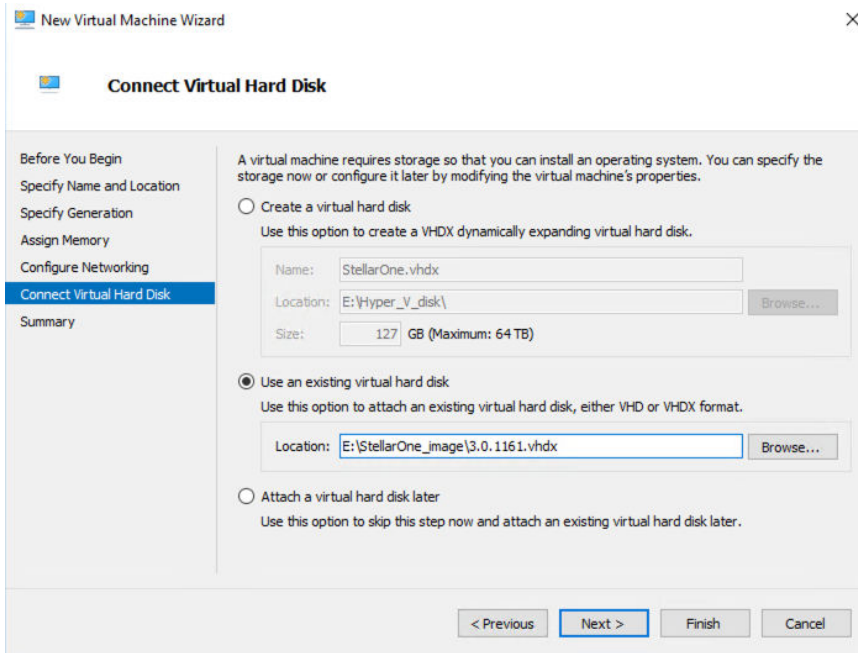


FIGURE 3-18. Connect Virtual Hard Disk

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

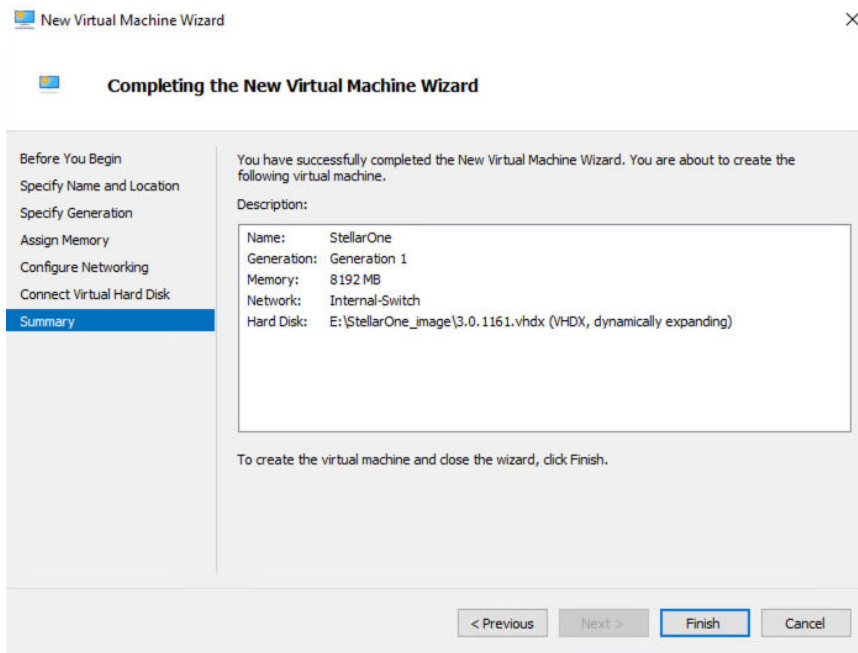


FIGURE 3-19. Completing the New VM Wizard

10. Add a new disk for the StellarOne virtual machine.



Note

Make sure the previous StellarOne instance is turned off.

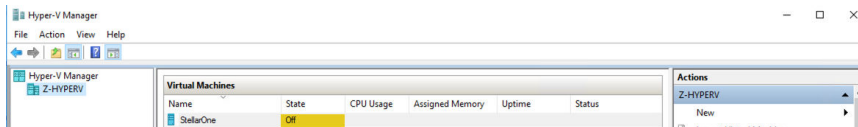


FIGURE 3-20. State of StellarOne instance is off

- a. Select the StellarOne virtual machine and right click to select **Settings** from the context menu.

- b. Select **Hard Drive** from the **IDE Contoller 0** item and click **Add**.

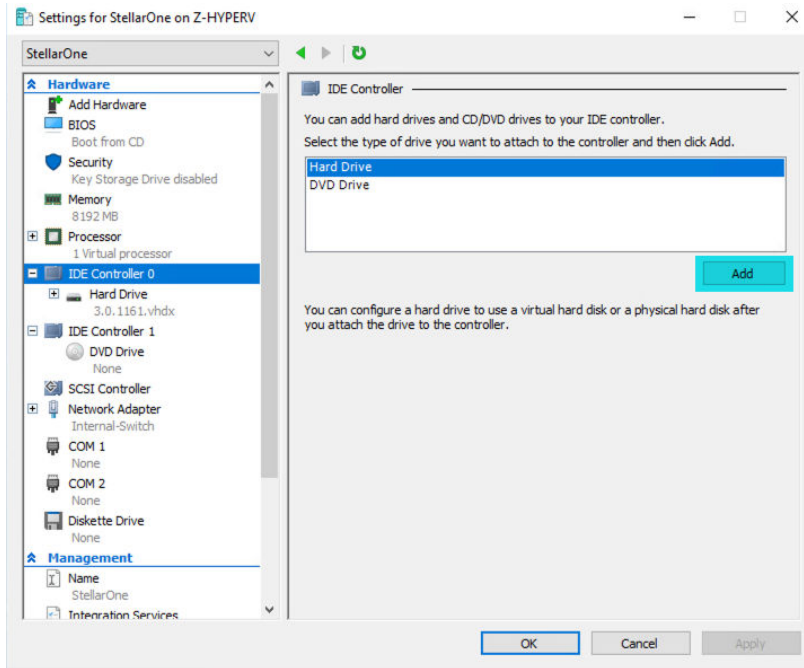


FIGURE 3-21. Settings for StellarOne - 1

- c. Click **New**.

