

**Installation Guide  
for  
OmniVista 2500 NMS  
Version 4.1.2.R03**



**January 2016  
Revision A  
Part Number 033057-10  
READ THIS DOCUMENT**

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

## Table of Contents

<b>OmniVista 2500 NMS Installation Guide</b> .....	<b>1</b>
<b>Installing OmniVista 2500 NMS</b> .....	<b>1</b>
Installing the OmniVista 2500 NMS Software .....	1
Configuring Java Settings on the Clients .....	8
Launching OmniVista 2500 NMS.....	11
Installing OmniVista 2500 NMS Security Certificates.....	12
Installing Security Certificates (Windows) .....	12
Installing the Web Security Certificate on the OV Server (Windows).....	12
Installing the Java Security Certificate on the OV Client (Windows).....	14
Importing the Certificate into the Trusted Certificate Store.....	18
Installing Security Certificates (Linux) .....	21
Installing the Web Security Certificate (Linux).....	21
Installing the Java Security Certificate (Linux) .....	23
Importing the Certificate into the Trusted Source Directory .....	26
Installing Web Browser Security Certificate on the OV Client .....	26
<b>Upgrading from a Previous Version of OmniVista 2500 NMS</b> .....	<b>26</b>
Upgrading from 3.5.7.....	26
Upgrading to a Windows/Linux Installation .....	26
Upgrading to a Virtual Appliance Installation.....	28
Upgrading from 4.1.2.R01 Post-GA .....	29
Upgrading From/To a Windows/Linux Installation.....	29
Upgrading From/To a Virtual Appliance Installation .....	30
Upgrading from 4.1.2.R02 GA .....	33
Upgrading From/To a Windows/Linux Installation.....	33
Upgrading From/To a Virtual Appliance Installation .....	34
Backup/Restore Procedures (Windows/Linux).....	35
Backup .....	35
Restore.....	36
<b>Uninstalling OmniVista 2500 NMS</b> .....	<b>37</b>
General Concepts for Uninstalling on Any Platform .....	37
Uninstalling on Windows .....	37
Uninstalling on Linux .....	37
<b>Deploying OmniVista 2500 NMS as a Virtual Appliance</b> .....	<b>38</b>
Deploying the Virtual Appliance.....	38
Launching the Console and Setting a Password.....	43
Configuring OmniVista 2500 NMS .....	44
Configuring the Default Gateway .....	45
Configuring the Hostname .....	45
Specifying a DNS Server .....	45
Specifying a Proxy Server .....	46
Setting the Time Zone .....	46
Configuring a Route .....	47
Configuring the Keyboard Layout .....	48
Review/Accept License Agreement .....	50
Configuring OmniVista 2500 Memory .....	50
Shutting Down OmniVista.....	51

## Table of Contents (continued)

<b>Using the Virtual Appliance Menu .....</b>	<b>52</b>
Configuring the Virtual Appliance .....	52
Configure Swap File .....	53
Updating the SSL Certificate .....	53
Running Watchdog CLI Command .....	54
Updating the Virtual Appliance .....	54
Backing Up or Restoring OmniVista 2500 NMS .....	55
Backup .....	56
Immediate Backup .....	56
Scheduled Backup .....	56
Restore .....	57
Changing the Virtual Appliance Password .....	58
Collecting Logs .....	59
Powering Off the Virtual Appliance .....	59
Rebooting the Virtual Appliance .....	59
Logging Out Of the Virtual Appliance .....	60
<b>Appendix A – Extending the VA Partition Size .....</b>	<b>A-1</b>

## OmniVista 2500 NMS Installation Guide

This document details the OmniVista 2500 NMS installation/upgrade process. 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 Screen).

Key applications in OmniVista 2500 NMS are web-based, others are java based (e.g., Discovery, Topology); however all are accessed through the OmniVista Web GUI. The Web GUI is supported on the following browsers: Internet Explorer 10+, Firefox 26+, and Chrome 26+. To access the java-based applications, you must have Java 7 or 8 installed on the Client machine.

Specific platform support and recommended system configuration information are available in the *OmniVista 2500 NMS Release Notes*.

**Important Note:** This document details [installing](#) OmniVista 2500 NMS as well as [upgrading from a previous version of OmniVista](#). **If you are upgrading from a previous version of OmniVista, there are upgrade tasks that must be performed before installing the new version of OmniVista.** If you are upgrading, go to the [upgrade](#) section.

### Installing OmniVista 2500 NMS

This section details the procedures for installing OmniVista 2500 NMS. Installation consists of the following steps:

- [Installing the OmniVista 2500 NMS Software](#)
- [Configuring Java Settings](#)
- [Launching OmniVista 2500 NMS](#)
- [Installing the OmniVista Security Certificates](#)

**Note:** OmniVista 2500 NMS uses an installer with a Graphical User Interface, and requires Graphics Libraries on RedHat and SUSE Linux to install the packages.

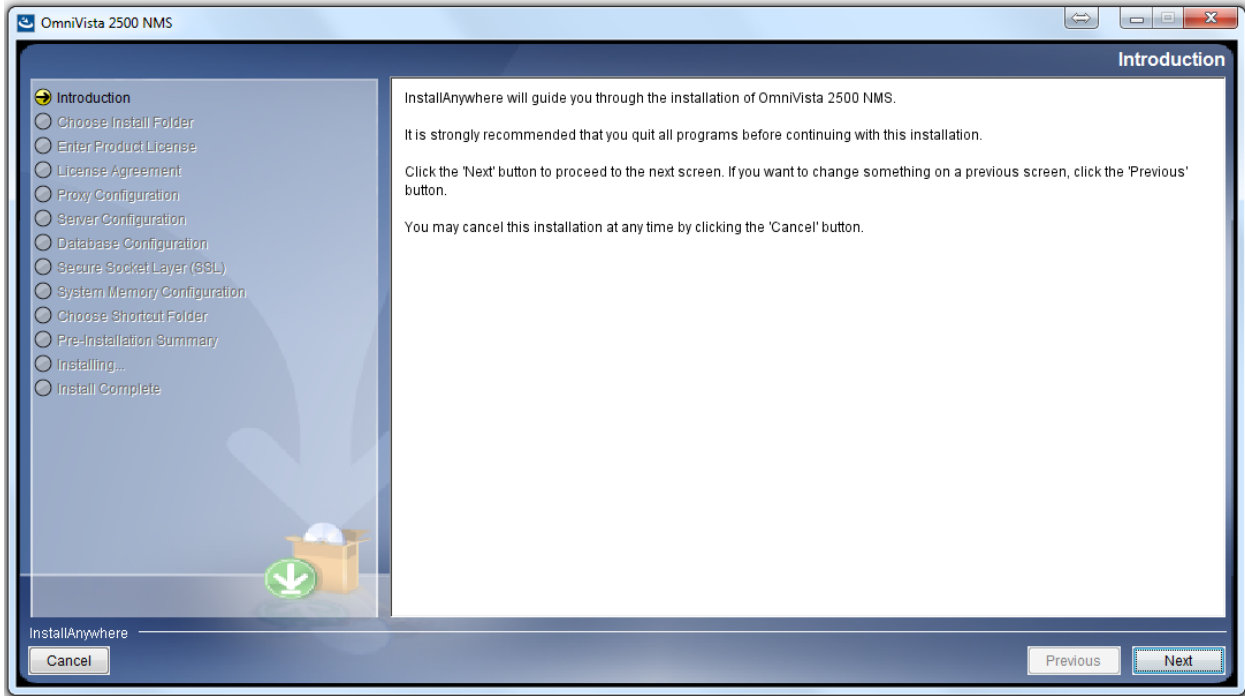
#### Installing the OmniVista 2500 NMS Software

1. Download the OmniVista 2500 NMS Application file.
2. Make sure IP address "1.1.1.1" is unreachable from the server on which you are installing OmniVista 2500 NMS.
3. Double-click on the file to start the Installation Wizard (for Windows, select and run .exe file; for Linux, change the permissions of the file and execute the .bin file).

**Note:** The installation process is GUI based so be sure the GUI can be launched from where the installation is attempted. (This might require starting up X-server on the Linux server and/or exporting the display appropriately.)

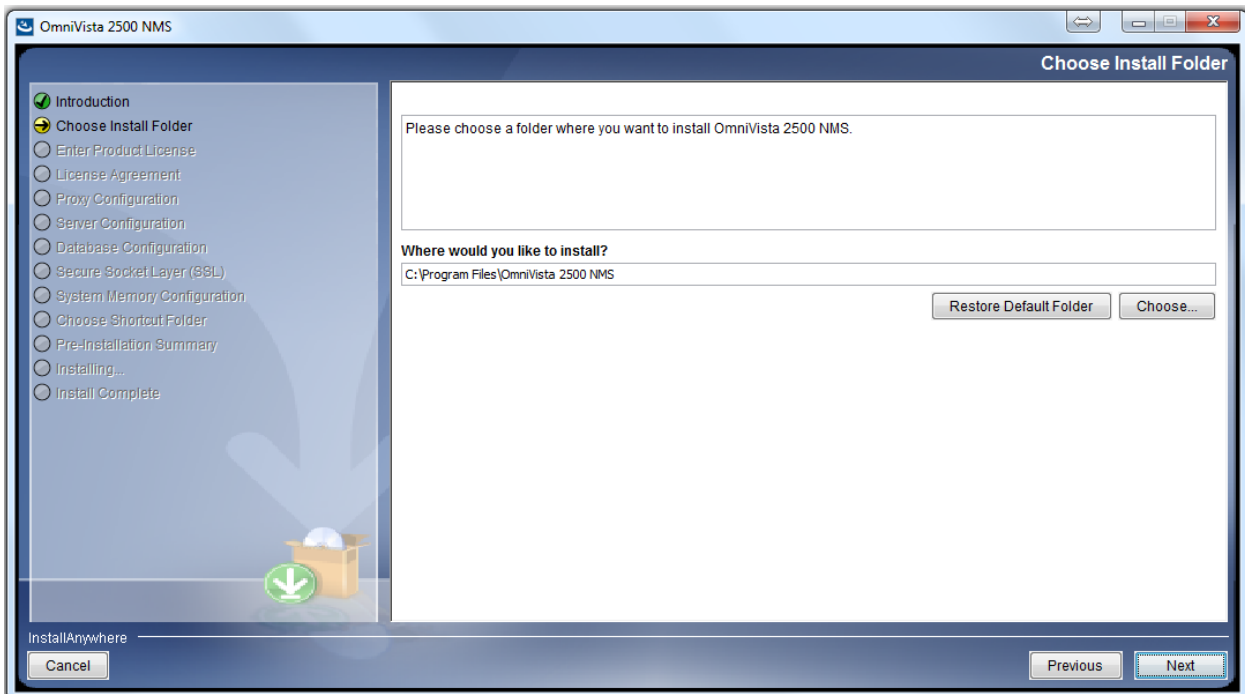
4. The InstallAnywhere Introduction displays. Click **Next** to continue.

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)



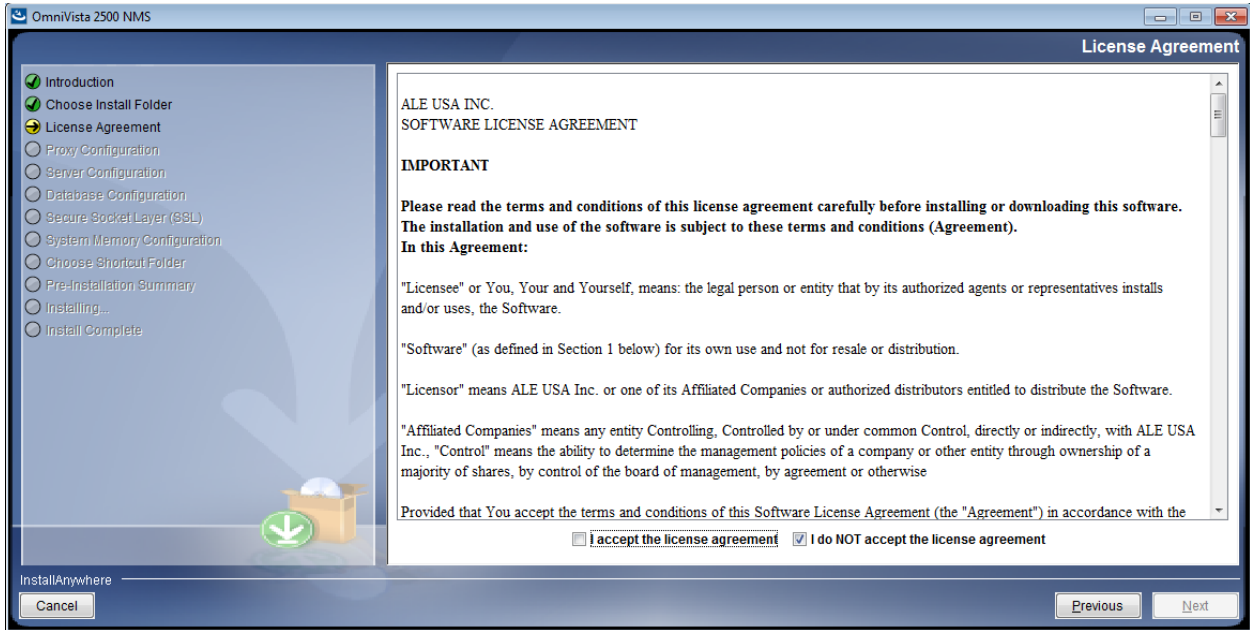
**5. Choose Install Folder.** Choose an Install Folder location. The default location automatically displays in the selection box (Windows - C:\Program Files\OmniVista 2500 NMS, Linux - /opt/OmniVista\_2500\_NMS). To change the location, select **Choose**. Click **Next** to continue.

**Important Note:** If you are [upgrading from OmniVista 4.1.1 or later](#), the Install Folder should be the same as the existing installation.

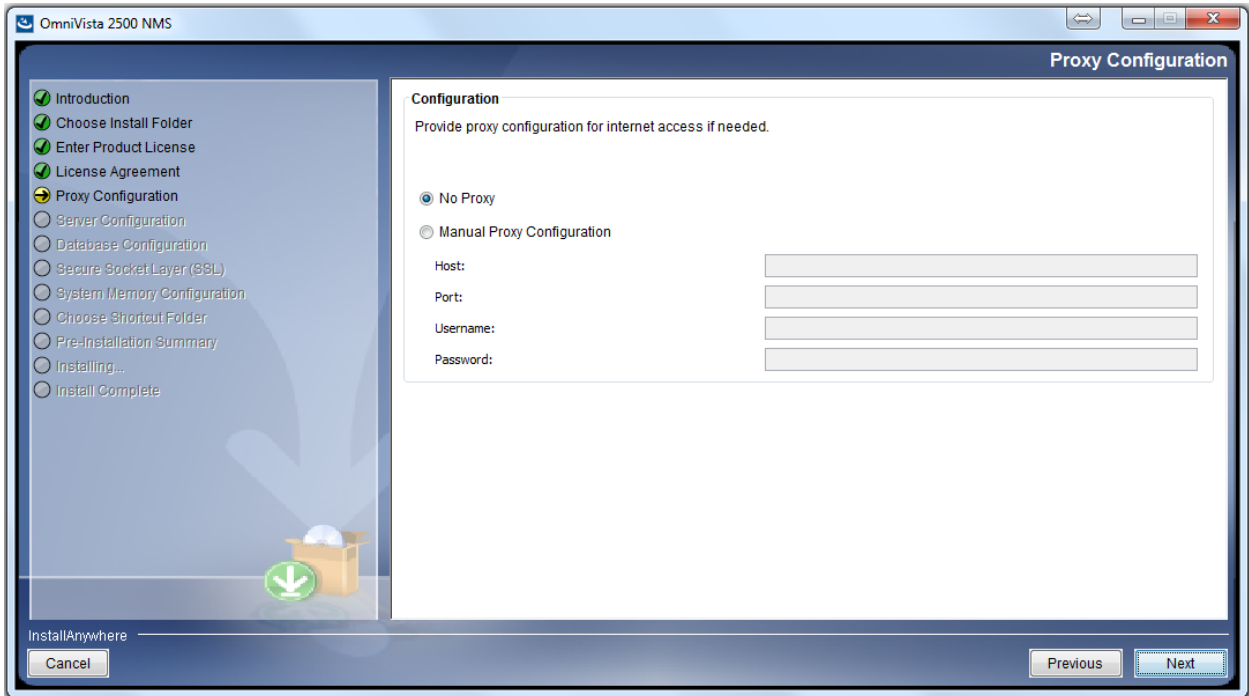


**6. License Agreement.** OmniVista displays the Software License Agreement in this panel. Read the agreement carefully and select “I accept the license agreement.” Click **Next** to continue.

**Note:** You must accept the ALE License to continue to the next step.



**7. Proxy configuration.** If using a proxy server, use this configuration screen to edit proxy settings for OmniVista 2500 NMS network connectivity. Click **Next** to continue.



## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

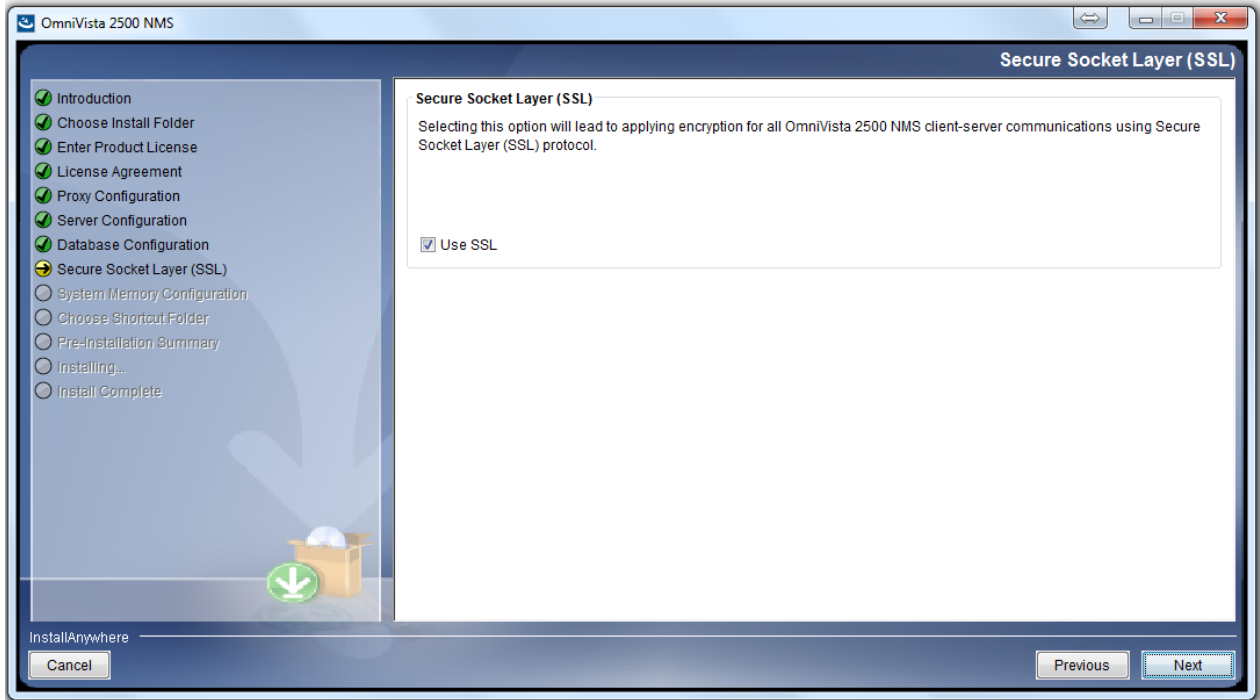
**8. Server Configuration.** This screen allows users to manually configure OmniVista 2500 NMS server information. Configure as required, or accept the default settings. Click **Next** to continue.

The screenshot shows the 'Server Configuration' window of the OmniVista 2500 NMS installer. The window title is 'OmniVista 2500 NMS' and the subtitle is 'Server Configuration'. On the left, a navigation pane lists the installation steps: Introduction, Choose Install Folder, License Agreement, Proxy Configuration, Server Configuration (highlighted), Database Configuration, Secure Socket Layer (SSL), System Memory Configuration, Choose Shortcut Folder, Pre-Installation Summary, Installing..., and Install Complete. The main area contains a 'Configuration' section with the instruction: 'Please provide configurations for OmniVista 2500 NMS server.' The configuration fields are: Application Server IP (135.115.206.45), Application Server HTTP Port (8071), Application Server HTTPs Port (8072), Auto redirect (checked), Core Server IP (135.115.206.45), Core Server Port (1127), ActiveMQ JMX Port (1099), ActiveMQ TCP Port (81616), ActiveMQ Jetty Port (8161), Service Port Range (7701 to 7721), LDAP Port (5389), Trap Port (162), and HSQLDB Port (9001). At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

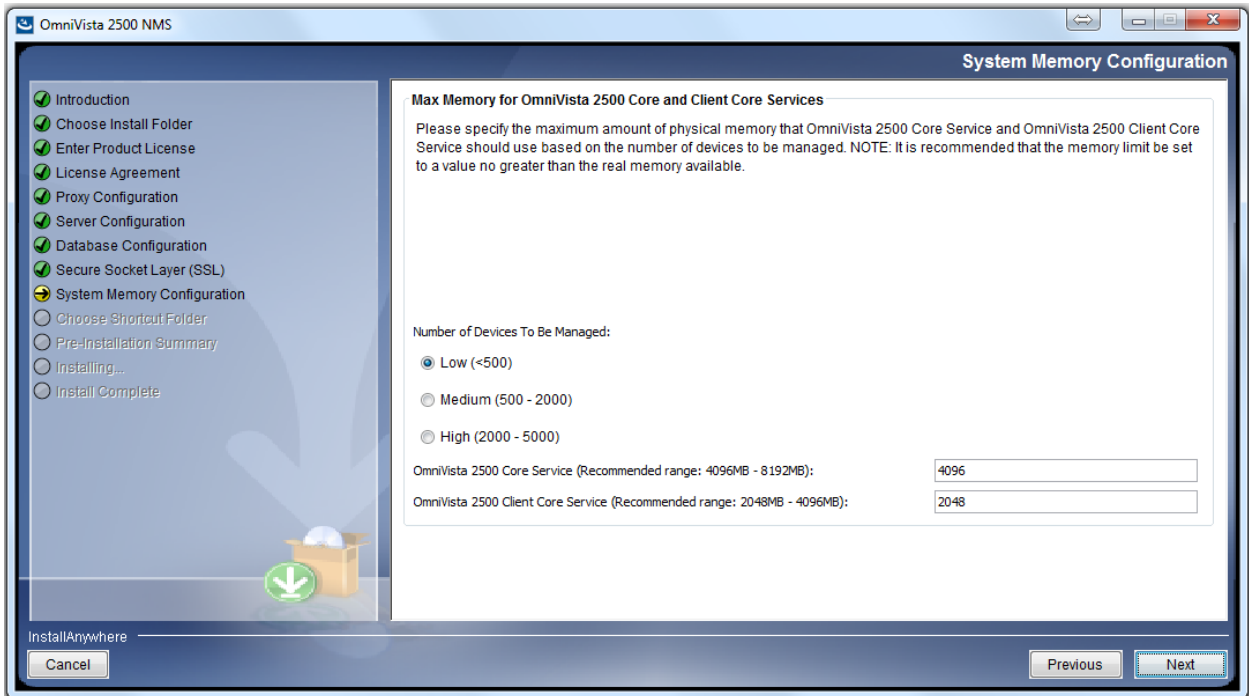
**9. Database Configuration.** Allows users to edit port, admin and password information for the Mongo database. Enter values for each field as needed. Click **Next** to continue.

The screenshot shows the 'Database Configuration' window of the OmniVista 2500 NMS installer. The window title is 'OmniVista 2500 NMS' and the subtitle is 'Database Configuration'. The navigation pane on the left is the same as in the previous screenshot, but 'Database Configuration' is now highlighted. The main area contains a 'Configuration' section with the instruction: 'The fields below contain basic configurations only. Advanced configurations can be made after the installation by editing mongod.conf file located in C:\Program Files\OmniVista 2500 NMS\ThirdParty\mongodb.' The configuration fields are: Port (27017), Administration Account (dbadmin), and Administration Password (masked with asterisks). At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

**10. Secure Socket Layer (SSL).** OmniVista supports SSL. By default, SSL is enabled. Accept the default value, or uncheck the “Use SSL” checkbox. Click **Next** to continue.

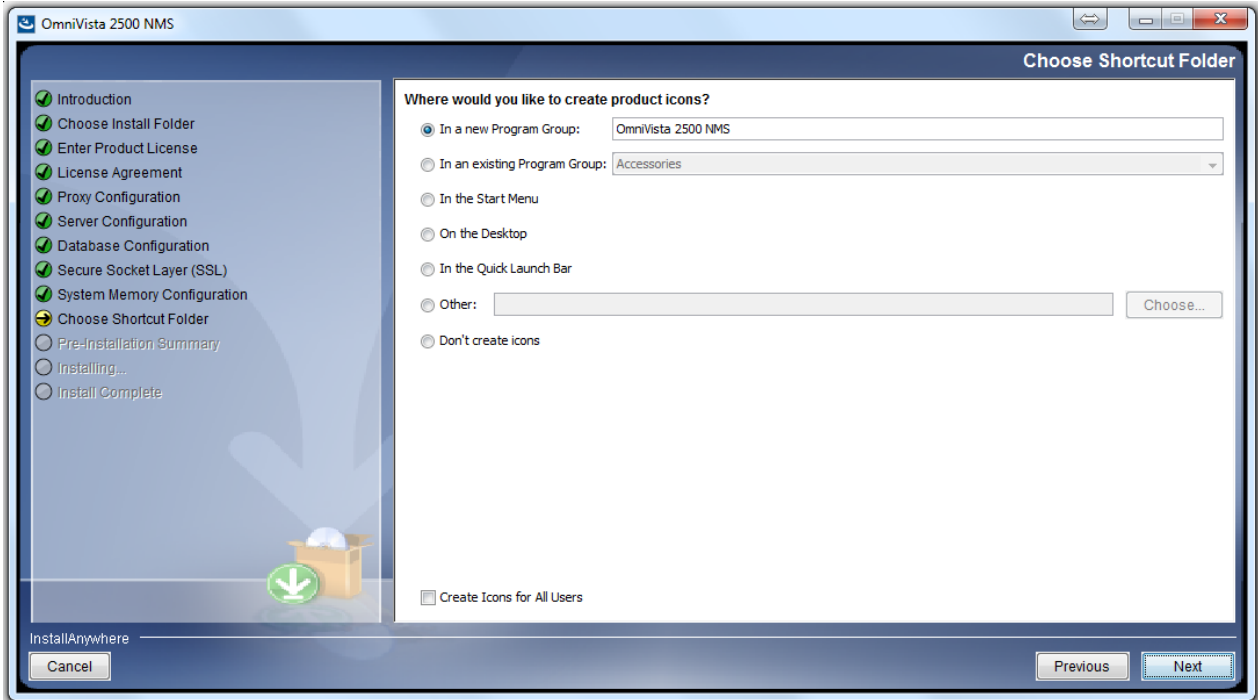


**11. System Memory Configuration.** This screen allows users to configure the maximum memory usage for OmniVista Core and Client Core Services. OmniVista displays minimum values in the recommended ranges. After configuring memory settings, click **Next** to continue.

