

Installation Guide
for
OmniVista 2500 NMS Enterprise
Version 4.2.1.R01
(Maintenance Release 2)



May 2017
Revision F
Part Number 060444-10
READ THIS DOCUMENT
OmniVista 2500 NMS
for
VMware ESXi: 5.5 and 6.0
VirtualBox: 5.0.10
MS Hyper-V: 2012 R2 and 2016

ALE USA Inc.
26801 West Agoura Road
Calabasas, CA 91301
+1 (818) 880-3500

Table of Contents

OmniVista 2500 NMS Enterprise 4.2.1.R02 (Maintenance Release 2) Installation Guide	1
Installing OV 2500 NMS-E 4.2.1.R01 (MR2)	2
Deploying the Virtual Appliance in VMware ESXi	2
Deploying the Virtual Appliance in VirtualBox	9
Deploying the Virtual Appliance in Hyper-V	14
Completing the OmniVista 2500 NMS-E 4.2.1.R01 (MR 2) Installation	19
Upgrading From OV 2500 NMS-E 4.2.1.R01 GA or MR1	22
Appendix A – Installing Virtual Box.....	A-1
Supported Hosts	A-1
Installing Virtual Box on Windows Hosts	A-1
Installing Virtual Box on Linux Hosts	A-2
Installing Virtual Box From a Debian/Ubuntu Package.....	A-2
Using the Alternative Installer (VirtualBox.run)	A-3
Performing a Manual Installation	A-3
Appendix B – Using the Virtual Appliance Menu.....	B-1
Help.....	B-2
Configure the Virtual Appliance	B-2
Run Watchdog Command	B-12
Upgrade/Backup/Restore VA.....	B-13
Change Password	B-15
Logging	B-16
Login Authentication Server.....	B-16
Power Off	B-17
Reboot	B-17
Advanced Mode	B-17
Set Up Optional Tools	B-18
Log Out	B-18

OmniVista 2500 NMS Enterprise 4.2.1.R02 (Maintenance Release 2) Installation Guide

This document details the OmniVista 2500 NMS Enterprise 4.2.1.R01 Maintenance Release 2 (MR 2) (OV 2500 NMS-E 4.2.1.R01 (MR2)) installation/upgrade process. OV 2500 NMS-E 4.2.1.R01 MR 2 can be installed as a [fresh installation](#) from a download file available on the Customer Support website; or you can [upgrade from OV 2500 NMS-E 4.2.1.R01 GA or MR1](#) using the OmniVista 2500 NMS Software Repository.

If you are upgrading from an earlier release (3.5.7 – 4.1.2.R03), you must first upgrade to 4.2.1.R01 GA. The Upgrade Matrix below shows the upgrade paths that must be followed. Click on the links below to download the applicable *OmniVista 2500 NMS Installation Guide* or go to the application section in this document for details.

OmniVista 4.2.1.R01 (MR2) Upgrade Matrix

From	To	
	OV 4.2.1 R01-GA (Build 69)	OV 4.2.1 R01-MR2 (Build 94)
OV 3.5.7	Direct Upgrade	Step 1: Upgrade to OV 4.2.1 R01-GA Step 2: Automatic upgrade to MR2 from VA Menu
OV 4.1.1 R01	Step 1: Upgrade to OV 4.1.2.R02 Step 2: Upgrade to OV 4.1.2 R03* Step 3: Upgrade to OV 4.2.1 R01-GA*	Step 1: Upgrade to OV 4.1.2.R02 Step 2: Upgrade to OV 4.1.2 R03* Step 3: Upgrade to OV 4.2.1 R01-GA* Step 4: Automatic upgrade to MR2 from VA Menu
OV 4.1.2 R01	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA*	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA* Step 3: Automatic upgrade to MR2 from VA Menu
OV 4.1.2 R02	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA*	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA* Step 3: Automatic upgrade to MR2 from VA Menu
OV 4.1.2 R03	Direct Upgrade*	Step 1: Upgrade to OV 4.2.1 R01-GA Step 2: Automatic upgrade to MR2 from VA Menu
OV 4.2.1 R01-GA (Build 69)		Step 1: Automatic upgrade to MR2 from VA Menu
OV 4.2.1 R01-MR1 (Build 85)		Step 1: Automatic upgrade to MR2 from VA Menu

* This step includes MongoDB Database Password change. Please make sure all the steps for changing the password are followed as detailed in the applicable *OmniVista 2500 NMS Installation Guide*.

This guide is specific to installing/upgrading to OV 2500 NMS-E 4.2.1.R01 (MR2). For procedures for upgrading from an Evaluation License, see the *OmniVista 2500 NMS-E 4.2.1.R01 Installation Guide (Rev. D)*. Specific platform support and recommended system configuration information are available in the *OmniVista 2500 NMS-E 4.2.1.R01 Release Notes (Rev. D)*.

For information on getting started with OmniVista 2500 NMS after installation (e.g., using the Web GUI, discovering network devices) see the *Getting Started Guide* in the OmniVista 2500 NMS on-line help (accessed from Help link at the top of the main OmniVista 2500 NMS Screen).

Installing OV 2500 NMS-E 4.2.1.R01 (MR2)

OV 2500 NMS-E 4.2.1.R01 (MR 2) is distributed as a Virtual Appliance only. It is run as a service using VirtualBox. There are no other standalone installers (e.g., Windows/Linux). OV 2500 NMS-E 4.2.1.R01 (MR 2) is installed as a Virtual Appliance, and can be deployed on the following hypervisors: VMware ESXi, VirtualBox, Hyper-V:

- VMware ESXi: 5.5 and 6.0
- VirtualBox: 5.0.10
- MS Hyper-V: 2012 R2 and 2016.

The sections below detail each of the steps required to deploy OV 2500 NMS-E 4.2.1.R01 (MR 2) as Virtual Appliance on [VMware](#), [VirtualBox](#), and [Hyper-V](#). If you are upgrading from OV 2500 NMS-E 4.2.1.R01 GA, see [Upgrading from OV 2500 NMS-E 4.2.1.R01 GA or MR1](#).

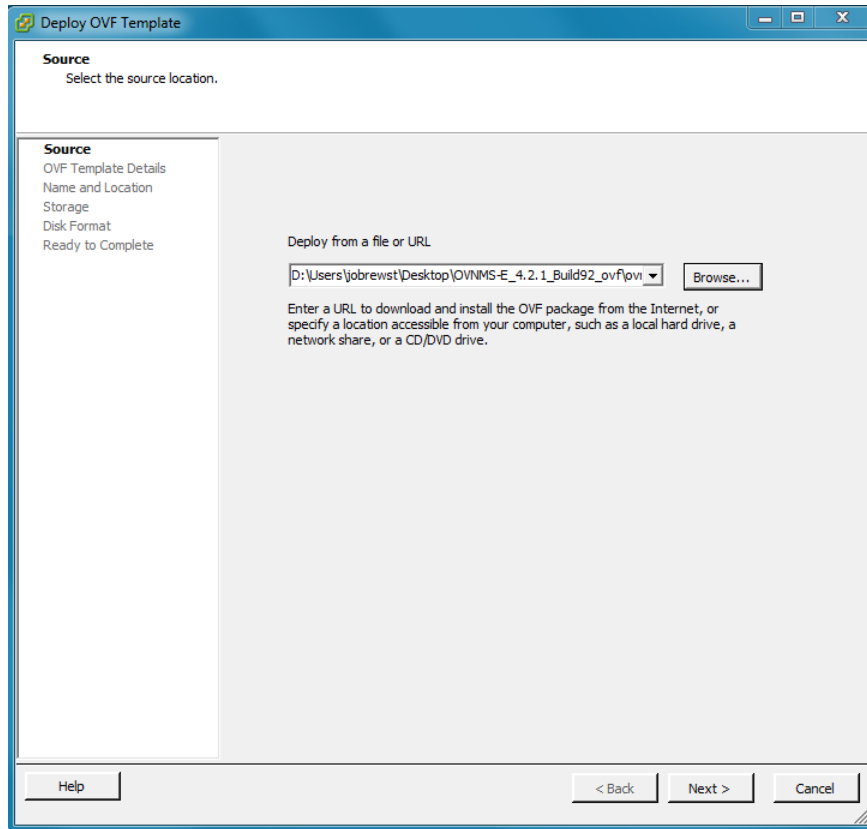
Note: If you are deploying OV 2500 NMS-E 4.2.1.R01 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download. See [Appendix A](#) for details.

Deploying the Virtual Appliance in VMware ESXi

Note that in the instructions below, vCenter is used for demonstration purposes.

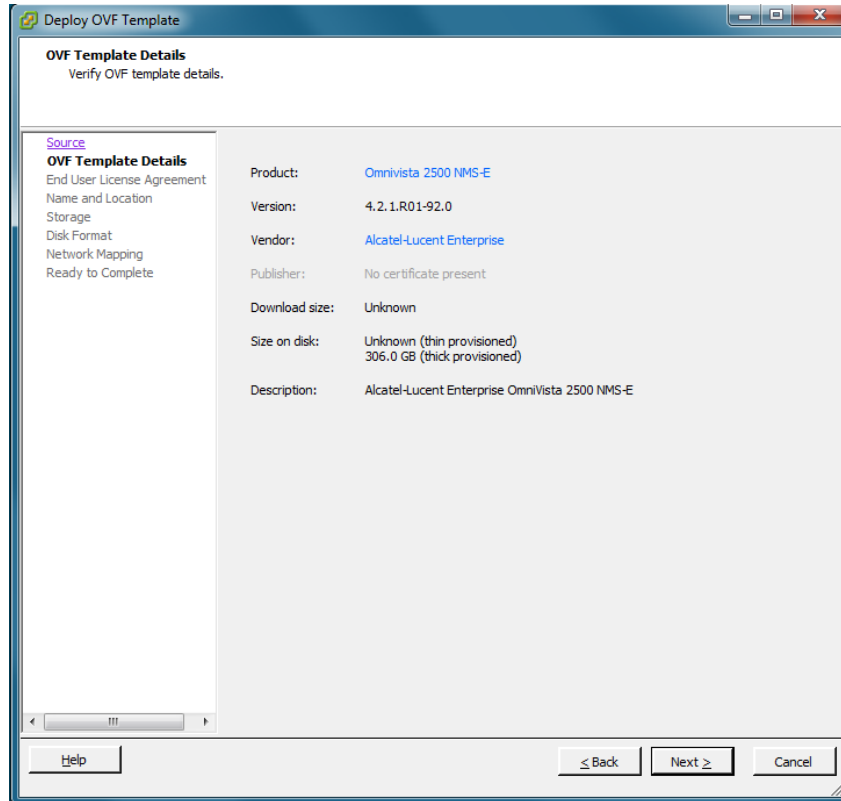
1. Download and unzip the OVF package.
2. Log into vCenter and open the vSphere client.
3. Select the Host on which you want to install OV 2500 NMS-E 4.2.1.R01 (MR 2), click on **File - Deploy OVF Template**. The Deploy OVF Template Wizard appears.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

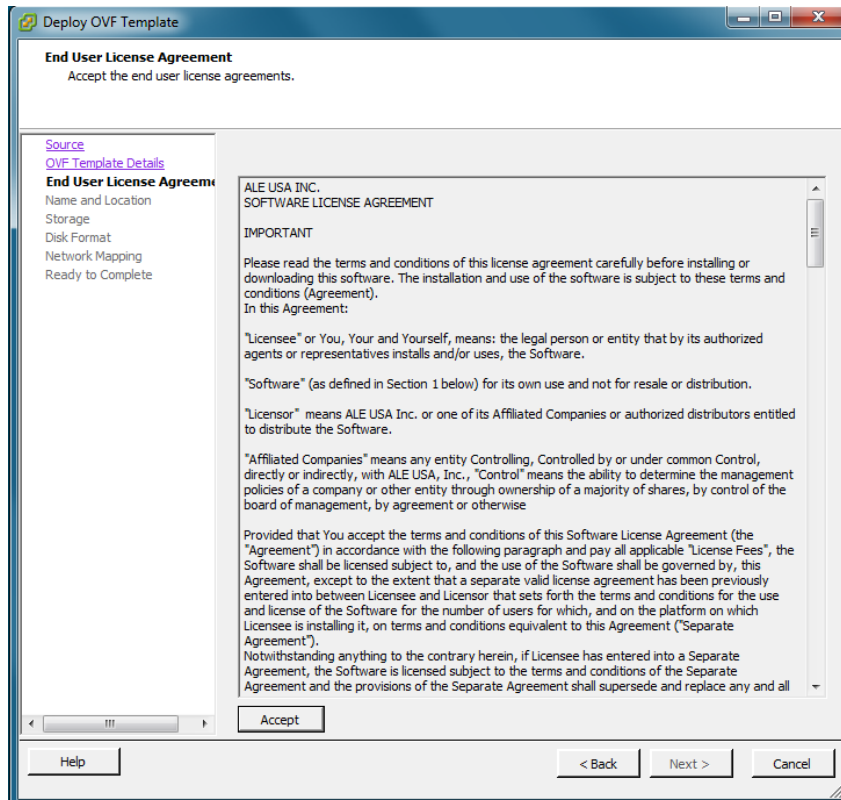


4. Click on the **Browse** button and locate the OV 2500 NMS-E 4.2.1.R01 (MR 2) Application file in the unzipped OVF folder (e.g., ovmse-4.2.1.R01-92.0.ovf).
5. Select the file and click **Open** (or double click on the file). The file will appear in the “Deploy from a file or URL” field. Click **Next**. The OVF Template Details Screen appears.