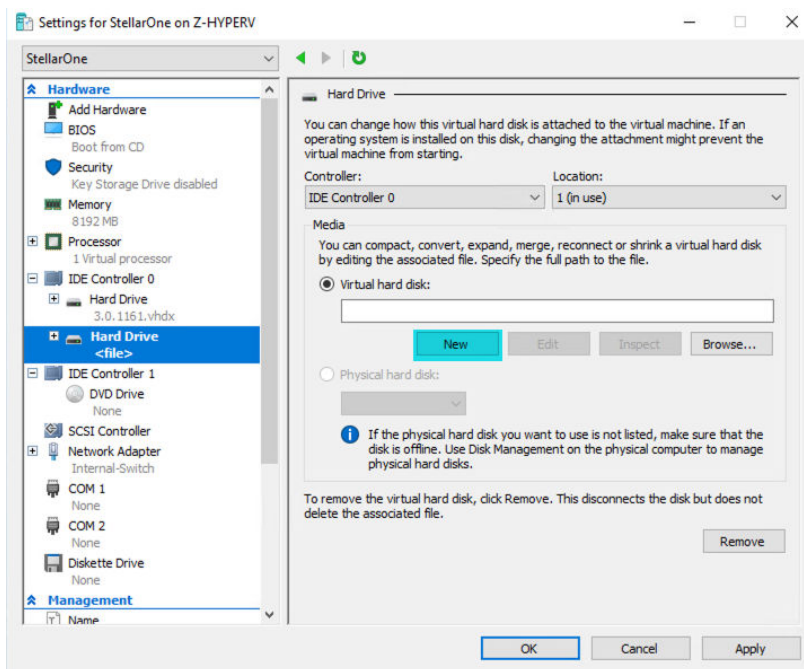


FIGURE 3-22. Settings for StellarOne - 2

- d. The **New Virtual Hard Disk Wizard** appears. Click **Next**.
- e. In **Choose Disk Format**, select **VHDX** as the disk format and click **Next**.

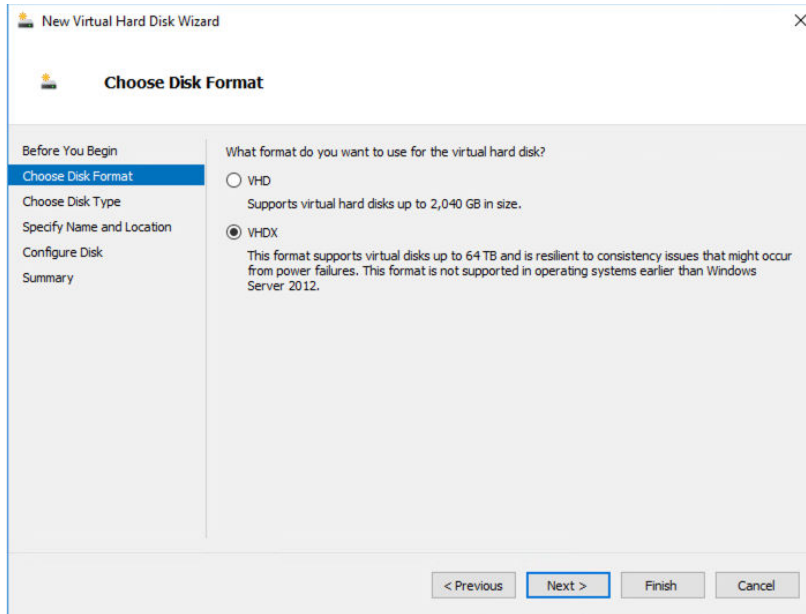


FIGURE 3-23. Choose Disk Format

- f. In **Choose Disk Type**, select **Dynamically expanding** as the disk type and click **Next**.

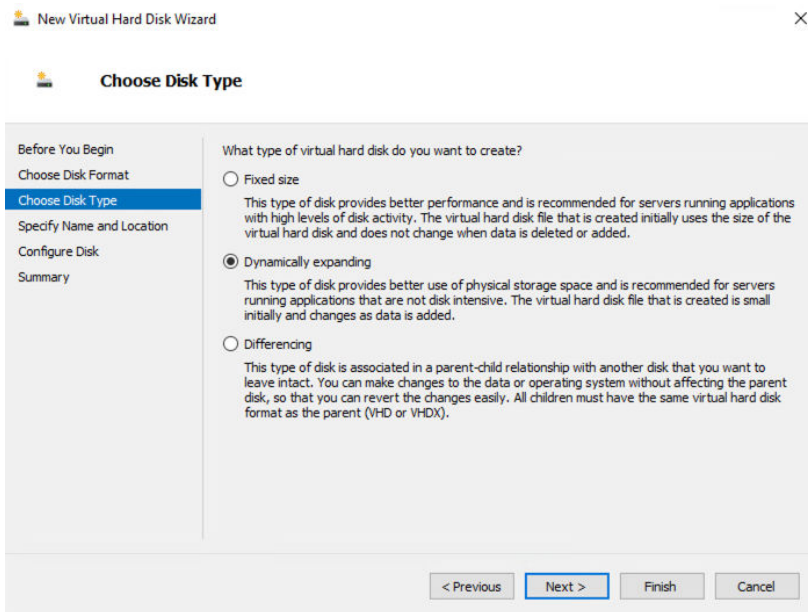


FIGURE 3-24. Choose Disk Type

- g. Specify the name and location of the virtual hard disk file.

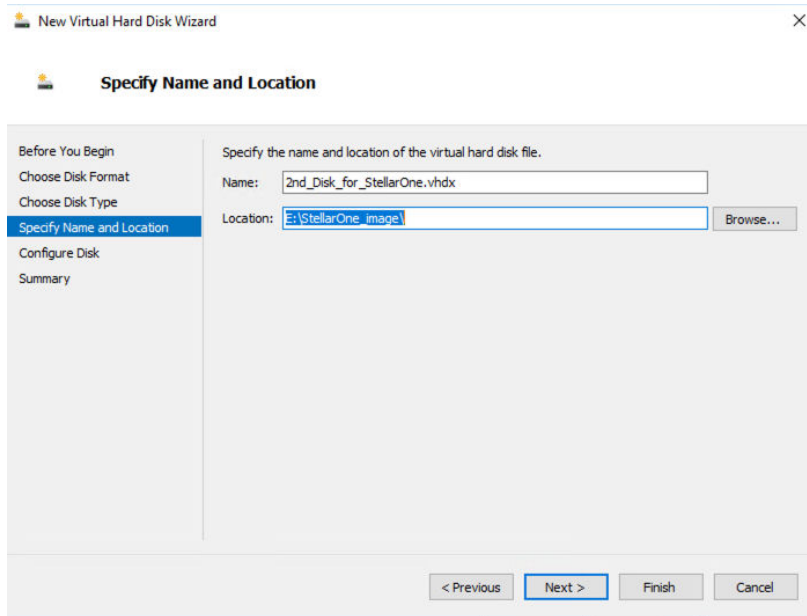


FIGURE 3-25. Specify Name and Location

- h.** Configure disk size.



Note

See [Hardware Requirements for Deploying StellarOne on VMware/Hyper-V/AWS EC2 on page 2-3](#) for the recommended 2nd disk size for StellarOne.