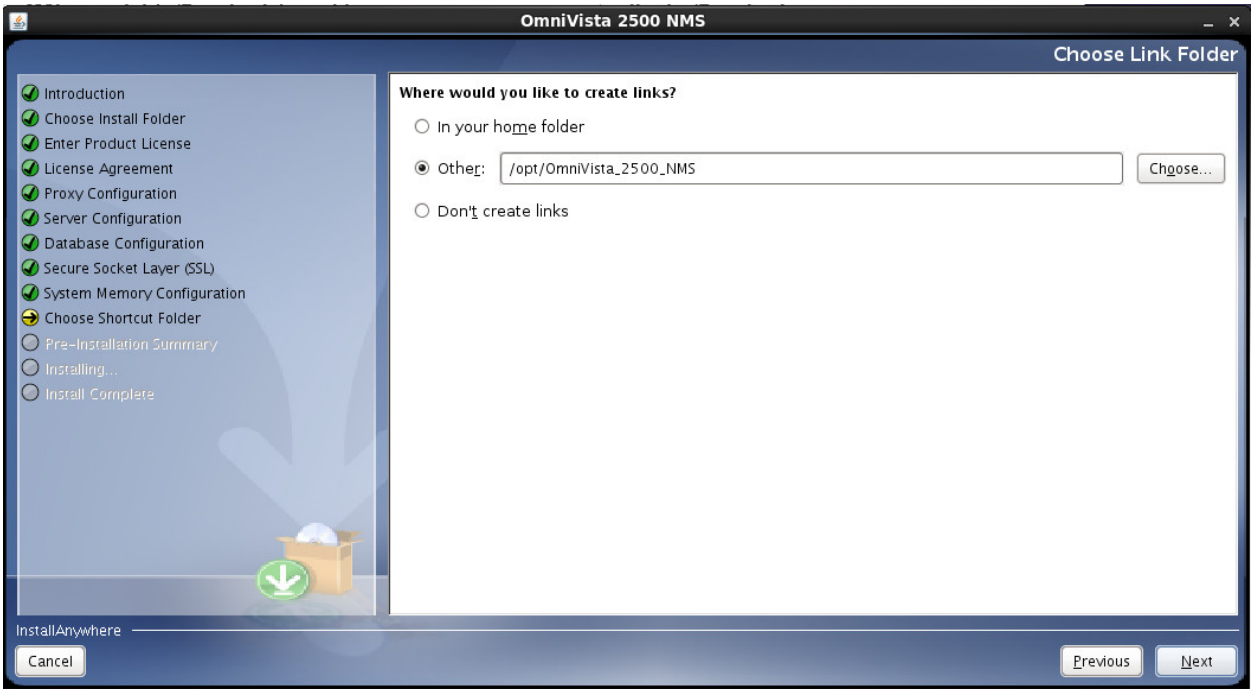




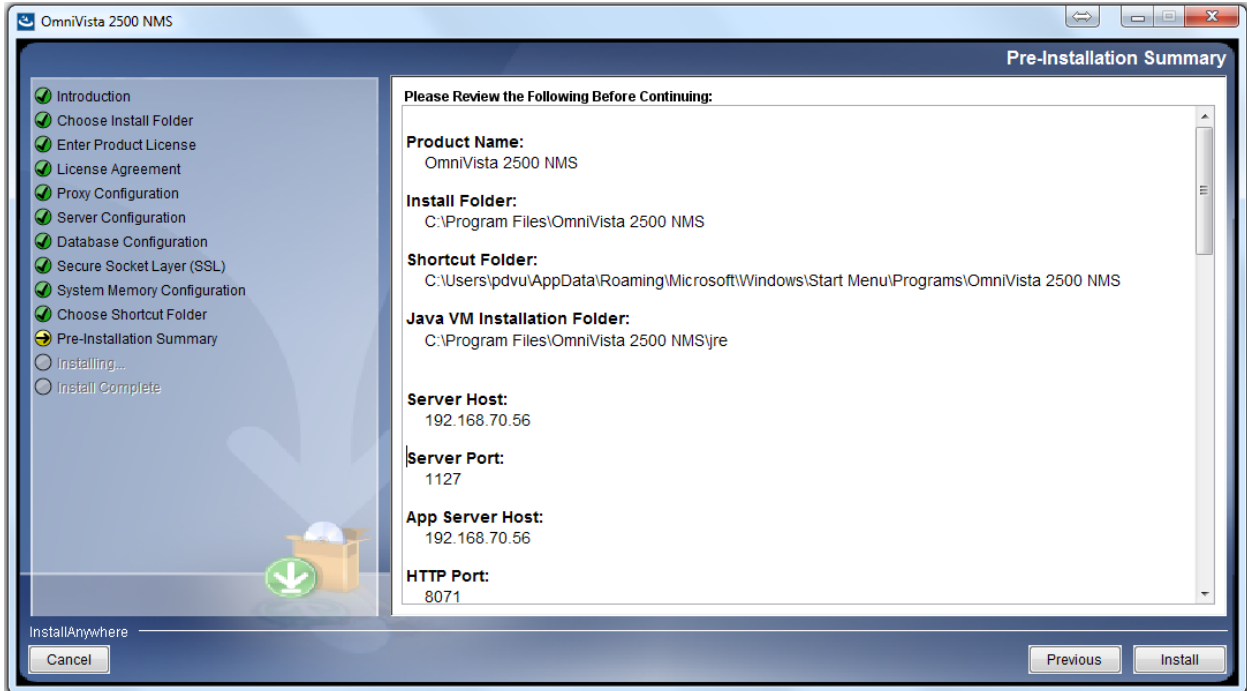
12. Choose Shortcut Folder. Select an option and click **Next** to continue.



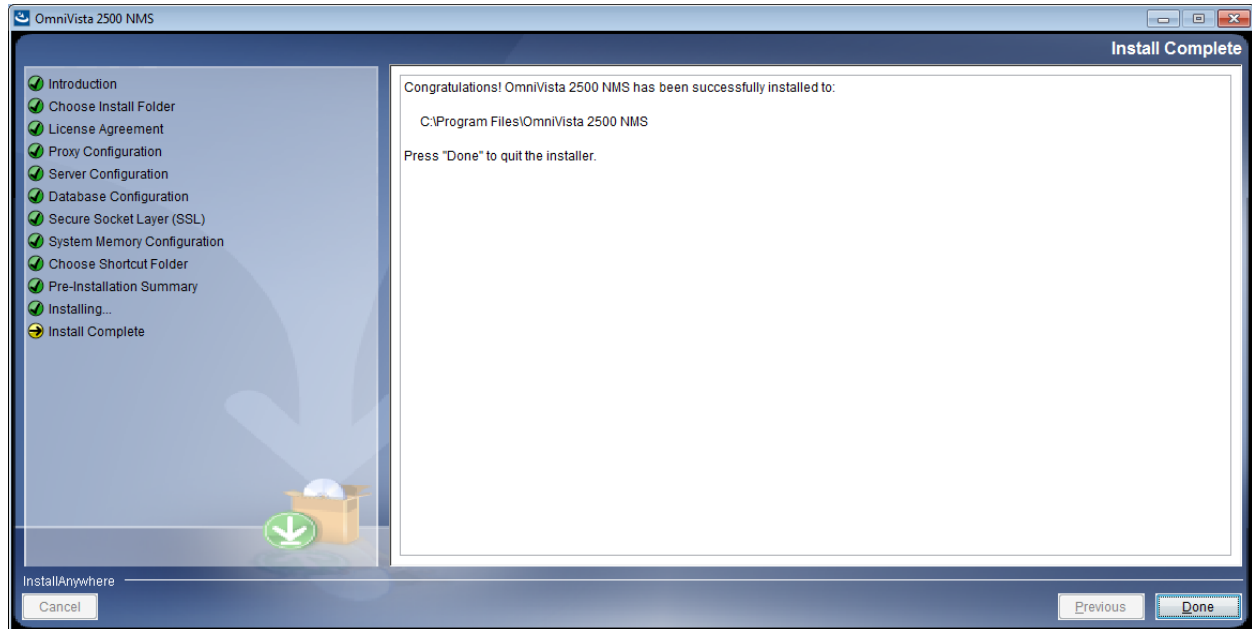
The “Choose Shortcut Folder” Screen **above** is displayed in a **Windows** installation. The screen **below** is displayed in a **Linux** installation.



**13. Pre-Installation Summary.** The Pre-Installation Summary screen displays the configuration that will install on the OmniVista Server. Review the configuration summary carefully before clicking **Install**. If settings require revisions, click the **Previous** button to go back and edit the settings as needed.



**14.** A progress bar displays at the bottom of the screen as the installation begins. Note that it can take several minutes to finish the installation.



**15.** Configure the java settings as described below.

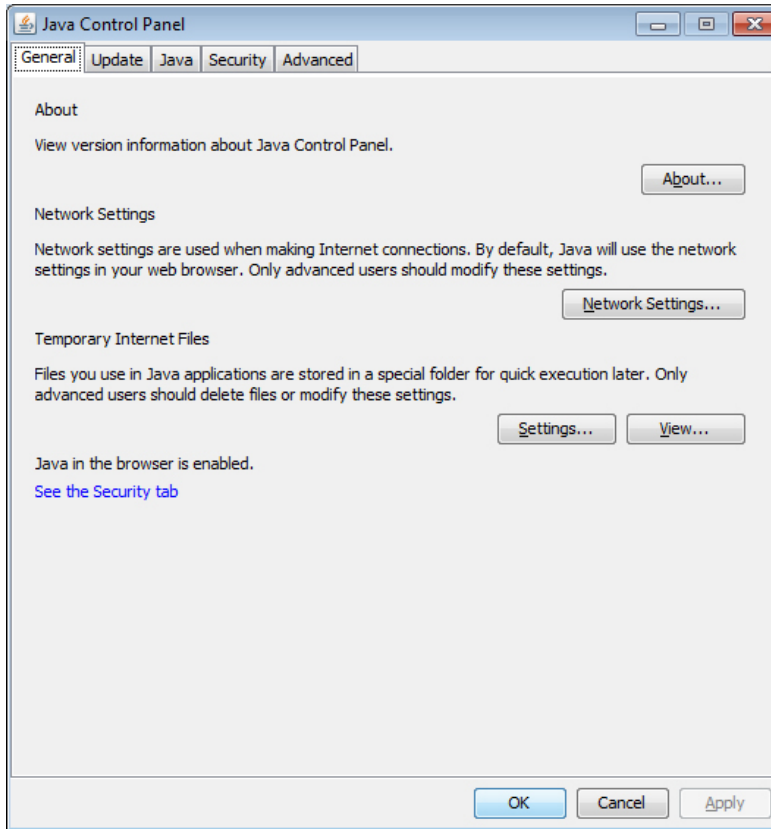
## Configuring Java Settings on the Clients

Follow the steps below to configure java control settings on any client that you will use to launch OmniVista 2500 NMS. This is required to enable OmniVista to launch java-based applications (e.g., Discovery, Topology) on the client.

Note that Java 7 and 8 are both supported on OmniVista Clients. The screens in the instructions below are from a client with Java 8 installed. Most of the Java Windows are the same for Java 7 and 8. If they are different, the difference is explained in the relevant step.

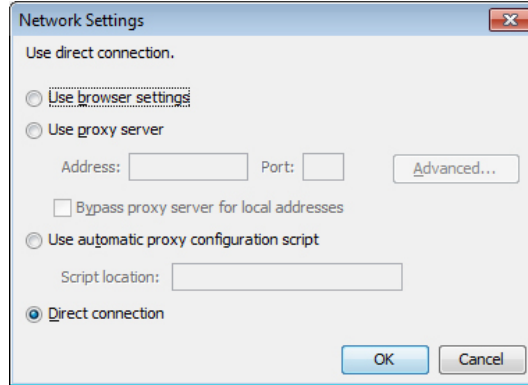
1. Go to the Java Control Panel.

- **Windows:** Start > Control Panel > Java.
- **Linux:** System > Preferences > Java or JRE\_HOME/bin/ControlPanel.



2. On the **General** Tab, click on the **Network Settings** button and configure the connection from the client system to the OmniVista Server.

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)



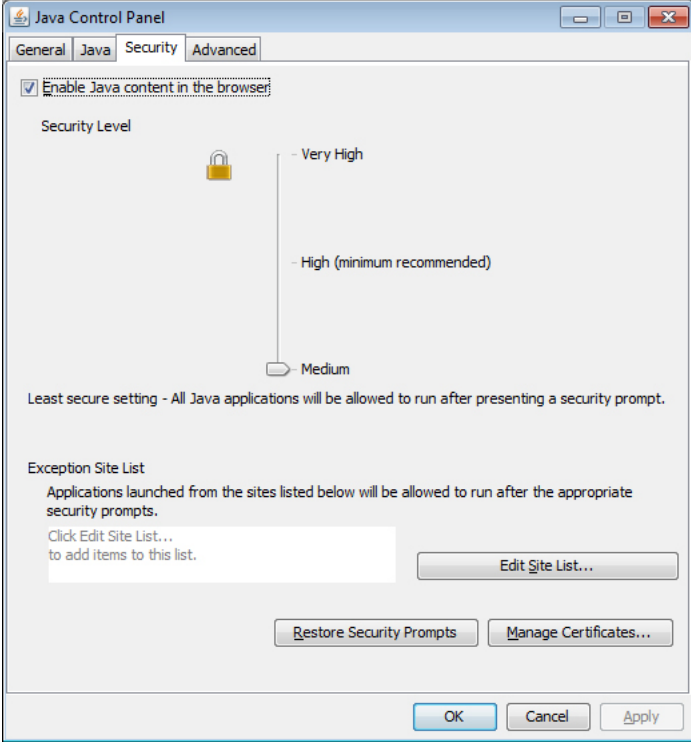
- **Use Browser Settings:** Select to use the browser default browser settings.
- **Use Proxy Server:** Set the address and port for a Proxy Server with the option to bypass it for local addresses. **OR** Click on the **Advanced** button to bring up the Advanced Settings dialog. In this panel, you can individually set the Proxy Server for HTTP, Secure, FTP, and Socks connections. You can also provide a list of address for which you do not want to use the Proxy Server.
- **Use Automatic Proxy Configuration Script:** Specify the location of the Java Script File (.js or .pac) that contains the FindProxyForURL Function. This function has the logic to determine the Proxy Server to use for a connection request.
- **Direct Connection:** Select if you do not need to use a proxy server to connect from this client to the OmniVista Server.

3. On the **Security Tab** (shown below), set the Security Level as follows **if you are using the OmniVista Self-Signed Security Certificate**.

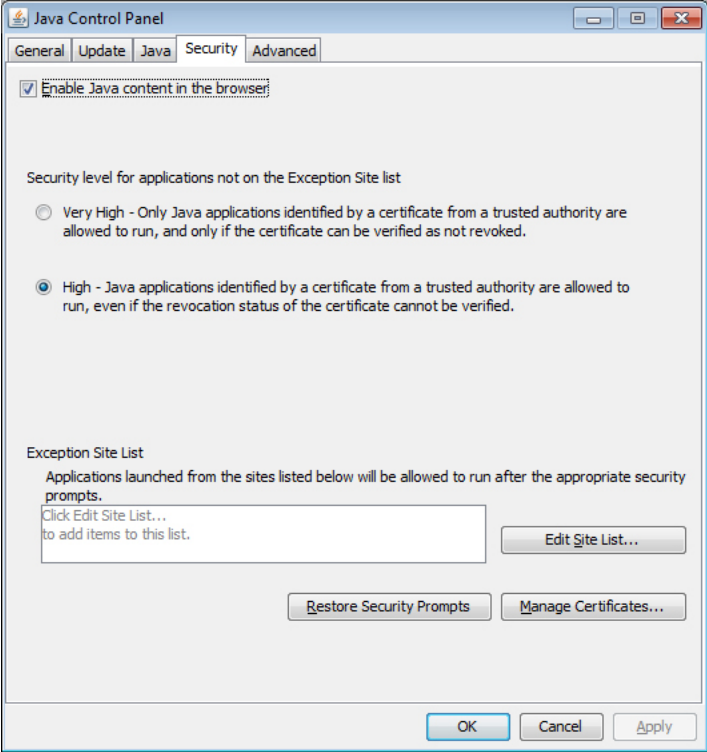
- **Java 7 Clients** - Set the Security Level Slider to **Medium**.
- **Java 8 Clients** - Select the **High** radio button.

**Note:** If you are obtaining a certificate from a certificate authority, you can use higher Security Levels.

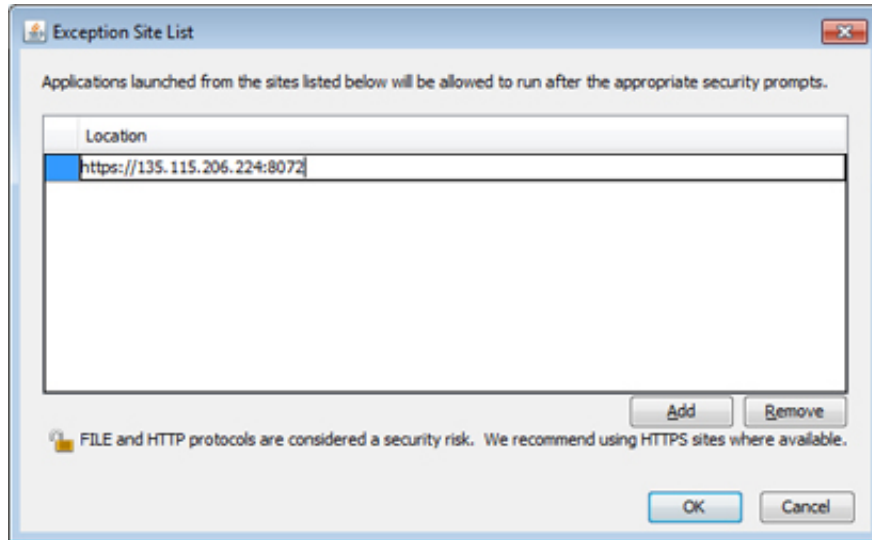
### Security Tab - Java 7 Client



### Security Tab - Java 8 Client



4. On the **Security Tab**, click on the **Edit Site List** button to bring up the Exception Site List window and add the OmniVista Server to the list. Click on the **Add** button and enter the full IP address (including port number) of the OmniVista Server (e.g., <https://135.115.206.224:8072>).



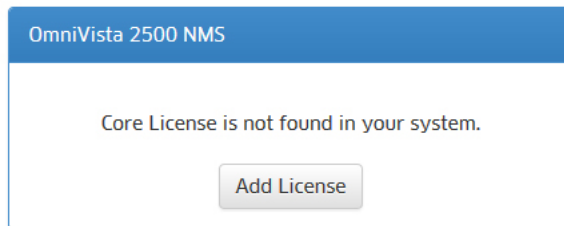
5. Click **OK**.

### Launching OmniVista 2500 NMS

To launch OmniVista 2500 NMS on Windows or Linux platforms, enter the IP address of the OmniVista Server and applicable port number in a supported web browser, for example: <https://IPAddress:8072/login.html>. Log in using the default Username and Password:

- **Username:** admin
- **Password:** switch

The first time you launch OmniVista, you will be prompted for the Core License Key after you enter the username and password.



Click on the **Add License** button to go to the Add or Import Management Screen. Paste the License Key into the License Key field and click the **Submit** button. The End User License Agreement Screen appears with the ProActive Lifecycle Management Feature enabled by default. To enable the feature, click the **Save** button, then click **OK** at the Results Screen. If you do not want to enable Proactive Lifecycle Management at this time, click the **Cancel** button, then click **OK** at the Results Screen. The OmniVista Dashboard appears.

**Note:** The ProActive Lifecycle Management Feature periodically gathers detailed information for all discovered devices on your network and uploads the information to the ProActive Lifecycle Management Web Portal. The information is also available to you

through a widget that can be displayed on the OmniVista 2500 NMS Dashboard for easy reference.

If you choose not to enable the ProActive Lifecycle Management Feature at installation, you can enable it at a later time in the Preferences Application. And if you enable it at install, you can disable it at a later time in the Preferences Application.

## Installing OmniVista 2500 NMS Security Certificates

Once you install the OmniVista 2500 NMS software and configure the java settings as described above, you will be able to access the OmniVista Web GUI. However, to launch Java-based applications (e.g., Discovery, Topology); you **must** install the necessary Security Certificates on [Windows](#) or [Linux](#) Clients as well as the browser described below.

### ***Installing Security Certificates (Windows)***

Install the [Web Security Certificate](#) on the OmniVista Server and the [Java Security Certificate](#) on the OmniVista Client as described below.

#### *Installing the Web Security Certificate on the OV Server (Windows)*

By default, the OmniVista 2500 NMS Installer creates a self-signed certificate for HTTPS connections. You can override this Self-Signed SSL certificate with your own, by creating a Valid Self-Signed SSL Certificate.

However, Launching OmniVista in a browser using self-signed certificates results in many security warnings. You can reduce the number of HTTPS security warnings by obtaining a valid SSL Server Certificate from a certificate authority. (e.g., VeriSign, Thawte, Geotrust, Comodo SSL). Once you create a valid self-signed certificate, or obtain one from a certificate authority, you must import the certificate using OmniVista's keystore.bat script.

**Note:** If you already own a valid SSL certificate, skip to [Importing the Certificate](#), below.

#### *Creating a Valid Self-Signed SSL Certificate*

Self-signed certificates are useful for users who require encryption but do not need to verify the identity of a requesting website or web application (e.g., OmniVista). Follow the steps below to create a valid self-signed certificate.

1. Open a command line with Administrator privileges.
2. cd to <OV\_Install\_Root>\ThirdParty\openssl\bin.
3. Generate a private key using OpenSSL. Options include *with password* or *without password*:
  - **With Password** - Enter the following: `openssl genrsa -des3 -out server.key 2048`
  - **Without Password** - Enter the following: `openssl genrsa -out server.key 2048`
4. Create a Certificate Signing Request (CSR) using Open SSL:  
`openssl req -new -key server.key -out server.csr -sha256`
5. Follow the prompts to specify country name, organization name, location, etc. Make sure the "Common Name" is the IP address of the OmniVista Server.

```

Administrator: Command Prompt
C:\Program Files\OmniVista 2500 NMS\ThirdParty\openssl\bin>openssl req -new -key
server.key -out server.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:Calabasas
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ALE
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:135.115.207.151
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\Program Files\OmniVista 2500 NMS\ThirdParty\openssl\bin>

```

#### 6 Generate a self-signed certificate:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt -sha256
```

#### 7. Once you have created the certificate, continue to [Importing the Certificate](#).

**Note:** After importing the self-signed certificate, you can [import the certificate into the Trusted Certificate Store](#) on your system to prevent any browser certificate warnings.

#### *Obtaining a Certificate from a Certificate Authority*

To obtain a certificate from a certificate authority, you must submit a Certificate Signing Request (CSR) from the provider (e.g., VeriSign, Thawte, Geotrust, Comodo SSL). To submit a CSR:

1. Open a command line and cd to <OV\_Install\_Root>\ThirdParty\openssl\bin.
2. Generate a private key using OpenSSL. Options include *with password* or *without password*:
  - **With Password** - Enter the following: `openssl genrsa -des3 -out server.key 2048`
  - **Without Password** - Enter the following: `openssl genrsa -out server.key 2048`
3. Create a Certificate Signing Request (CSR) using Open SSL:

```
openssl req -new -key server.key -out server.csr
```
4. Follow the prompts to specify your name, organization name, location, etc.
5. Submit the generated CSR file to your chosen certificate authority. Refer to the Certificate Authority's website for steps and information.
6. Once you have obtained the certificate from the provider, continue to [Importing the Certificate](#).



### *Importing the Certificate*

1. Locate the OmniVista **keystore.bat** file. This file can be found in the OmniVista scripts directory, located in the OmniVista 2500 NMS Program File folder (e.g., C:\Program Files\OmniVista 2500 NMS\scripts). Run it with **Administrator** privileges.
2. At the “Please input your certificate” prompt, enter the directory path and name of the certificate file (e.g., C:\Program Files\OmniVista 2500 NMS\ThirdParty\openss\bin\server.crt).
3. At the “Please input your private key” prompt, enter the directory path and name of the key file (e.g., C:\Program Files\OmniVista 2500 NMS\ThirdParty\openss\bin\server.key).
4. From the command line, cd to <OV\_Install\_Root>\Watchdog.
5. Stop Apache Tomcat using the Watchdog CLI:  

```
watchdog-cli stopservice -n ovtomcat
```
6. Restart Apache Tomcat using the Watchdog CLI:  