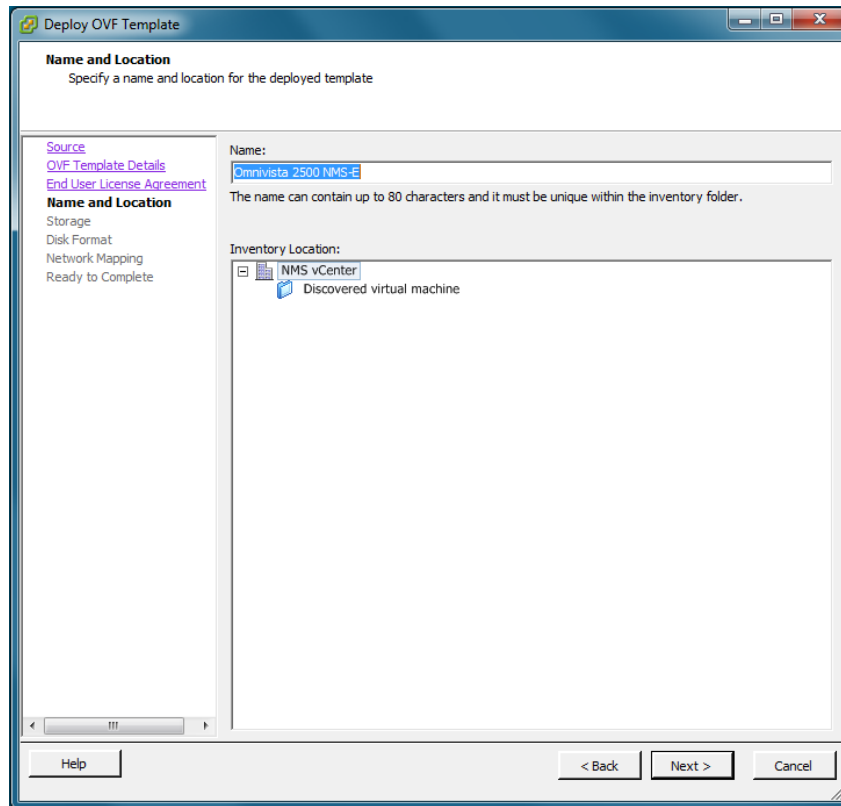
OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide



6. Review the OVF details and click **Next**. The End User License Agreement Screen appears.



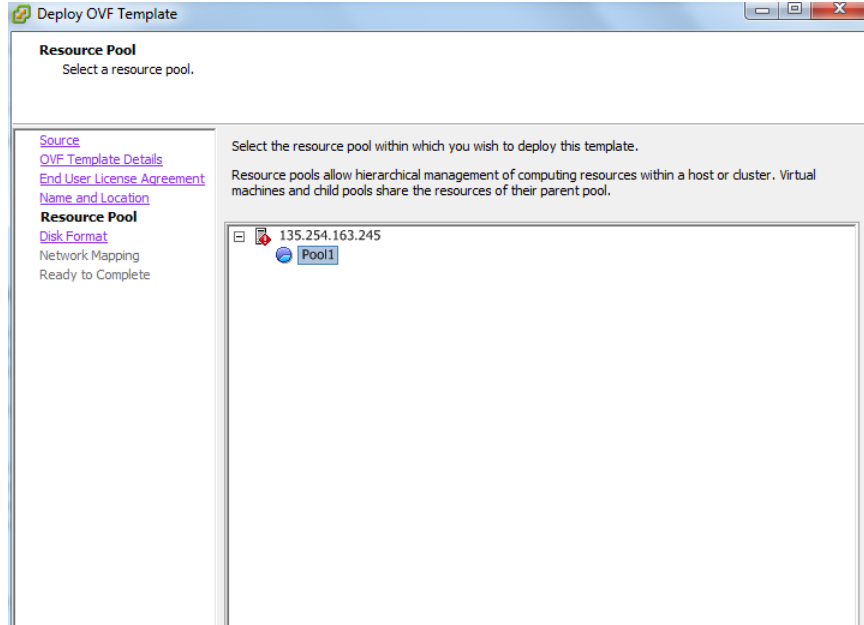
7. Review the License Agreement, click **Accept**, then click **Next**. The Name and Location Screen appears.



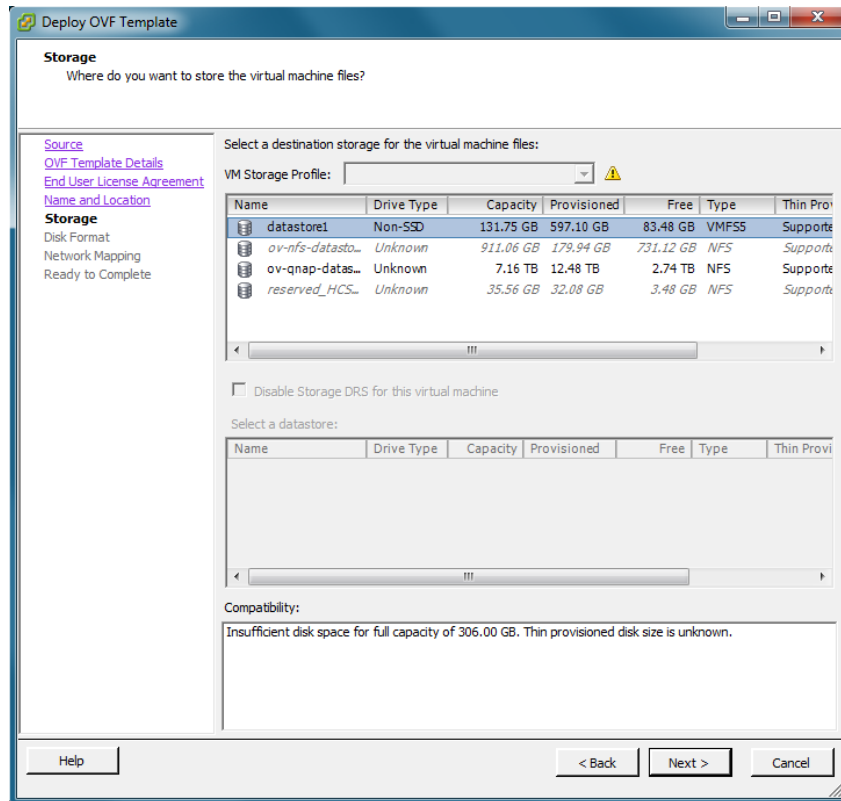
8. Specify a Name and Inventory Location for the deployed template (e.g., OmniVista 2500 NMS-E421R01.B92), then click **Next**.

9. If you have configured a Resource Pool, the Resource Pool Screen (below) appears. Select the host server and click **Next**.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

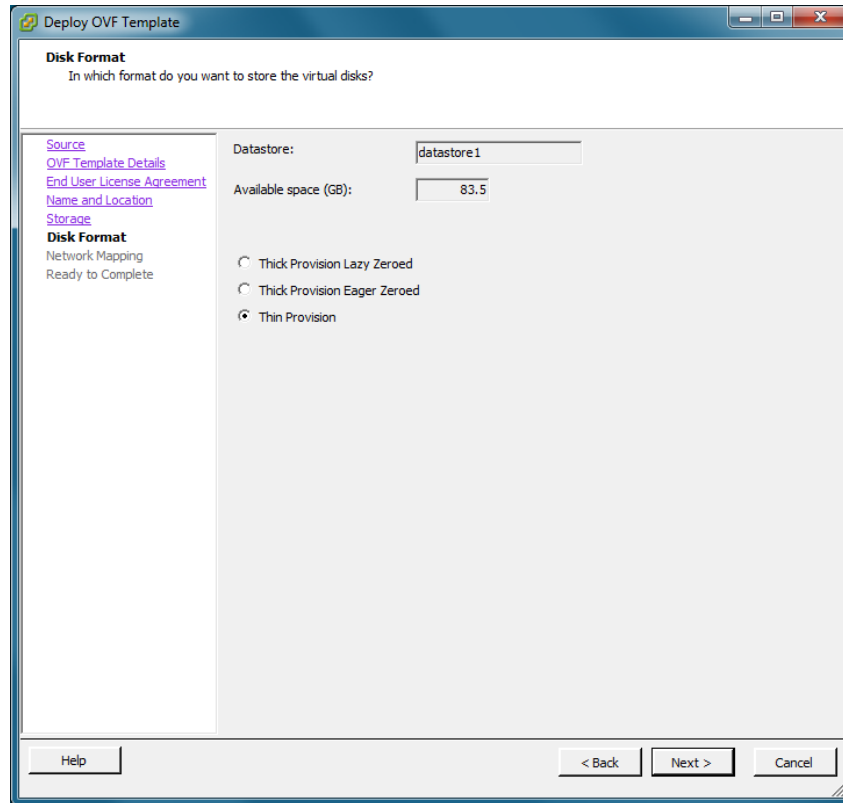


If a host server only has storage configured, the Disk Format Screen will appear. If you have multiple storage locations configured, the Storage Screen (below) appears. Select the destination storage where the template is to be deployed, then click **Next**.

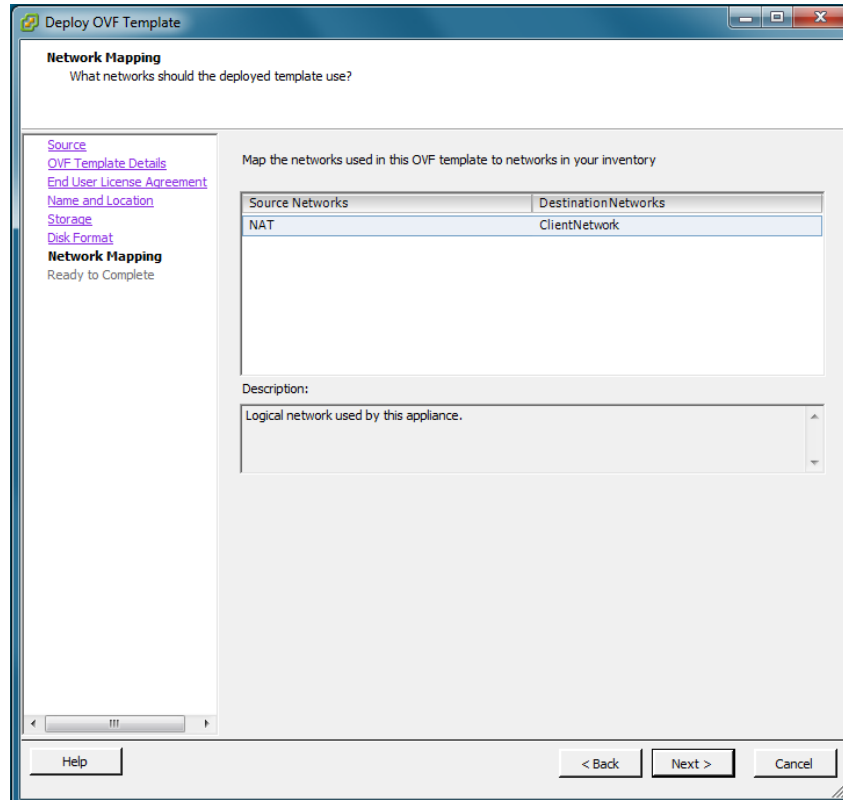


The Disk Format Screen appears.

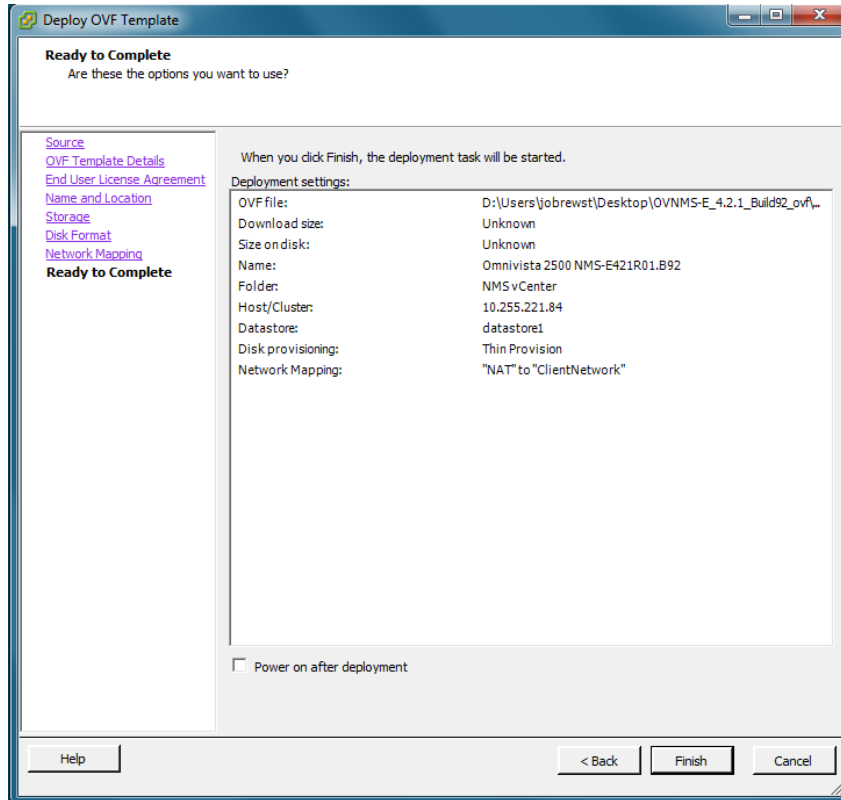
OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide



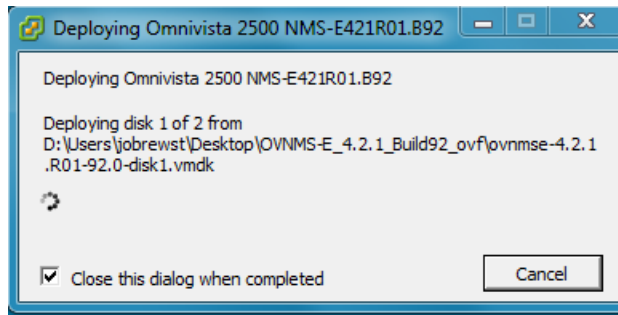
10. Select **Thin Provision**, then click **Next**. The Network Mapping Screen appears.



11. Select network that the deployed OVF template will use, then click **Next**. The Ready to Complete Screen appears.



12. Review the configuration and click **Finish**. (You can select the “Power on after deployment” option to automatically power on the VA when deployment is complete.) A status window appears and displays the progress of the deployment. If you select the “Close this dialog when completed” option, the progress window will automatically close when the deployment is complete. If not, click **Close** at the completion of the deployment to close the window.



13. If the new Virtual Appliance was not powered on via the deployment wizard, power on the VM now. Right-click on the VM in the Navigation Tree and select **Power - Power On**.

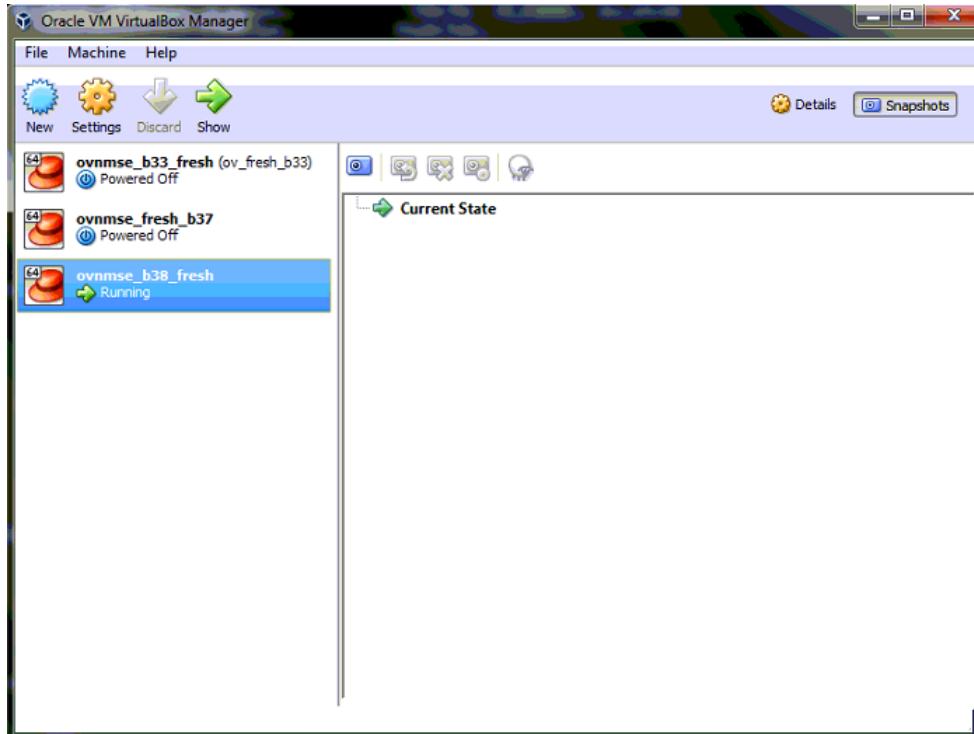
Once the Virtual Appliance is powered on, go to [Completing the OmniVista 2500 NMS-E 4.2.1.R01 \(MR 2\) Installation](#) to complete the installation.

Deploying the Virtual Appliance in VirtualBox

Note that in the instructions below, VirtualBox 5.0.10 in Windows 7 is used for demonstration purposes.