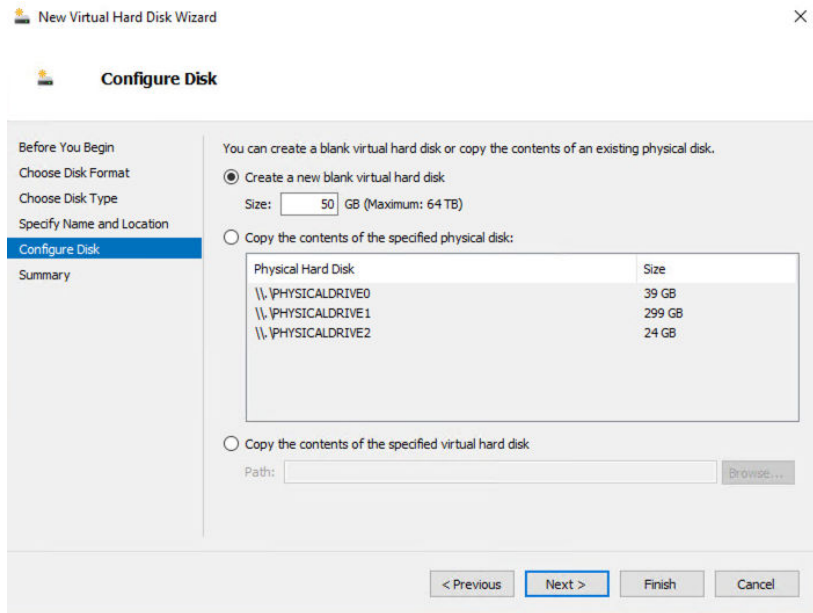


FIGURE 3-26. Configure Disk for StellarOne

- i. Click **Next** to check your settings.

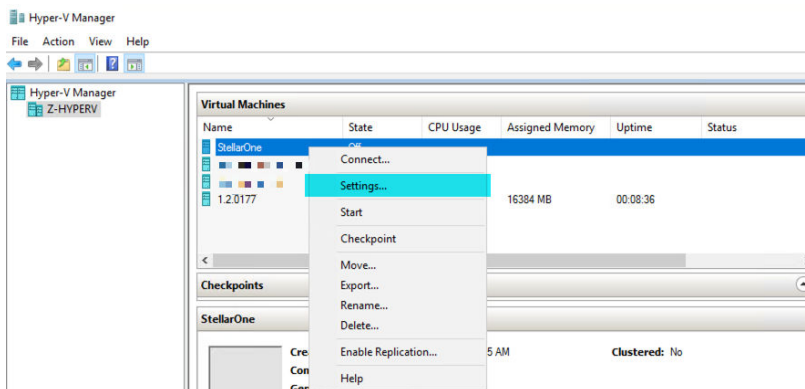


FIGURE 3-28. Configure the settings of StellarOne instance

- b.** In **Processor**, configure the number of virtual processors and the associated resource control settings. Click **OK** to complete the settings.

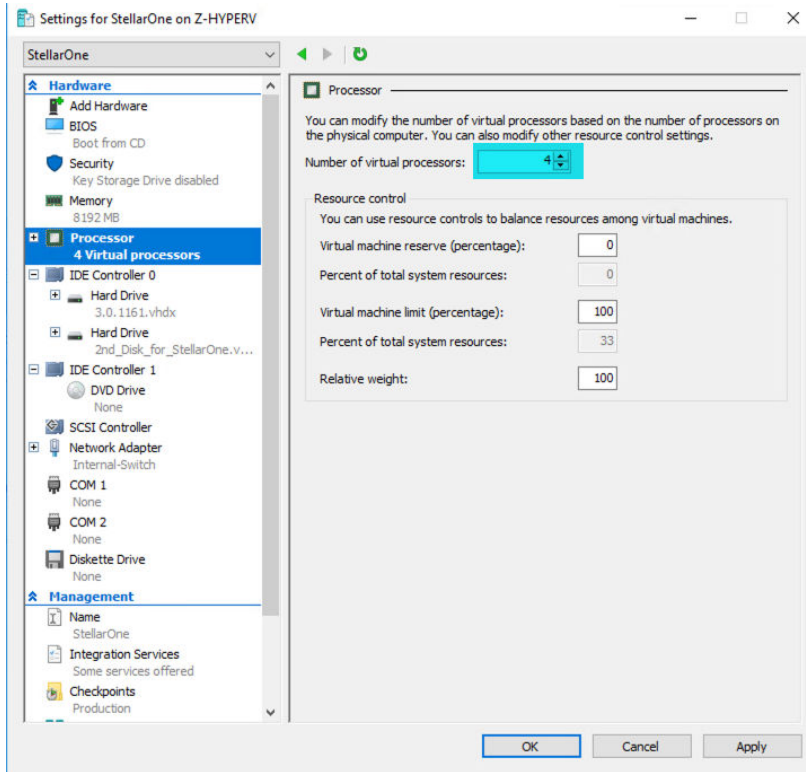


FIGURE 3-29. Configure the processor settings of StellarOne instance

- c. In the **Memory** section, specify the amount of memory that the StellarOne instance can use.

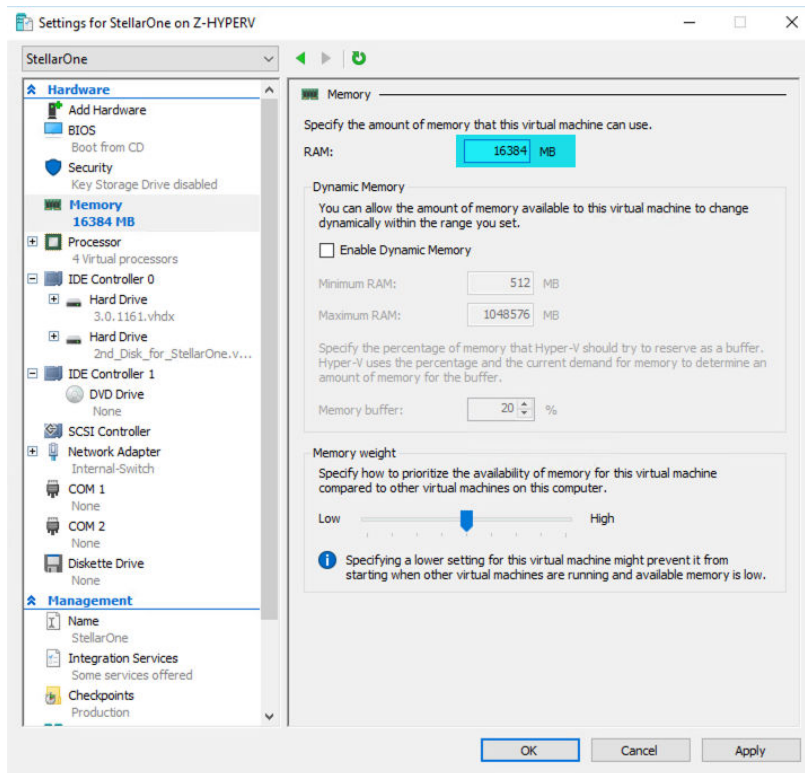


FIGURE 3-30. Configure the memory settings of StellarOne instance

- 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 navigation bar with links for 'Product Detail', 'Subscribe', 'Configure', and 'Launch'. The main content area is titled 'Launch this software' and includes a sub-header 'Review the launch configuration details and follow the instructions to launch this software.' A red box highlights the 'Configuration details' section, which contains 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 is a 'Usage instructions' button. A second red box highlights the 'Select a launch action' dropdown menu, which has 'Launch through EC2' selected. To the right of this dropdown is the text 'Choose this action to launch from this website'. Below the dropdown is the 'EC2 Instance Type' section, which shows 'm3.medium' selected in a dropdown menu. To the right of the instance type dropdown are the following specifications:

- Memory: 3.75 GiB
- CPU: 3 EC2 Compute Units (1 virtual core)
- Storage: 1 x 4 GiB SSD
- Network Performance: Moderate

FIGURE 3-31. 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.