```
watchdog-cli startservice -n ovtomcat
```
7. Once the certificate has successfully imported, launch OmniVista 2500 NMS in a supported browser to view results.

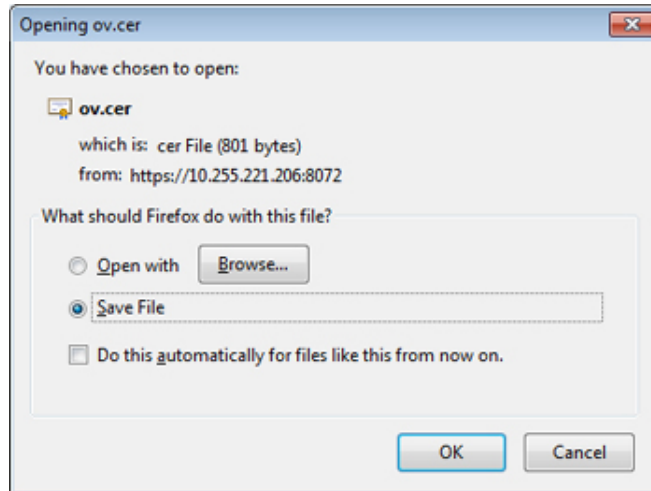
### *Installing the Java Security Certificate on the OV Client (Windows)*

Once you install the OmniVista 2500 NMS software and configure the java settings, you will be able to access the OmniVista Web GUI. However, to launch Java-based applications (e.g., Discovery, Topology), and you **must** add the OmniVista Server address to the Java Exception Site List on the OmniVista client and install the necessary Web Security Certificates.

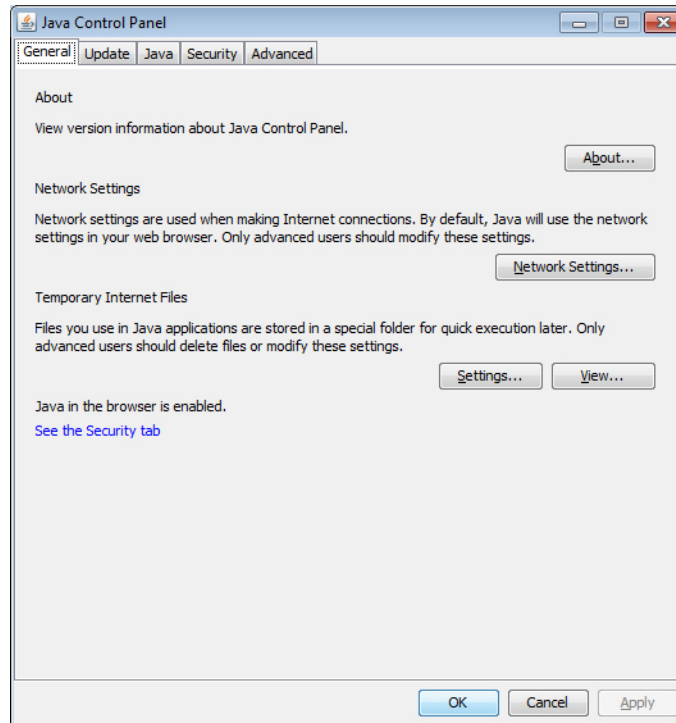
**Note:** The Certificates must be installed on clients running Java 8. The Certificates are not required on clients running Java 7; however, you will receive a number of security warnings. To streamline the launch, it is recommended that you install the Certificate on clients running Java 7.

1. Log into OmniVista 2500 NMS.
2. Download the default OmniVista certificate from the OmniVista Server. In the browser window, enter the OmniVista Server IP address and port number, followed by **/webstart/ov.cer**, then press **Enter**. For example, if your OmniVista Server IP address is 10.255.221.209, you would enter `https://10.255.221.209:8072/webstart/ov.cer`. The following window appears.
3. Click **OK** to download the certificate.

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

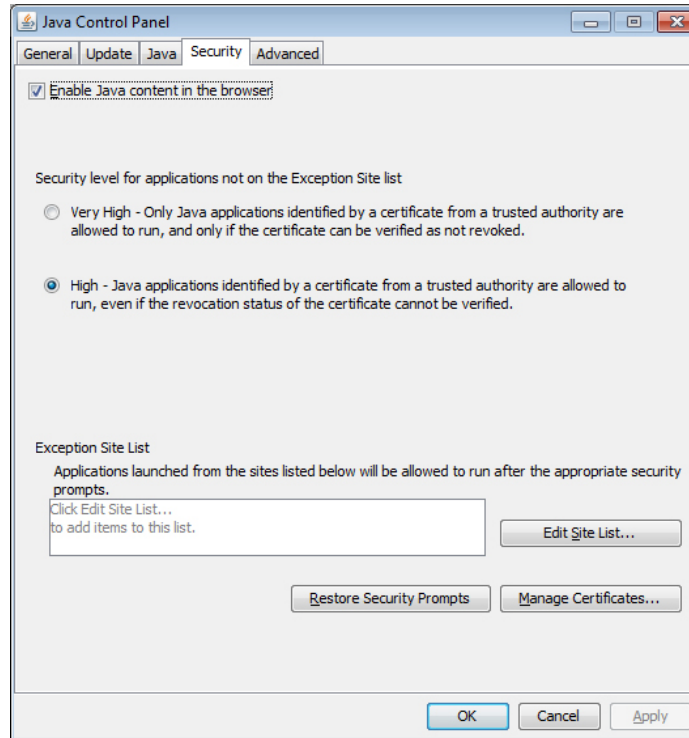


4. Open the **Java Control Panel** - Start > Control Panel > Java.

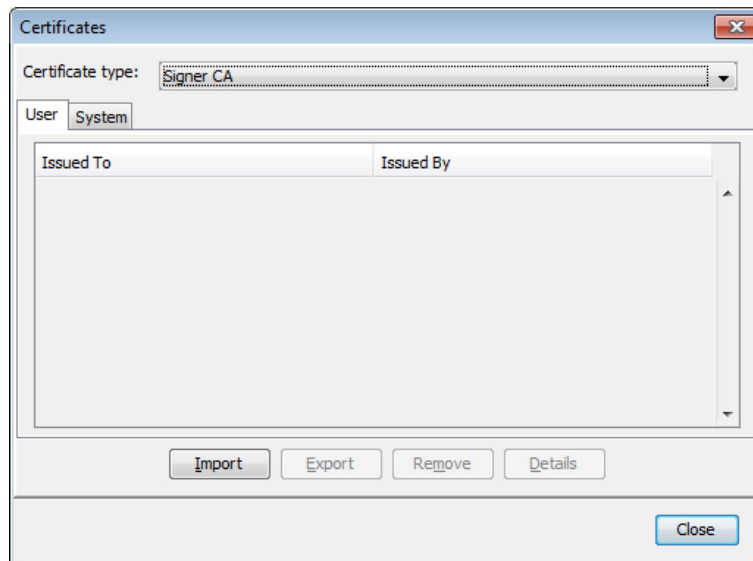


5. Click on the **Security** tab.

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

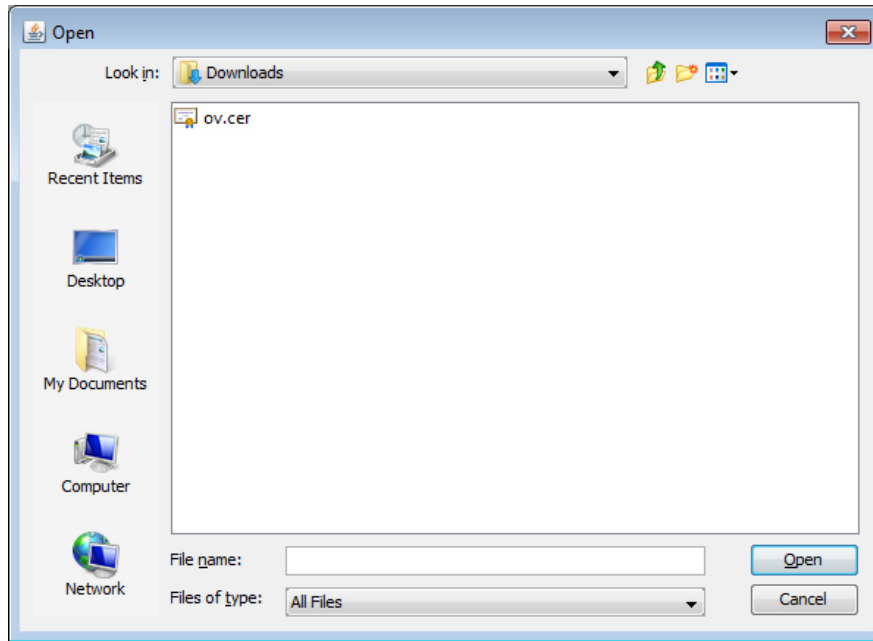


6. Click on the **Manage Certificates** button to bring up the Certificates window. *Note that the Security Tab on Java 7 clients is slightly different. However, you will still click on the **Manage Certificates** button to bring up the Certificates window.*



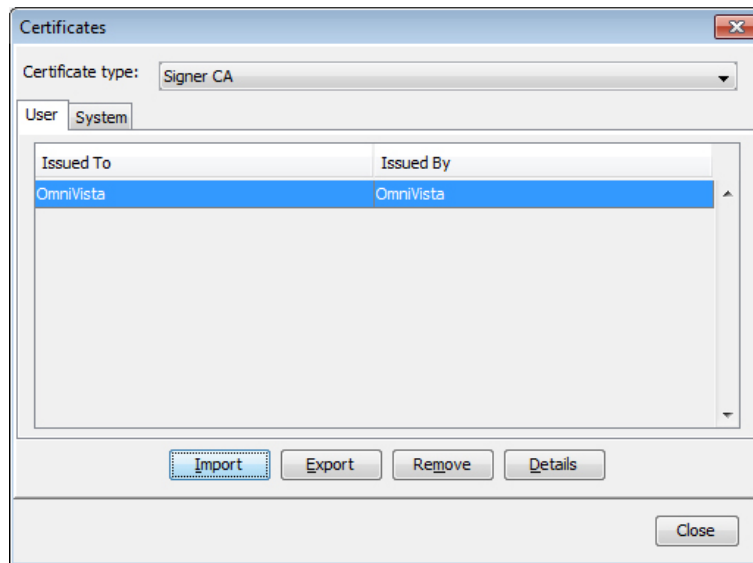
7. In the **Certificate Type** pull-down, select **Signer CA**, then click **Import**.

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)



8. Make sure the **File Type** at the bottom of the window is set to “All Files”, and locate the Certificate file you downloaded in Step 3 (ov.cer). Select the file and click **Open**.

9. You will be returned to the Certificates Screen with the OmniVista Certificate displayed in the User Certificate table, as shown below.

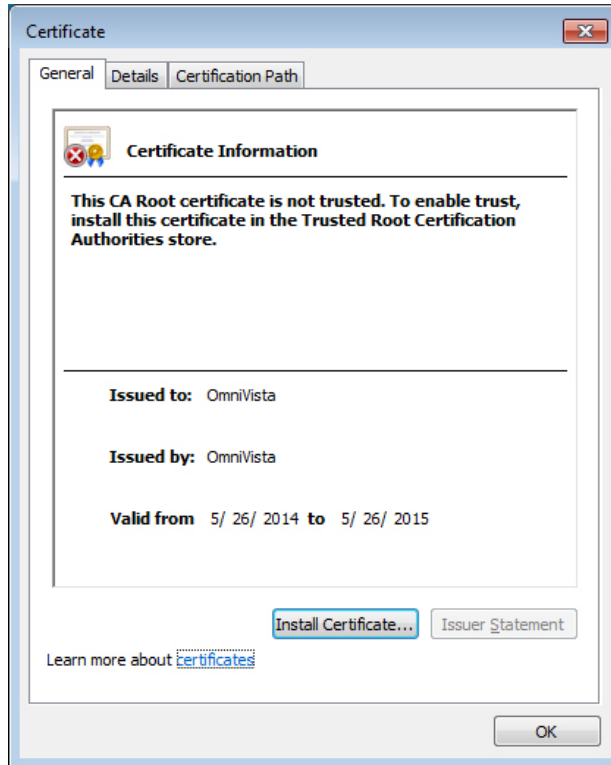


10. Click **Close** to exit.

11. Import the certificate into the Trusted Certificate Store as described [below](#).

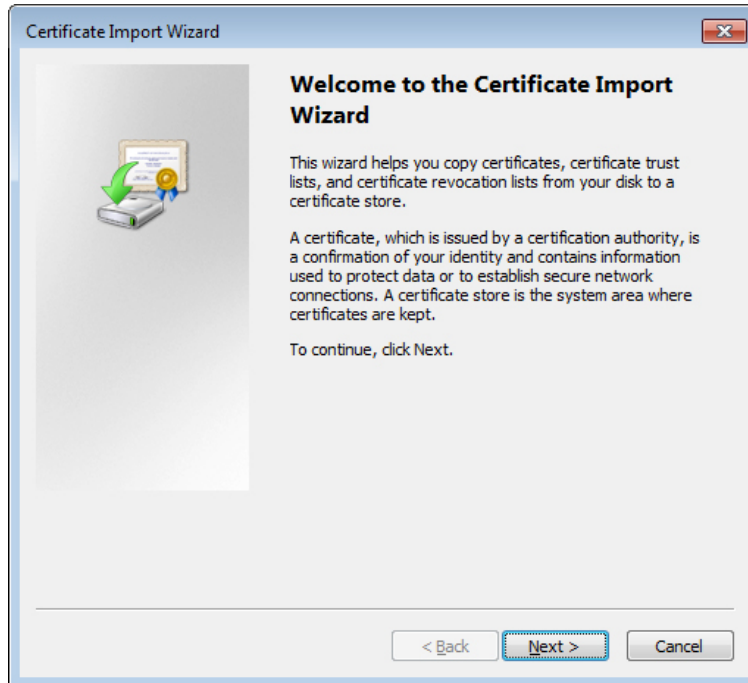
Importing the Certificate into the Trusted Certificate Store

1. Use Explorer to locate the Java Certificate file (*ov.cer*) that you downloaded in the above section, and double click on the file.
2. The certificate's General Information window appears.

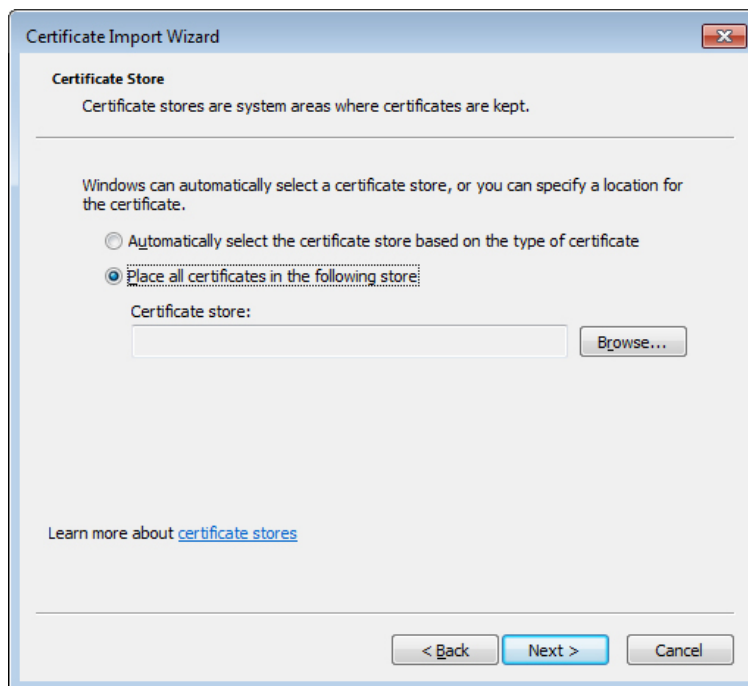


3. Click the **Install Certificate** button. The first screen of the Certificate Import Wizard appears.

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

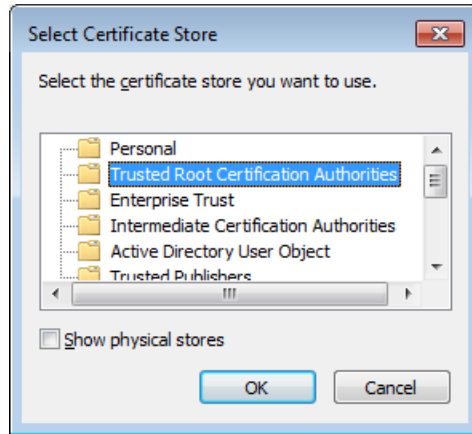


4. Click **Next**. Page 2 of the Wizard appears.

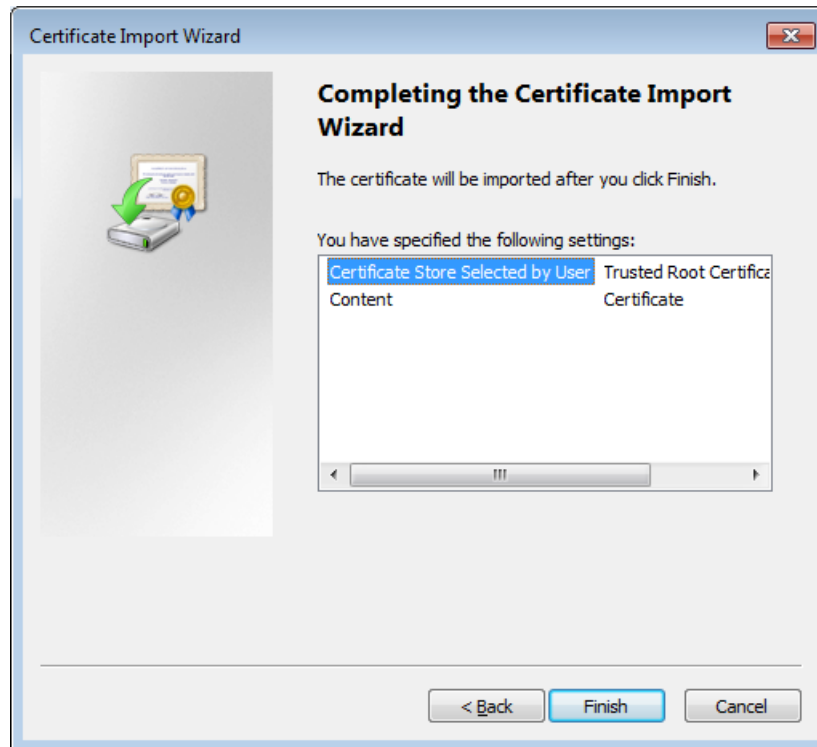


5. Select the “Place all certificates in the following store” radio button, then click **Browse**. The Select Certificate Store window appears.

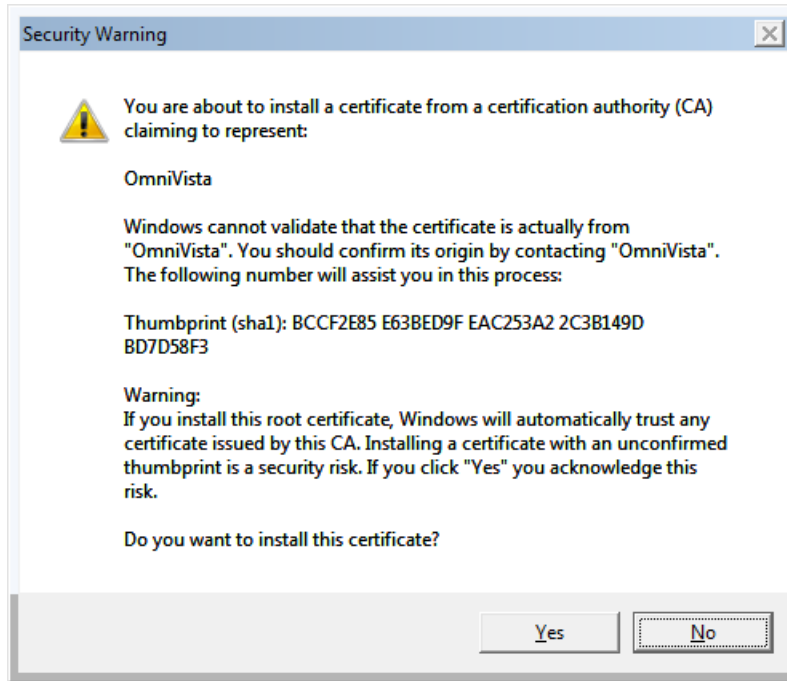
## OmniVista 2500 NMS Installation Guide (4.1.2.R03)



6. Select the **Trusted Root Certificate Authorities** Folder and click **OK**, then click **Next**. The final Wizard screen appears.



7. Click the **Finish** button. The following warning screen will appear.



8. Click **Yes**.

### ***Installing Security Certificates (Linux)***

Install the [Web Security Certificate](#) and the [Java Security Certificate](#) as described below.

#### ***Installing the Web Security Certificate (Linux)***

By default, the OmniVista 2500 NMS Installer creates a self-signed certificate for HTTPS connections. You can override this Self-Signed SSL certificate with your own, by creating a Valid Self-Signed SSL Certificate.

However, Launching OmniVista in a browser using self-signed certificates results in many security warnings. You can reduce the number of HTTPS security warnings by obtaining a valid SSL Server Certificate from a certificate authority. (e.g., VeriSign, Thawte, Geotrust, Comodo SSL). Once you create a valid self-signed certificate, or obtain one from a certificate authority, you must import the certificate using OmniVista's keystore.bat script.

**Note:** If you already own a valid SSL certificate, skip to [Importing the Certificate](#), below.

#### ***Creating a Valid Self-Signed SSL Certificate***

Self-signed certificates are useful for users who require encryption but do not need to verify the identity of a requesting website or web application (e.g., OmniVista). Follow the steps below to create a valid self-signed certificate.

**Note:** For Linux, openssl is included with the OS, so the command can be run from any location.



1. Generate a private key using OpenSSL. Options include *with password* or *without password*:

- **With Password** - Enter the following: `openssl genrsa -des3 -out server.key 2048`
- **Without Password** - Enter the following: `openssl genrsa -out server.key 2048`

2. Create a Certificate Signing Request (CSR) using Open SSL:

```
openssl req -new -key server.key -out server.csr -sha256
```

3. Follow the prompts to specify your name, organization name, location, etc.

4. Generate a self-signed certificate:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt -sha256
```

5. Once you have created the certificate, continue to [Importing the Certificate](#).

**Note:** After importing a **self-signed** certificate, you can [import the certificate into the Trusted Source Directory](#) on your system to prevent any browser certificate warnings.

### *Obtaining a Certificate from a Certificate Authority*

To obtain a certificate from a certificate authority, you must submit a Certificate Signing Request (CSR) from the provider (e.g., VeriSign, Thawte, Geotrust, Comodo SSL). To submit a CSR:

1. Generate a private key using OpenSSL. Options include *with password* or *without password* :

- **With Password** - Enter the following: `openssl genrsa -des3 -out server.key 2048`
- **Without Password** - Enter the following: `openssl genrsa -out server.key 2048`

2. Create a Certificate Signing Request (CSR) using Open SSL:

```
openssl req -new -key server.key -out server.csr
```

3. Follow the prompts to specify your name, organization name, location, etc.

4. Submit the generated CSR file to your chosen certificate authority. Refer to the Certificate Authority's website for steps and information.

5. Once you have obtained the certificate from the provider, continue to [Importing the Certificate](#).

### *Importing the Certificate*

1. Locate the OmniVista **keystore.sh** file. This file can be found in the scripts directory, located in the OmniVista 2500 NMS root directory (e.g., /opt/OmniVista\_2500\_NMS/scripts). Run it with **root** privileges.

2. At the “Please input your certificate” prompt, enter the name of the certificate file (server.csr). If necessary, enter the full directory path and name (e.g., /opt/OmniVista\_2500\_NMS/scripts/server.csr).

3. At the “Please input your private key” prompt, enter the name of the key file (server.key). If necessary, enter the full directory path and name (e.g., /opt/OmniVista\_2500\_NMS/scripts/server.key).

4. From the command line, cd to <OV\_Install\_Root>\Watchdog.

5. Stop Apache Tomcat using the Watchdog CLI:

```
watchdog-cli stopservice -n ovtomcat
```

6. Restart Apache Tomcat using the Watchdog CLI:

```
watchdog-cli startservice -n ovtomcat
```

7. Once the certificate has successfully imported, launch OmniVista 2500 NMS in a supported browser to view results.

Installing the Java Security Certificate (Linux)

When launching the OmniVista 2500 NMS Java client, especially the first time, several pop-up notices display. To streamline launch and reduce the number of pop-ups, the default OmniVista Certificate should be downloaded, imported and then stored in the Trusted Publishers certificate directory. To download, import, and store the certificate, follow the steps below.

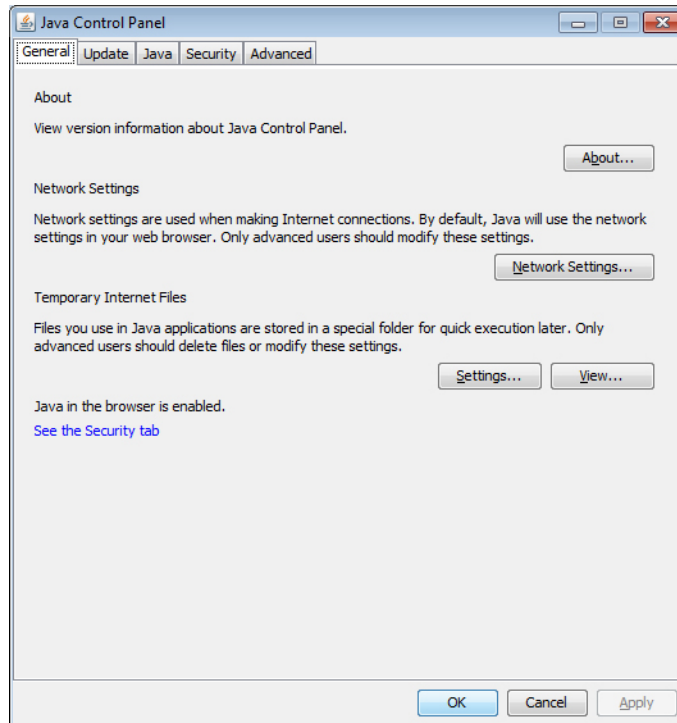
**Note:** The Certificate **must** be installed on clients running **Java 8**. The Certificate is not required on clients running Java 7; however, you will receive a number of security warnings. To streamline the launch, it is **recommended** that you install the Certificate on clients running **Java 7**.

1. Log into OmniVista 2500 NMS.

2. Download the default OmniVista certificate from the OmniVista Server. In the browser window, enter the OmniVista Server IP address and port number, followed by **/webstart/ov.cer**. For example, if your OmniVista Server IP address is 10.255.221.209, you would enter *https://10.255.221.209:8072/webstart/ov.cer*.

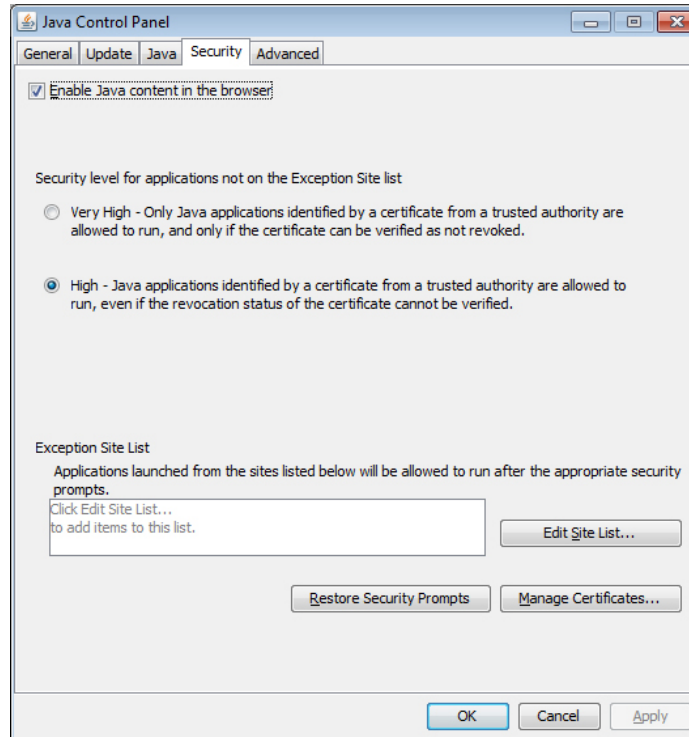
3. Press **Enter** to download the certificate.