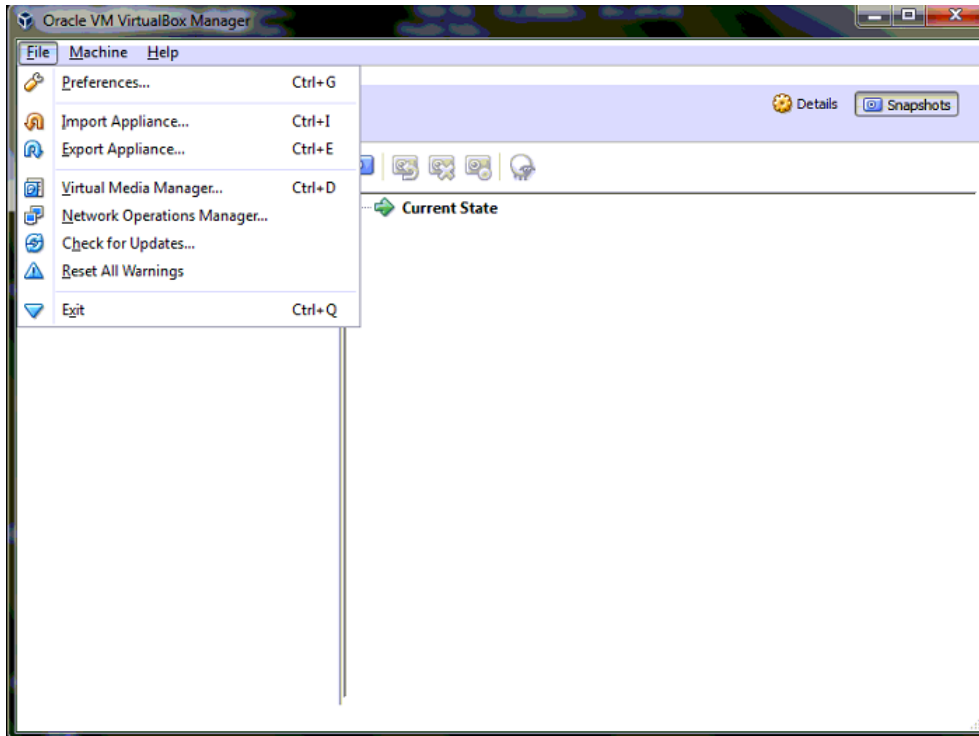
Note: If you are deploying OV 2500 NMS-E 4.2.1.R01 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download. See [Appendix A](#) for details.

1. Download and unzip the OVF package.
2. Log into Windows 7 and open the Oracle VM VirtualBox tool.

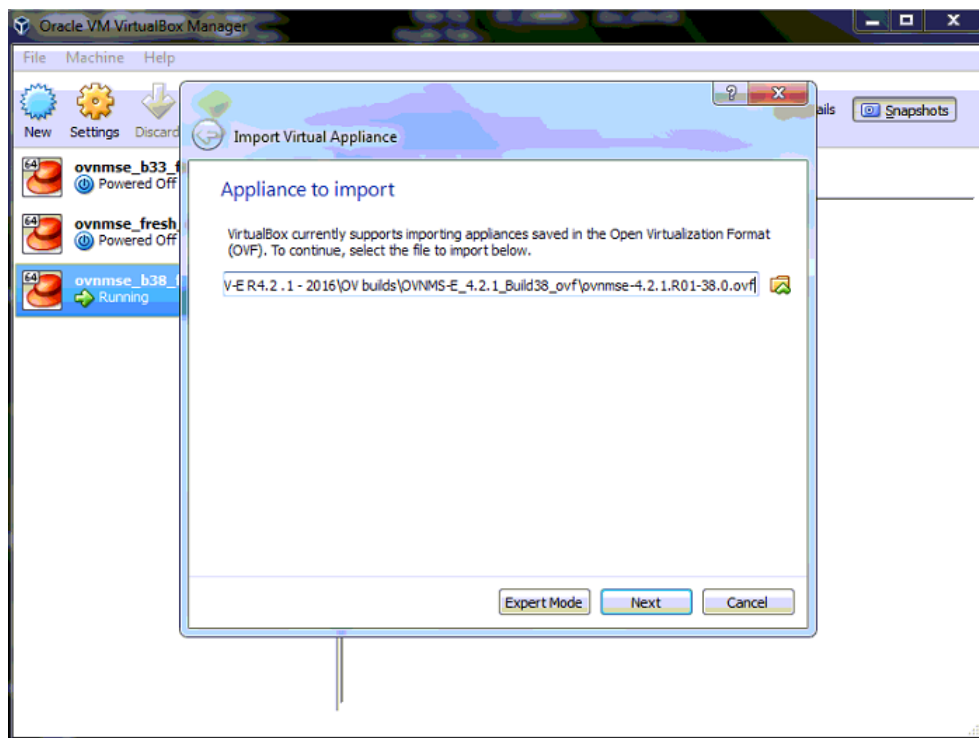


3. Click **File > Import Appliance**.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

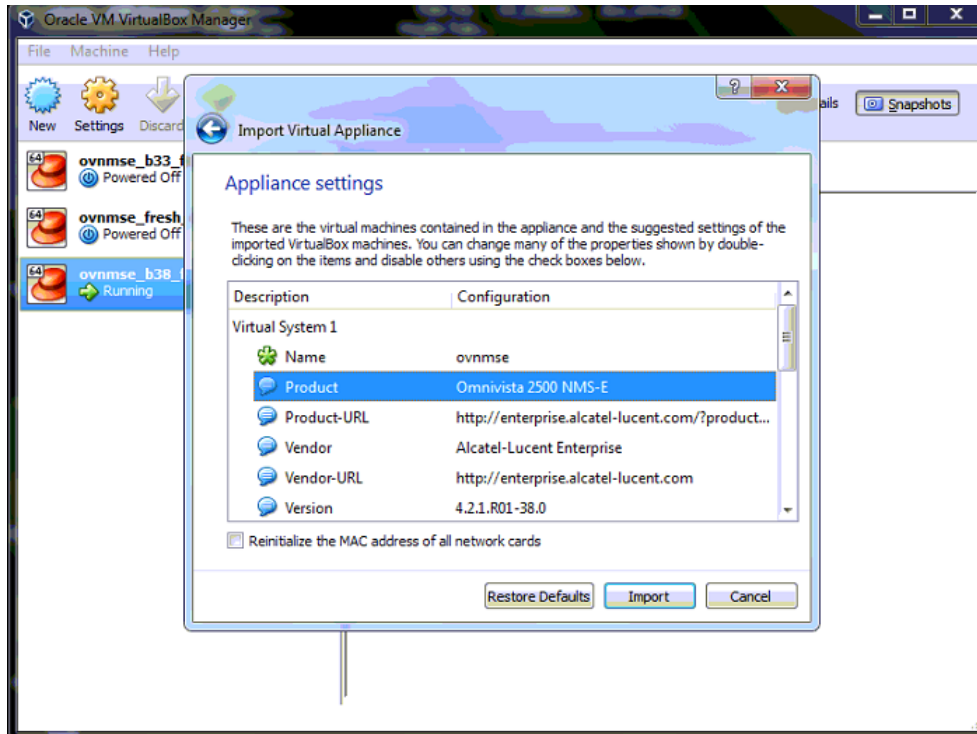


4. Click **browse** icon then select the **folder** which you extracted at step 1 above, then click **Next**.

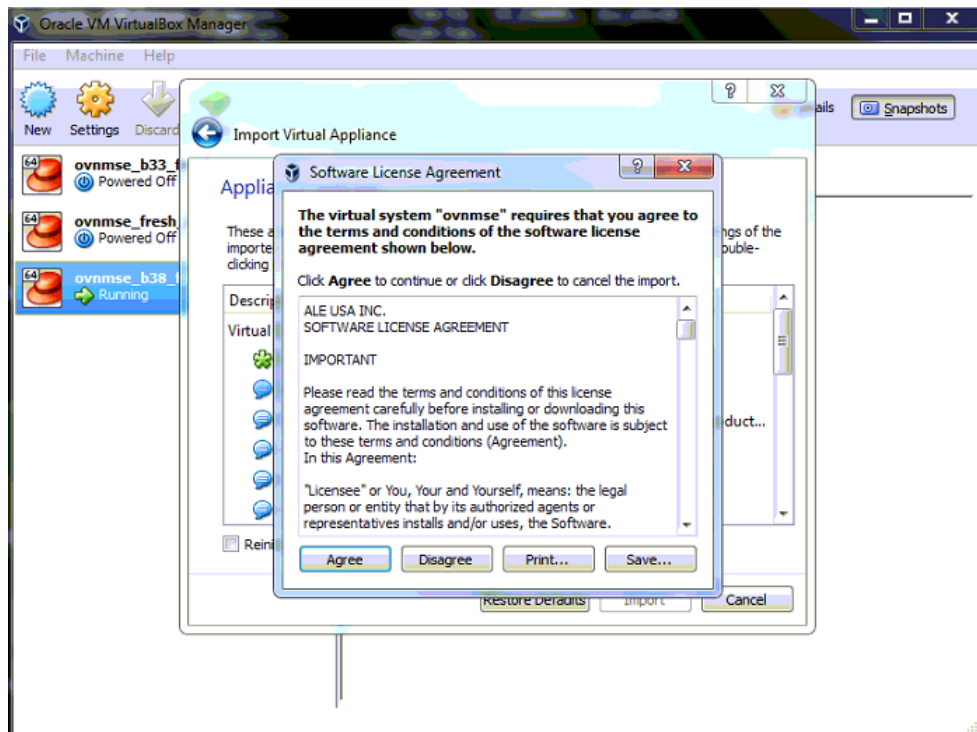


5. Review the configuration and click **Import**.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

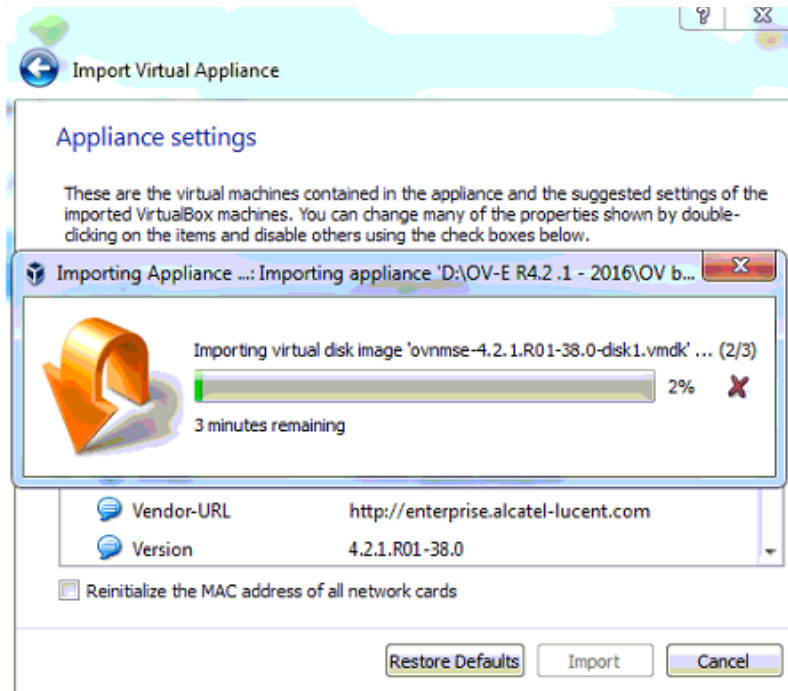


6. The **Software License Agreement** window displays, click on **Agree**.

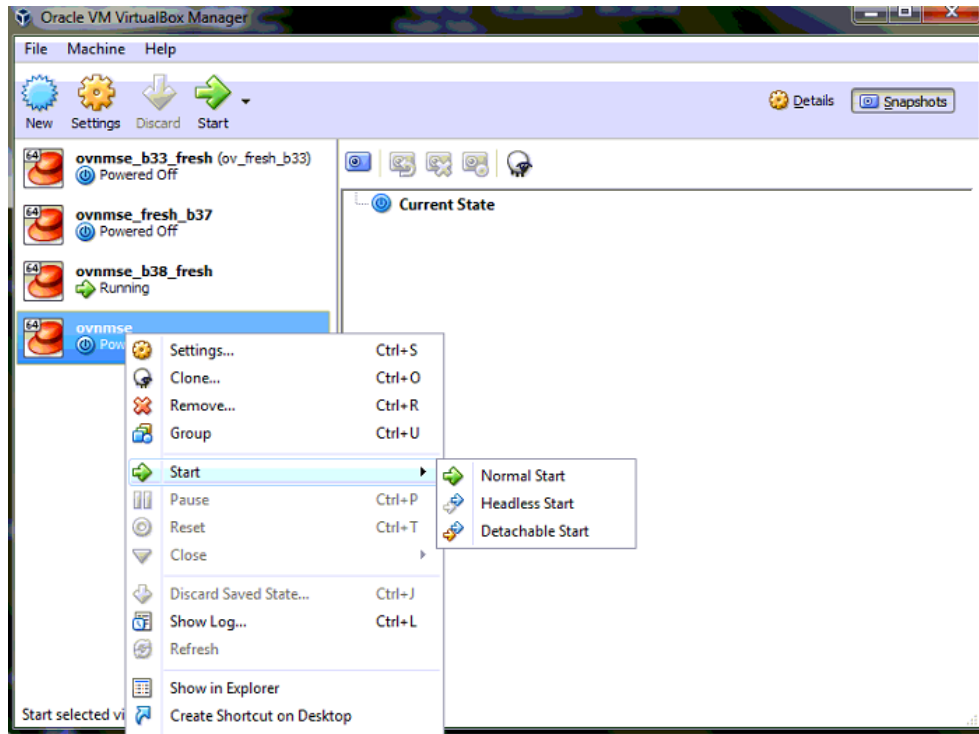


7. A status window appears and displays the progress of the deployment.

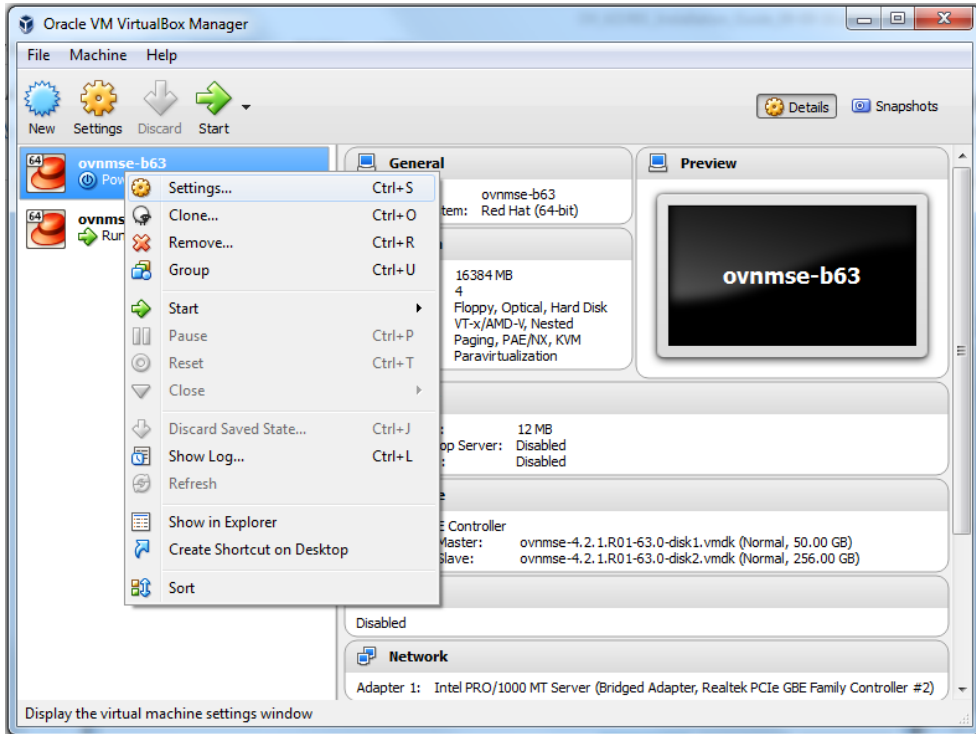
OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide