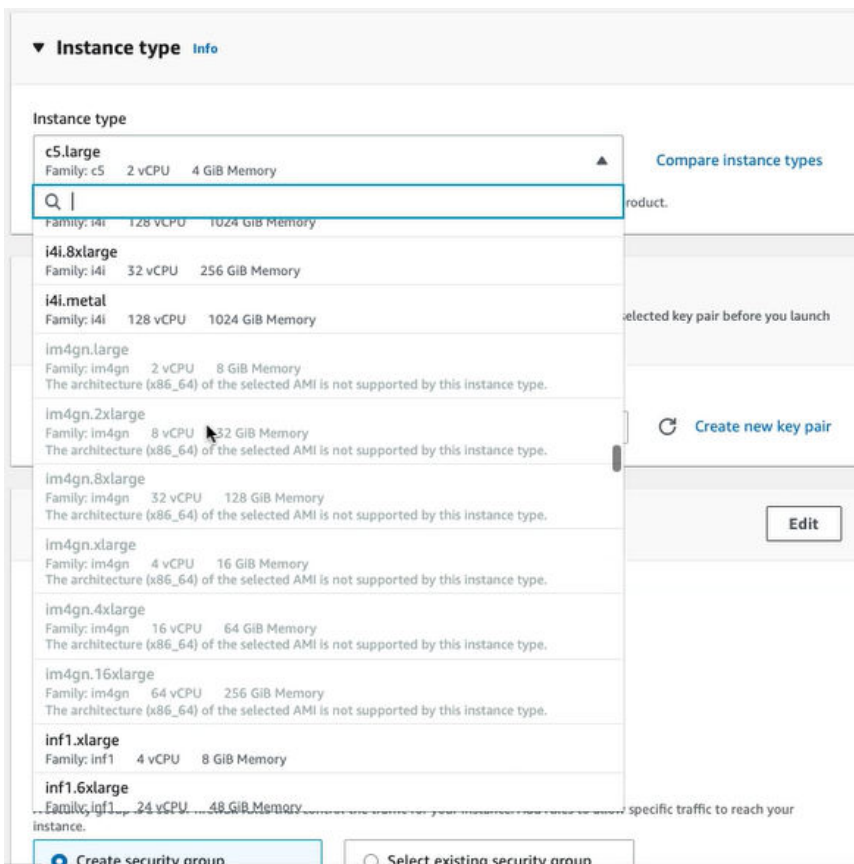
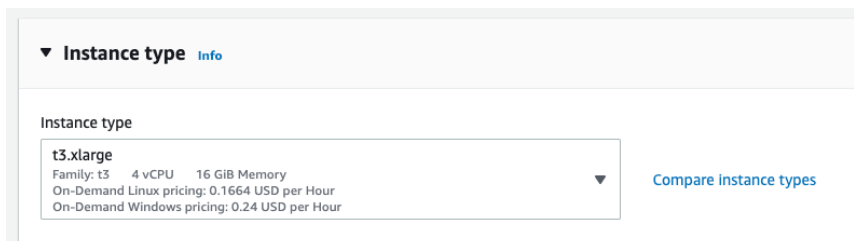


FIGURE 3-32. Select an Instance Type



▼ Instance type [Info](#)

Instance type

t3.xlarge
 Family: t3 4 vCPU 16 GiB Memory
 On-Demand Linux pricing: 0.1664 USD per Hour
 On-Demand Windows pricing: 0.24 USD per Hour

[Compare instance types](#)

FIGURE 3-33. Information of the Selected Instance Type

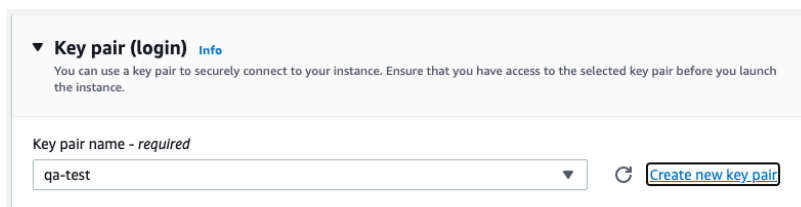


Note

- The instance types that do not meet StellarOne's deployment requirements will be unavailable for selection.
- See [Hardware Requirements for Deploying StellarOne on VMware/Hyper-V/AWS EC2 on page 2-3](#) for determining which instance type to use.

12. Configure the instance settings:

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



▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

qa-test

[Create new key pair](#)

FIGURE 3-34. 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**

See *Ports and FQDN Used on page 2-6* 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 recommended 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
0.0.0.0/0
Helps you connect to your instance
- 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 3-35. 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 25 GiB gp3 Root volume (Not encrypted)

1x 50 GiB gp3 EBS volume (Not encrypted) Remove

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

Add new volume

0 x File systems Edit

FIGURE 3-36. 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 for EC2 instances. 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 'Instances' (New), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances' (New), 'Dedicated Hosts', 'Scheduled Instances', and 'Capacity Reservations'. The main content area displays 'Instances (1/1) Info' for a single instance named 'qa-test' with ID 'i-026...'. The instance state is 'Running'. Below the instance list, the details for 'Instance: i-026...' are shown, including 'IP name: ip-172-...', 'Answer private resource DNS name', 'IPv4 (A)', and 'Auto-assigned IP address'. The 'Auto-assigned IP address' is highlighted with a red box, and a tooltip shows 'Auto-assigned IP address 3.94' with a green checkmark and 's copied'.

FIGURE 3-37. Auto-assigned IP address



Note

The auto-assigned IP address may change if the instance has been rebooted. See [Associating the Elastic IP Address with an Instance on page 3-39](#) for assigning a static IPv4 address to your instance.