4. Open the **Java Control Panel** - Start > Control Panel > Java.

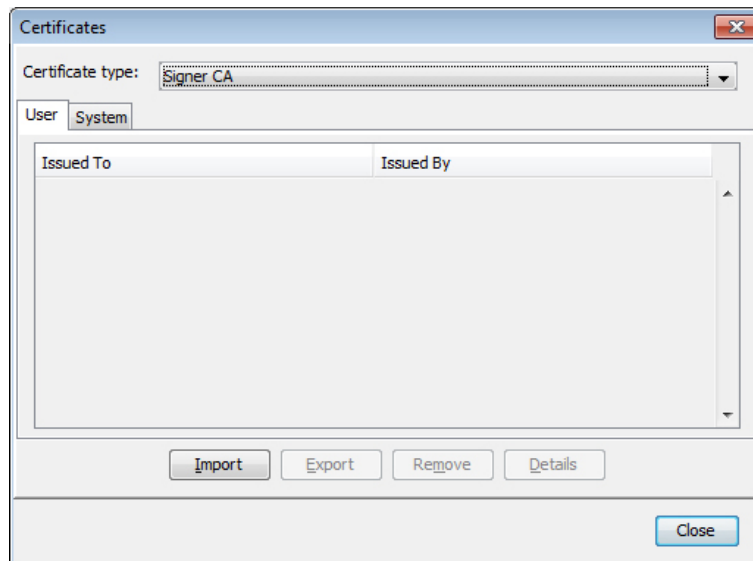


## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

5. Click on the **Security** tab.

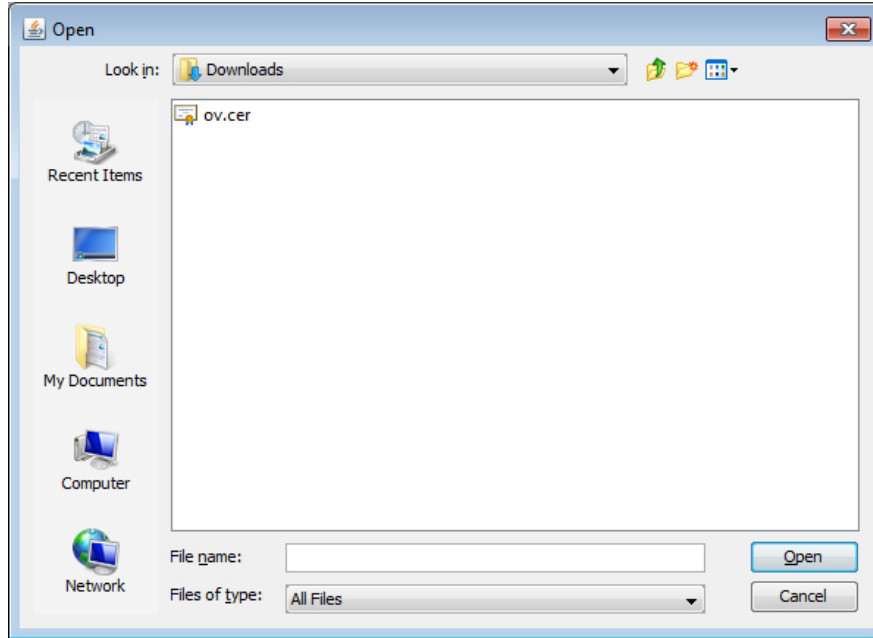


6. Click on the **Manage Certificates** button to bring up the Certificates window. *Note that the Security Tab on Java 7 clients is slightly different. However, you will still click on the **Manage Certificates** button to bring up the Certificates window.*



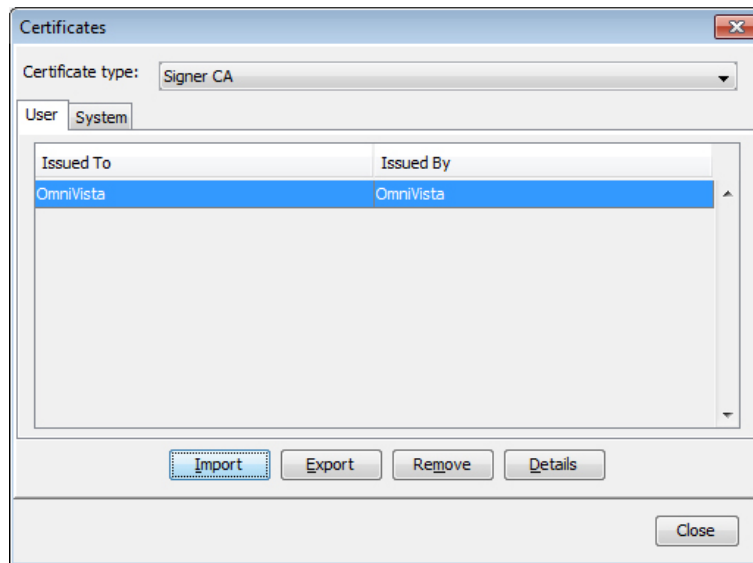
7. In the **Certificate Type** pull-down, select **Signer CA**, then click **Import**.

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)



8. Make sure the **File Type** at the bottom of the window is set to “All Files”, and locate the Certificate file you downloaded in Step 3 (ov.cer). Select the file and click **Open**.

9. You will be returned to the Certificates Screen with the OmniVista Certificate displayed in the User Certificate table, as shown below.



10. Click **Close** to exit.

11. Import the certificate into the Trusted Certificate Store as described [below](#).

### Importing the Certificate into the Trusted Source Directory

Use the “ca-certificates” package to import the Certificate (*ov.cer*) that you downloaded in the above section into the Trusted Source Directory.

- Make sure you have the “ca-certificates” package installed.

**rpm -qa | grep certificate**

- If you **do** have the package installed, **go to Step 2** in the previous section. If not, install it using the following command:

**yum install ca-certificates**

- Enable the dynamic CA configuration feature:

**update-ca-trust enable**

- Copy the file to the `/etc/pki/ca-trust/source/anchors/` Directory:

**cp ov.cer /etc/pki/ca-trust/source/anchors/**

- Extract the file:

**update-ca-trust extract**

### **Installing Web Browser Security Certificate on the OV Client**

To eliminate browser certificate warnings, download the OV Web Security Certificate from the OV Server using your current browser. Consult the documentation for the browser you are using for procedures on downloading the certificate. After downloading the certificate import it into the applicable Trusted Directory (Windows - Trusted Root Certificate Authorities Directory, Linux - Trusted Source Directory) following the same procedures used to import the *ov.cer* certificate. For Windows procedures, click [here](#). For Linux procedures, click [here](#).

### **Upgrading from a Previous Version of OmniVista 2500 NMS**

Follow the steps below to backup an existing OmniVista 2500 NMS Database and restore it to the new installation. The procedure is different depending on whether your existing installation is [3.5.7](#), [4.1.2.R01](#), or [4.1.2.R02](#).

**Note:** You cannot upgrade directly from OmniVista 4.1.1 to 4.1.2.R03. You must first upgrade from 4.1.1 to 4.1.2.R02.

#### **Upgrading from 3.5.7**

The following sections detail procedures for upgrading from OmniVista 3.5.7 to a [Windows/Linux](#) installation or to a [Virtual Appliance](#) installation.

#### **Upgrading to a Windows/Linux Installation**

Follow the steps below to upgrade from OmniVista 3.5.7 to a Windows/Linux installation. If you are upgrading to a Virtual Appliance installation, click [here](#) for procedures.

1. On the existing installation of OmniVista 2500 NMS (OmniVista 3.5.7), change “admin” user's password to “switch”.

2. On the existing installation of OmniVista 2500 NMS, open the **Server Backup** Application and perform a backup. Store the Backup File in a safe place outside of the installation server. See the Server Backup Application on-line help for more information on performing a backup.

3. [Install OmniVista 4.1.2.R03](#). Be sure to also [configure Java Settings](#) and [install the necessary security certificates](#) on any clients you will be using to access OmniVista.

**Note:** If you are installing 4.1.2.R03 **on the same server** as the existing installation, uninstall the existing installation completely and rename the existing installation folder (e.g., 'C:\Program Files\OmniVista 2500 NMS' to 'C:\Program Files\OmniVista 2500 NMS OLD'). Click [here](#) for uninstall procedures.

4. Wait for the OmniVista Server to start completely and [login to the OmniVista 2500 NMS 4.1.2.R03 Web UI](#).

5. Open the Server Backup application (**Administrator > Server Backup**). Perform a restore using the OmniVista 3.5.7 backup file you created.

**Note:** This will stop the web application server and you will lose your Web UI session. But the Server Backup UI window will remain open.

6. On the previously opened Server Backup window, perform a restore using the OmniVista 3.5.7 backup file you created. From the main Server Backup screen:

- Click on the **Restore** button to launch the Restore wizard.
- Click on the **New** button. In the **Backup Directory** field, enter the backup directory path that contains the Server Backup file to be restored, and click **OK**.
- Click on the **Next** button to move to the second page of the Restore Wizard.
- Click on the **New** button to create a Server Backup repository with the **same** Base File Name as that of the server backup file to be restored:
  - Enter the Base File name in the **Base File Name** field and click **OK**. The new Server Backup Repository will appear (pre-selected) in the Server Backup Repositories table. (If it is not selected or you de-select it, make sure to select it.)
  - Select the Server Backup file (\*.osb) that you want to use for the restore from the **Repository Files** drop-down list.
- Click on the **Restore** button to complete the restore.

**Note:** The restore may take some time, depending on the amount of data backed up. To check the status of the restore:

- Go to the <OV\_Install\_Root>\ov2500server\data\logs directory. The server.txt file displays the status of the OmniVista Server. After the restore is complete and the OmniVista Server is up, the log will display a "Services Ready!" message. You can also review the details of the restore in the backuprestore.txt file.

7. After a successful restore, start the OmniVista Client Core Service and the OmniVista Apache Tomcat Service on the OmniVista Server. The commands below can be executed from CMD in Windows or Terminal in Linux. Change to the Watchdog directory under the install directory base (chosen during Installation).

- **Windows:**

```
watchdog-cli startservice -n ovclient
```

```
watchdog-cli startservice -n ovtomcat
```

- **Linux:**

*watchdog-cli.sh startservice -n ovclient*

*watchdog-cli.sh startservice -n ovtomcat*

8. After these services startup successfully, you will be able to login to the OmniVista 2500 NMS Web UI again.

### ***Upgrading to a Virtual Appliance Installation***

Follow the steps below to upgrade from 3.5.7 to a Virtual Appliance (VA) installation.

1. On the existing installation of OmniVista 2500 NMS (OmniVista 3.5.7), change “admin” user's password to “switch”.

2. On the existing installation of OmniVista 2500 NMS, open the **Server Backup** Application and perform a backup. See the Server Backup Application On-Line Help for more information.

3. [Perform a fresh deployment](#) of OmniVista 2500 NMS 4.1.2.R03 VA.

**Note:** If you have not shutdown the 3.5.7 installation, make sure there is no IP address conflict between the 3.5.7 installation and the 4.1.2.R03 installation.

4. Use an FTP client to copy backup file generated in Step 2 above, to a fresh installation of OmniVista 2500 NMS VA.

- FTP User: admin
- FTP Password: admin
- FTP Port: 8888

**Note:** Do not change the directory after logging into the FTP session. After a successful FTP, the file will be present in the directory `/home/admin/omnivista/ng_shared/temp/admin` on the VA.

5. Login to the OmniVista 2500 NMS 4.1.2.R03 Web UI.

6. Open the Server Backup application (**Administrator > Server Backup**). Perform a restore using the OmniVista 3.5.7 backup file you created.

**Note:** This will stop the web application server and you will lose your Web UI session. But the Server Backup UI window will remain open.

7. On the previously opened Server Backup window (from Step 6), perform a restore using the OmniVista 3.5.7 backup file you FTPed to the default directory (`/home/admin/omnivista/ng_shared/temp/admin`). From the main Server Backup screen:

- Click on the **Restore** button to launch the Restore wizard.
- Click on the **New** button. In the **Backup Directory** field, enter the following path: `/home/admin/omnivista/ng_shared/temp/admin`, and click **OK**.
- Click on the **Next** button to move to the second page of the Restore Wizard.
- Click on the **New** button to create a Server Backup repository with the **same** Base File Name as that of the server backup file to be restored:
  - Enter the Base File name in the **Base File Name** field and click **OK**. The new Server Backup Repository will appear (pre-selected) in the Server Backup Repositories table. (If it is not selected or you de-select it, make sure to select it.)

- Select the Server Backup file (\*.osb) that you want to use for the restore from the **Repository Files** drop-down list.
- Click on the **Restore** button to complete the restore.

**Note:** The restore may take some time, depending on the amount of data backed up. To check the status of the restore:

- Use the “Collect Logs” option in the Virtual Appliance Menu to collect and view VA Logs. The server.txt file (located in the ov2500server\data\logs folder of the zip file) displays the status of the OmniVista Server. After the restore is complete and the OmniVista Server is up, the log will display a “Services Ready!” message. You can also review the details of the restore in the backuprestore.txt file (also located in the ov2500server\data\logs folder). Click [here](#) for more information on collecting logs for a VA.

**8.** After a successful restore, start the OmniVista Client Core Service and the OmniVista Apache Tomcat Service from the VA menu:

- Select Option **2** to run Watchdog commands.
- At the CLI prompt, enter: `startservice -n ovclient`
- Select Option **2** again to run Watchdog commands.
- At the CLI prompt, enter: `startservice -n ovtomcat`

**9.** After the OmniVista Services start up, you will be able to login to the Web UI of OmniVista 2500 NMS VA.

### Upgrading from 4.1.2.R01 Post-GA

The following sections detail procedures for upgrading from OmniVista 4.1.2.R01 Post-GA from/to a [Windows/Linux](#) installation or from/to a [Virtual Appliance](#) installation.

#### **Upgrading From/To a Windows/Linux Installation**

Follow the steps below to upgrade from OmniVista 4.1.2.R01 post-GA to 4.1.2.R03 (Windows/Linux installation). When upgrading from OmniVista 4.1.2.R01 post-GA, you basically install the new version over the previous one. If you are upgrading from/to a Virtual Appliance installation, click [here](#) for procedures.

**Note:** Before you begin the upgrade, perform a backup of the existing installation of OmniVista and FTP it to a safe place outside of this server. Detailed backup procedures are provided [below](#). Also, make a note of where the existing version of OmniVista 2500 NMS is installed (e.g., C:\Program Files\OmniVista 2500 NMS).

Install the new version in that same directory following the instructions in [Installing the OmniVista 2500 NMS Software](#) (beginning with Step 3). The installation procedures are the same, except you will accept the following warning prompts that appear when installing the upgrade.

- “Existing Data” dialog asks you to confirm if you want to migrate data, select “Yes”.
- “Overwrite Existing File” dialog prompts for confirmation before overwriting an existing file, select “Yes to All”.



- Information dialog pops-up informing you the file “mibsets.txt” will be renamed to “mibsets.txt.bak”, select “OK”.

### Upgrading From/To a Virtual Appliance Installation

Follow the steps below to upgrade from OmniVista 4.1.2.R01 GA to 4.1.2.R03 (Virtual Appliance installation).

1. Open a Console on the VM to access the Virtual Appliance Menu. Type **4** and press **Enter** to choose the **Backup/Restore OmniVista 2500 NMS** option.

```
*****
* The Virtual Appliance Menu
*****
* [1] Configure the Virtual Appliance
* [2] Run Watchdog command
* [3] Update VA
* [4] Backup/Restore OmniVista 2500 NMS
* [5] Log out
* [6] Reboot
* [0] Power off
*****
Type your option? _
```

2. Enter **1** and press **Enter** to choose **Backup OmniVista 2500 NMS** option from the Backup/Restore OmniVista 2500 NMS menu.

```
*****
* Backup/Restore OmniVista 2500 NMS
*****
* [1] Backup OmniVista 2500 NMS
* [2] Restore OmniVista 2500 NMS
* [0] Exit
*****
Type your option? _
```

3. Enter the Backup’s base name (default is “ov2500nms”), then press **Enter**. If no base name is specified, “ov2500nms” will be used as the default base name. The backup will begin.

```
*****
* Backup/Restore OmniVista 2500 NMS
*****
* [1] Backup OmniVista 2500 NMS
* [2] Restore OmniVista 2500 NMS
* [0] Exit
*****
Type your option? 1

Enter base name (default is "ov2500nms"):
Stopping services...
Backing up data...
Generating backup file...
Starting services...
Completed! (Output file: "ov2500nms_2016-01-20--16-15.bk")
```

After backup is finished, the output filename will be displayed: <base name>\_<yyyy-MM-dd--HH-mm>.bk (e.g., ov2500nms\_2016-01-20- -16-15.bk). A backup includes OV2500 data backup (.osb), MongoDB data backup (.mgb) and license data backup (.lic).

4. [Perform a fresh deployment](#) of OmniVista 2500 NMS 4.1.2.R03 VA.

5. Use an FTP client to copy the backup file generated in Step 3 above, to the fresh installation of OmniVista 2500 NMS VA.

- **FTP User:** admin
- **FTP Password:** admin
- **FTP Port:** 8888

**Note:** Do not change the directory after logging into the FTP session. After a successful FTP, the file appear in the /home/admin/omnivista/ng\_shared/temp/admin directory on the VA.

6. After the installation is complete, open a Console on the VA, and from the Virtual Appliance Menu, enter **5** and press **Enter** to choose the **Change Password** option.

```
*****
* The Virtual Appliance Menu *
*****
* [1] Configure the Virtual Appliance *
* [2] Run Watchdog command *
* [3] Update VA *
* [4] Backup/Restore OmniVista 2500 NMS *
* [5] Change Password *
* [6] Collect logs *
* [7] Power off *
* [8] Reboot *
* [0] Log out *
*****
Type your option? _
```

7. Enter **2** and press **Enter** to choose the **Change Mongo Database Password** option.

```
*****
* Change Password the Virtual Appliance *
*****
* [1] Change admin password *
* [2] Change mongo database password *
* [0] Exit menu and continue *
*****
Type your option? _
```

8. Change mongo administrator and ngnms user password as follows:

- Password of mongo administrator: **password**
- Password for ngnms app user: **dbpassword**

```
*****
Type your option?
Provide option [1 OR 2]. Option 1 for changing password of mongo administrator;
2 for ngnms application user :_
```

9. After completing the password change, go to the Virtual Appliance Menu to shutdown and start all services.

```
*****
* The Virtual Appliance Menu *
*****
* [1] Configure the Virtual Appliance *
* [2] Run Watchdog command *
* [3] Update VA *
* [4] Backup/Restore OmniVista 2500 NMS *
* [5] Change Password *
* [6] Collect logs *
* [7] Power off *
* [8] Reboot *
* [0] Log out *
*****
Type your option? _
```

10. Enter **2** and press **Enter** to choose the Run Watchdog Command option. At the prompt, enter the following commands:

- Enter *watchdog-cli shutdown* to shutdown all services. When all services have stopped, enter *watchdog-cli start* to restart all services.

11. When all services have started successfully, upload the backup file from Step 4 to the OmniVista NMS 2500 VA with FTP Client.

12. From the Virtual Appliance Menu, enter **4**, then press **Enter** to select the **Backup/Restore OmniVista 2500 NMS** option.

```
*****
* The Virtual Appliance Menu *
*****
* [1] Configure the Virtual Appliance *
* [2] Run Watchdog command *
* [3] Update VA *
* [4] Backup/Restore OmniVista 2500 NMS *
* [5] Log out *
* [6] Reboot *
* [0] Power off *
*****
Type your option? _
```

13. Enter **2** and press **Enter** to choose **Restore OmniVista 2500 NMS** option from the Backup/Restore OmniVista 2500 NMS menu.

```
*****
* Backup/Restore OmniVista 2500 NMS *
*****
* [1] Backup OmniVista 2500 NMS *
* [2] Restore OmniVista 2500 NMS *
* [0] Exit *
*****
Type your option? _
```

14. Choose a Backup File by selecting the number (e.g., 1) in the list and pressing **Enter**.

15. Press **y** at the confirmation prompt, then press **Enter**.

```
*****
* Backup/Restore OmniVista 2500 NMS
*****
* [1] Backup OmniVista 2500 NMS
* [2] Restore OmniVista 2500 NMS
* [0] Exit
*****
Type your option? 2

Backups available:
  [1] ov2500nms_2016-01-20--16-15
Choose a backup file to restore (choose 0 to exit): 1
Are you sure of restoring from
  [1] ov2500nms_2016-01-20--16-15
(y/n): y_
```

16. After completing the Restore, you will be prompted to restore license information. If you select **Yes**, the current license will be overwritten with the one from the Backup File.

After the OmniVista Services start up, you will be able to login to the Web UI of OmniVista 2500 NMS VA.

### Upgrading from 4.1.2.R02 GA

The following sections detail procedures for upgrading from OmniVista 4.1.2.R02 GA from/to a [Windows/Linux](#) installation or from/to a [Virtual Appliance](#) installation.

#### **Upgrading From/To a Windows/Linux Installation**

Follow the steps below to upgrade from OmniVista 4.1.2.R02 GA to 4.1.2.R03 (Windows/Linux installation). When upgrading from OmniVista 4.1.2.R01 post-GA, you basically install the new version over the previous one. If you are upgrading from/to a Virtual Appliance installation, click [here](#) for procedures.

**Note:** Before you begin the upgrade, perform a backup of the existing installation of OmniVista and FTP it to a safe place outside of this server. Detailed backup procedures are provided [below](#). Also, make a note of where the existing version of OmniVista 2500 NMS is installed (e.g., C:\Program Files\OmniVista 2500 NMS).

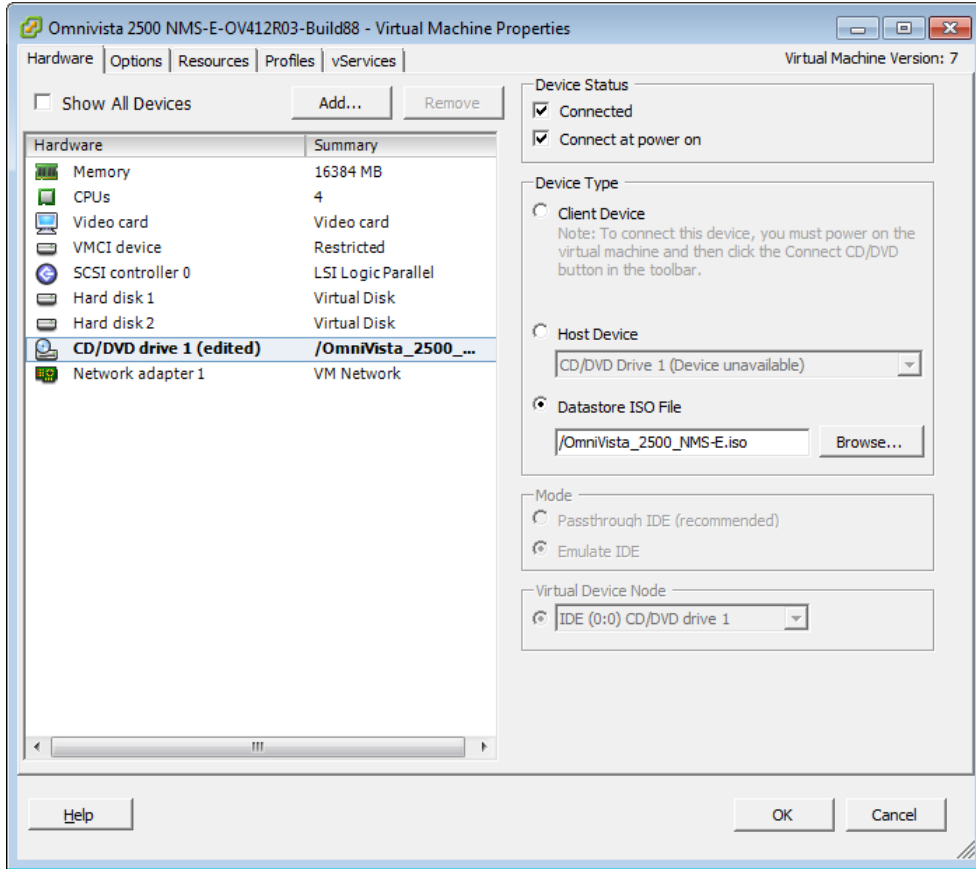
Install the new version in that same directory following the instructions in [Installing the OmniVista 2500 NMS Software](#) (beginning with Step 3). The installation procedures are the same, except you will accept the following warning prompts that appear when installing the upgrade.

- “Existing Data” dialog asks you to confirm if you want to migrate data, select “Yes”.
- “Overwrite Existing File” dialog prompts for confirmation before overwriting an existing file, select “Yes to All”.
- Information dialog pops-up informing you the file “mibsets.txt” will be renamed to “mibsets.txt.bak”, select “OK”.

### Upgrading From/To a Virtual Appliance Installation

Follow the steps below to upgrade from OmniVista 4.1.2.R02 GA to 4.1.2.R03 (Virtual Appliance installation). Before you begin the upgrade, perform a backup of the existing installation of OmniVista and FTP it to a safe place outside of this server. Click [here](#) for backup/restore procedures. After a successful restore, reboot the Virtual Appliance from console.

1. Insert the OV 4.1.2.R03 .iso file into the VM.



2. Open a Console on the VM. If necessary, enter the login/password to bring up the Virtual Appliance Menu.

```
*****
* The Virtual Appliance Menu
*****
* [1] Configure the Virtual Appliance
* [2] Run Watchdog command
* [3] Update VA
* [4] Backup/Restore OmniVista 2500 NMS
* [5] Power off
* [6] Reboot
* [7] Upgrade VA
* [8] Log out
*****
Type your option? _
```

3. Select the “Update VA” option (enter 3, then press **Enter**).

4. Select “Check current version” (enter **1**, then press **Enter**) to verify the current version.
5. Select “Check available updates” (enter **2**, then press **Enter**) to check available updates.
6. Select the “Install upgrade” option (enter **3**, then press **Enter**) to initiate the upgrade.
7. Type **latest** and press **Enter**.
8. When the process is complete, the “Update VA” Menu will appear.
9. Select the “Exit” option (enter **0** and press **Enter**) to exit to the Main Menu.
10. Select the “Reboot” option (enter **6** and press **Enter**) to finalize the upgrade.

### Backup/Restore Procedures (Windows/Linux)

Follow the steps below to [backup/restore](#) restore OmniVista 2500 NMS on Windows/Linux installations.

#### *Backup*

Go to the scripts directory of the OmniVista 2500 NMS installation folder and execute “backup-ngnms.bat” (for Windows) or “backup-ngnms.sh” (for Linux). **You must run it with Administrator privilege.** You can perform an [immediate](#) backup or [schedule](#) a repeating backup for a later time.