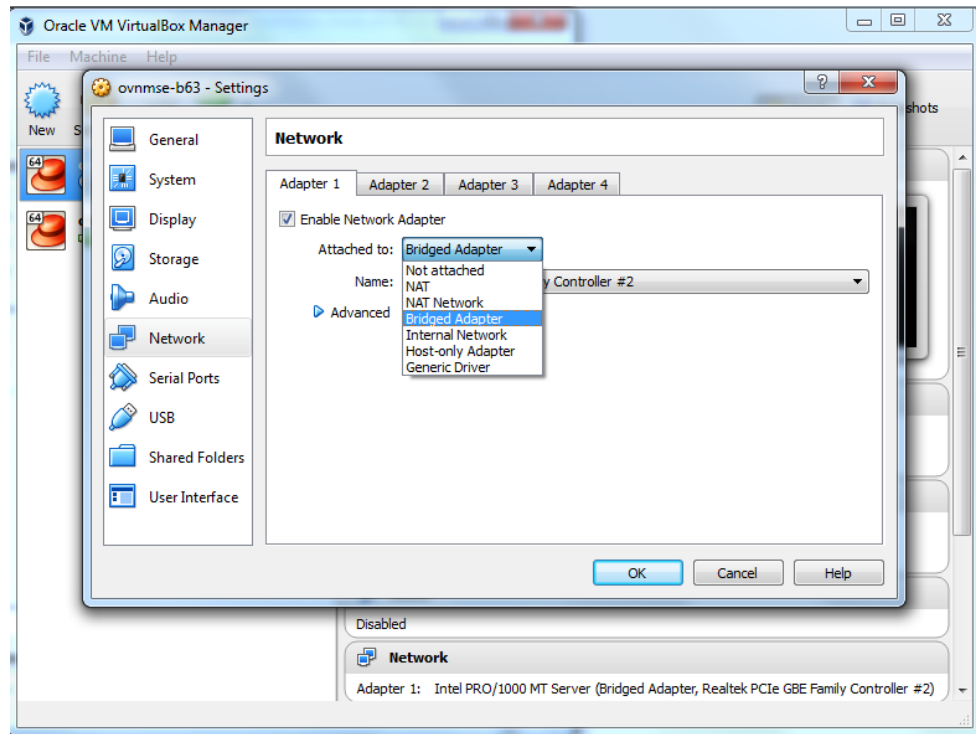
8. After the process is completed, right-click on the VM in the Navigation Panel and select **Start - Normal Start**.



9. Configure the Network Adapter. Right-click on the VA and select **Settings**.



10. Select **Network**, then select the Network Adaptor that you created when you configured VirtualBox.



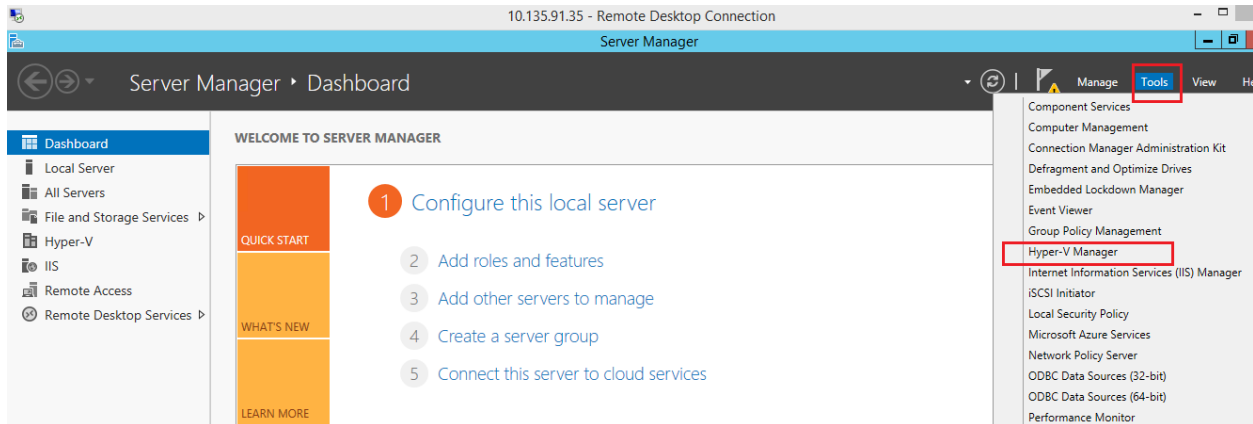
OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

Once the Virtual Appliance is powered on, go to [Completing the OmniVista 2500 NMS-E 4.2.1.R01 \(MR 2\) Installation](#) to complete the installation.

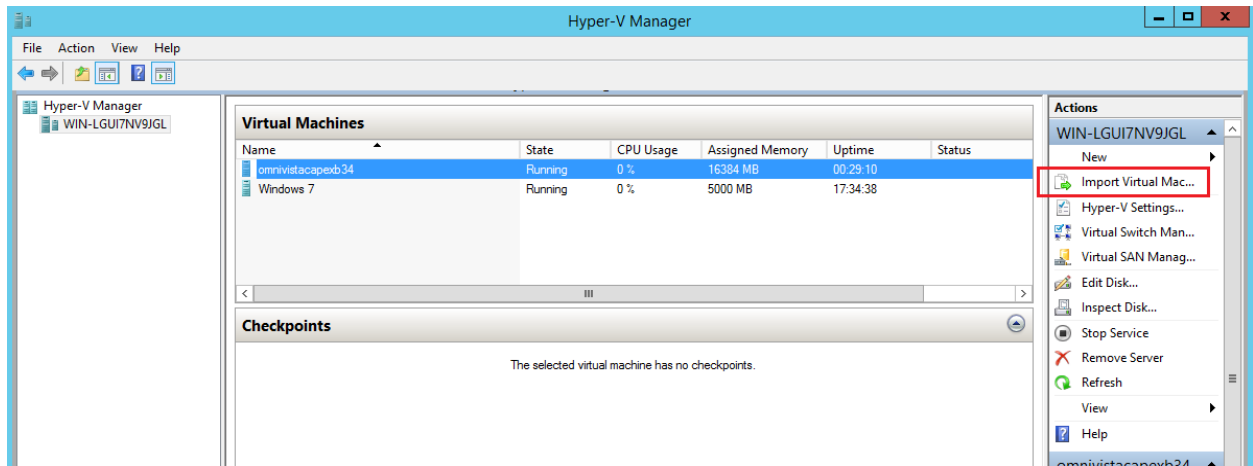
Deploying the Virtual Appliance in Hyper-V

Note that in the instructions below, Hyper-V in Windows 2012 is used for demonstration purposes.

1. Download and unzip the OVF Hyper-V package.
2. Log into Windows 2012 and open the Hyper-V tool.

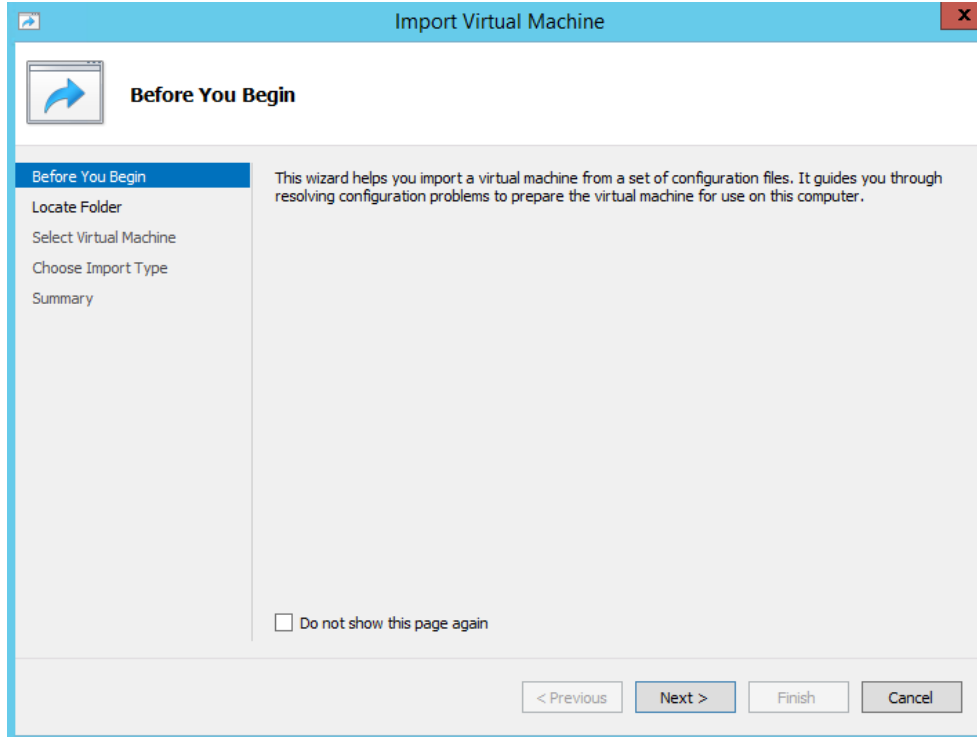


3. Select the Host on which you want to install OmniVista 2500 NMS, click on **Actions > Import Virtual Machine**.

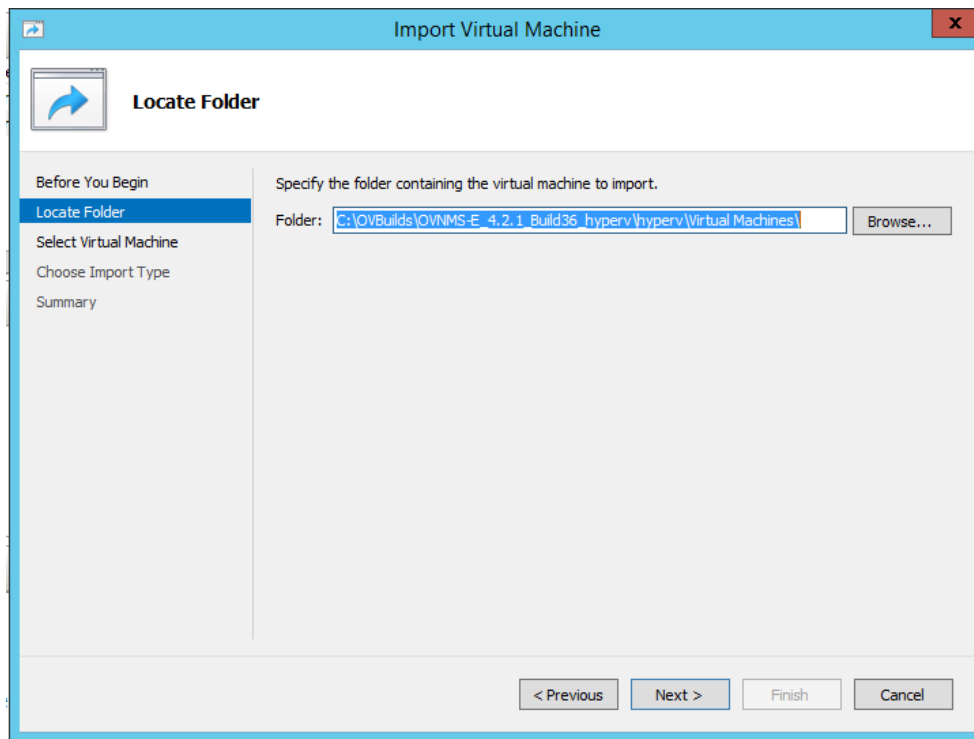


4. The Import Virtual Machine Wizard appears.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

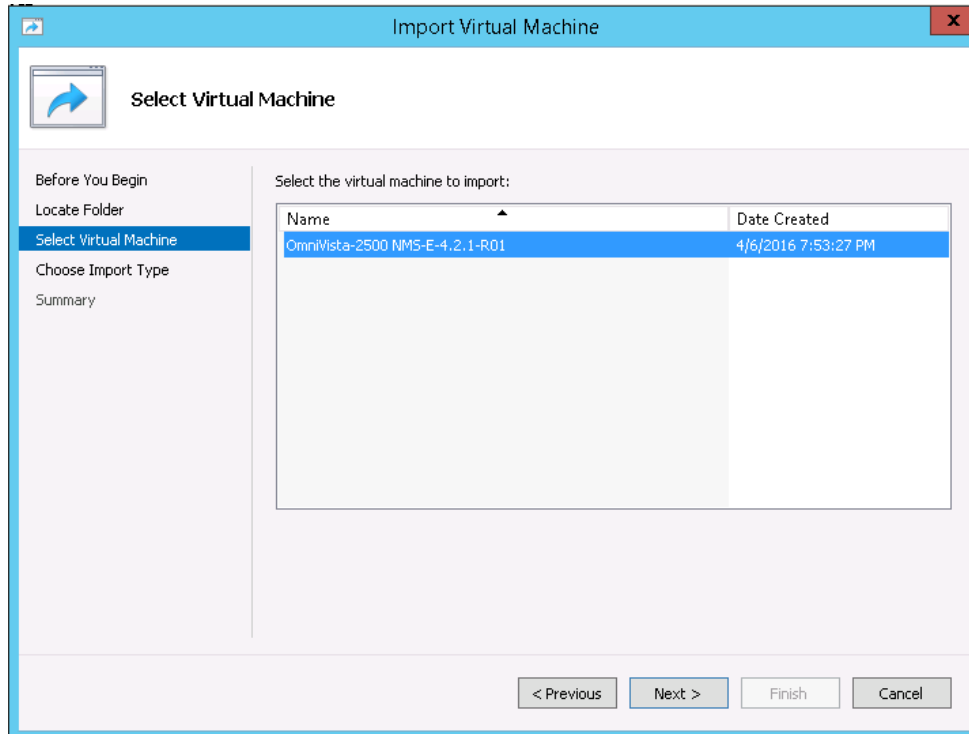


5. Click **Next** to go to the Locate Folder Screen, select the **Folder** that you extracted in Step 1, then click **Next**.