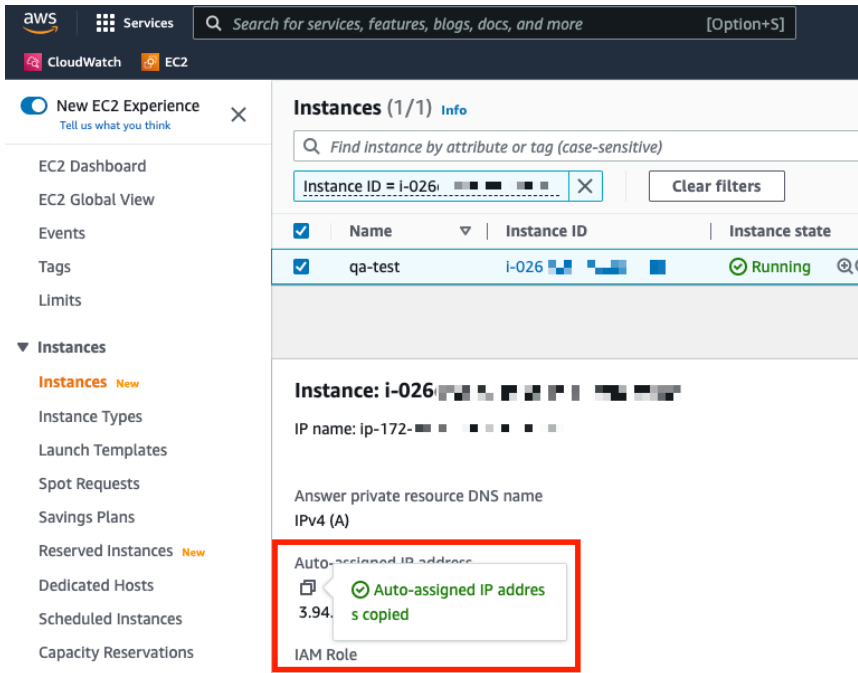
14. See [Opening StellarOne Management Console on page 3-43](#) for logging on StellarOne via a web browser, or [Accessing StellarOne via SSH on page 3-37](#) for accessing StellarOne via SSH.

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.



The screenshot shows the AWS Management Console interface for EC2 instances. The left sidebar contains navigation options like 'New EC2 Experience', 'EC2 Dashboard', and 'Instances'. The main content area displays a table of instances with columns for Name, Instance ID, and Instance state. One instance named 'qa-test' with ID 'i-026...' is highlighted. Below the table, the details for the selected instance are shown, including 'IP name: ip-172-...', 'Answer private resource DNS name', and 'IPv4 (A)'. The 'Auto-assigned IP address' section is highlighted with a red box, showing the IP address '3.94...' and a green checkmark indicating it has been copied.

FIGURE 3-38. 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 3-39](#) 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 (35.168.1.1)

Elastic IP address: 35.168.1.1

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

Private IP address
The private IP address with which to associate the Elastic 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 3-40. Associate the Elastic IP Address with an Instance

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

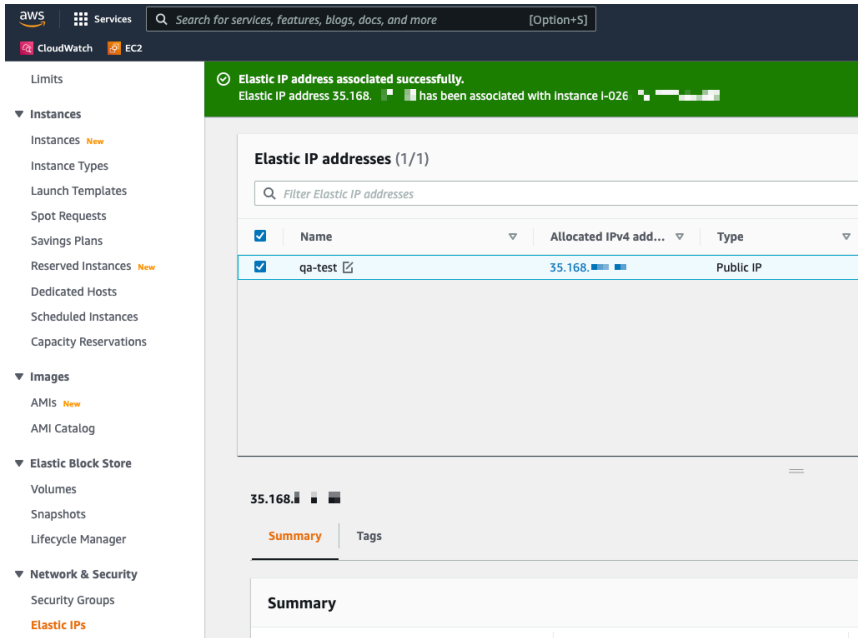


FIGURE 3-41. Associate Elastic IP Address

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. For VMware or Hyper-V system, launch the StellarOne instance and then run the OOB process in the setup CLI.
 - a. Use the default credentials when logging on for the first time:
 - Username: `root`
 - Password: `txone`
 - b. Change the default credentials to your desired username and password.
-



Important

To enhance security, it is recommended to create a safe username and strong password.



Note

For StellarOne instance deployed from AMI on AWS EC2 platform, the OOB process is not required.

2. Open a web browser and enter the StellarOne address in the following format: `https://<targetserver IP address>`. The logon screen appears.
3. 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`
4. Click **Log On**.
5. If this is the first time the StellarOne instance being logged on, follow procedures below 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 cannot 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. StellarOne recognizes two license formats (**License Key** and **Activation Code**) available from different sales channels. See [Comparison of License Formats on page 3-46](#) first to find the license format that matches the given license data.
- e. See the following instructions for how to activate license depending on the network environment.
- **StellarOne has Internet connection**
 1. Click **License Key**.
 2. Specify the License Key or Activation Code in the text field.
 - **StellarOne has NO Internet connection**
 - If the given license format is Activation Code, click **License Key** and specify the Activation Code in the text field.

- If the given license format is License Key, use it to download the License File (a .txt file). See [Getting the License File on page 3-46](#) for the detailed procedures. After getting the License File, click **License File** and import it.
- f. Click **Apply**.
 - g. A success message appears. The license information also appears at the bottom of the **License Activation** window. Check if it matches the given license data.

**Note**

See [Resolving Licensing Issues on page 6-4](#) if licensing related error messages appear.

- 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 recommended to enable **TXOne OT Intelligent Trust** to enhance security deployment. See [OT Intelligent Trust on page 3-48](#) 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.

6. (Optional) You can change your password by clicking the ID icon at the top right corner of the screen, and then selecting **Change Password**.

7. (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.

Comparison of License Formats

StellarOne recognizes two formats of product license purchased from TXOne Networks or from a TXOne Networks authorized reseller.

TABLE 3-1. Comparison of Two Different License Formats

		LICENSE KEY	ACTIVATION CODE
Length		19 characters	37 characters
Example		FIJN-HPYB-XXXX-XXXX	TE-24RF-Q9UN9-S9QQN-XXXXX-XXXXX-XXXXX
New license	Online	√	√
	Offline	License File	√
License renewal	Online	√	√
	Offline	License File	N/A

**Note**

A License Key is required for downloading a License File.