#### *Immediate Backup*

1. To perform an immediate backup, enter **n**, then press **Enter** at the "Schedule" prompt.
2. Enter the path of the Backup Directory (default is “C:\backup” on Windows and “/root/Desktop/defaultbackupdir” on Linux), then press **Enter**.
3. Enter the Backup’s base name (default is “ov2500nms”), then press **Enter**.

A “Stopping services” message will appear as the services are automatically stopped. This may take some time to complete. When the services have been stopped, the backup will start. When the process is complete, a confirmation message will appear and the backup file will be stored in the configured backup directory under the name: <base name>\_<yyyy-MM-dd--HH-mm>.bk.

```
[root@localhost scripts]# ./backup-ngnms.sh
Would you like to schedule the backup? (y/n)[n]:
Enter full name of the folder to store the backup file (default is /root/Desktop/defaultbackupdir):
Enter base name for the backup file (default is ov2500nms):
Watchdog is running. So, Omnivista 2500 NMS services will have to be stopped before backup.
Start backup
Stopping services. Please wait as this will take a while...
Backing up OV2500 data. Please wait as this will take a while...
Backing up the Database. Please wait as this will take a while...
Backing up License data
Backing up openstack data directory.
Backing up captiveportal data directory.
Backing up afn data directory.
Backing up report data directory.
Backing up Locator data directory
Archiving the backup files
Starting Services. Please wait as this will take a while...
Complete. Backup file ov2500nms-2015-12-01--17-40.bk is stored in /root/Desktop/defaultbackupdir
[root@localhost scripts]# █
```

**Note:** Old Backup Files are not automatically purged. Monitor and maintain the Backup Directory to optimize disk space.

### *Scheduled Backup*

1. To schedule a repeating backup for a later time, enter **y**, then press **Enter** at the "Schedule" prompt.
2. Enter the path of the Backup Directory (default is "C:\backup" on Windows and "/root/Desktop/defaultbackupdir" on Linux), then press **Enter**.
4. Enter the Backup's base name (default is "ov2500nms"), then press **Enter**.
5. Enter a start time for the backup in HH:MM format (e.g., 22:00), then press **Enter**.
6. Enter the time between scheduled backups, in days (e.g., 5), then press **Enter**. A confirmation message will appear.

```
[root@localhost scripts]# ./backup-ngnms.sh
Would you like to schedule the backup? (y/n)[n]: y
Enter full name of the folder to store the backup file (default is /root/Desktop/defaultbackupdir):
Enter base name for the backup file (default is ov2500nms):
Enter start time (format is HH:mm; default is 10:40): 11:00
Enter the time between backups (default is 1 day): 5
00 11 * /5 * * /opt/OmniVista_2500_NMS/scripts/backup-task.sh "/root/Desktop/defaultbackupdir" "ov2500nms"
The backup has been scheduled.
[root@localhost scripts]# █
```

**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:** Old Backup Files are not automatically purged. Monitor and maintain the Backup Directory to optimize disk space.

### Restore

Go to the scripts directory of the OmniVista 2500 NMS installation folder and execute "restore-ngnms.bat" (for Windows) or "restore-ngnms.sh" (for Linux).

**Note:** The default Mongo DB password was changed in OmniVista 4.1.2.R03. If you are restoring from a previous version of OmniVista, you must change the Mongo DB password to the previous password. If you are restoring from 4.1.3.R03 or later, press **Enter** at the warning prompt.

1. At the prompt, input the path of the Backup Directory (default is "C:\backup" on Windows, and "/root/Desktop/defaultbackupdir" on Linux), then press **Enter**. If there are no backups in the directory, the process will be stopped. Otherwise, a list of backup files is displayed.
2. Choose a Backup File by selecting the number (e.g., 3) in the list and pressing **Enter**.
3. Press **y** at the confirmation prompt, then press **Enter**.

A "Stopping services" message will appear as the services are automatically stopped. This may take some time to complete. When the services have been stopped, the restore will start. When the process is complete, you will be prompted to restore license information. If you select Yes, the current license will be overwritten with the one from the Backup File.

4. Press **Enter** to exit. An overview of the process is shown in the screen below.

```

C:\WINDOWS\System32\cmd.exe
WARNING: Please change mongo password to similar with mongo password of backup file before restore
Press enter to continue or Ctrl-C to quit the script now
Matchdog is running. So, Omnivista 2500 NMS services will have to be stopped before restore.
Press enter to continue or Ctrl-C to quit the script now
Enter full name of the folder to store the backup file (default is "C:\backup"):
C:\backup\december2015
Backups available:
[1] ov2500nms-2015-12-01--17-05
[2] ov2500nms-2015-12-01--18-33
[3] ov2500nms-2015-12-01--18-47
Choose a backup file to restore (choose 0 to exit): 3
Are you sure of restoring from [3] ov2500nms-2015-12-01--18-47 (y/n): y
Extracting the backup file
Stopping services. Please wait as this will take a while...
-

```

## Uninstalling OmniVista 2500 NMS

### General Concepts for Uninstalling on Any Platform

When you uninstall OmniVista 2500 NMS, the directory where you installed OmniVista is not removed. For example, on Windows the default installation directory is: C:\Program Files\OmniVista 2500 NMS. If you wish to completely uninstall OmniVista 2500 NMS and delete **all** data and files pertaining to it, delete this directory manually **after** the uninstall.

**Important Note:** When performing an uninstall, you **must** delete your old data and configuration files. When you get to the “Delete Data and Configuration Files” Screen in the Uninstall Wizard, select **Yes** (No is selected by default).

### Uninstalling on Windows

To uninstall OmniVista 2500 NMS on a Windows platform.

Select Start > Control Panel > Programs and Features, select OmniVista 2500 NMS from the list of programs and select **Uninstall**.

### Uninstalling on Linux

At the command prompt, change to the installation directory, then enter: ./Uninstall\_OmniVista.

**Note:** The uninstall process is GUI based so be sure the GUI can be launched from where the installation is attempted. (This might require starting up X-server on the Linux server and/or exporting the display appropriately.)



## Deploying OmniVista 2500 NMS as a Virtual Appliance

OmniVista 2500 NMS Virtual Appliance can be deployed on the following supported platforms:

- VMware ESXi 5.1 and 5.5
- VMware Player 4.0 and above
- VMware vCenter Server 5.0 and above

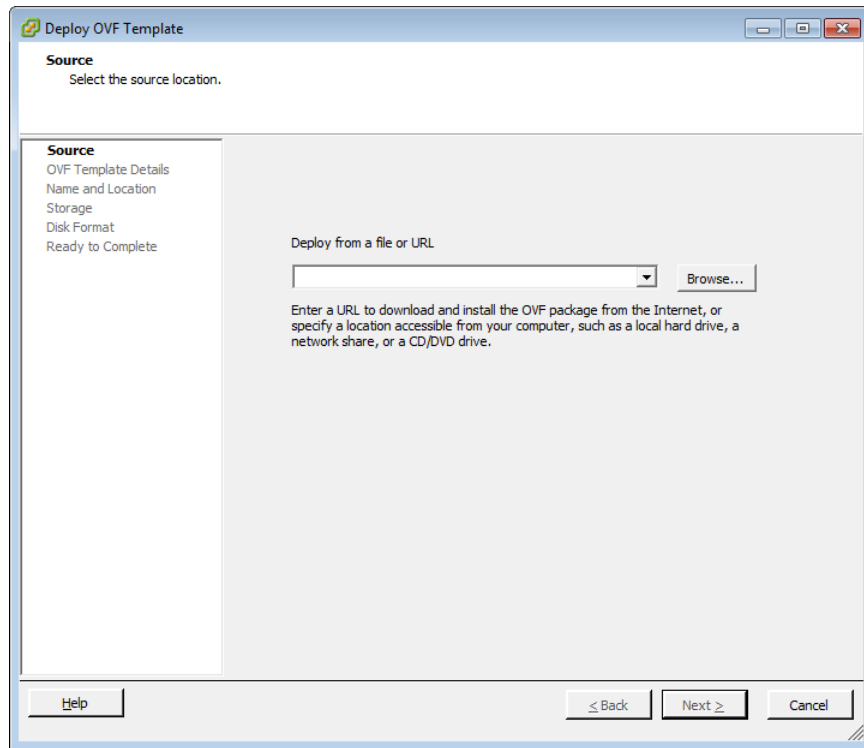
The sections below detail each of the steps required to deploy OmniVista 2500 NMS as Virtual Appliance.

**Important Note:** The default provisioned size of the hard disk is 256GB. This will support managing up to 500 devices. If you are managing more than 500 devices, it is recommended that you increase the size of the provisioned hard disk after deploying OmniVista. (See the *OmniVista 4.1.2.R03 Release Notes* for recommended disk configurations). [See Appendix A – Extending the VA Partition Size](#) for detailed procedures on increasing the provisioned hard disk size using the GParted utility.

### Deploying the Virtual Appliance

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

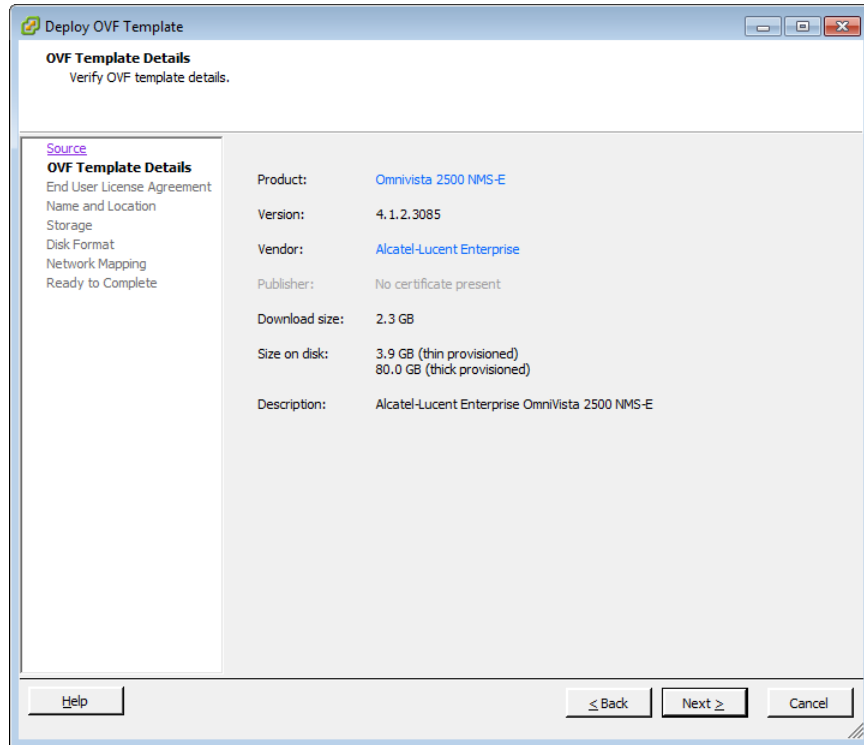
1. Download and unzip the OVF package.
2. Log into vCenter and open the vSphere client.
3. Select the Host on which you want to install OmniVista, click on **File - Deploy OVF Template**. The Deploy OVF Template Wizard appears.



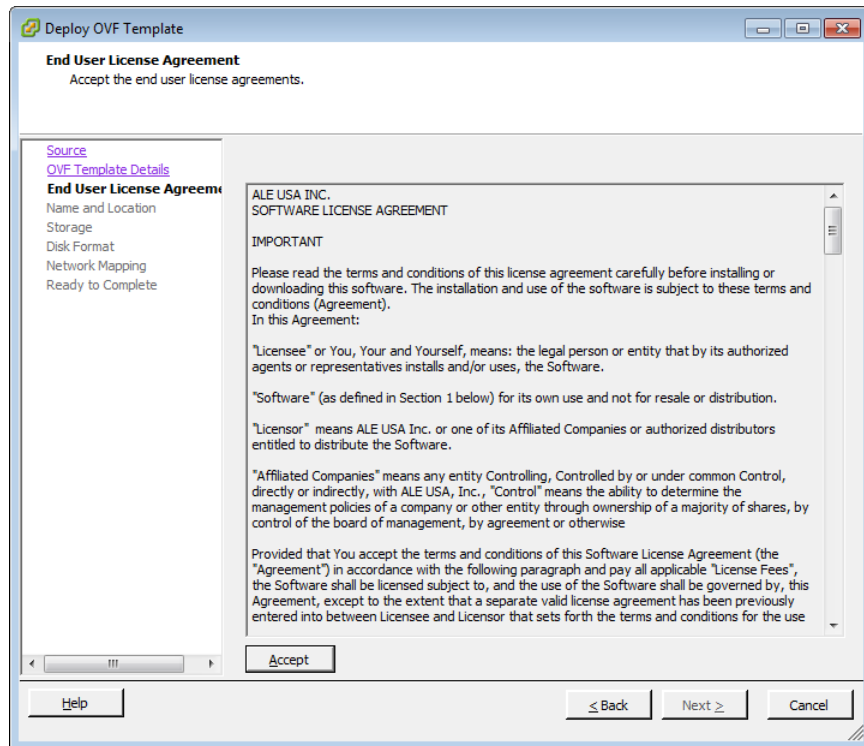
4. Click on the **Browse** button and locate the OmniVista 2500 NMS Application file in the unzipped OVF folder (e.g., ov412R03\_64bit\_OVF10build85.ovf).

## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

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.

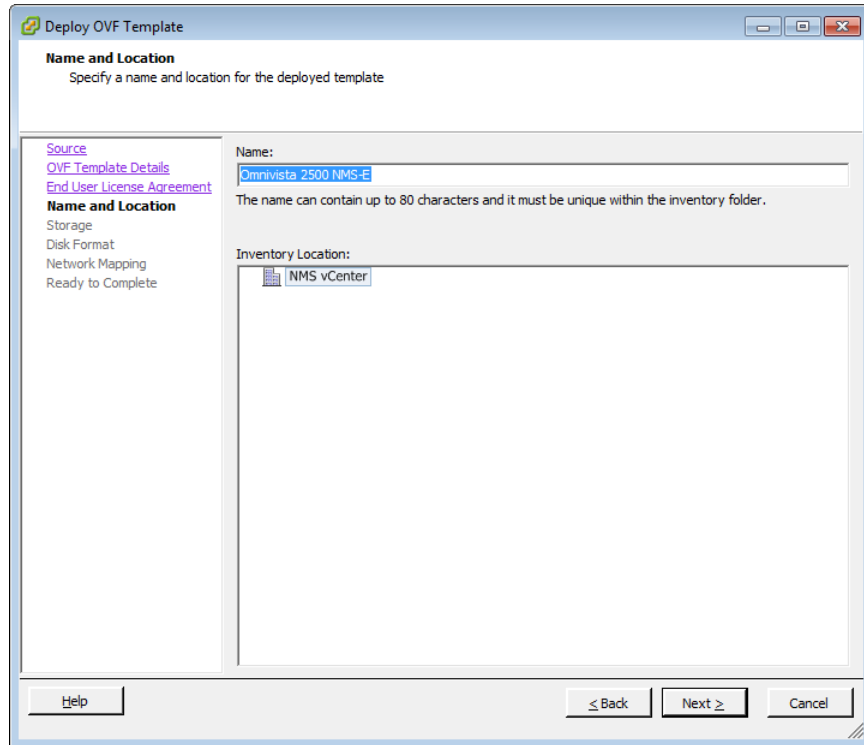


6. Review the OVF details and click **Next**. The End User License Agreement Screen appears.

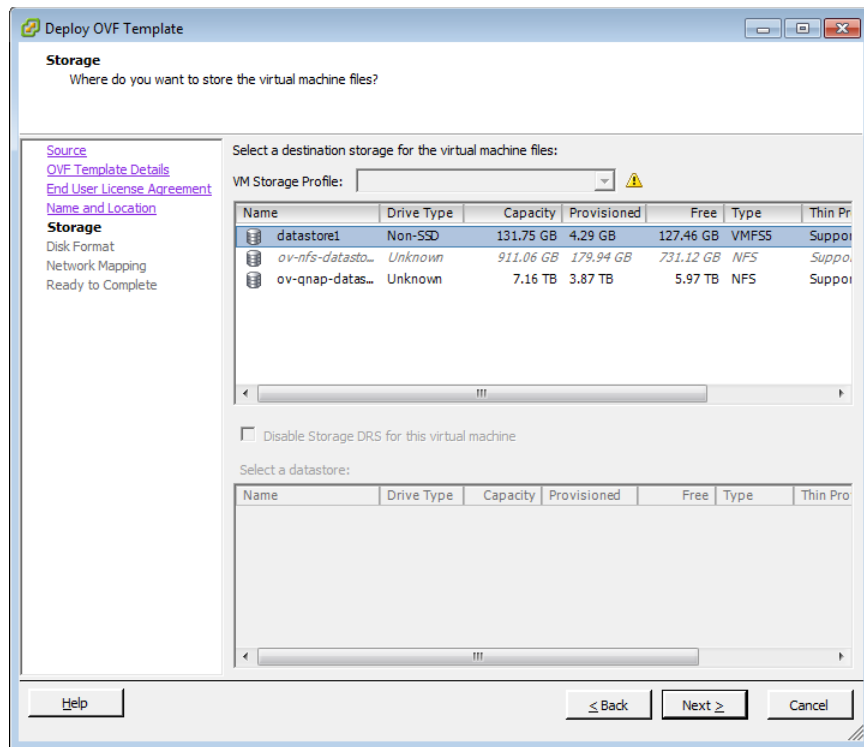


## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

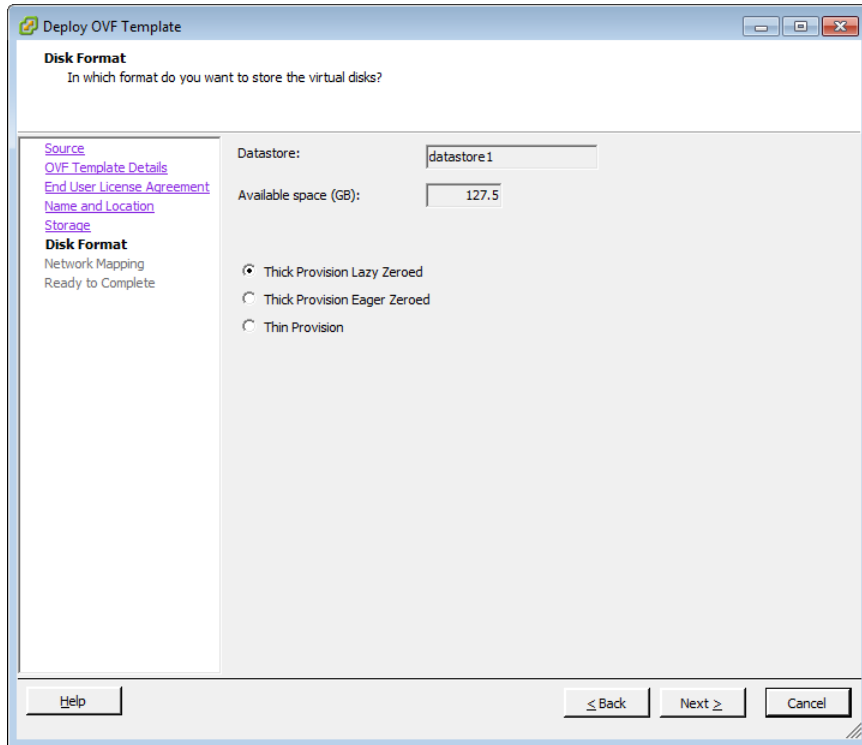
7. Review the License Agreement, click **Accept**, then click **Next**. The Name and Location Screen appears.



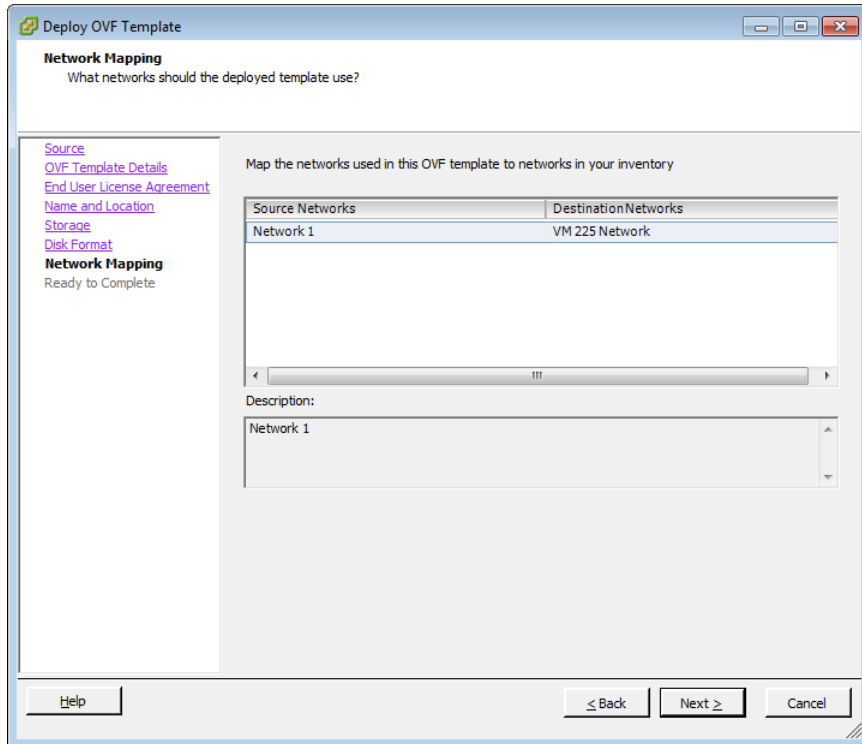
8. Specify a Name and Inventory Location for the deployed template, then click **Next**. The Storage Screen appears.



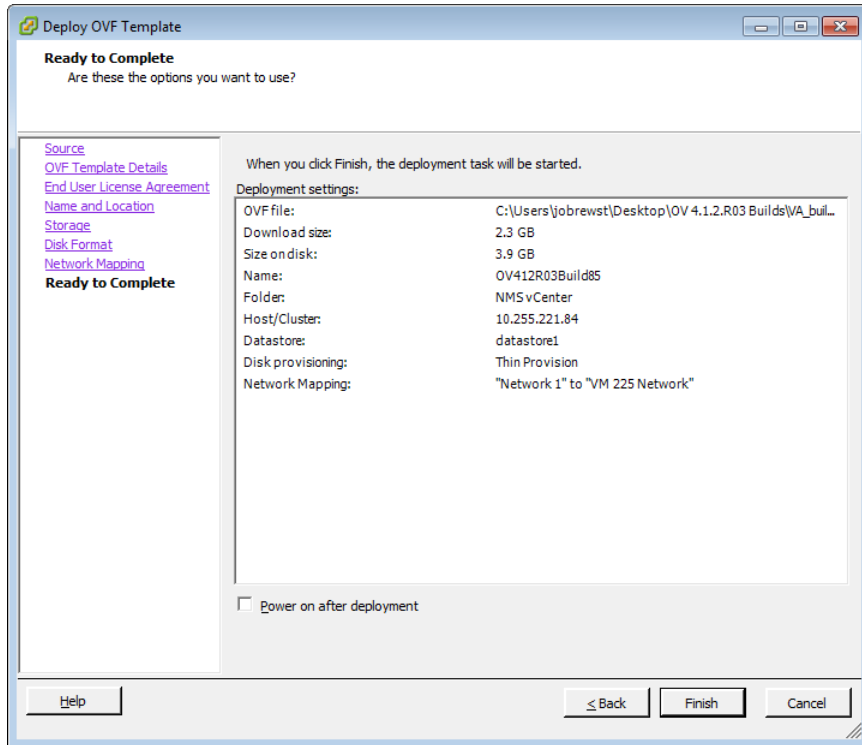
9. Select the host or cluster where the template is to be deployed, then click **Next**. The Disk Format Screen appears.



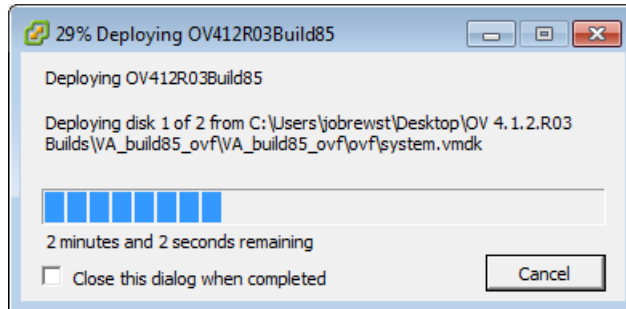
10. Select **Thin Provision**, then click **Next**. The Network Mapping Screen appears.



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**. 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**.

## Launching the Console and Setting a Password

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 admin user...
=====
Changing password for user admin.
New password:
    
```

2. Specify a new administrative password, then re-enter to confirm the new password. The Configure the Virtual Appliance Main Menu is displayed.

**Note:** The password should be an alpha-numeric string with a minimum of eight (8) characters and should not be based on dictionary words. 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 the Virtual Appliance  *
*****
* [1] Display current configuration  *
* [2] Configure OmniVista 2500 NMS  *
* [3] Configure Default Gateway     *
* [4] Configure Hostname            *
* [5] Configure DNS Server          *
* [6] Configure Proxy Server        *
* [7] Configure Timezone            *
* [8] Configure Route               *
* [9] Configure Keyboard Layout     *
* [0] Exit menu and continue        *
*****
Type your option? _
    
```

3. Enter 1 and press **Enter** to display the current configuration.

```

*****
* Product Name: OmniVista 2500 NMS-E *
* Revision: 4.1.2.R03                *
* Build Number: 85                   *
*                                     *
* IPv4 Address: 10.255.225.243        *
* NetMask: 255.255.255.0              *
*                                     *
* HTTP Port: 8071                    *
* HTTPS Port: 8072                   *
* Data Port: 1127                    *
*                                     *
* Default gateway v4: 10.255.225.254 *
*                                     *
* Hostname: omnivista                 *
*                                     *
* DNS Server 1: 192.168.1.3          *
*                                     *
* Timezone: America/Los_Angeles     *
*                                     *
*****
Press Enter to continue. . .
    
```

4. Press **Enter**. The Virtual Appliance Main Menu is displayed.

### Configuring OmniVista 2500 NMS

1. At the Main Menu, enter **2** and press **Enter** to configure OmniVista 2500 NMS. Configuring the OmniVista 2500 NMS provides options for two (2) system settings:

- Configuring the System IP
- Configuring the System Port

2. Enter **y** at the "Configure system IP" prompt.

3. Enter an IPv4 address. (Press **Enter** to accept the default value.)

4. Enter the IPv4 network mask. (Press **Enter** to accept the default value.)

5. An IPv6 address is optional. To configure an IPv6 address, enter **y** at the "Do you want to use IPv6?" prompt. (If no IPv6 is being configured, go to Step 7).