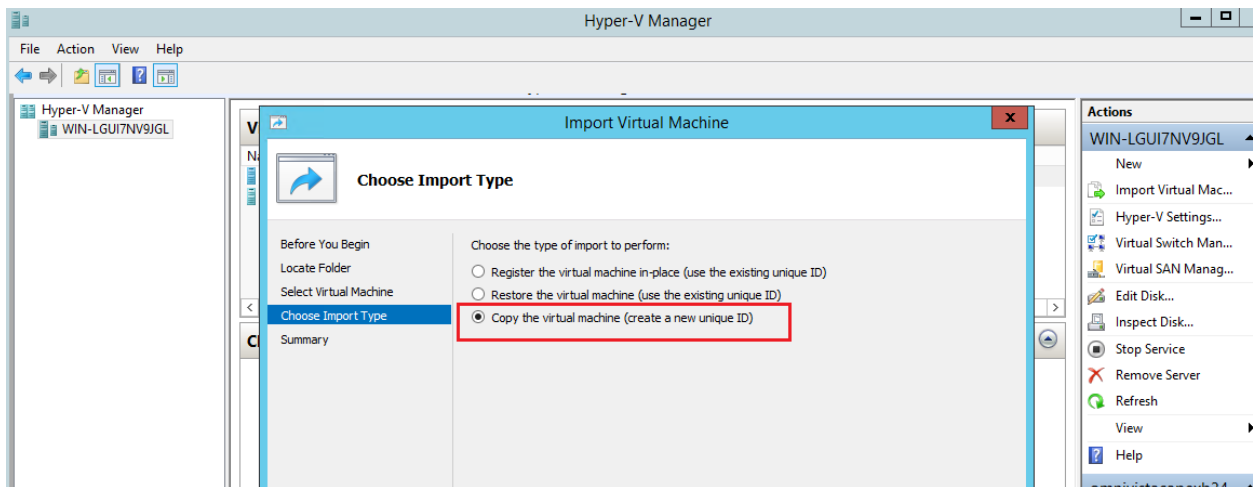


6. Select the Virtual Machine to import (Default = **OmniVista-2500 NMS-E-4.2.1.R01**), then click **Next**.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

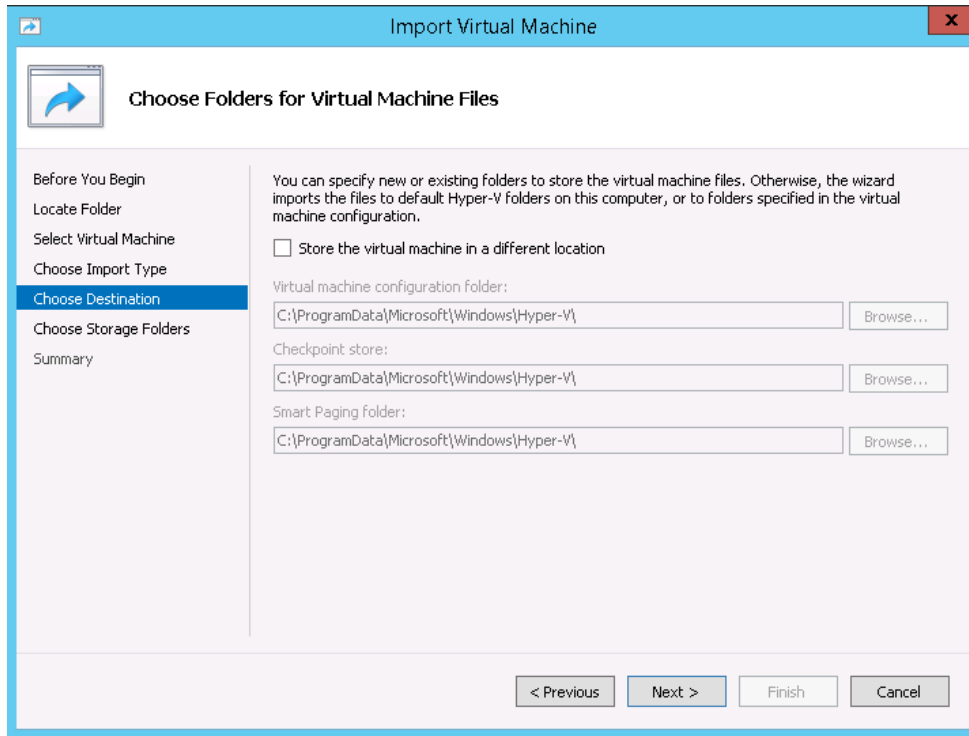


7. Select the default Import Type: **Copy the virtual machine (create a new unique ID)**, then click **Next**.

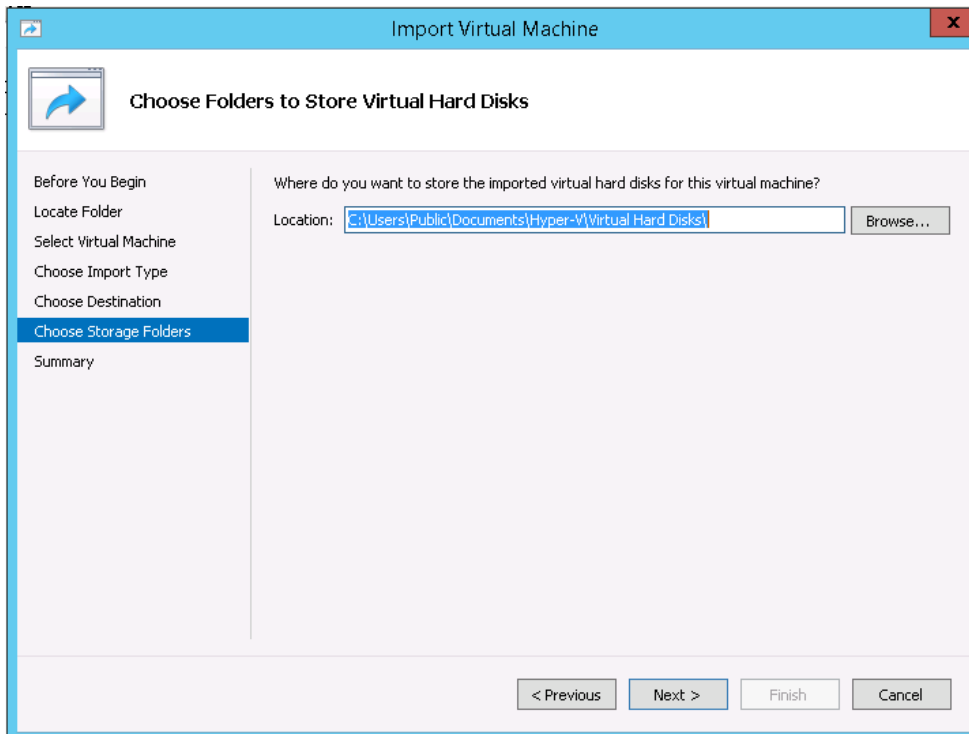


8. Specify folders to store the Virtual Machine files (or accept the default folders), then click **Next**.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide



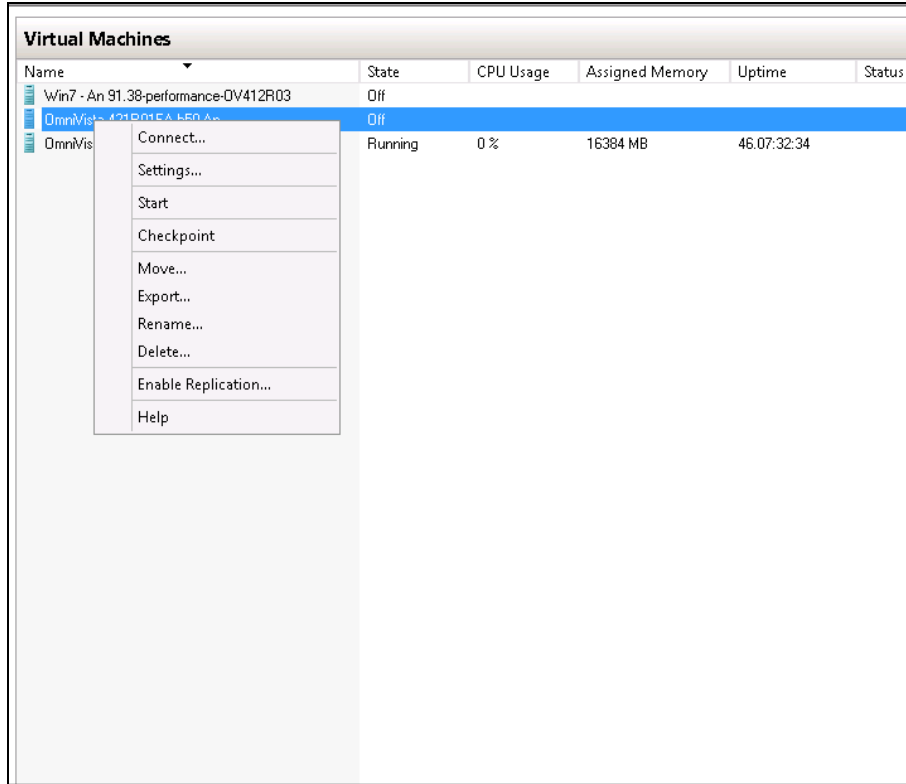
9. Choose folders to store the Virtual Hard Disks or accept the default location and click **Next**.



10. Review the import configuration and click **Finish**. (Click **Previous** to return to a screen and make changes.)

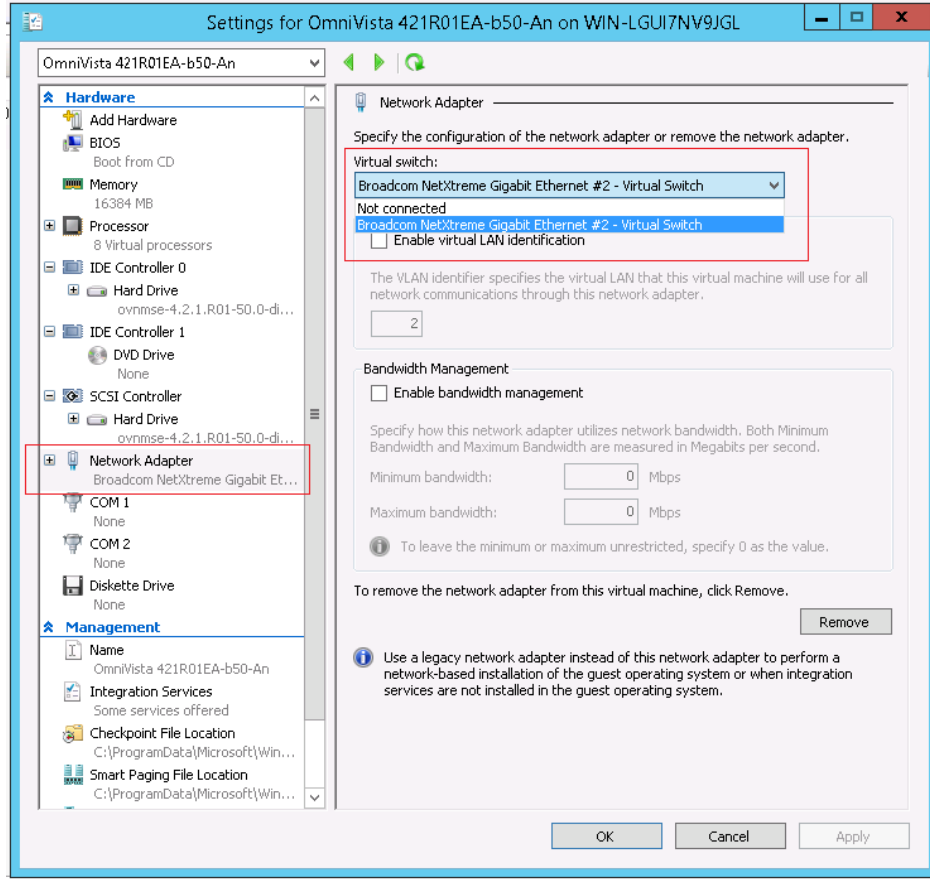
11. Configure the Network Adapter. Right-click on the VA and select **Settings**.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide



12. Select **Network Adapter**, then select the Virtual Switch that you created when you configured Hyper-V.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide



After the process is completed, right-click on the VM in the Navigation Panel and select **Start**. Once the Virtual Appliance is powered on, go to [Completing the OmniVista 2500 NMS-E 4.2.1.R01 \(MR 2\) Installation](#) to complete the installation.

Completing the OmniVista 2500 NMS-E 4.2.1.R01 (MR 2) Installation

Follow the steps in the following sections to complete the OV 2500 NMS-E 4.2.1.R01 (MR 2) installation.

1. Launch the Console for the new VM. (In vCenter, this can be done by right-clicking on the VM in the Navigation Tree and selecting **Open Console**.) The password prompt appears.

```
*****
* Configure "cliadmin" password
*****
You must remember the new passwords in order to manage the Virtual Appliance and OmniVista.
Length of new password must be >= 8 and <= 32 characters
The new password must contain AT LEAST :
  a. one (1) letter (a-z)
  b. one (1) capitalized letter (A-Z)
  c. one (1) special character (%^*()-_+=[]{}:~",.?)
  d. and one (1) digit (0-9)
Enter new password:
```

2. Specify a new administrative password, then re-enter to confirm the new password. Press **Enter** to configure System IP.

Note: Follow the guidelines on the screen when creating the password. Be sure to store the password in a secure place. Users will be prompted for the password at the end of the installation. Lost passwords cannot be retrieved.

```
*****
* Configure IP
*****
(*) Please input IPv4: 10.255.221.228
Please input subnet mask [255.0.0.0]: 255.255.255.0
Would you like to configure:
    IPv4: 10.255.221.228
    subnet mask: 255.255.255.0
[yin] (y): y
The configuration has been set
Press [Enter] to continue
```

3. Enter an IPv4 address.
4. Enter the IPv4 network mask.
5. Press **y** and **Enter** to confirm, then press **Enter** to continue.
6. The **Memory Configuration Based on Network Size** option is displayed.

```
*****
* Memory Configuration Based on Network Size
*****
Choose the number of devices:
[1] Low (lower than 500)
[2] Medium (500-2000)
[3] High (2000-5000)
[4] Very High (5000-10000)
(*) Type your option: _
```

Select the number of devices OV 2500 NMS-E 4.2.1.R01 (MR 2) will manage. To select a range, enter its corresponding number at the command prompt (e.g., enter **2** for Medium). Ranges include:

- Low (fewer than 500 devices)
- Medium (500 to 2,000 devices)
- High (2,000 to 5,000 devices)
- Very High (5,000 to 10,000 devices).

Press **y** and **Enter** to confirm, then press **Enter** to display the Configure the Virtual Appliance Main Menu.

7. The Configure The Virtual Appliance Main Menu is displayed.

```
*****  
* Configure The Virtual Appliance *  
*****  
* [1] Help *  
* [2] Display Current Configuration *  
* [3] Configure IP *  
* [4] Configure Ports *  
* [5] Configure Default Gateway *  
* [6] Configure Hostname *  
* [7] Configure DNS Server *  
* [8] Configure Timezone *  
* [9] Configure Route *  
* [10] Configure Network Size *  
* [11] Configure Keyboard Layout *  
* [12] Update SSL Certificate *  
* [13] Configure NTP Client *  
* [14] Configure Proxy *  
* [15] Import JRE CA Certificate *  
* [0] Exit *  
*****
```

8. Enter **2** and press **Enter** to display the current configuration.

```
*****  
* Current configuration *  
*****  
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.1.R01 MR-2  
Build Number: 92  
Patch Number: 0  
Build Date: 05/13/2017  
  
IPv4 Address: 10.255.221.50  
NetMask: 255.255.255.0  
  
HTTP Port: 80  
HTTPS Port: 443  
  
Default gateway v4: 10.255.221.254  
  
Hostname: omnivista  
  
Timezone: America/Los_Angeles  
  
Data LUM size: 256G  
Data LUM available (free) space: 235G  
  
Network Size: Low (lower than 500) devices  
  
License CORE: Not Yet Applied  
License UMM: Not Yet Applied  
  
Proxy Status: Disabled  
Proxy is not set  
  
Press [Enter] to continue
```

The current OV appliance configuration is displayed. You can go to the Configure The Virtual Appliance Menu to configure additional settings (e.g., Default Gateway, Proxy, DNS) that may be required to access OV 2500 NMS-E 4.2.1.R01 (MR 2) and perform upgrades. Please configure other settings as required. See [Appendix B](#) for VA Menu information.

Note: OV 2500 NMS-E 4.2.1.R01 (MR 2) makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.2.1.R01 (MR 2) to connect to the OmniVista 2500 NMS External Repository.