Getting the License File

Procedure

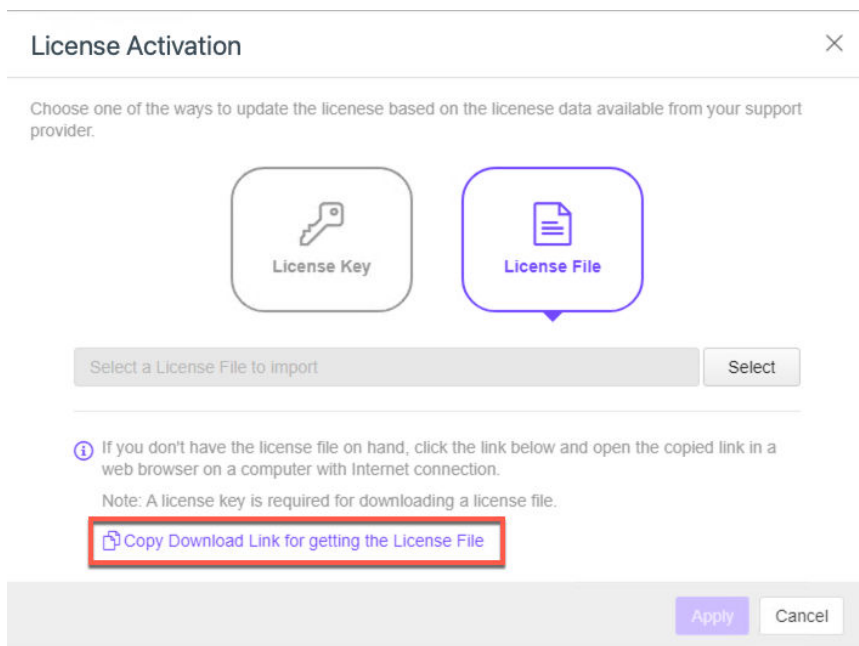
1. When you log on StellarOne using your new credentials after the **Login Information Setup** procedure, the **License Activation** window appears.
2. Click **License File**.
3. Click **Copy Download Link for getting the License File** at the bottom of the **License Activation** window.



Important

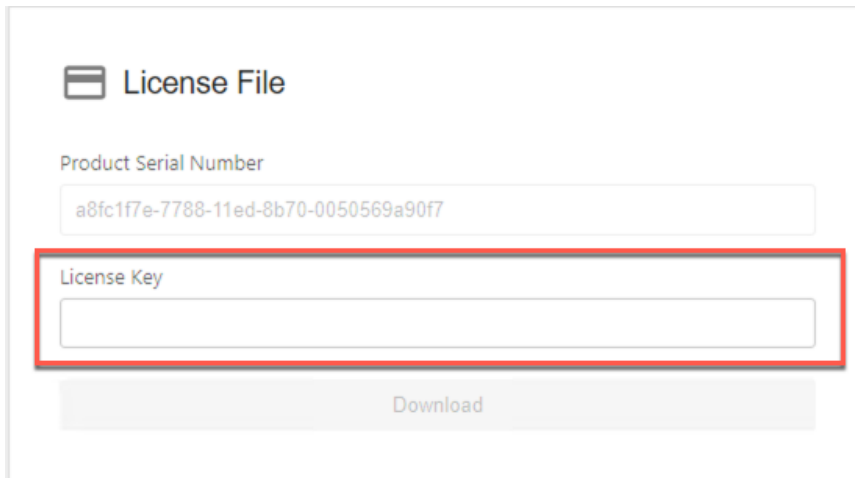
A License Key is required for downloading a License File.

FIGURE 3-42. Copy Download Link for License File



4. **The Download Link has been copied** toast message appears.

5. Open the copied link in a web browser on a computer with Internet connection.
6. You will be directed to the TXOne **License File Management** screen. Specify the given 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 this, 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 3-43. TXOne License File Management

7. 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 entering the username and password changed during the OOBЕ process. See [Opening StellarOne Management Console on page 3-43](#) for more details.



Note

For StellarOne instance deployed from AMI on AWS EC2 platform, the OOBЕ process is not required. You can just enter `admin` to log on.

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
```

**Note**

It is suggested to configure the StellarOne advertise address for the agents to communicate with if there's possibility to change StellarOne IP address in the future. See [Configuring the Advertise Address via CLI on page 4-6](#) for more details.

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
chk         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 info 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
```

**Note**

You can choose to specify the IP address, FQDN, or type `default` to use the default IP address for StellarOne.

- (Optional) If the specified advertise address can not be resolved, type the `--force` command after it to force the setup:

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

- Reload the StellarOne web console by typing:

```
service reload
```

```
$ env advertise-addr S1.txone.com
vShell: unable to resolve address S1.txone.com or it's an invalid IP. Try to add --force after the address to force the setup.
$ env advertise-addr S1.txone.com --force
Successfully set up advertise address: S1.txone.com. Please reload the service to take effect.
$ service reload
Start to reload services...
```

- Type the following command to check the advertise address settings.

```
env ls
```

```
$ env ls
Hostname:                ODC
Status:                  RUNNING
Product Serial Number:  b2
Version:                 2.2.1148
Advertise Address:      S1.txone.com
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 4-6. Checking Advertise Address Settings

- After the setup, the agent installer package and the SAML SSO (Single Sign-On) metadata file downloaded from StellarOne should contain the configured advertise address, allowing the quick deployment for the