6. Enter an IPv6 address and a prefix value. (Valid prefix range: 0 to 128.)

**Note:** New port values must be unique (i.e., they must differ from any previously-configured ports). If an error occurs, settings will revert to default values.

```
=====
Configure the OmniVista 2500 NMS...
=====
Would you like to configure system IP (y/n) [n]: y
Please input IPv4 [10.255.225.243]:
Please input Netmask [255.255.255.0]:
Do you want to use IPv6 (y/n) [y]: n

Are you sure to set:
  IPv4: 10.255.225.243
  Netmask: 255.255.255.0
  Don't use IPv6
(y/n): _
```

7. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to bring up the System Port prompt.

```
Would you like to configure system Port (y/n) [n]: y
Please input HTTP port [8071]: _
```

8. At the prompt, enter **y** and press **Enter**. Configure a system port by entering **HTTP**, **HTTPS** and **Data Port** values.

- HTTP Port (Valid range: 1024 to 65535)
- HTTPS Port (Valid range: 1024 to 65535)
- Data Port (Valid range: 1024 to 65535)

**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).

9. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to access the Main Menu.

## Configuring the Default Gateway

1. At the Main Menu, enter **3** and press **Enter** to configure default gateway settings.
2. Enter an IPv4 default gateway.
3. If an IPv6 address was configured at the previous steps, enter an IPv6 gateway address. Otherwise, go to Step 4.

```

=====
Configure the Default Gateway...
=====
Please input IPv4 Default Gateway [10.255.225.254]:

Are you sure to set:
    Default Gateway v4: 10.255.225.254
(y/n): y
The configuration has been set
Press Enter to continue
    
```

**Note:** You can press **Enter** to keep default values. If an error occurs, settings will revert to default values.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to access the Main Menu.

## Configuring the Hostname

1. At the Main Menu prompt, enter **4** and press **Enter** to configure the hostname.
2. Enter a hostname.

```

=====
Configuring Hostname...
=====
Please enter a hostname [omnivista]:

Are you sure to set:
    Hostname: omnivista
(y/n): _
    
```

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to access the Main Menu.

## Specifying a DNS Server

1. At the Main Menu prompt, enter Option **5** 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. (Press **Enter** to accept the default values.)

```

=====
Configuring DNS Server...
=====

Are you sure to use a DNS Server? (y/n): y
Please input DNS Server 1 [192.168.1.3]:
Please input DNS Server 2 [ignore]:

Are you sure to set:
    DNS Server 1: 192.168.1.3
    DNS Server 2: ignore
(y/n): _
    
```



**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 access the Main Menu.

### Specifying a Proxy Server

1. At the Main Menu prompt, enter Option **6**, to specify whether the VM will use a Proxy Server.
2. If the VM will use a proxy server, enter the Proxy Server, along with the port (e.g., proxy\_serv.com:8080).

```
=====  
Configuring Proxy Server...  
=====  
Are you sure to use a Proxy Server to reach the Internet? (y/n): y  
Please enter Proxy Server (http:// will be auto prepended): tma.com.vn  
Please enter port: 8080  
  
Are you sure to set:  
    Proxy Server: http://tma.com.vn:8080  
(y/n): _
```

**Note:** If **n** (No) is selected, all proxy servers will be disabled. The prefix “http://” will prepend automatically.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to access the Main Menu.

### Setting the Time Zone

1. At the Main Menu prompt, enter Option **7** 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**).

```
=====  
Configuring Timezone...  
=====  
Are you sure to set Timezone of system? (y/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**).

```

#? 10
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).

```

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
#? 21
Are you sure to set TZ=America/Los_Angeles (y/n): _

```

5. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to access the Main Menu.

### Configuring a Route

1. At the Main Menu prompt, enter **8** and press **Enter** to begin configuring a route.
2. Configure an IPv4 route by entering **1** at the command prompt.

```

*****
* Configure Route *
*****
* [1] Add Route v4 *
* [2] Add Route v6 *
* [3] Del Route v4 *
* [4] Del Route v6 *
* [0] Exit *
*****
Type your option? _

```

3. Enter the subnet, netmask and gateway.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure Route menu. (To exit, select option 0.)

```

*****
* Configure Route
*****
* [1] Add Route v4
* [2] Add Route v6
* [3] Del Route v4
* [4] Del Route v6
* [0] Exit
*****
Type your option? _
    
```

5. Configure an IPv6 route (optional) by selecting Option 2 from the Configure Route Menu.
6. Enter the subnet, prefix and gateway for the IPv6 route. (The valid prefix range is 0 to 128.)

```

Please input Subnet: 1::1
Please input Prefix: 64
Please input Gateway: 2001::2

Are you sure to set:
    Route v6: 1::1/64 via 2001::2
(y/n): _
    
```

7. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure Route Menu.
8. Enter **0** and press **Enter** to access to the Main Menu.

### Configuring the Keyboard Layout

1. At the Main Menu prompt, enter **9** and press **Enter** to specify the keyboard layout.
2. Enter a keyboard language (e.g., us).
3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to access the Main Menu.

```

=====
Configuring Keyboard Layout...
=====
Please input Keyboard Layout: us

Are you sure to set:
    Keyboard Layout: us
(y/n): _
    
```

The table below lists all supported keyboard layouts.

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

### OmniVista 2500 NMS Installation Guide (4.1.2.R03)

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

## Review/Accept License Agreement

1. At the Main Menu prompt, enter **0** and press **Enter** to exit. The OmniVista License Agreement will display. All users are required to have a valid Core License and must accept the Alcatel-Lucent Enterprise end user license agreement (EULA). (VMM and Application Visibility licenses are optional).

```
17. Notices. If Licensee has any questions concerning this product or would like
to otherwise contact ALE USA Inc., please write to:
ALE USA Inc., 26801 West Agoura Road, Calabasas, CA 91301
ATTN: Sales.

Copyright 2015 ALE USA Inc.

Accept End user licensing agreement (y/n): _
```

2. Scroll through the License Agreement to review. At the end of the agreement, enter **y** and press **Enter** to accept the agreement.

3. Configure an optional proxy for ProActive Lifecycle Management. The ProActive Lifecycle Management Feature periodically gathers detailed information for all discovered devices on your network and periodically uploads the information to the ProActive Lifecycle Management Web Portal. The information is also available to you through a widget that can be displayed on the OmniVista 2500 NMS Dashboard for easy reference.

If you choose not to enable the ProActive Lifecycle Management Feature at installation, you can enable it at a later time in the Preferences Application. And if you enable it at install, you can disable it at a later time in the Preferences Application.

To enable a Proxy for the ProActive Lifecycle Management feature, enter **y** and press **Enter** at the command prompt. Otherwise, enter **n** to bypass Proxy configuration. If configuring a Proxy, enter the host name, port, user name and password.

## Configuring OmniVista 2500 Memory

1. When configuring memory settings, begin by selecting the number of devices OmniVista 2500 NMS 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)

```

=====
Configuring OV2500 memory...
=====
Number of devices
  [1] Low (lower than 500)
  [2] Medium (500-2000)
  [3] High (2000-5000)
Please choose one: 1

OmniVista 2500 Core Service Memory (Recommended range: 4096MB - 8092MB): 9000
The memory setting specified for OmniVista 2500 Core Service is out of the recom
mended range, do you want to continue? (y/n): y
The total physical memory on the system is less than the memory of OmniVista 250
0 Core Service, do you want to continue? (y/n): y
OmniVista 2500 Client Core Service Memory (Recommended range: 2048MB - 4096MB):
3000

Are you sure to set:
  OmniVista 2500 Core Service Memory: 9000MB
  OmniVista 2500 Client Core Service Memory: 3000MB
(y/n): y_

```

2. Set the Core Service Memory value. The recommended range is 4098MB to 8092MB. Users will be prompted to confirm the memory specified.


**Note:** If the memory is out of the recommended range, a warning displays. In addition, if the system's total physical memory is less than the amount specified, a warning displays. When a warning message is served, a "Continue?" prompt displays. Enter **y** to continue or **n** to enter a new memory value.

3. Set the Client Core Service Memory value. The recommended range is 2048MB to 4096MB.

4. Confirm the memory specified for both the Core and Client Core Service Memory. Enter **y** to accept the values or **n** to enter new memory values.

After configuring the OmniVista Memory, you can [launch OmniVista](#).

### Shutting Down OmniVista

You can shut down OmniVista using the Watchdog Screen in the GUI, or using CLI commands. To shut down OmniVista using the GUI, go to Administrator - Control Panel – Watchdog and click on the Shutdown icon  at the top of the screen. This will shutdown all services (including the Watchdog Service) and the OmniVista Server. To shutdown OmniVista using CLI commands, open a Console on the VM to access the Virtual Appliance Menu and select the Run Watchdog Command option. Enter the following command: *watchdog-cli shutdown*.

**Important Note:** You **must** shutdown OmniVista **before** powering down the VM.

## 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.

```
CentOS release 6.6 (Final)
Kernel 2.6.32-504.el6.x86_64 on an x86_64

Product Name: OmniVista 2500 NMS-E
Revision: 4.1.2.R03
omnivista login: _
```

1. Enter the login (admin) 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] Configure the Virtual Appliance *
* [2] Run Watchdog command *
* [3] Update VA *
* [4] Backup/Restore OmniVista 2500 NMS *
* [5] Change Password *
* [6] Collect logs *
* [7] Power off *
* [8] Reboot *
* [0] Log out *
*****
Type your option? _
```

The Virtual Appliance Menu provides the following options:

- [1: Configure the Virtual Appliance](#)
- [2: Run Watchdog CLI command](#)
- [3: Update VA](#)
- [4: Backup/Restore OmniVista 2500 NMS](#)
- [5: Change Password](#)
- [6: Collect Logs](#)
- [7: Power Off](#)
- [8: Reboot](#)
- [0: Log out](#)

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

## Configuring the Virtual Appliance

The “Configure the Virtual Appliance” selection displays the selections described in the previous sections, with the addition of several options described below. For menu options 1 through 8, refer to the sections above.

```

*****
* Configure the Virtual Appliance *
*****
* [1] Display current configuration *
* [2] Configure OmniVista 2500 NMS *
* [3] Configure Default Gateway *
* [4] Configure Hostname *
* [5] Configure DNS Server *
* [6] Configure Proxy Server *
* [7] Configure Timezone *
* [8] Configure Route *
* [9] Configure Swap file *
* [10] Configure Keyboard Layout *
* [11] Update SSL Certificate *
* [0] Exit *
*****
Type your option? _
    
```

### Configure Swap File

1. At the Main Menu prompt, enter Option **9** and press **Enter**.

```

*****
* Configure Swap File *
*****
* [1] Add Swap file *
* [2] Delete Swap file *
* [0] Exit *
*****
Type your option? _
    
```

2. Enter the swap file size. Enter **y** and press **Enter** at the confirmation prompt.

### Updating the SSL Certificate

To update the SSL Certificate, you must first generate a \*.crt and \*.key file and upload the files to the /home/admin/omnivista/ng\_shared/temp/admin/keys directory.

1. At the Main Menu prompt, enter Option **11** 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): _
    
```



## Running Watchdog CLI Command

The Watchdog command set is used to start and stop managed services used by OmniVista 2500. To access the Watchdog CLI Command Menu, enter **2** at the command prompt. The following prompt displays:

“Please type Watchdog command options and press <Enter>:”

The command prefix is “watchdog-cli.” To display a list of available commands, enter “?” or “Help” at the prompt. Command options include:

- status
- startservice
- stopservice
- shutdown
- help
- ?
- startall
- stopall

For detailed information on using individual commands, use the following syntax: `watchdog-cli help -c <command>`. For example: `watchdog-cli help -c stopall`

**Note:** Watchdog CLI command prompt allows one watchdog-related command entry at a time. Following command entry, users must re-enter option **2** at the VA menu to access “Run Watchdog command.”

## Updating the Virtual Appliance

To view information about the current version of the OmniVista VA, and to update the OmniVista VM, enter **3** at the command prompt. Menu options include:

- Option 1: Check current version of VA
- Option 2: Check available updates
- Option 3: Install update.
- Option 0: Exit menu

```
Type your option? 3
*****
* Update VA *
*****
* [1] Check current version *
* [2] Check available updates *
* [3] Install update *
* [0] Exit *
*****
Type your option? _
```

1. Enter "1" to check current version:

```
Type your option? 1

Current version of Virtual Appliance:
Version - Build 72
Description - Enterprise OmniVista 2500 NMS
```

2. Enter "2" to check available updates:

```
Type your option? 2

Available updates of Virtual Appliance:

Checking for available updates, this process can take a few minutes.....
Available Updates -
  Build 73
```

3. If the latest update is available, enter "3" to install the latest version:

```
Type your option? 3

Please type version to update and press <Enter>:
latest
Installing version - Build 73
....._
```

4. After successful message is displayed, wait until all services are started. Then we can login to OmniVista 2500 NMS Web UI.

## Backing Up or Restoring OmniVista 2500 NMS

The sections below detail the [backup/restore](#) steps for virtual appliance installations. Open a Console on the VM to access the Virtual Appliance Menu. Type **4** and press **Enter** to choose the **Backup/Restore OmniVista 2500 NMS** option.

```
*****
* The Virtual Appliance Menu *
*****
* [1] Configure the Virtual Appliance *
* [2] Run Watchdog command *
* [3] Update UA *
* [4] Backup/Restore OmniVista 2500 NMS *
* [5] Change Password *
* [6] Collect logs *
* [7] Power off *
* [8] Reboot *
* [0] Log out *
*****
Type your option? _
```

You can access the Virtual Appliance for sending/receiving backup files via FTP:

- **FTP User:** admin
- **FTP Password:** admin
- **FTP Port:** 8888

## Backup

You can perform an [immediate](#) backup or [schedule](#) a repeating backup for a later time.

### Immediate Backup

1. Enter **1** and press **Enter** to choose **Backup OmniVista 2500 NMS** option from the Backup/Restore OmniVista 2500 NMS menu.

```
*****
* Backup/Restore OmniVista 2500 NMS *
*****
* [1] Backup OmniVista 2500 NMS *
* [2] Restore OmniVista 2500 NMS *
* [0] Exit *
*****
Type your option? _
```

2. Enter the Backup's base name (default is "ov2500nms"), then press **Enter**.

3. To perform an immediate backup, enter **n**, then press **Enter** at the "Schedule" prompt.

```
*****
* Backup/Restore OmniVista 2500 NMS *
*****
* [1] Backup OmniVista 2500 NMS *
* [2] Restore OmniVista 2500 NMS *
* [0] Exit *
*****
Type your option? 1

Enter base name (default is "ov2500nms"):
Would you like to schedule the backup? (y/n)[n]: n
Start backup
Stop services
Backup OV2500 data
Backup MongoDB data
Backup HSQLDB data
Backup openstack file dir
Backup captiveportal file dir
Backup afn file dir
Backup report file dir
Backup License
Start services
```

After backup is finished, the output filename will be: <base name>\_<yyyy-MM-dd--HH-mm>.bk.

### Scheduled Backup

1. Enter **1** and press **Enter** to choose **Backup OmniVista 2500 NMS** option from the Backup/Restore OmniVista 2500 NMS menu.

```
*****
* Backup/Restore OmniVista 2500 NMS *
*****
* [1] Backup OmniVista 2500 NMS *
* [2] Restore OmniVista 2500 NMS *
* [0] Exit *
*****
Type your option? _
```

2. Enter the Backup's base name (default is "ov2500nms"), then press **Enter**.
3. To schedule a backup for a later time, enter **y**, then press **Enter** at the "Schedule" prompt.
4. Enter a start time for the backup in HH:MM format (e.g., 22:00), then press **Enter**.
5. Enter the time between scheduled backups, in days (e.g., 5), then press **Enter**.

```
*****
* Backup/Restore OmniVista 2500 NMS *
*****
* [1] Backup OmniVista 2500 NMS *
* [2] Restore OmniVista 2500 NMS *
* [0] Exit *
*****
Type your option? 1

Enter base name (default is "ov2500nms"):
Would you like to schedule the backup? (y/n)[n]: y
Enter start time (format is HH:mm; default is 13:07): 22:00
Enter the time between backups (default is 1 day): 5
```

### Restore

1. Enter **2** and press **Enter** to choose **Restore OmniVista 2500 NMS** option from the Backup/Restore OmniVista 2500 NMS menu.

```
*****
* Backup/Restore OmniVista 2500 NMS *
*****
* [1] Backup OmniVista 2500 NMS *
* [2] Restore OmniVista 2500 NMS *
* [0] Exit *
*****
Type your option? 1
```

**Note:** The default Mongo DB password was changed in OmniVista 4.1.2.R03. If you are restoring from a previous version of OmniVista, you must change the Mongo DB password to the previous password. If you are restoring from 4.1.3.R03 or later, press **Enter** at the warning prompt and go to Step 1.

2. If there are no backups in the directory, the process will be stopped. Otherwise, a list of backup files is displayed. Choose a Backup File by selecting the number (e.g., 5) in the list and pressing **Enter**.
3. Press **y** at the confirmation prompt, then press **Enter**.

```

*****
* Backup/Restore OmniVista 2500 NMS *
*****
* [1] Backup OmniVista 2500 NMS *
* [2] Restore OmniVista 2500 NMS *
* [0] Exit *
*****
Type your option? 2

WARNING: Please change mongo password to similar with mongo password of backup f
ile before restore
Press enter to continue
Backups available:
  [1] ov2500nms-2015-11-30--16-33
  [2] ov2500nms-2015-12-01--08-52
  [3] ov2500nms-2015-12-01--20-13
  [4] ov2500nms-2015-12-02--08-52
  [5] ov2500nms-2015-12-02--12-40
Choose a backup file to restore (choose 0 to exit): 5
Are you sure of restoring from
  [5] ov2500nms-2015-12-02--12-40
(y/n): y_
    
```

4. After completing the Restore, you will be prompted to restore license information. If you select **Yes**, the current license will be overwritten with the one from the Backup File.

### Changing the Virtual Appliance Password

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

```

*****
* Change Password the Virtual Appliance *
*****
* [1] Change admin password *
* [2] Change mongo database password *
* [0] Exit menu and continue *
*****
Type your option? _
    
```

To change the VA Admin password, enter **1**, then press **Enter**. At the prompts, enter the current password, then enter the new password.

To change the mongo database password, enter **2**, then press **Enter**. You have two options when changing the mongo database password.

```

*****
Type your option?
Provide option [1 OR 2]. Option 1 for changing password of mongo administrator;
2 for ngnms application user :_
    
```

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.

**Note:** If you change the mongo database password, you will be prompted to restart the Watchdog service for the change to take place. To stop and restart the Watchdog Service, cd to <OV\_Install\_Root>\Watchdog and enter the following commands:

- Shutdown:
  - *watchdog-cli.bat shutdown* (Windows)
  - *watchdog-cli.sh shutdown* (Linux)
- Startup
  - *watchdog-cli.bat start* (Windows)
  - *watchdog-cli.sh start* (Linux)

## Collecting Logs

You can view OmniVista Logs using the “Collect Logs” option. Enter **6**, then press **Enter**.

```
*****
Type your option? 6
Enter the date which you want to collect only log files created after that (Date
format is dd-MM-yyyy) 07-12-2015_
```

Enter the “beginning” date for collecting logs (dd-MM-yyyy format). Log information from this date to the present date/time will be collected. To view the logs, FTP to the VA and go to the logs Directory:

- FTP User: admin
- FTP Password: admin
- FTP Port: 8888

The logs are contained in a zip file labeled with the date/time they were collected.

## Powering Off the Virtual Appliance

Before powering off the VM, you must go to the Watchdog Screen in the OmniVista Web GUI and stop all OmniVista services. Navigate to **Administrator >Control Panel > Watchdog**, and click on the **Stop All** button  in the upper-right corner of the screen. The status of OmniVista services can be checked by typing ‘status’ at the Watchdog command prompt in the Virtual Appliance menu. After all the services are stopped, enter **7** at the command line to power off the VM. Confirm power off by entering **y**. The power off may take several minutes to complete.

**Note:** OmniVista 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.

## Rebooting the Virtual Appliance

Before rebooting the VM, you must go to the Watchdog Screen in the OmniVista Web GUI and stop all OmniVista services. Navigate to **Administrator >Control Panel > Watchdog**, and click on the **Stop All** button  in the upper-right corner of the screen. The status of OmniVista services can be checked by typing ‘status’ at the Watchdog command prompt in the Virtual Appliance menu. 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 admin user and password prompts. Note that OmniVista functions continue following reboot.

### Logging Out Of the Virtual Appliance

To log out of the VM and return to the admin login prompt, enter **0** at the command line. Confirm logout by entering **y**. Note that OmniVista functions continue following logout.

## Appendix A – Extending the VA Partition Size

If necessary, you can use the GParted Partition Manager to resize VA partitions. GParted is a free partition manager tool that can be downloaded for free [here](#). After downloading GParted, follow the steps below to extend the partition size of an existing VA installation.

- [Step 1: Power off the VA.](#)
- [Step 2: Download and mount the GParted Live CD to the CD drive.](#)
- [Step 3: Increase the Disk Provisioned Size of the Hard Disk.](#)
- [Step 4: Configure the bootup Force BIOS setup.](#)
- [Step 5: Change the boot order to boot from the CD-ROM Drive.](#)
- [Step 6: Boot the VA from the GParted Live CD.](#)
- [Step 7: Open GParted.](#)
- [Step 8: Select device /dev/sda and select partition /dev/sda3 then click Resize/Move.](#)
- [Step 9: Extend the disk size for /dev/sdb and /dev/sdb1.](#)
- [Step 10: Select Apply and confirm.](#)
- [Step 11: Wait for the process to finish and reboot the VA.](#)
- [Step 12: Reboot from the local drive.](#)

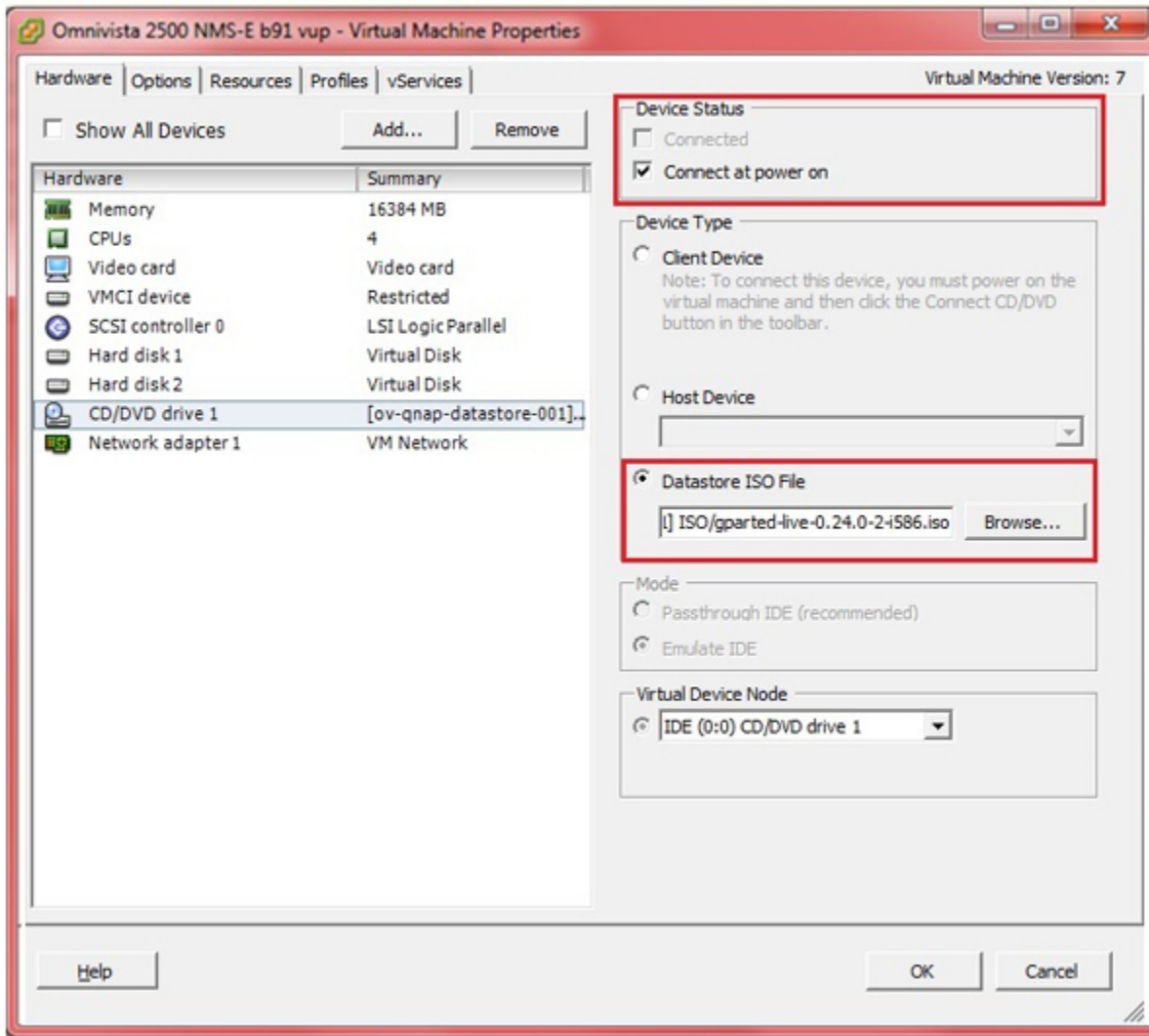
**Step 1:** Open a Console on the VA with admin account. Use option 7 to power off the VA.

```
*****
* The Virtual Appliance Menu
*****
* [1] Configure the Virtual Appliance
* [2] Run Watchdog command
* [3] Update VA
* [4] Backup/Restore OmniVista 2500 NMS
* [5] Change Password
* [6] Collect logs
* [7] Power off
* [8] Reboot
* [0] Log out
*****
Type your option? 7
```



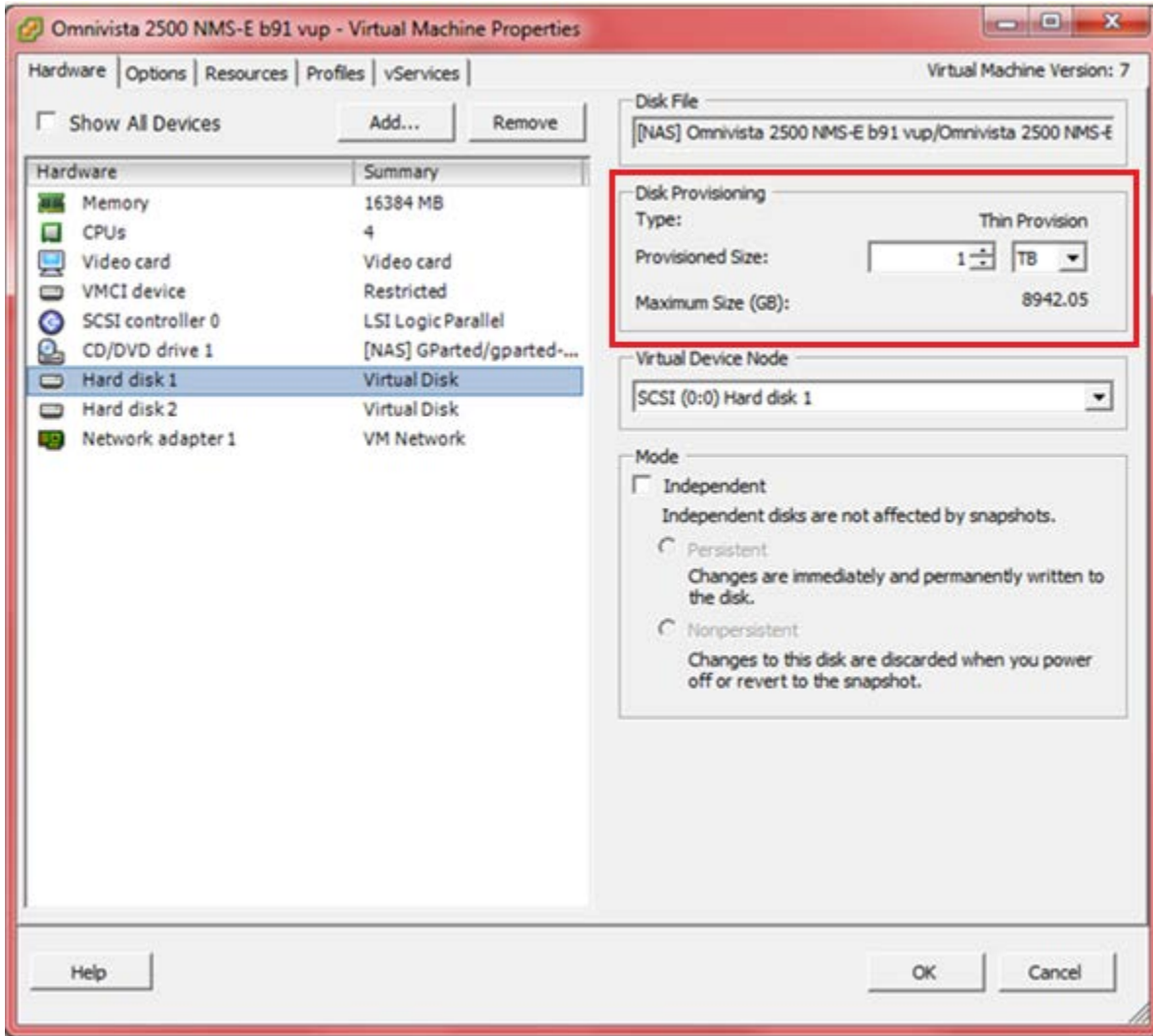
## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

**Step 2:** Download and mount the GParted Live CD to the CD drive (make sure “Connect at power on” option is selected in the Device Status area).