9. Press **Enter**. The Virtual Appliance Menu is displayed again.

10. After completing all required settings (and after all services are running), enter `https://<OVServerIPaddress>` in a supported browser to launch OV 2500 NMS-E 4.2.1.R01 (MR 2).

Note: If you changed the default HTTPs port (443) during VA configuration, you must enter the port after the IP address (e.g., `https://<OVServerIPaddress>:<HTTPsPort>`).

Upgrading From OV 2500 NMS-E 4.2.1.R01 GA or MR1

Follow the steps below to use the “Upgrade/Restore” option in the Virtual Appliance Menu to upgrade from OV 2500 NMS-E 4.2.1.R01 GA/MR1 to OV 2500 NMS-E 4.2.1.R01 (MR 2). Remember, if you are upgrading from an older version (3.5.7 or 4.1.2.R03), you must first upgrade to 4.2.1.R01 GA before upgrading to 4.2.1.R01 (MR 2). See the *OmniVista 2500 NMS-E 4.2.1.R01 Installation Guide (Rev. D)* for details. **It is recommended that you perform a VM backup prior to the upgrade.**

Note: OV 2500 NMS-E 4.2.1.R01 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **14 – Configure Proxy**.

1. Open a Console on the OV 2500 NMS-E 4.2.1.R01 Virtual Appliance.

```
*****
* The Virtual Appliance Menu                                     *
*****
* [1] Help                                                     *
* [2] Configure The Virtual Appliance                         *
* [3] Run Watchdog Command                                    *
* [4] Upgrade/Restore VA                                     *
* [5] Change Password                                        *
* [6] Logging                                                 *
* [7] Login Authentication Server                             *
* [8] Power Off                                              *
* [9] Reboot                                                 *
* [10] Advanced Mode                                         *
* [0] Log Out                                                *
*****
(*) Type your option: _
```

2. On the Virtual Appliance Menu, select option **4 - Upgrade/Restore VA**.


```

*****
* Upgrade VA
*****
* [1] Help
* [2] 4.2.1.R01 (Current Release)
* [3] Enable Repository (Selected - ALE Central Repo)
* [4] Configure Custom Repositories
* [5] Configure "Update Check Interval" (Selected - Disabled)
* [6] Restore OV2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

3. On the Upgrade VA Menu, select option **2 - 4.2.1.R01 (Current Release)**. Information on the current installation is displayed and OmniVista checks the OV Repository for the latest upgrade packages.

```

*****
(*) Type your option: 2
*****
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.1.R01 GA
Build Number: 69
Patch Number: 0

Checking available packages for 4.2.1.R01 operation is in progress...
Upgrade information for 4.2.1.R01
Available Packages
Name       : ovmse
Arch       : x86_64
Version    : 4.2.1.R01
Release    : 93.0.e17
Size       : 455 M
Repo       : CustomRepo3_4.2.1.R01
Summary    : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL        : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&
;page=overview
License    : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

Would you like to upgrade the package [y/n] (n): _
    
```

In the example above, the current Build Number is 69 (shown in the “Current Version” section at the top of the screen). The available upgrade is Build 93 (shown in the “Available Packages” section - Release: 93.0.e17).

Note: If you are unable to connect to the ALE Central Repository, you will receive the following error message instead of the screen above: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select **2 - Configure The Virtual Appliance** to access the menu).

4. At the “Would you like to upgrade the package” prompt, type **y** and press **Enter**. You will be reminded to perform a backup before proceeding with the upgrade.

```

Would you like to upgrade the package [y/n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot prior to this.
Are you ready to proceed [y/n] (n): _
    
```

5. Type **y** and press **Enter** to begin the upgrade. The upgrade may take 30 – 45 minutes. When the upgrade is complete, a “Completion” message will appear and the VM will automatically reboot.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

6. When the reboot is complete, log into the VM. You can verify the upgrade by going to the Virtual Appliance Menu and selecting option **4 - Upgrade/Restore VA**, then selecting option **2 - 4.2.1.R01 (Current Release)**. The current OmniVista Release information is displayed (e.g., Build Number: 84).

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.1.R01 MR
Build Number: 84
Patch Number: 0

Checking available packages for 4.2.1.R01 operation is in progress...
No package available for 4.2.1.R01
Press [Enter] to continue
```

Appendix A – Installing Virtual Box

If you are deploying OV 2500 NMS-E 4.2.1.R01 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download.

Go to https://www.virtualbox.org/wiki/Download_Old_Builds_5_0_pre18. Scroll down to **Virtual Box 5.0.10** and click on the applicable download link (e.g., Windows Hosts, Linux Hosts). The sections below provide procedures for installing Virtual Box on [Windows](#) or [Linux](#) Hosts. See the Oracle VM Virtual Box documentation for additional information.

Supported Hosts

Virtual Box runs on the following host operating systems:

- **Windows Hosts:**
 - Windows Vista SP1 and later (32-bit and 64-bit).
 - Windows Server 2008 (64-bit)
 - Windows Server 2008 R2 (64-bit)
 - Windows 7 (32-bit and 64-bit)
 - Windows 8 (32-bit and 64-bit)
 - Windows 8.1 (32-bit and 64-bit)
 - Windows 10 RTM build 10240 (32-bit and 64-bit)
 - Windows Server 2012 (64-bit)
 - Windows Server 2012 R2 (64-bit).
- **Linux Hosts (32-bit and 64-bit):**
 - Ubuntu 10.04 to 15.04
 - Debian GNU/Linux 6.0 ("Squeeze") and 8.0 ("Jessie")
 - Oracle Enterprise Linux 5, Oracle Linux 6 and 7
 - Redhat Enterprise Linux 5, 6 and 7
 - Fedora Core / Fedora 6 to 22
 - Gentoo Linux
 - openSUSE 11.4, 12.1, 12.2, 13.1
 - Mandriva 2011.

Installing Virtual Box on Windows Hosts

The Virtual Box installation can be started by double-clicking on the downloaded executable file (contains both 32- and 64-bit architectures), **or** by entering:

```
VirtualBox.exe -extract
```

on the command line. This will extract both installers into a temporary directory in which you will find the usual .MSI files. You can then perform the installation by entering:

```
msiexec /i Virtual Box-<version>-MultiArch_<x86|amd64>.msi
```

In either case, this will display the installation welcome dialog and allow you to choose where to install Virtual Box to and which components to install. In addition to the Virtual Box application, the following components are available:

- USB Support:
 - This package contains special drivers for your Windows host that Virtual Box requires to fully support USB devices inside your virtual machines.
- Networking
 - This package contains extra networking drivers for your Windows host that Virtual Box needs to support Bridged Networking (to make your VM's virtual network cards accessible from other machines on your physical network).
- Python Support
 - This package contains Python scripting support for the Virtual Box API. For this to work, an working Windows Python installation on the system is required.

The Virtual Box 5.0.10 Setup Wizard will guide you through the installation. Depending on your Windows configuration, you may see warnings about "unsigned drivers", etc. Please allow these installations as otherwise Virtual Box might not function correctly after installation.

With standard settings, Virtual Box will be installed for all users on the local system; and the installer will create a "Virtual Box" group in the Windows "Start" menu which allows you to launch the application and access its documentation.

Installing Virtual Box on Linux Hosts

Virtual Box is available in a number of package formats native to various common Linux distributions. In addition, there is an alternative generic installer (.run) which should work on most Linux distributions.

Note: If you want to run the Virtual Box graphical user interfaces, the following packages must be installed before starting the Virtual Box installation (some systems will do this for you automatically when you install Virtual Box):

- Qt 4.8.0 or higher;
- SDL 1.2.7 or higher (this graphics library is typically called `libsdl` or similar).

Specifically, Virtual Box, the graphical Virtual Box manager, requires both Qt and SDL. VBoxSDL, our simplified GUI, requires only SDL. If you only want to run VBoxHeadless, neither Qt nor SDL are required.

Installing Virtual Box From a Debian/Ubuntu Package

Download the appropriate package for your distribution. The following examples assume that you are installing to a 32-bit Ubuntu Raring system. Use `dpkg` to install the Debian package:

```
sudo dpkg -i virtualbox-5.0_5.0.10_Ubuntu_raring_i386.deb
```

You will be asked to accept the Virtual Box Personal Use and Evaluation License. Unless you answer "yes" here, the installation will be aborted.

The installer will also search for a Virtual Box kernel module suitable for your kernel. The package includes pre-compiled modules for the most common kernel configurations. If no suitable kernel module is found, the installation script tries to build a module itself. If the build process is not successful, a warning is displayed and the package will be left unconfigured. In this case, check `/var/log/vbox-install.log` to find out why the compilation failed. You may have to install the appropriate Linux kernel headers.

After correcting any problems, enter `sudo rcvboxdrv setup` to start a second attempt to build the module. If a suitable kernel module was found in the package or the module was successfully built, the installation script will attempt to load that module.

Once Virtual Box has been successfully installed and configured, you can start it by selecting "Virtual Box" in your start menu or from the command line.

Using the Alternative Installer (VirtualBox.run)

The alternative installer performs the following steps:

- It unpacks the application files to the target directory, `/opt/Virtual Box/`, which cannot be changed.
- It builds the Virtual Box kernel modules (`vboxdrv`, `vboxnetflt` and `vboxnetadp`) and installs them.
- It creates `/sbin/rcvboxdrv`, an init script to start the Virtual Box kernel module.
- It creates a new system group called `vboxusers`.
- It creates symbolic links in `/usr/bin` to the a shell script (`/opt/Virtual Box/VBox`) which does some sanity checks and dispatches to the actual executables, `Virtual Box`, `VBoxSDL`, `VBoxVRDP`, `VBoxHeadless` and `VboxManage`.
- It creates `/etc/udev/rules.d/60-vboxdrv.rules`, a description file for udev, if that is present, which makes the USB devices accessible to all users in the `vboxusers` group.
- It writes the installation directory to `/etc/vbox/vbox.cfg`.

The installer must be executed as root with either `install` or `uninstall` as the first parameter.

```
sudo ./VirtualBox.run install
```

If you do not have the "sudo" command available, run the following as root instead:

```
./VirtualBox.run install
```

Then put every user requiring access to USB devices from Virtual Box guests into the group `vboxusers`, either through the GUI user management tools or by running the following command as root:

```
sudo usermod -a -G vboxusers username
```

Note: The `usermod` command of some older Linux distributions does not support the `-a` option (which adds the user to the given group without affecting membership of other groups). In this case, determine the current group memberships using the `groups` command and add these groups in a comma-separated list to the command line after the `-G` option (e.g., `usermod -G group1,group2,vboxusers username`.)

Performing a Manual Installation

If, for any reason, you cannot use the shell script installer described previously, you can also perform a manual installation. Invoke the installer by entering:

```
./VirtualBox.run --keep --noexec
```

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

This will unpack all the files needed for installation in the `install` directory under the current directory. The Virtual Box application files are contained in `VirtualBox.tar.bz2` which you can unpack to any directory on your system. For example:

```
sudo mkdir /opt/Virtual Box
sudo tar jxf ./install/VirtualBox.tar.bz2 -C /opt/Virtual Box
```

or as root:

```
mkdir /opt/Virtual Box
tar jxf ./install/VirtualBox.tar.bz2 -C /opt/Virtual Box
```

The sources for VirtualBox's kernel module are provided in the `src` directory. To build the module, change to the directory and issue the following command:

```
make
```

If everything builds correctly, issue the following command to install the module to the appropriate module directory:

```
sudo make install
```

If you do not have `sudo`, switch the user account to root and enter:

```
make install
```

The Virtual Box kernel module needs a device node to operate. The above `make` command will tell you how to create the device node, depending on your Linux system. The procedure is slightly different for a classical Linux setup with a `/dev` directory, a system with the now deprecated `devfs` and a modern Linux system with `udev`.

On certain Linux distributions, you might experience difficulties building the module. You will have to analyze the error messages from the build system to diagnose the cause of the problems. In general, make sure that the correct Linux kernel sources are used for the build process. Note that the `/dev/vboxdrv` kernel module device node must be owned by `root:root` and must be read/writable only for the user.

Next, you will have to install the system initialization script for the kernel module:

```
cp /opt/Virtual Box/vboxdrv.sh /sbin/rcvboxdrv
```

(assuming you installed Virtual Box to the `/opt/Virtual Box` directory) and activate the initialization script using the right method for your distribution, you should create VirtualBox's configuration file:

```
mkdir /etc/vbox
echo INSTALL_DIR=/opt/Virtual Box > /etc/vbox/vbox.cfg
```

and, for convenience, create the following symbolic links:

```
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/Virtual Box
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/VBoxManage
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/VBoxHeadless
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/VBoxSDL
```

Appendix B – Using the Virtual Appliance Menu

To access the Main Virtual Appliance Menu for a VM, launch the Console. (In vCenter, this can be done by right-clicking on the VM in the Navigation Tree and selecting **Open Console**.) The login prompt is displayed.

Note: You can also access the Virtual Appliance Menu by connecting via SSH using port 2222, user **cliadmin**, and password set when deploying VA (e.g., `ssh cliadmin@192.160.70.230 -p 2222`).

```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.1.R01 EA
Build Number: 67
Patch Number: 0
Build Date: 09/09/2016
Hint: Num Lock on

omnivista login:
```

1. Enter the login (**cliadmin**) and press **Enter**.
2. Enter the password and press **Enter**. The password is the one you created when you first [launched the VM Console](#) at the beginning of the installation process. The Virtual Appliance Menu is displayed.

```
*****
* The Virtual Appliance Menu *
*****
* [1] Help *
* [2] Configure The Virtual Appliance *
* [3] Run Watchdog Command *
* [4] Upgrade/Backup/Restore VA *
* [5] Change Password *
* [6] Logging *
* [7] Login Authentication Server *
* [8] Power Off *
* [9] Reboot *
* [10] Advanced Mode *
* [11] Set Up Optional Tools *
* [0] Log Out *
*****
```

The Virtual Appliance Menu provides the following options:

- [1 - Help](#)
- [2 - Configure the Virtual Appliance](#)
- [3 - Run Watchdog Command](#)
- [4 - Upgrade/Backup/Restore VA](#)
- [5 - Change Password](#)
- [6 - Logging](#)
- [7 - Login Authentication Server](#)
- [8 - Power Off](#)
- [9 - Reboot](#)
- [10 - Advanced Mode](#)

- [11 - Set Up Optional Tools](#)
- [0 - Log out](#)

For information on these menu options, refer to the sections below.

Help

Enter **1** and press **Enter** to bring up help for the Virtual Appliance Menu.

Configure the Virtual Appliance

The “Configure the Virtual Appliance” menu provides the following options:

- [1 - Help](#)
- [2 - Display Current Configuration](#)
- [3 - Configure IP](#)
- [4 - Configure Ports](#)
- [5 - Configure Default Gateway](#)
- [6 - Configure Hostname](#)
- [7 - Configure DNS Server](#)
- [8 - Configure Timezone](#)
- [9 - Configure Route](#)
- [10 - Configure Network Size](#)
- [11 - Configure Keyboard Layout](#)
- [12 - Update SSL Certificate](#)
- [13 - Configure NTP Client](#)
- [14 - Configure Proxy](#)
- [15 - Import JRE Certificat](#)
- [0 - Exit](#)

```
*****
* Configure The Virtual Appliance *
*****
* [1] Help *
* [2] Display Current Configuration *
* [3] Configure IP *
* [4] Configure Ports *
* [5] Configure Default Gateway *
* [6] Configure Hostname *
* [7] Configure DNS Server *
* [8] Configure Timezone *
* [9] Configure Route *
* [10] Configure Network Size *
* [11] Configure Keyboard Layout *
* [12] Update SSL Certificate *
* [13] Configure NTP Client *
* [14] Configure Proxy *
* [15] Import JRE CA Certificate *
* [0] Exit *
*****
```

Help

Enter **1** and press **Enter** to bring up help for the Configure The Virtual Appliance Menu.