```

<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:protocol" >
    <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 xmlns="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://10.8.150.84/saml/acs" Index="1"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://10.8.150.84/saml/acs" Index="2"/>
  </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:protocol" >
    <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 xmlns="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://s1.txone.com/saml/acs" Index="1"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://s1.txone.com/saml/acs" Index="2"/>
  </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 2-6*.

```
$ 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.



Important

Since some requirements such as the sizing table or ports and FQDN used by StellarOne may differ in different versions, it is recommended to check [Installation Planning on page 2-1](#) before performing the upgrade.

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	3.1	3.1 Patch 1	√	√
	3.0 Service Pack 1	3.1 / 3.1 Patch 1	√	√
	3.0	3.0 Service Pack 1 / 3.1 / 3.1 Patch 1	√	√
	2.2	3.0 / 3.0 Service Pack 1 / 3.1 / 3.1 Patch 1	√	√
	2.1	2.2 / 3.0 / 3.0 Service Pack 1 / 3.1 / 3.1 Patch 1	√	√
	2.0	2.1 / 2.2 / 3.0 / 3.0 Service Pack 1 / 3.1 / 3.1 Patch 1	√	√
	1.2 Patch 1 (1.2.2114)	2.0 / 2.1 / 2.2 / 3.0 / 3.0 Service Pack 1 / 3.1 / 3.1 Patch 1	N/A	√
	1.2	2.0 / 2.1	N/A	√
	1.2	1.2 Patch 1 (1.2.2114)	√	√
	VMWare	1.1	1.2 / 1.2 Patch 1 (1.2.2114)	√
1.0		1.1	N/A	√

**Important**

- Though StellarOne 3.0 requires more external disk capacity to use the advanced Operations Behavior Anomaly Detection feature, please upgrade StellarOne to 3.0 first for optimizing the disk usage before increase the 2nd disk space .
 - The 2nd disk space requirement for StellarOne varies depending on whether certain feature is enabled. See [Hardware Requirements for Deploying StellarOne on VMware/Hyper-V/AWS EC2 on page 2-3](#) to check if the storage requirement is fulfilled.
 - Do not use firmware upgrade to update StellarOne 1.0, 1.2, or 1.2 Patch1 to a later version (except for upgrading 1.2 to 1.2 patch 1). 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 5-5](#) or [Mount Upgrade \(Hyper-V\) on page 5-7](#) for more details.
 - 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-Vsystem.

**Note**

Since StellarProtect and StellarProtect (Legacy Mode) agent events will be combined into one display page after upgrading StellarOne to version 3.1, some events may exceed the limit and thus be deleted. Ensure you check the current event quantities and adjust the **Log Purge** configuration before the upgrade. Refer to the *StellarOne Administrator's Guide* for more information about how to adjust the **Log Purge** settings.

Topics in this section include:

- [Firmware Upgrade on page 5-4](#)
- [Mount Upgrade \(VMware\) on page 5-5](#)
- [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-3.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.

FIRMWARE

Update downloaded. StellarOne is ready to install. Please click the Install button to start the installation. After completing Installation, the system may restart all services.

Notice

- The installation may take 5 to 10 minutes to finish. Please do not shut down the StellarOne during the installation
- We highly recommended you to back up your data before starting the installation.
- The system will not support downgrading to an earlier version.

 Install Now

 Abort

FIGURE 5-1. Firmware Install



Note

Before executing the firmware upgrade, please create a back up of the VM files first.

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

Mount Upgrade (VMware)

This section describes how to perform mount upgrade for StellarOne on VMware ESXi 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 backup of the VM files first.
 - StellarOne 2.0 ONLY supports mount upgrade from version 1.2 or 1.2 Patch 1. Make sure you upgrade StellarOne 1.1 to 1.2 or 1.2 Patch 1 before upgrading to 2.0.
 - StellarOne 1.1 ONLY supports mount upgrade from version 1.0.
-

Procedure

1. Deploy a new StellarOne instance. See [Deploying StellarOne on the VMware ESXi on page 3-2](#) for detailed instructions.
2. Close the previous StellarOne instance.

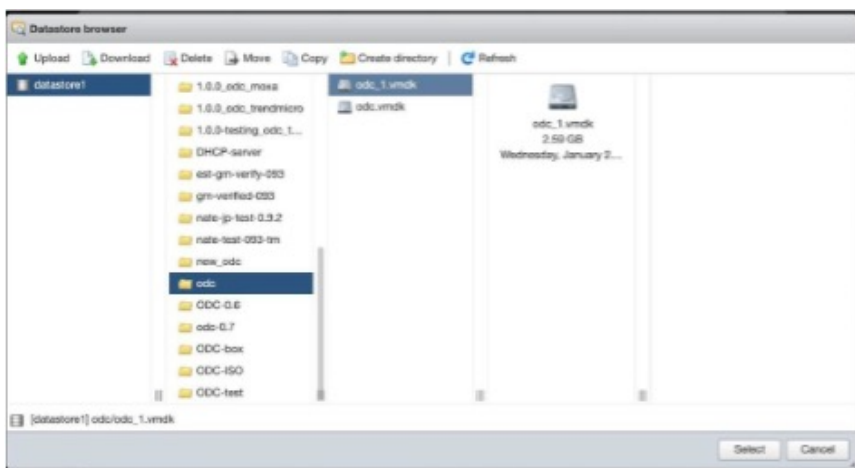


FIGURE 5-4. Attach to New VM

4. Boot up the new StellarOne instance.



Note

The data of the previous StellarOne instance has been migrated to the 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 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 backup of the VM files first.
 - StellarOne 2.0 ONLY supports mount upgrade from version 1.2 or 1.2 Patch 1.
-

Procedure

1. Deploy a new StellarOne instance. See [Deploying StellarOne to a Hyper-V System on page 3-12](#) 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.

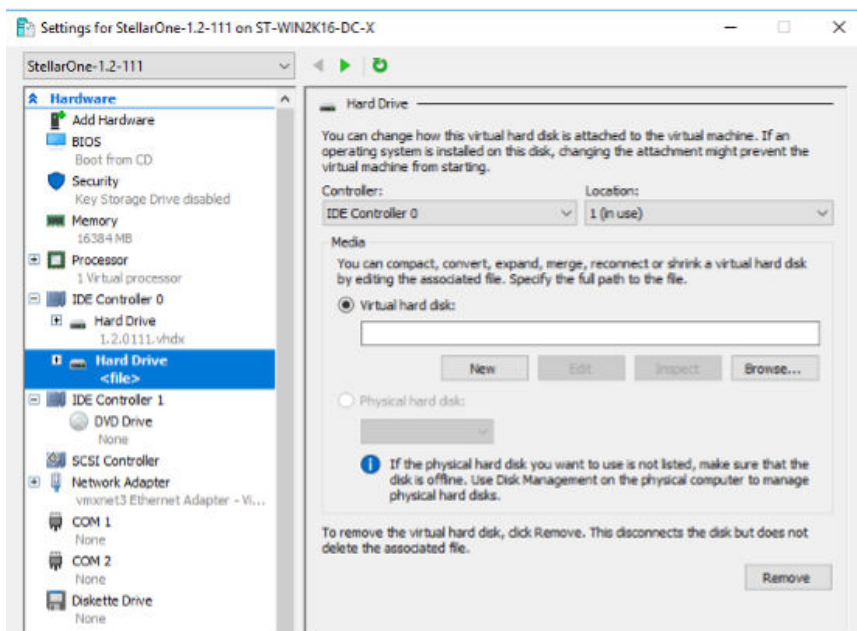


FIGURE 5-5. Shut Down the Previous VM

5. Boot up the new StellarOne instance.



Note

The data of the previous StellarOne instance has been migrated to the 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 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

Getting Help and Troubleshooting

Learn about the following topics:

- *Troubleshooting Resources on page 6-2*
- *Contacting TXOne Networks on page 6-6*
- *Other Resources on page 6-7*

Troubleshooting Resources

Before contacting technical support, consider visiting the following TXOne Networks online resources.

Self-Diagnosis

Identify and troubleshoot low disk space issues with StellarOne.

- [Resolving Low Disk Space Issues on page 6-2](#)
- [Resolving Licensing Issues on page 6-4](#)

Resolving Low Disk Space Issues

To keep you informed of your disk usage, and any potential issues that may arise, StellarOne displays banners or modal windows at certain disk usage thresholds. When encountering such errors, you can check the following table for the features affected and take actions as suggested in the **Workaround** column.

However, the most efficient way to get rid of low disk space error caused by the 2nd HDD is to add more space to the drive or partition. Follow the procedures:

1. Go to **Dashboard** to check the Disk Usage widgets.
2. Check the following table for the features that will become unavailable at certain usage thresholds.
3. Extend the drive or partition which is running out of space.

**Note**

- If you take snapshots for the StellarOne virtual machine, ensure the snapshot files be consolidated before extending the partition space.
 - Contact your support provider if you need to fix the low disk space error caused by the 1st HDD.
-

TABLE 6-1. Unavailable Features List due to Low Disk Space

UNAVAILABLE FEATURES	MENU PATH	DESCRIPTION	USAGE THRESHOLD	WORKAROUND