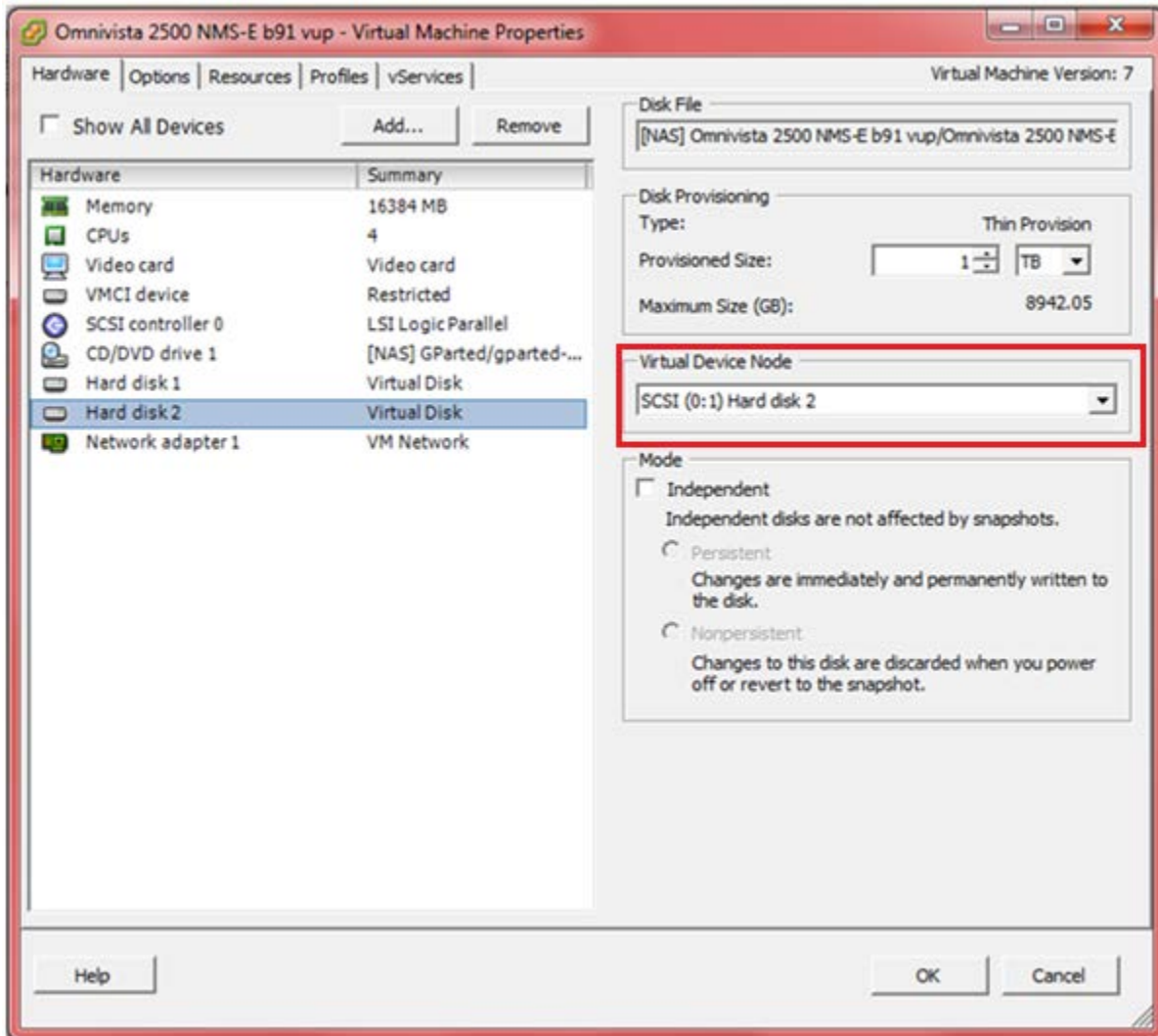
### OmniVista 2500 NMS Installation Guide (4.1.2.R03)

**Step 3:** Increase the Disk Provisioned Size of the Hard Disk. Select Hard disk 1 and increase the Disk Provisioned Size from the default of 256GB to the recommended size (e.g. 1TB). Data and System files are stored in 2 virtual disks. You must change the provision size for **both** disks. By default, “Hard disk 1” appears in the **Virtual Device Node** drop-down menu. Update the **Provisioned Size** to the recommended size and click **OK**.



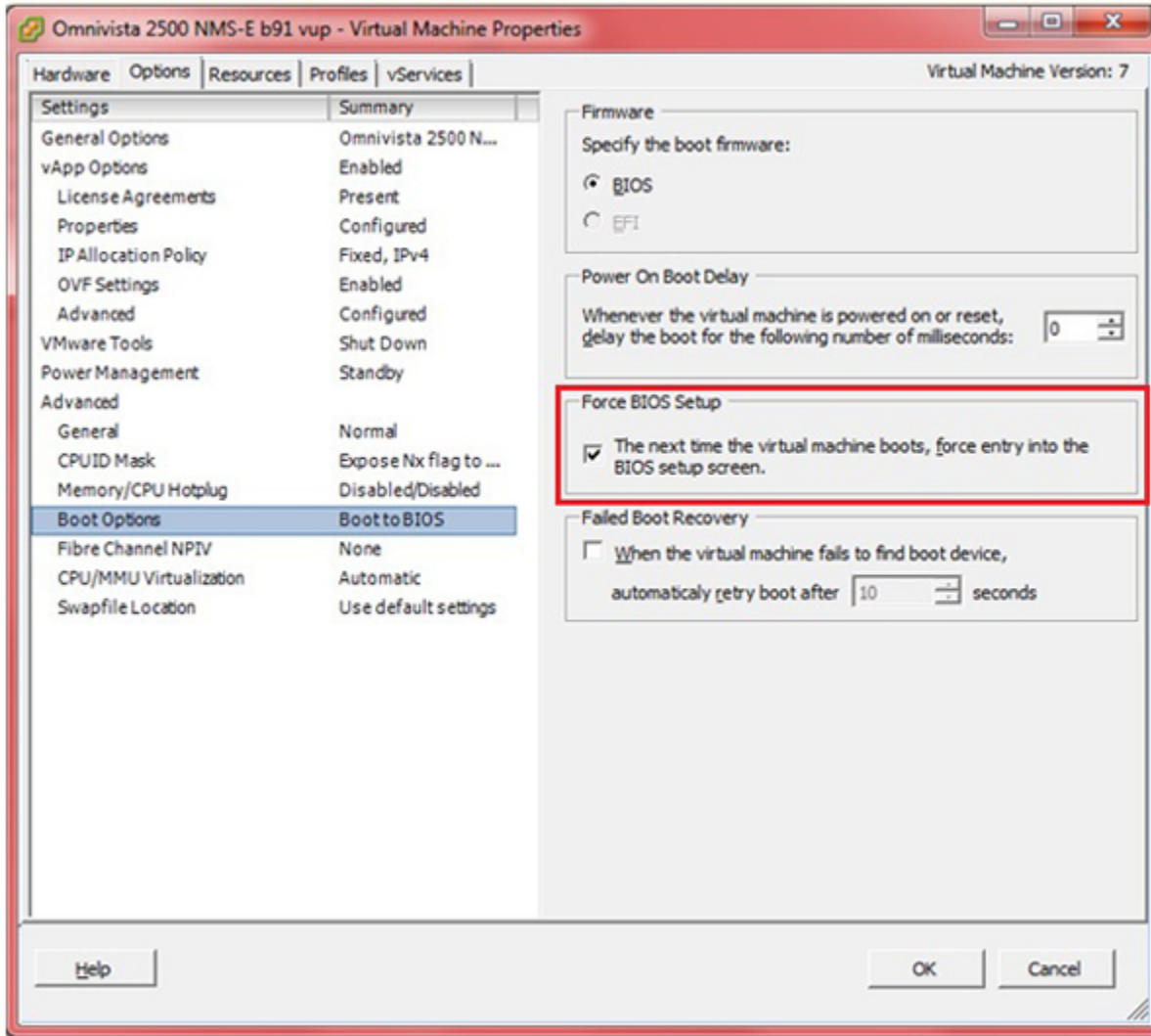
## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

Then select “Hard disk 2” in the **Virtual Device Node** drop-down menu. Change the **Provisioned Size** to the recommended size and click **OK**, as shown below.

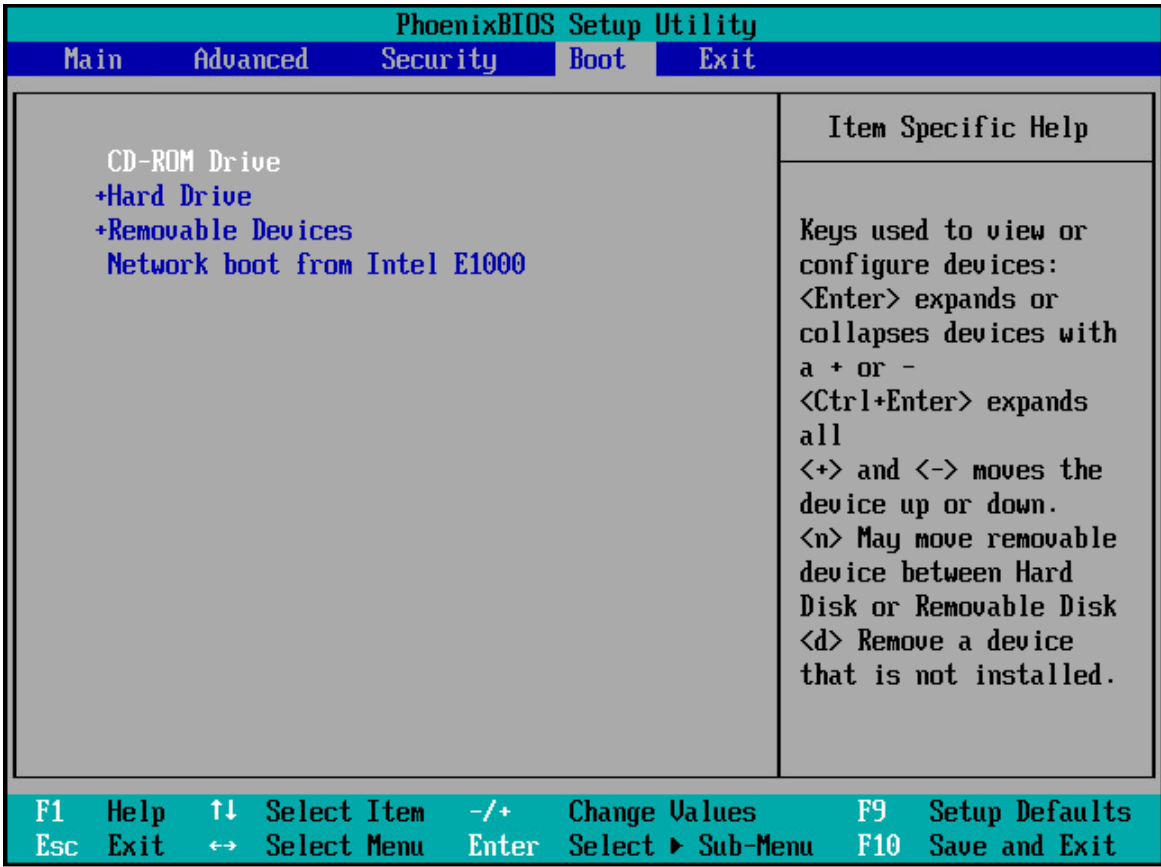


## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

**Step 4:** Configure the bootup Force BIOS setup. Click on the **Options** tab, select **Boot options**, then select the checkbox in the **Force BIOS Setup** area. Click **OK**.

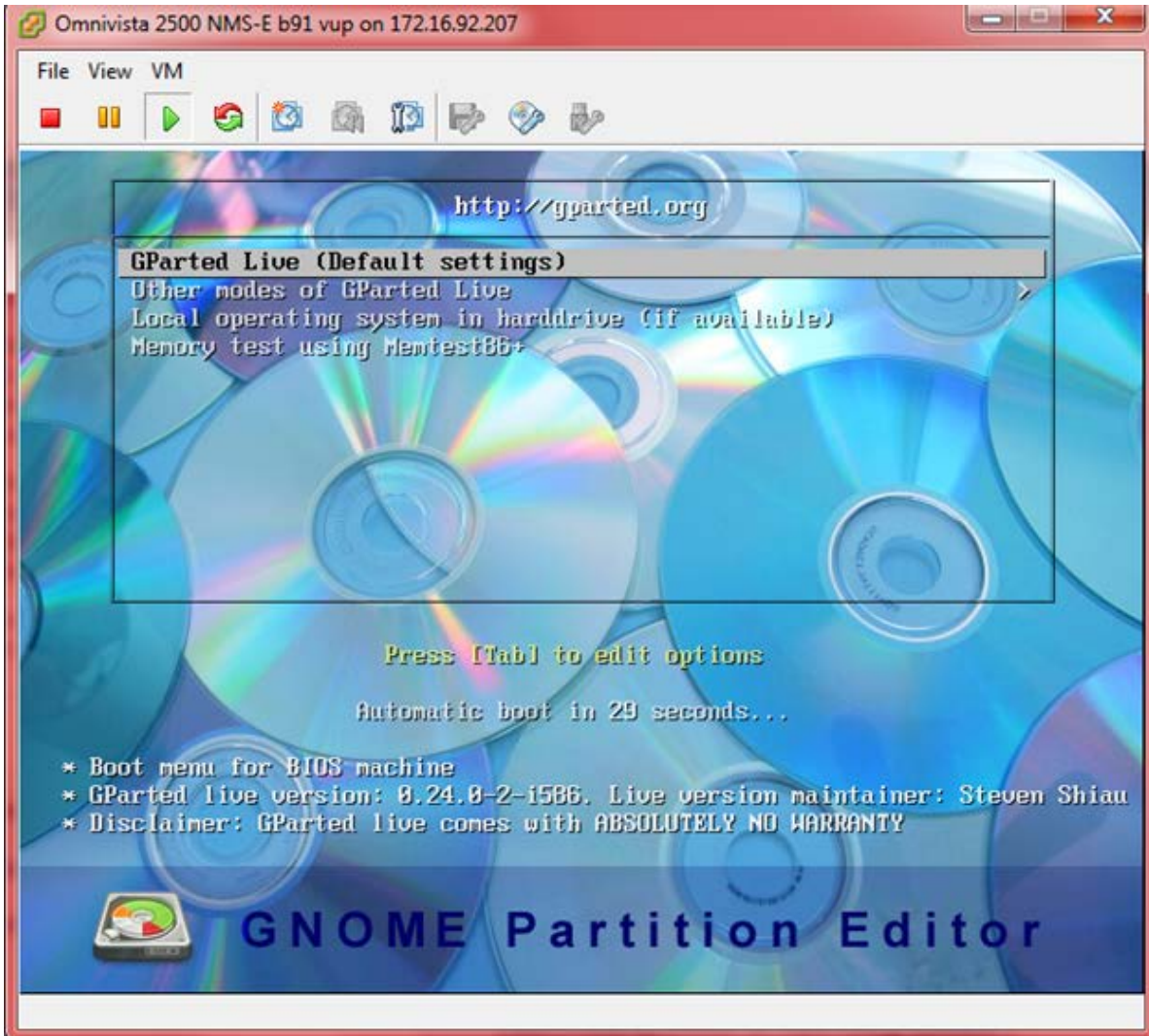


**Step 5:** Start the VA. Change the boot order to boot from the CD-ROM Drive. Go to the Boot tab and use the +/- keys to move the CD-ROM Drive to the top of the list. Press **F10** and select **Yes** at the confirmation prompt to save and exit.

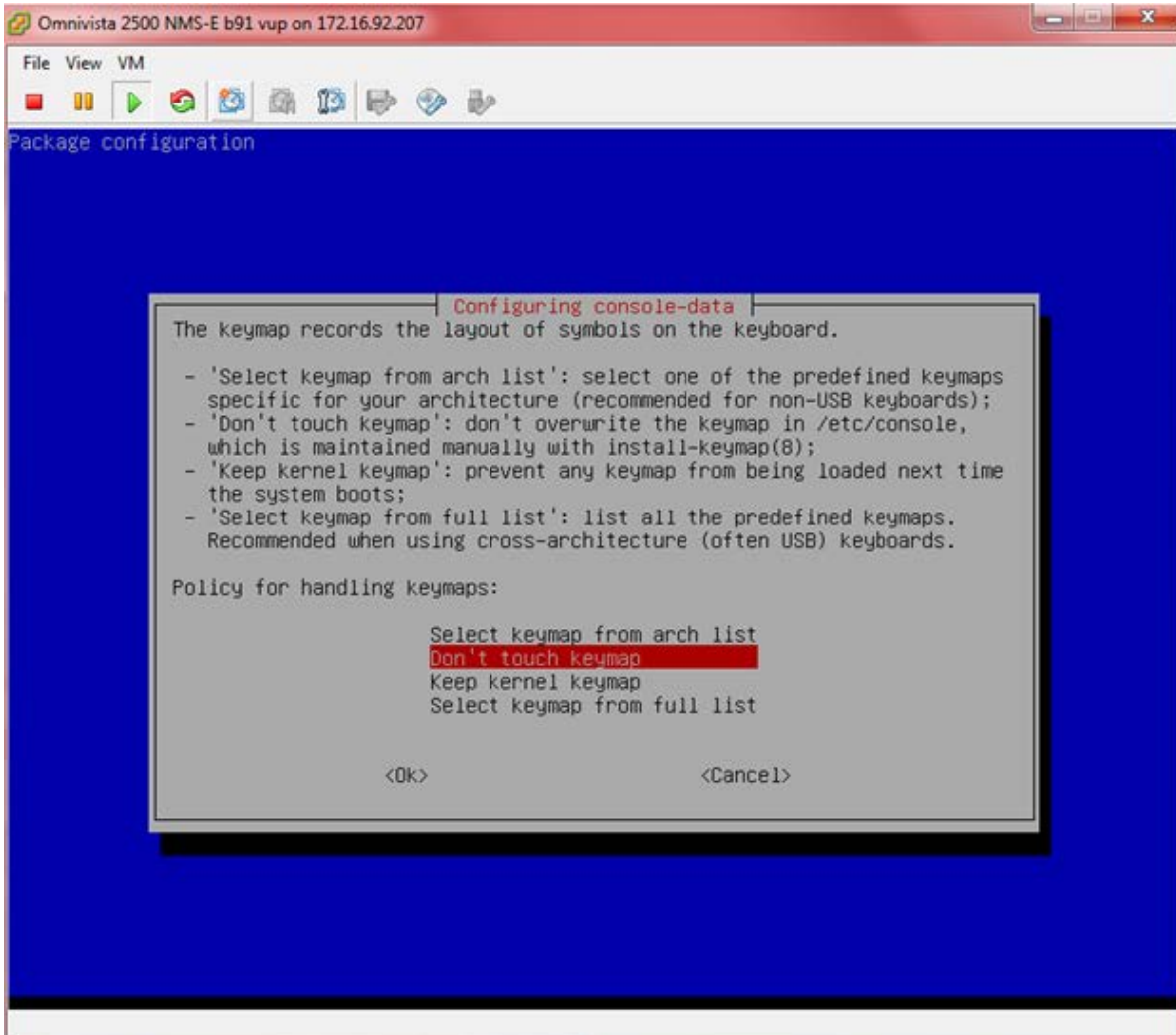


**Step 6:** Boot the VA from the GParted Live CD.

Select **GParted Live (Default Settings)**.

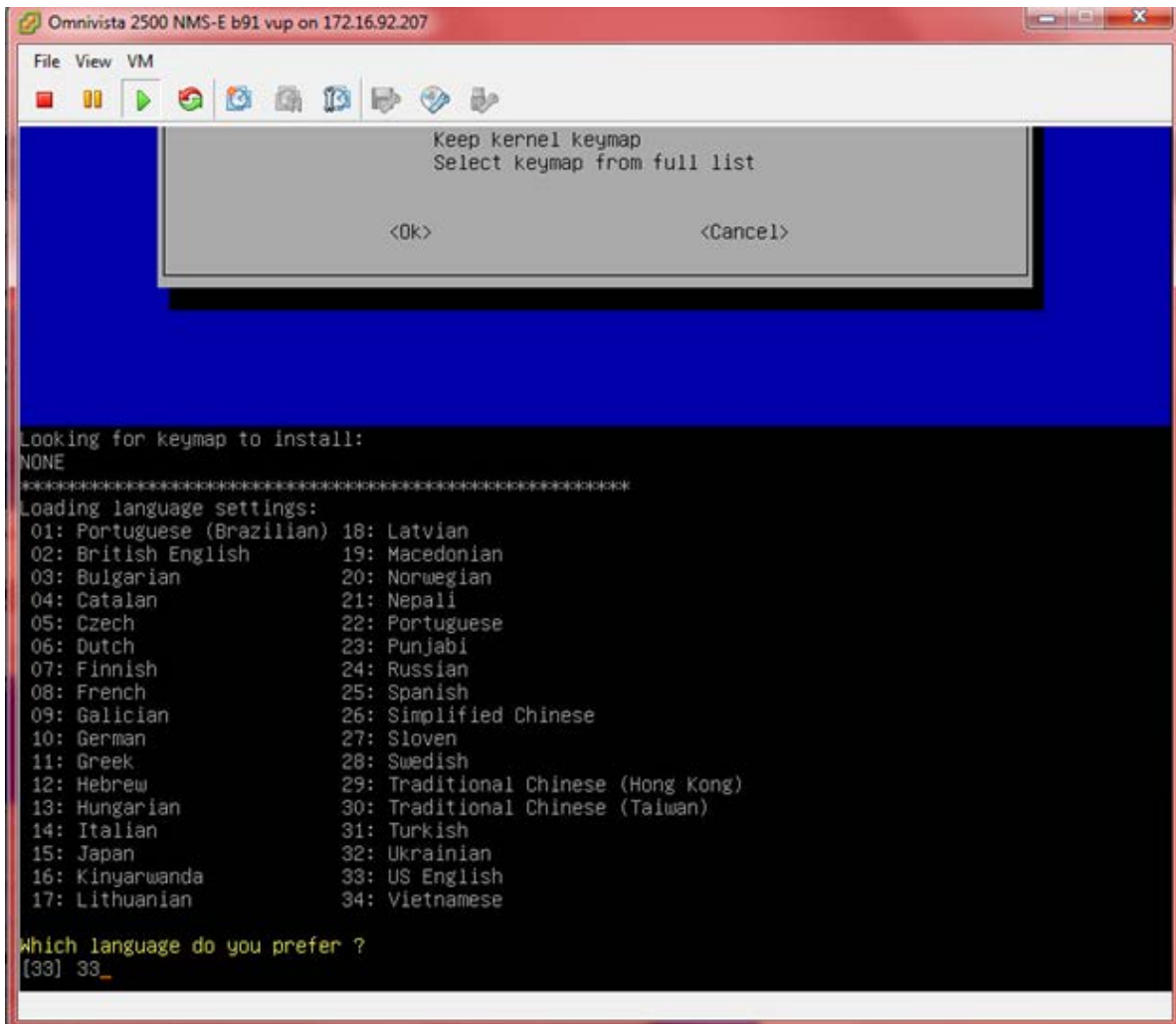


Select **Don't Touch Keymap**



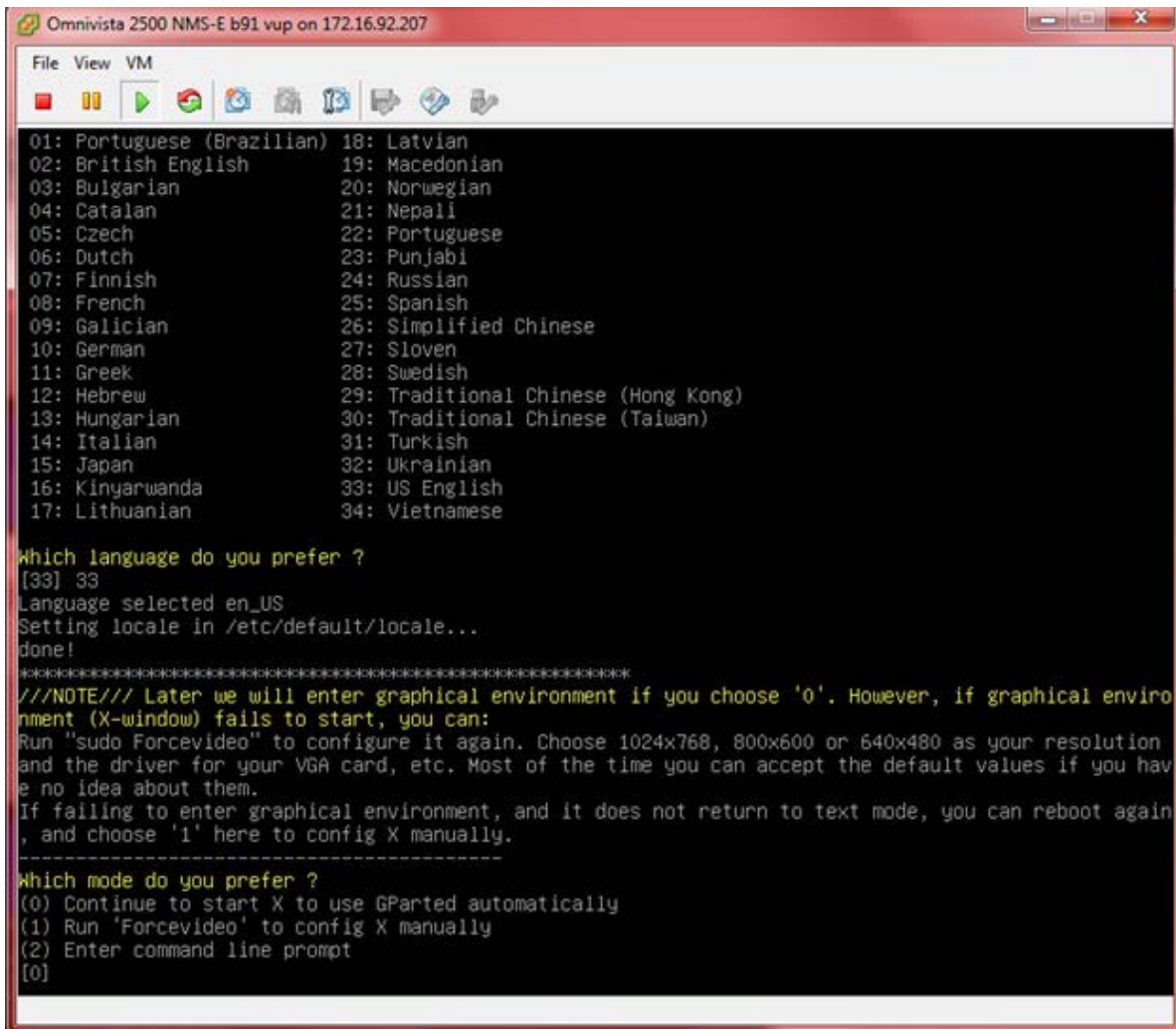
## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

Select the preferred language.