Display Current Configuration

Enter **2** and press **Enter** to display the current VA configuration. Press **Enter** to return to the Configure The Virtual Appliance Menu.

```
*****
* Current configuration
*****
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.1.R01 EA
Build Number: 67
Patch Number: 0
Build Date: 09/09/2016

IPv4 Address: 10.255.221.224
NetMask: 255.255.255.0

HTTP Port: 80
HTTPS Port: 443

Default gateway v4: 10.255.221.254

Hostname: omnivista

Timezone: America/Los_Angeles

Data LUM size: 256G
Data LUM available (free) space: 234G

Network Size: Low (lower than 500) devices

Proxy Status: Enabled
Proxy: ost: 10.255.10.80:8080
Proxy username:
Proxy password:

Press [Enter] to continue
```

Configure IP

1. If you want to re-configure the System IP, enter **3** and press **Enter**.

```
*****
* Configure IP
*****
Please input IPv4 [10.255.221.224]:
Please input subnet mask [255.0.0.0]:
Would you like to configure:
    IPv4: 10.255.221.224
    subnet mask: 255.0.0.0
[yin] (y):
```

2. Enter an IPv4 IP address and subnet mask.

3. Enter **y** at the confirmation prompt and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Ports

1. Enter **4** and press **Enter** to configure System Ports.

```
*****  
* Configure Ports *  
*****  
Please input http port [80]:  
Please input https port [443]:  
Would you like to configure:  
    http port: 80  
    https port: 443  
[y|n] (y): _
```

2. At the prompt, enter an HTTP value and press **Enter**. Enter an HTTPS value and press **Enter**.

- HTTP Port (Valid range: 1024 to 65535, Default = 80)
- HTTPS Port (Valid range: 1024 to 65535, Default = 443)

Note: You can press **Enter** to accept default values. New port values must be unique (i.e., they must differ from any previously-configured ports).

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

After entering values and confirming, you must restart all services for the changes to take effect. Use the **Restart All Services** option in the **Run Watchdog** command in the Virtual Appliance Menu.

Configure Default Gateway

1. Enter **5** and press **Enter** to configure default gateway settings.

```
*****  
* Configure Default Gateway *  
*****  
Please input default gateway v4 [10.255.221.254]:  
Would you like to configure:  
    default gateway: 10.255.221.254  
[y|n] (y): y  
The configuration has been set  
Press [Enter] to continue
```

2. Enter an IPv4 default gateway.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Hostname

1. The default Hostname is **omnivista**. If you want to change the default Hostname, enter **6** and press **Enter**.

```
*****  
* Configure Hostname *  
*****  
Please input hostname [omnivista]:  
Would you like to configure:  
    hostname: omnivista  
[y|n] (y):  
The configuration has been set  
Press [Enter] to continue
```

2. Enter a hostname.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure DNS Server

1. Enter **7** to specify whether the VM will use a DNS Server.
2. If the VM will use a DNS server, enter **y**, then press **Enter**. Enter the IPv4 address for Server 1 and Server 2, if applicable.

```

*****
* Configure DNS Server
*****
Would you like to use dns servers [y|n] (n): y
(*) Please input dns server 1: 192.168.70.226
Would you like to use dns server 2 [y|n] (n): y
(*) Please input dns server 2: 192.168.1.3
Would you like to configure:
    dns server 1: 192.168.70.226
    dns server 2: 192.168.1.3
[y|n] (y): _
    
```

Note: If **n** (No) is selected, all DNS Servers will be disabled.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Timezone

1. Enter **8** and press **Enter** to begin setting up the time zone; then confirm by typing **y** at the prompt.
2. Select the region for the VM by entering its corresponding numeric value (e.g., **10**).

```

*****
* Configure Timezone
*****
Would you like to configure Timezone of system [y|n] (n): y
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa          4) Arctic Ocean      7) Australia        10) Pacific Ocean
2) Americas        5) Asia              8) Europe
3) Antarctica      6) Atlantic Ocean   9) Indian Ocean
#?
    
```

3. Select a country within the region by entering its corresponding numeric value (e.g., **25**).

```

Please select a country.
1) Chile          15) Northern Mariana Islands
2) Cook Islands  16) Palau
3) Ecuador        17) Papua New Guinea
4) Fiji           18) Pitcairn
5) French Polynesia 19) Samoa (American)
6) Guam           20) Samoa (western)
7) Kiribati       21) Solomon Islands
8) Marshall Islands 22) Tokelau
9) Micronesia     23) Tonga
10) Nauru          24) Tuvalu
11) New Caledonia 25) United States
12) New Zealand   26) US minor outlying islands
13) Niue           27) Vanuatu
14) Norfolk Island 28) Wallis & Futuna
#?
_
    
```

4. If prompted, enter the numeric value for the specific time zone within the country (e.g., **21**).

```
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? _
```

5. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Route

- 1. If you want to add a static route from the VM to another network enter **9** and press **Enter**.
- 2. Add an IPv4 route by entering **3** at the command prompt.

```
*****
* Configure Route
*****
* [1] Help
* [2] Show Current Routes
* [3] Add Route v4
* [4] Del Route v4
* [0] Exit
*****
```

- 3. Enter the subnet, netmask and gateway.
- 4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Network Size

1. At the Main Menu prompt, enter **10** and press **Enter** to begin configuring a Network Size.

```
*****
* Configure Network Size
*****
* [1] Help
* [2] Configure OV2500 Memory
* [3] Configure Swap File
* [4] Extend Data Partition
* [0] Exit
*****
```

2. You can re-configure OV 2500 NMS-E 4.2.1.R01 memory settings by selecting option **2**. Select an option (e.g., Low, Medium, High) based on the number of devices being managed and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt. You will be prompted to restart the Watchdog Service for the change to take effect.

3. Configure Swap file by selecting option **3**.

- **1 - Show Current Swap Files** - Enter **1** and press **Enter** to display information about any configured Swap Files.
- **2 - Add Swap File** - Enter the size of the Swap File in MB (Range = 1 - 4096). Enter **y** and press **Enter** at the Confirmation Prompt.
- **3 - Delete Swap File** - Select the Swap File you want to delete and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt.

4. Configure Data Partition by selecting option **4**.

By default, OV 2500 NMS-E 4.2.1.R01 is partitioned as follows: HDD1:50GB and HDD2:256GB. If you are managing more than 500 devices it is recommended that you increase to provisioned hard disk using the Configure Network Size option in the Configure The Virtual Appliance Menu (Configure The Virtual Appliance Menu – Configure Network Size (10) - Configure Data Partition (4)).

Configure Keyboard Layout

1. Enter **11** and press **Enter** to specify a keyboard layout.

```
*****
* Configure Keyboard Layout
*****
The available keyboard layouts will be shown (press [q] to exit view mode)
Press [Enter] to continue
```

2. Press **Enter** to see the list of keyboard layouts.

3. Enter **q** and press **Enter** to quit the view mode. At the prompt, enter a keyboard layout then press **Enter**. Press **y** at the confirmation prompt.

```
Please input keyboard layout [us]: us
Would you like to set:
    keyboard layout: us
[y;n] (y):
```

The table below lists all supported keyboard layouts.

OmniVista 2500 NMS Enterprise 4.2.1.R01 (MR 2) Installation Guide

amiga-de	amiga-us	atari-uk-falcon	atari-se
atari-us	atari-de	pt-olpc	es-olpc
sg-latin1	hu	sg	fr_CH
de-latin1-nodeadkeys	fr_CH-latin1	de-latin1	de_CH-latin1
cz-us-qwertz	sg-latin1-lk450	croat	slovene
sk-prog-qwertz	sk-qwertz	de	cz
wangbe	wangbe2	fr-latin9	fr-old
azerty	fr	fr-pc	be-latin1
fr-latin0	fr-latin1	tr_f-latin5	trf-fgGlod
backspace	ctrl	applkey	keypad
euro2	euro	euro1	windowkeys
unicode	se-latin1	cz-cp1250	il-heb
ttwin_cplk-UTF-8	pt-latin1	ru4	ruwin_ct_sh-CP1251
ruwin_alt-KOI8-R	no-latin1	pl1	cz-lat2
nl2	mk	es-cp850	bg-cp855
by	uk	pl	ua-cp1251
pt-latin9	sk-qwerty	se-lat6	bg_bds-cp1251
ruwin_cplk-UTF-8	br-abnt	la-latin1	sr-cy
ruwin_ctrl-CP1251	ua	dk	ru-yawerty
mk-cp1251	ruwin_cplk-KOI8-R	kyrgyz	defkeymap_V1.0
se-fi-lat6	ruwin_ctrl-UTF-8	ro	fi
sk-prog-qwerty	trq	fi-latin9	gr
ru3	us	ruwin_ct_sh-KOI8-R	nl
ro_std	ttwin_alt-UTF-8	trf	ruwin_alt-UTF-8
it-ibm	il	by-cp1251	it
emacs	fi-latin1	pc110	bg_bds-utf8
tralt	defkeymap	bg_pho-utf8	ua-ws
cf	hu101	bg_pho-cp1251	se-ir209
ttwin_ctrl-UTF-8	cz-lat2-prog	br-latin1-us	mk-utf
cz-qwerty	ruwin_cplk-CP1251	ttwin_ct_sh-UTF-8	ru1
ruwin_ctrl-KOI8-R	ru-ms	no	us-acentos
pl2	sv-latin1	br-latin1-abnt2	et
ru-cp1251	ruwin_alt-CP1251	ru	it2
lt.l4	ua-utf	bywin-cp1251	bg-cp1251
ru_win	emacs2	dk-latin1	kazakh
br-abnt2	es	pl4	mk0
is-latin1	is-latin1-us	il-phonetic	fi-old
et-nodeadkeys	jp106	lt	ru2
ruwin_ct_sh-UTF-8	pt	se-fi-ir209	gr-pc
lt.baltic	tr_q-latin5	pl3	ua-utf-ws
bashkir	no-dvorak	dvorak-r	dvorak
ANSI-dvorak	dvorak-l	mac-euro	mac-euro2
mac-fr_CH-latin1	mac-us	mac-de-latin1	mac-be
mac-es	mac-pl	mac-se	mac-dvorak
mac-fi-latin1	mac-template	mac-dk-latin1	mac-de-latin1-nodeadkeys

mac-fr	mac-pt-latin1	mac-uk	mac-it
mac-de_CH	sunt4-no-latin1	sunt5-cz-us	sundvorak
sunt5-de-latin1	sunt5-us-cz	sunt5-es	sunt4-fi-latin1
sunkeymap	sunt4-es	sunt5-ru	sunt5-uk
sun-pl	sunt5-fr-latin1	sunt5-fi-latin1	sun-pl-altgraph

4. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Update SSL Certificate

To update the SSL Certificate, you must first generate a *.crt and *.key file and use an SFTP Client to upload the files to the VA. Make sure the destination directory is "keys".

Note: If the certificate was issued by a private CA (i.e., not in the OV default Java trust store), you will also need to import the private CA's root certificate, see [Import JRE CA Certificate](#) below.

- **SFTP User:** cliadmin
- **SFTP Password:** <password when deploying VA>
- **SFTP Port:** 22

1. Enter **12** and press **Enter**.

2. Choose a file certificate file (.crt) and enter **y** and **Enter**. Choose a private key file (.key) and enter **y** and **Enter**. The Tomcat service will be restarted.

```

=====
Update the SSL Certificate for OV 2500 NMS...
=====
Certificates available in directory /home/admin/omnivista/ng_shared/temp/admin/keys:
    [1] server.crt
Choose the certificate file to apply (choose 0 to exit): 1
Are you sure you want to apply this certificate?
    [1] server.crt
(y/n): y
Private keys available in directory /home/admin/omnivista/ng_shared/temp/admin/keys :
    [1] server.key
Choose the private key file to apply (choose 0 to exit): 1
Are you sure you want to use this private key?
    [1] server.key
(y/n): _
    
```

Configure NTP Client

1. Enter **13** and press **Enter** to configure an NTP Server.

```

*****
* Configure NTP Client
*****
* [1] Help
* [2] Configure NTP Server IP
* [3] Status NTP Client
* [4] Disable NTP Client
* [5] Enable NTP Client
* [0] Exit
*****
    
```

2. Enter **2** and press **Enter**.

3. Enter the IP address of the NTP Server and press **Enter**.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu. You can enable the server when you create it, or enable it at a later time using option 5.

Configure Proxy

OV 2500 NMS-E 4.2.1.R01 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management. If the OV 2500 NMS-E 4.2.1.R01 Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OmniVista to connect to the OmniVista 2500 NMS External Repository.

1. Enter **14** and press **Enter** to specify whether the VM will use a Proxy Server. Enter **1** and press **Enter** to configure a Proxy Server.

```
*****
* Configure Proxy
*****
* [1] Setup Proxy
* [2] Enable/Disable Proxy
* [0] Exit
*****
```

2. If the VM will use a proxy server, enter the Proxy Server IP address, along with the port (e.g., 8080).

```
(*) Type your option: Proxy is not set
(*) Please input proxy IP: (*) Please input proxy port: Please input proxy username :
Would you like to configure proxy with:
    IP: 10.255.10.80
    Port: 8080
    Username:
    Password:
[yin] (y):
```

Note: If **n** (No) is selected, all proxy servers will be disabled.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Import JRE CA Certificate

To import a JRE CA Certificate (e.g., *.pem), you must first use an SFTP Client to upload the files to the VA. Make sure the destination directory is "keys".

- **SFTP User:** cliadmin
- **SFTP Password:** <password when deploying VA>
- **SFTP Port:** 22

1. Enter **15** and press **Enter** to import a Private CA Certificate.


```

*****
* Import JRE CA Certificate
*****
* Available self sign certificate(s)
*****
* [1] TashRootCA.pem
* [0] Exit
*****
(*) Type your option: 1
Would you like to use this self sign certificate?
    [1] TashRootCA.pem
Type(n): y
(*) Please input alias: tash
    
```

2. Enter the number for the certificate you want to import (e.g., 1) and press **Enter**.

3. Enter an alias for the certificate and press **Enter**. The certificate will be imported.

```

Issuer: EMAILADDRESS=tash.rozi@al-enterprise.com, CN=Tash Rozi, OU=NMS, O=ALE, L=Calabasas, ST=CA, C=US
Serial number: c3a3953b2754770f
Valid from: Mon May 09 17:45:46 PDT 2016 until: Wed Feb 27 16:45:46 PST 2019
Certificate fingerprints:
    MD5: CB:CA:A5:F7:48:ED:7C:E5:2E:45:FF:A2:4C:81:D5:55
    SHA1: 30:3F:74:B1:B3:25:46:AB:71:09:89:3C:68:C2:F1:92:FF:CB:D8:A9
    SHA256: 65:3E:3A:5B:95:F2:D6:A1:83:B5:62:D1:BB:A3:4A:54:A7:1B:92:D1:F1:8C:7D:41:65:64:3E:56:15:D4:0A:D8
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:
#1: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: D0 58 71 0C 47 47 EF B7 53 91 B9 7B 43 F7 3F 9F .Xq.GG..S...C?.
0010: FC DA 6B 95 ..k.
]
]

#2: ObjectID: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]

#3: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: D0 58 71 0C 47 47 EF B7 53 91 B9 7B 43 F7 3F 9F .Xq.GG..S...C?.
0010: FC DA 6B 95 ..k.
]
]

Trust this certificate? [no]: _
    
```

4. Enter **y** at the confirmation prompt and press **Enter**. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Exit

Enter **0** and press **Enter** to return to the Virtual Appliance Menu.