Firmware upgrade	Administration > Update > Firmware	Unable to import the StellarOne firmware for upgrade	<ul style="list-style-type: none"> • 1st HDD disk space less than 3 GB • 2nd HDD disk space on System partition less than 3 GB 	Free up the 2nd HDD disk space on System partition by: <ul style="list-style-type: none"> • Deleting unused patch files • Purging unwanted agent debug logs
Agent patch file import	Administration > Downloads/ Updates > Agent	Unable to import Agent patch files	<ul style="list-style-type: none"> • 2nd HDD disk usage on System partition less than 20% 	
Agent debug tool collection	StellarOne debug page (for SEG purpose)	Unable to collect the debug logs for StellarProtect or StellarProtect (Legacy Mode)	<ul style="list-style-type: none"> • 2nd HDD disk usage on Database partition less than 20% 	
Debug log level selection		Unable to select the Info or Verbose log level. Only the Warn (Default) level logs can be collected.		
Server debug tool collection		Unable to collect the debug logs for the StellarOne server		

Resolving Licensing Issues

The following table provides more information about some licensing error messages and possible actions to take when issues occur during license activation or renewal.

TABLE 6-2. Licensing Error Messages and Suggested Actions

ERROR MESSAGE	DESCRIPTION	POSSIBLE ACTIONS
Unable to convert the license from full to trial version. To continue using the product, please contact your sales representative for renewing the license.	Once upgraded to a full license, the full license cannot be converted to a trial license.	<ul style="list-style-type: none"> • Ensure you enter the valid full license data. • Contact your sales representative for renewing the full license.
Activation Code detected as the currently used license format. This trial license can only be used once. Please contact your sales representative for a trial License Key or upgrading to a full license.	Based on the terms and conditions, the trial Activation Code can only be used once. An example of the Activation Code : TE-24RF-Q9UN9-S9QQN-XXXXX-XXXXX-XXXXX See Comparison of License Formats on page 3-46 for more details.	To continue using the product, contact your sales representative for a trial License Key or upgrading to a full license.
License Key detected as the currently used license format. Please contact your sales representative for extending the license.	Based on the terms and conditions, the trial License Key can be extended under certain circumstances. You can also choose to upgrade to a full license for a minimum period of one-year protection coverage. If you're using a full license, consider renewing the license. An example of the License Key : FIJN-HPYB-XXXX-XXXX	To continue using the product, contact your sales representative for extending the trial license, upgrading to a full license, or renewing the full license.

ERROR MESSAGE	DESCRIPTION	POSSIBLE ACTIONS
Unable to connect to the license server. Proxy authentication is required.	This message signifies unspecified or invalid proxy authentication causes this issue that StellarOne cannot connect to the license server for license activation or renewal.	Check your proxy settings.
StellarOne has no Internet connection. You may try it again or choose to activate the license by importing the license file.	Due to unidentified network issues, StellarOne cannot connect to the license server to complete the license activation.	<ul style="list-style-type: none"> • Check your network settings and then try to activate or renew license again. • You can also use the License File to activate or renew license in the offline environment. The License Key is required for downloading the License File. See Getting the License File on page 3-46 for more information.
StellarOne has no Internet connection. You may try it again or click New License to get and import the updated license file.	Due to unidentified network issues, StellarOne cannot connect to the license server to complete the license renewal.	
Unable to renew license. Make sure your network connection between StellarOne and license server is active or check your proxy settings and then try again.	<p>Due to unidentified network issues, StellarOne cannot connect to the license server. Check your network settings and try again later.</p> <p>The Activation Code cannot be used to renew license offline.</p>	Check your network settings and then try to renew license again.

Using the Support Portal

The TXOne Networks 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://help.txone.com/>.
2. Click the appropriate button to search for solutions.

3. Use the **Search** box to search for available solutions.
4. If no solution is found, click **Live Chat** or **VoIP** service to submit a support case online.

A TXOne Networks support engineer investigates the case and responds in 24 hours or less.



Important

If the StellarOne virtual machine has been encrypted, ensure that you decrypt it for problem analysis.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. TXOne Networks 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.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 TXOne Networks

TXOne Networks representatives are available by phone or chat/VoIP services:

TABLE 6-3. TXOne Networks Contact Information

U.S.	+1 (346) 586-7975
Netherland	+31 402-310-122
Taiwan	+886 (2) 7727-5120
Chat/VoIP services	https://help.txone.com/
Website	https://www.txone.com/contact/

- TXOne Networks product documentation:

<https://my.txone.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
- Product serial number and license file, or license key
- Detailed description of the environment where the agent is installed
- Exact text of any error message received

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://my.txone.com/>

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
 - No. of Agents Deployed, 2-5
 - Total Bandwidth / Deployment Task, 2-5

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, 5-4

H

- Hardware requirements, 2-3

I

- installation, 3-29
 - Deploy on AWS EC2, 3-30
- Installation, 3-2, 3-12
 - Deploy on Hyper-V, 3-12
 - Deploy on VMware ESXi, 3-2
- Installation flow, 3-2
- Instance data encryption, 2-9

M

- Mount upgrade
 - Hyper-V, 5-7

VMware, 5-5

N

- Network bandwidth for agent deployment, 2-4

P

- Ports and FQDN, 2-6
 - FQDN, 2-6, 2-7
 - function, 2-6, 2-7
 - open port, 2-6, 2-7

R

- reference table
 - Agent Remote Patch, 2-5
 - Full Pattern Update, 2-5
 - Incremental Pattern Update, 2-5
- requirements, 2-2

S

- StellarOne Occupied Ports, 2-7
 - NTP, 2-7
 - SSH, 2-7
 - StellarOne internal service, 2-7
 - StellarProtect (Legacy Mode)
 - default port, 2-7
 - StellarProtect default port, 2-7
 - Web, 2-7
- support
 - resolve issues faster, 6-7
- Supported agent version, 2-8
- system requirements, 2-2

T

- technical support, 6-1

contact, 6-6

troubleshooting resources, 6-2

U

Upgrade paths, 5-2