Run Watchdog Command

The Watchdog command set is used to start and stop managed services used by OV 2500 NMS-E 4.2.1.R01. If you stop certain framework services (e.g., ActiveMQ, Apache Tomcat) or a service that these services depend on, the web server will shut down, and you will have to restart the service manually. You will receive a warning prompt whenever you try to shut down one of these services.

To access the Watchdog CLI Command Menu, enter **3** at the command prompt. The following displays:

```

*****
* Run Watchdog Command
*****
* [1] Help
* [2] Display Status Of All Services
* [3] Start All Services
* [4] Stop All Services
* [5] Restart All Services
* [6] Start a Service
* [7] Stop a Service
* [8] Start Watchdog
* [9] Shutdown Watchdog
* [0] Exit
*****
(*) Type your option: _
    
```

The following options are available:

- **Display Status Of All Services** - Displays the status of all of the services used by OmniVista (Running/Stopped). To display the status for all services just once (Default), Enter **n** and press **Enter** at the "Continuous Status" Prompt (or just press **Enter**). The status will be displayed and you will be returned to the Run Watchdog Command Menu. To run and display continuous status checks for all services, Enter **y** then press **Enter** at the "Continuous Status" Prompt. To stop the display and return to the Run Watchdog Command Menu, enter **Ctrl C**.
- **Start All Services** - Starts all services. Enter **y** and press **Enter** at the Confirmation Prompt.
- **Stop All Services** - Stop all services. Enter **y** and press **Enter** at the Confirmation Prompt.
- **Restart All Services** - Stop and restart all services. Enter **y** and press **Enter** at the Confirmation Prompt.
- **Start a Service** - Starts a single service. Enter the service name at the prompt and press **Enter**. At the "Start Tree" option, enter **y** and press **Enter** to start all dependent services; enter **n** if you do not want to start dependent services. Press **Enter** at the Confirmation Prompt to start the service(s).
- **Stop a Service** - Stops a single service. Enter the service name at the prompt and press **Enter**. At the "Stop Tree" option, enter **y** and press **Enter** to stop all dependent services; enter **n** if you do not want to stop dependent services. Press **Enter** at the Confirmation Prompt to stop the service(s).
- **Start Watchdog** - Starts the Watchdog Service, which starts all services.
- **Shutdown Watchdog** - Stops the Watchdog Service, which stops all services.

Upgrade/Backup/Restore VA

The Upgrade/Backup/Restore VA command set is used to display information about the currently-installed OmniVista 2500 NMS software, upgrade OmniVista software, configure the OV Build Repository, and backup/restore OV software. OV software and updates are stored on an external repository (ALE Central Repository). By default, the OV Virtual Appliance points to the ALE Central Repository, which contains the latest builds and software updates. If a proxy has been configured, make sure to configure the proxy to connect to the external repository.

```

*****
* Upgrade VA
*****
* [1] Help
* [2] 4.2.1.R01 (Current Release)
* [3] 4.2.2.R01 (New Release)
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
    
```

To view information about the currently-installed version of the OV 2500 NMS-E 4.2.1.R01 VA, and to update the VM, enter **4** at the command prompt. The following options are available:

- 4.2.1.R01 (Current Release)** - Displays information about the currently-installed OmniVista NMS software (e.g., Release Number, Build Number). It also checks for, and displays information about, any available updates. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. If an upgrade is available, enter **y** and press **Enter** to install the upgrade.

Note that you can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available. Also note that if a new version is available (e.g., R01 to R02), and you do not have the latest R01 software patches installed, you will first be prompted to install the latest R01 patches, and will then be prompted to install R02.

- 4.2.2.R01 (New Release)** - Displays information about the next available OmniVista NMS Software Release (e.g., 4.2.2.R01). If a new release is available, the release information is displayed and the user is prompted select whether or not to upgrade to the new release. If a new release is available, enter **y** and press **Enter** to install the upgrade.

Note that if a new release is available (e.g., 4.2.2.R01), you can only upgrade if you are running the latest version of the previous release. For example, you can only upgrade from 4.2.1.R01 (MR2) to 4.2.2.R01 if you are running the latest version of 4.2.1.R01 (MR2). If you are not running the latest version of the previous release, you will first be prompted to install the latest version, and will then be prompted to install the new release.

- Enable Repository** - Enable an OV Build Repository. This is the repository that OmniVista 2500 NMS will use to retrieve OV upgrade software. Select a repository from the list, enter **y** and press **Enter** at the Confirmation Prompt to enable the repository. Only one (1) repository can be enabled at a time.
- Configure Custom Repositories** - Configure a custom repository. By default, the OV Virtual Appliance points to the external ALE Central Repository, which contains the latest OV software. However, you can configure up to three (3) custom repositories. Select a repository (e.g., [1] "Custom Repo 1" Repository) and press **Enter**. Complete the fields as described below, then enter **y** and press **Enter** at the Confirmation Prompt:

- **Repository Name** - User-configured repository name.
- **Repository URL Host** - The IP address of the custom repository (e.g., 192.168.70.10).
- **Repository URL Location** - The directory location of the upgrade software (e.g., repo/centos)
- **Repository Full URL** - Is automatically completed by OV after confirming the configuration.

Only one (1) repository can be enabled at a time. The user is responsible for ensuring that the custom repository contains the latest OV software.

- **Configure Update Check Interval** - Configure how often the OmniVista 2500 NMS Server will check the OV Build Repository for updates. You can perform a check immediately or schedule the check to be performed at regular intervals. The results of the scheduled checks are displayed on the Welcome Screen.
 - **Check Now** - Run the Update Check Task immediately and displays the results. Enter **2** and press **Enter**. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. If an upgrade is available, enter **y** and press **Enter** to install the upgrade. Note that you can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available. Also note that if a new release is available (e.g., R01 to R02), and do not have the latest R01 software patches installed, you will first be prompted to install the latest R01 patches, and will then be prompted to install R02.
 - **Check Daily/Weekly/Monthly** - Run the Update Check Task at the configured intervals and displays the results on the Welcome Screen. Select an interval and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt.
 - **Disable (Default)** - Disable the Update Check Task. Enter **6** and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt.
- **Backup/Restore OV2500 NMS Data** - Backup/Restore OmniVista 2500 NMS data. The following options are available:
 - **Configure Backup Retention Policy** - Configure the maximum number of days that you want to retain backups (Range = 1 – 30, Default = 7), and the maximum number of backups that you want to retain (Range = 1 – 30, Default = 5). Backup files are automatically deleted based on the Backup Retention Policy.
 - **Backup Now** - Perform an immediate backup. Enter an optional name for the backup (default = ov2500nms) and press **Enter**. Press **y** at the confirmation prompt. When the backup is complete, it will be stored in the “backups” Directory (/opt/OmniVista_2500_NMS/data/file_server/cliadmin/backups) with the backup name and the date and time of the backup (<base name>_<yyyy-MM-dd--HH-mm>.bk). If you do not enter a name, the backup will be stored as ov2500nms-yyyy-MM-dd--HH-mm>.bk.
 - **Schedule Backup** – You can schedule an automatic backup to begin at a specific time and repeat at a specific daily interval. Enter a time for the backup to begin (HH:mm format) and press **Enter**. Enter the time between backups (Range = 1 – 30 Days, Default = 1) and press **Enter**. You can change the backup schedule at any time.

Note: Scheduled backups utilize the Task Scheduler (Windows) and Cron Job (Linux) utilities. If necessary, these utilities can be used to modify a scheduled backup.

Note: Backup files are automatically deleted based on the Backup Retention Policy. Monitor and maintain the Backup Directory to optimize disk space.

- **Restore** - Select a backup and press **Enter**. Press **y** at the Confirmation Prompt and press **Enter**.

Note: You can only perform a restore using a backup from the same release (e.g., you can only restore a 4.2.1.R01 (MR2) configuration using a 4.2.1.R01 (MR 2) Backup File.) OmniVista will not allow you to perform a restore using a backup from a previous release.

Note: If you want to perform a restore using an MR 2 Backup File residing on a different system, you must change the IP address of the system on which you are performing the restore to match the IP address of the system from which the backup file was taken **before** performing the restore. After the restore is complete, you can use the Configure The Virtual Appliance Menu ([Option 3 - Configure IP](#)) to return the restored system to its original IP address.

For example, if you want to use a backup file on System A (IP A) to perform a restore on the System B (IP B), you must change the IP address of System B to the IP address of System A (IP A) **before** performing the restore. After the restore is complete, you can use the Configure The Virtual Appliance Menu ([Option 3 - Configure IP](#)) to change the IP address on System B back to its original IP address (IP B).

- **View Backup Configurations** - View the backup retention policies. The policies are configured using Option 2 – Configure Backup Retention Policy.

Change Password

You can change the Virtual Appliance cliadmin password and/or mongo database password.

```
*****
* Change Password
*****
* [1] Help
* [2] Change "cliadmin" Password
* [3] Change MongoDB Database Password
* [4] Configure Root Password
* [0] Exit
*****
```

To change the VA cliadmin password, enter **2**, then press **Enter**. At the prompts, enter the current password, then enter the new password.

To change the mongo database password, enter **3**, then press **Enter**. You have two options when changing the mongo database password.

```
(*) Type your option: 3
Would you like to change password for
    [1] Mongo administrator
    [2] Ngnms application user
Provide your option [1 OR 2]: _
```

Enter **1** to change the mongo administrator password. Enter **2** to change the application user password. At the prompts, enter the current password, then enter the new password.

To change the password of the “root” user of the VA enter **4**, then press **Enter**. Enter the old password at the prompt and press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

Logging

You can view OV 2500 NMS-E 4.2.1.R01 Logs using the “Logging” option. Enter **6**, then press **Enter**.

```
*****  
* Configure Logging *  
*****  
* [1] Help *  
* [2] Change Log Level *  
* [3] Collect Log Files *  
* [4] Collect JVM Information *  
* [0] Exit *  
*****
```

The following options are available:

- **Change Log Level** - Changes the logging level for OV services. Enter the number corresponding to the OV service for which you want to change the logging level (e.g. 13 - ovsip) and press **Enter**. Enter the number corresponding to the package for which you want to change the logging level (e.g. 1 - com.alu.ov.ngms.sip.service) and press **Enter**. Enter the number corresponding to the log level you want to set (e.g., 2 - DEBUG) and press **Enter**.
- **Collect Log Files** - Collects all log files from a specific date to the current date. Enter the date from which you want to collect log files in dd-MM-yyyy format (e.g., 10-15-2016) and press **Enter**. When finished, a "Collecting completed" message is displayed. The log files are stored in a zip file in the "logs" Directory with the date and time the logs were collected appended to the file name (e.g., ovlogs-15-10-2016_12-04-18.zip). SFTP to the VA using the "cliadmin" username and password to view the log files (Port 22).
- **Collect JVM Information** - Collects and archives Java Virtual Machine (JVM) information. Enter **y** and press **Enter** at the confirmation prompt to collect JVM information. When finished, a "Collecting completed" message is displayed along with the JVM information file name. The file is stored in the "jvm-info" directory with date and time the file was created collected appended to the file name (e.g., jvm-info-02016-10-15-12-08-43.jar). SFTP to the VA using the "cliadmin" username and password to view the log file (Port 22).

Login Authentication Server

The Login Authentication Server is used to view/change the OV 2500 NMS-E 4.2.1.R01 Login Authentication Server.

```
*****  
* Login Authentication Server *  
*****  
* [1] Help *  
* [2] Current Login Authentication Server *  
* [3] Change Login Authentication Server to local *  
* [0] Exit *  
*****  
(* ) Type your option: _
```

Enter **2** and press **Enter** to display the current Login Authentication Server. If the server is remote, the IP address is displayed. If the server is local, "local" is displayed.

If the current Login Authentication Server is a remote server, enter **3** and press **Enter** to change the Login Authentication Server to "local". Enter **y** and press **Enter** at the Confirmation Prompt.

Power Off

Before powering off the VM, you must stop all OV 2500 NMS-E 4.2.1.R01 services using the **Stop All Services** option in the **Run Watchdog Command**. After all the services are stopped, enter **7** at the command line to power off the VM. Confirm the power is off by entering **y**. The power off may take several minutes to complete.

Note: OV 2500 NMS-E 4.2.1.R01 functions stop running following power off. The VM must be powered back on via the VMware client software and you must log back into the VM via the console.

Reboot

Before rebooting the VM, you must stop all OV 2500 NMS-E 4.2.1.R01 services using the **Stop All Services** option in the **Run Watchdog Command**. After all services are stopped, enter **8** at the command line to reboot the VM. Confirm reboot by entering **y**. The reboot may take several minutes to complete. When rebooted, you will be prompted to log in through the cliadmin user and password prompts. Note that OV 2500 NMS-E 4.2.1.R01 functions continue following reboot.

Advanced Mode

Advanced Mode enables you to use read-only UNIX commands for troubleshooting. Enter **9**, then press **Enter** to bring up the CLI prompt. Enter **exit** and press **Enter** to return to the Virtual Appliance Menu. The following commands are supported:

- /usr/bin/touch
- /usr/bin/mktemp
- /usr/bin/dig
- /usr/bin/cat
- /usr/bin/nslookup
- /usr/bin/which
- /usr/bin/less
- /usr/bin/tail
- /usr/bin/vi
- /usr/bin/tracepath
- /usr/bin/tty
- /usr/bin/systemctl
- /usr/bin/grep
- /usr/bin/egrep
- /usr/bin/fgrep
- /usr/bin/dirname
- /usr/bin/readlink
- /usr/bin/locale
- /usr/bin/ping

- /usr/bin/traceroute
- /usr/bin/netstat
- /usr/bin/id
- /usr/bin/ls
- /usr/bin/mkdir
- /usr/sbin/ifconfig
- /usr/sbin/route
- /usr/sbin/blkid
- /usr/sbin/sshd-keygen
- /usr/sbin/consotype
- /usr/sbin/ntpdate
- /usr/sbin/ntpq
- /usr/bin/ntpstat
- /usr/bin/abrt-cli
- /usr/sbin/init
- /usr/sbin/tcpdump
- /bin/mountpoint

Set Up Optional Tools

The Setup Optional Tools command set is used to install/upgrade Hypervisor Optional Tools Packages.

```
*****
* Optional Tool Of Supervisors Menu                               *
*****
* [1] Help                                                       *
* [2] VMware Tools                                             *
* [3] VirtualBox Guest Additions                               *
* [4] Hyper-V Linux Integration Services                       *
* [0] Exit                                                      *
*****
(*) Type your option:
```

Enter the number corresponding to the Hypervisor you are using (**2 - VMWare**, **3 - Virtual Box**, **4 - Hyper-V**) and press **Enter**. Information about available packages is displayed. If a new package is available, type **y** and press **Enter** at the "Would you like to install the package" prompt. The package will automatically be downloaded from the OV Repository and installed (this may take several minutes). When the "Installation Complete" message is displayed, press **Enter** to continue. Press **Enter** again to restart the Virtual Appliance.

Log Out

To log out of the VM and return to the cliadmin login prompt, enter **0** at the command line. Confirm logout by entering **y**. Note that OV 2500 NMS-E 4.2.1.R01 functions continue following logout.