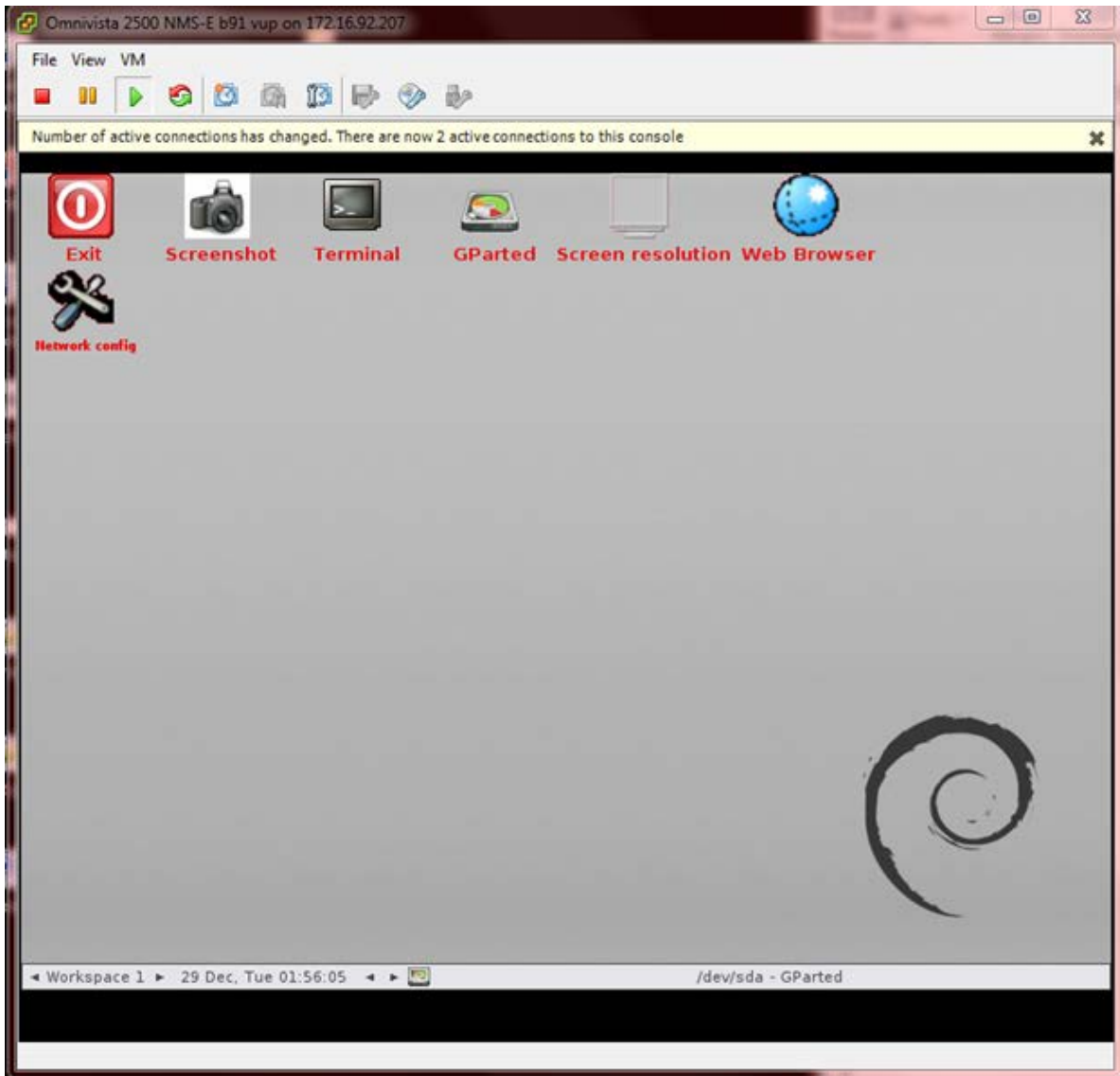


Select **(0) Continue to start X to use GParted automatically.**



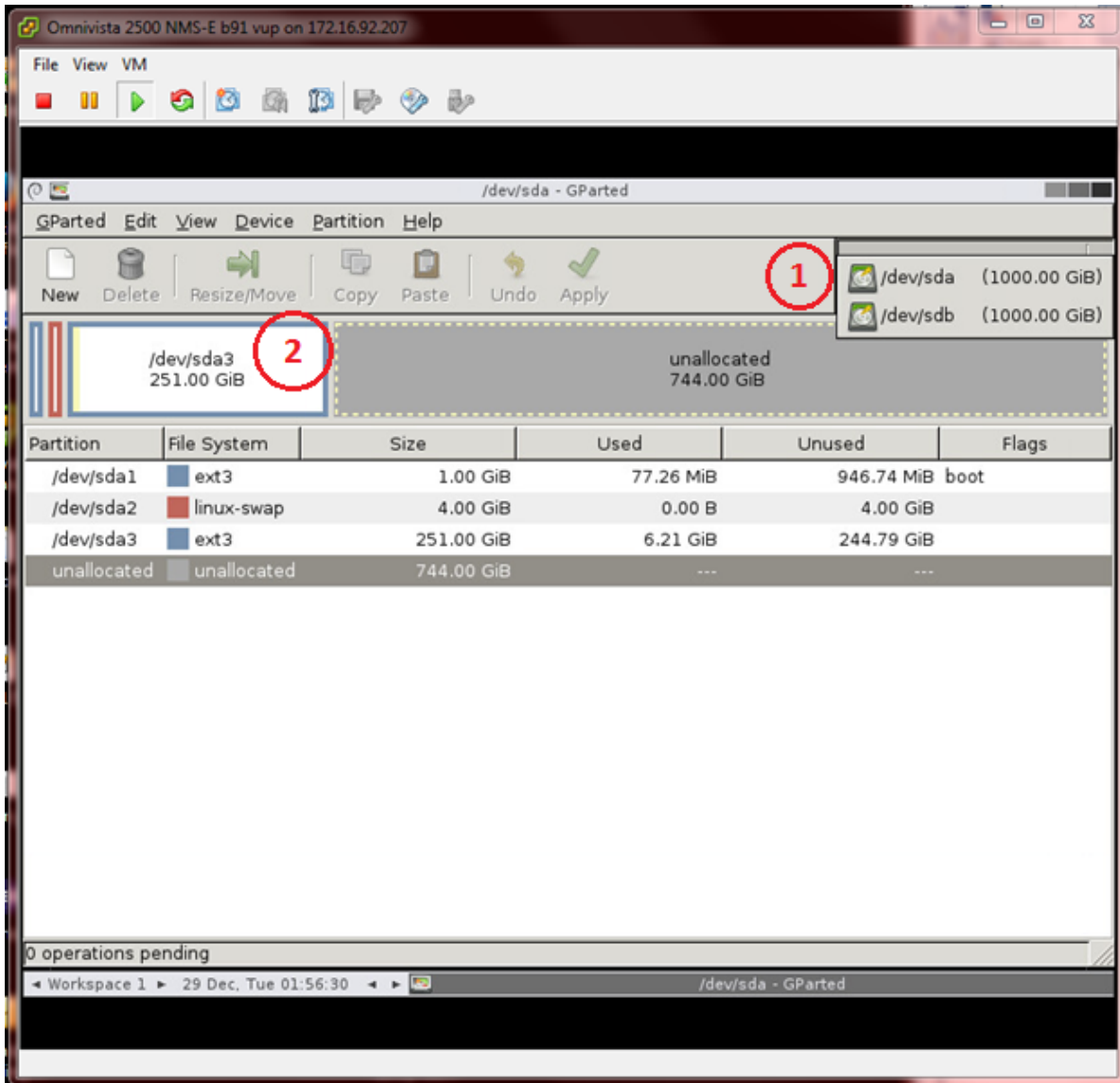
## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

**Step 7:** GParted should launch automatically. If not, click on the **GParted** icon to open GParted, as shown below.



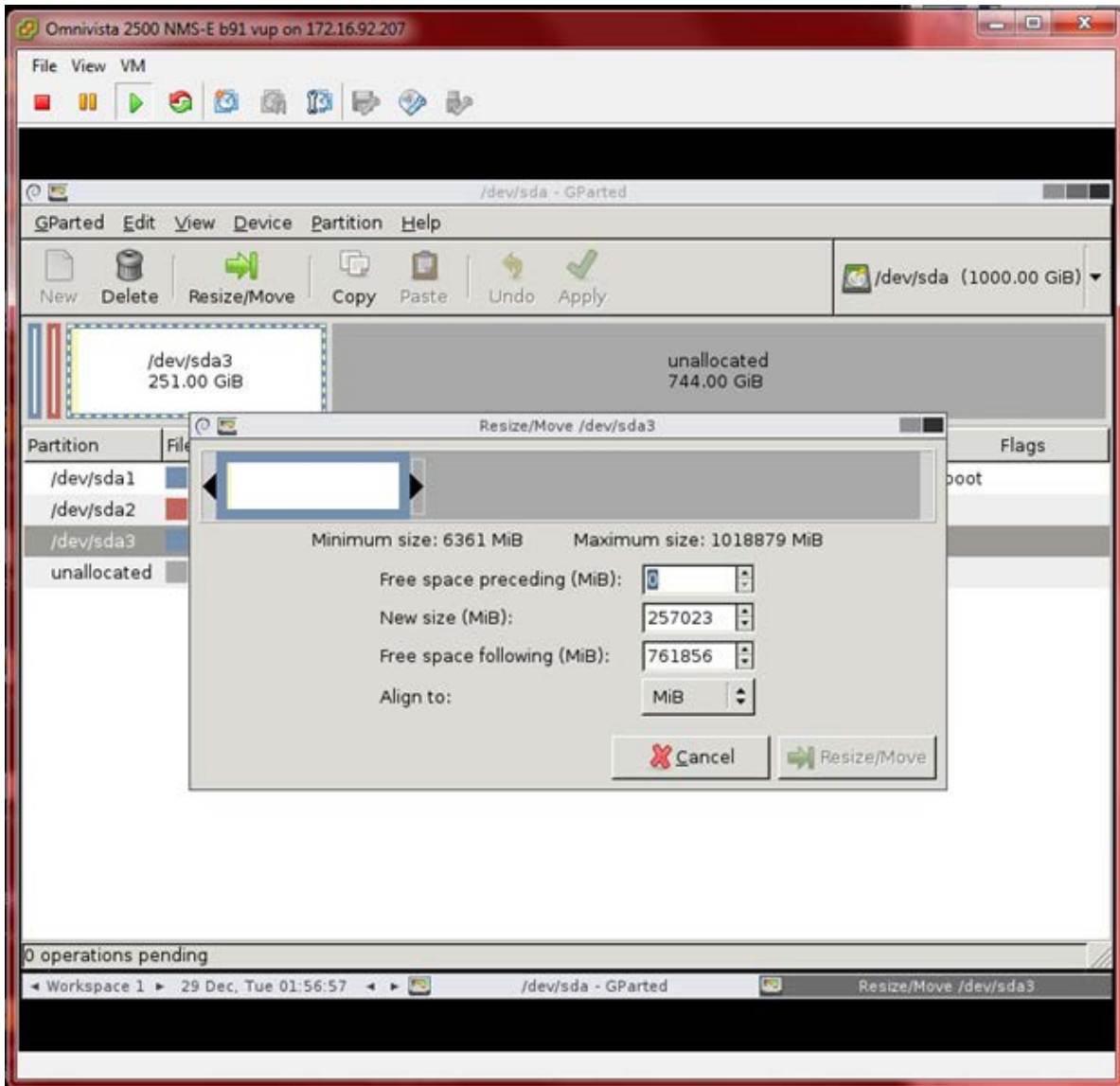
## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

**Step 8:** Select device /dev/sda and select partition /dev/sda3 then click **Resize/Move**.

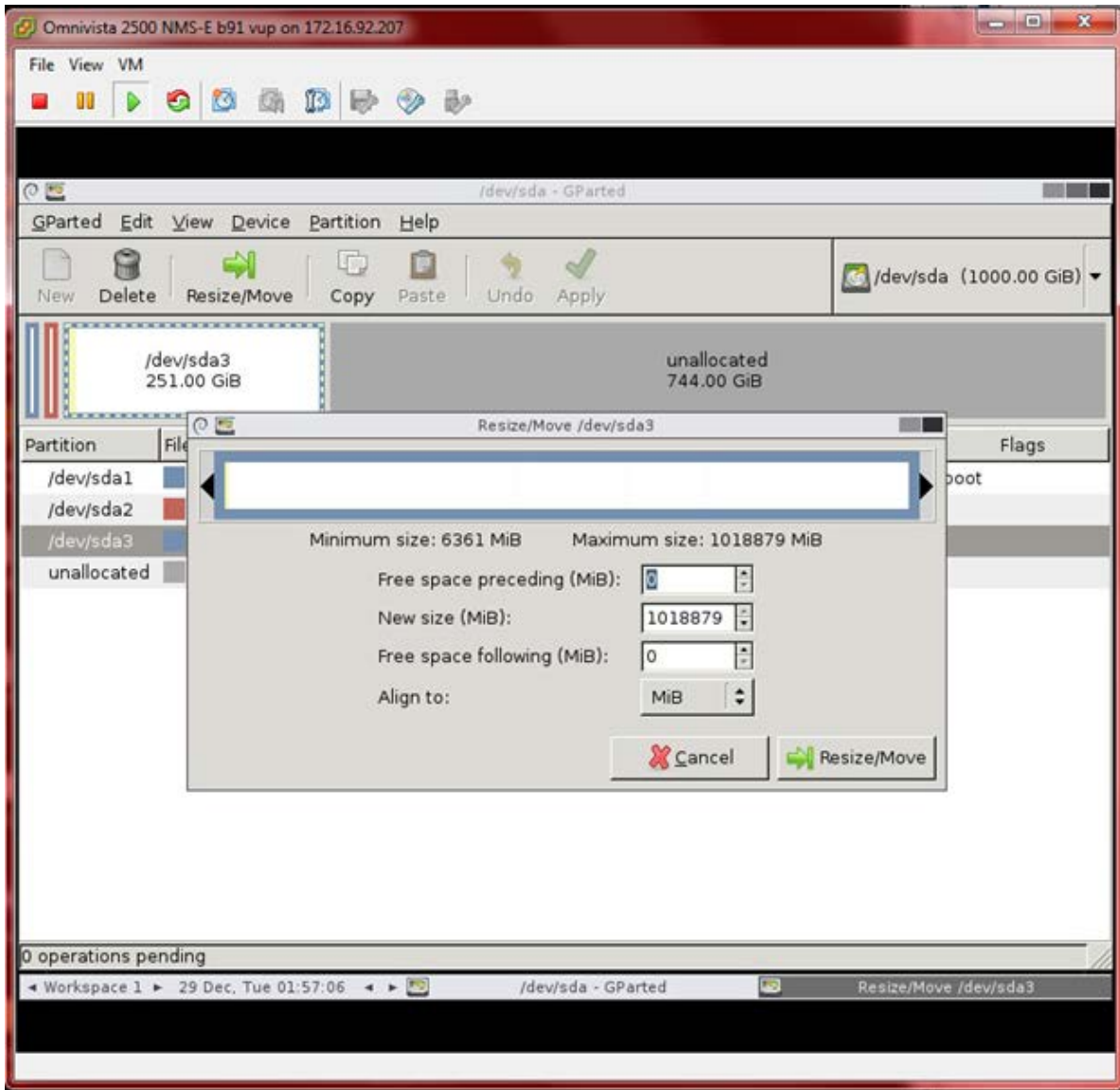


Use the UI menu to change the partition size. Or use the input menu below to enter the size for the partition. When complete, click on the **Resize/Move** button.

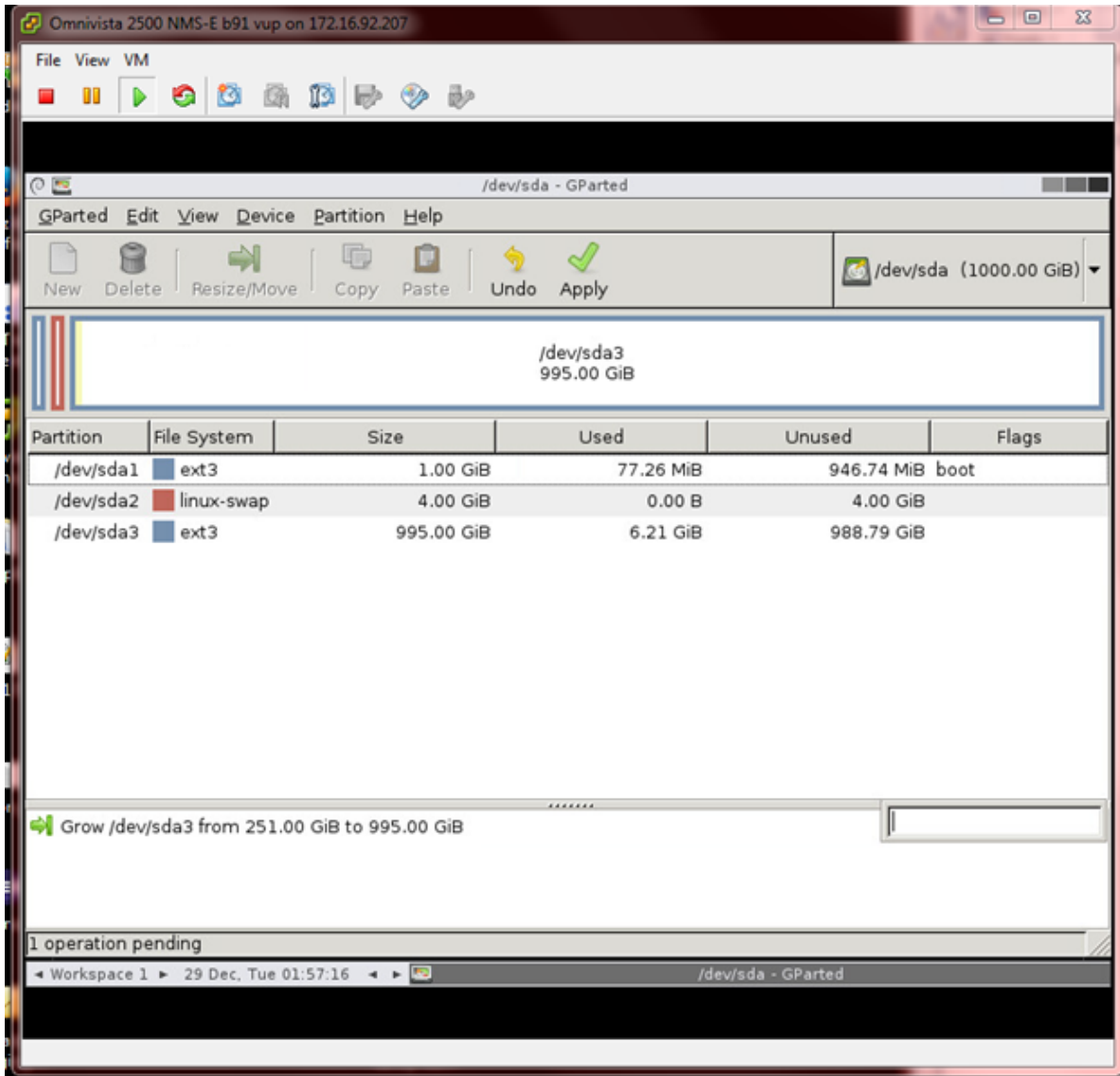
Before



After

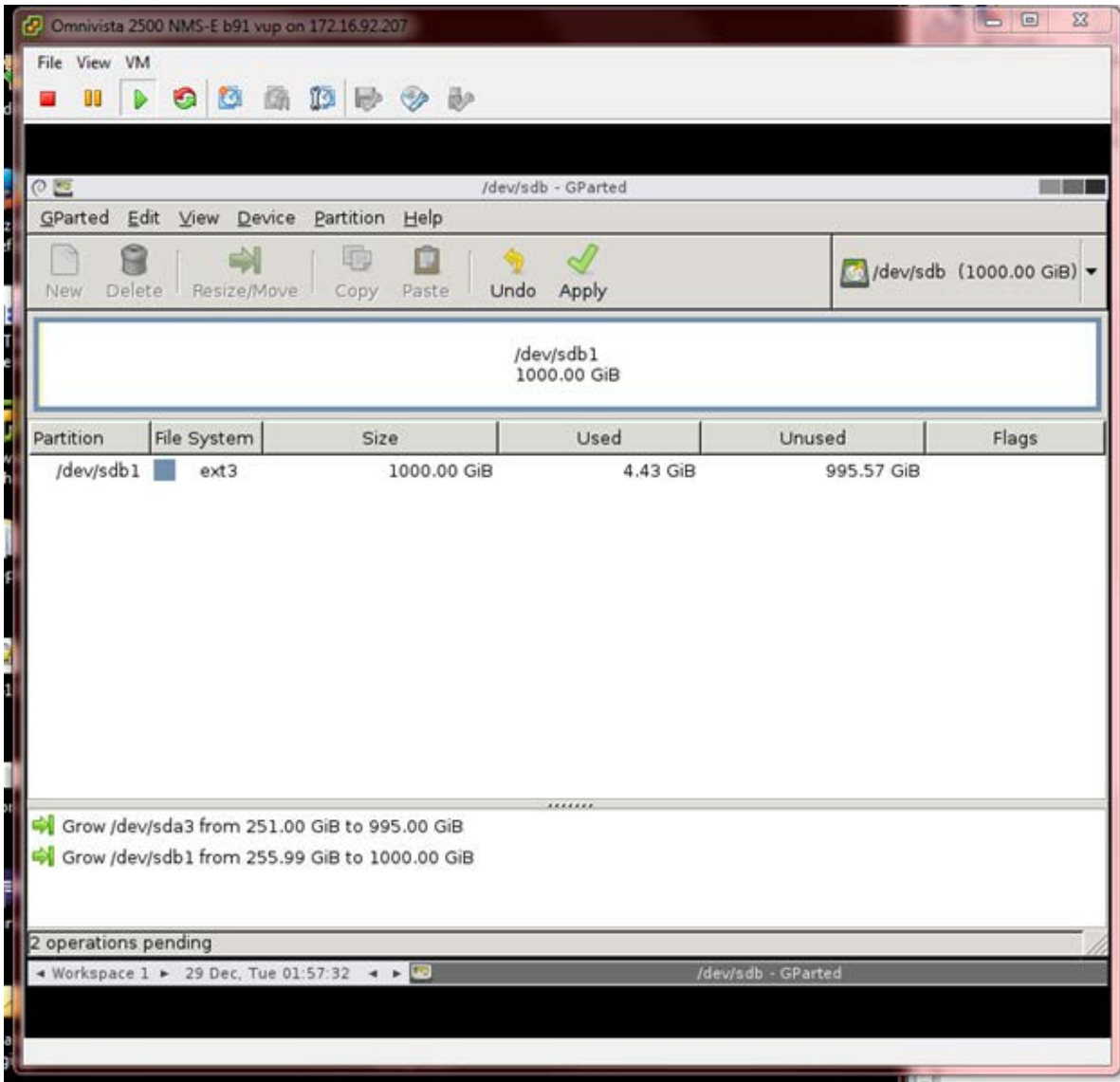


# OmniVista 2500 NMS Installation Guide (4.1.2.R03)

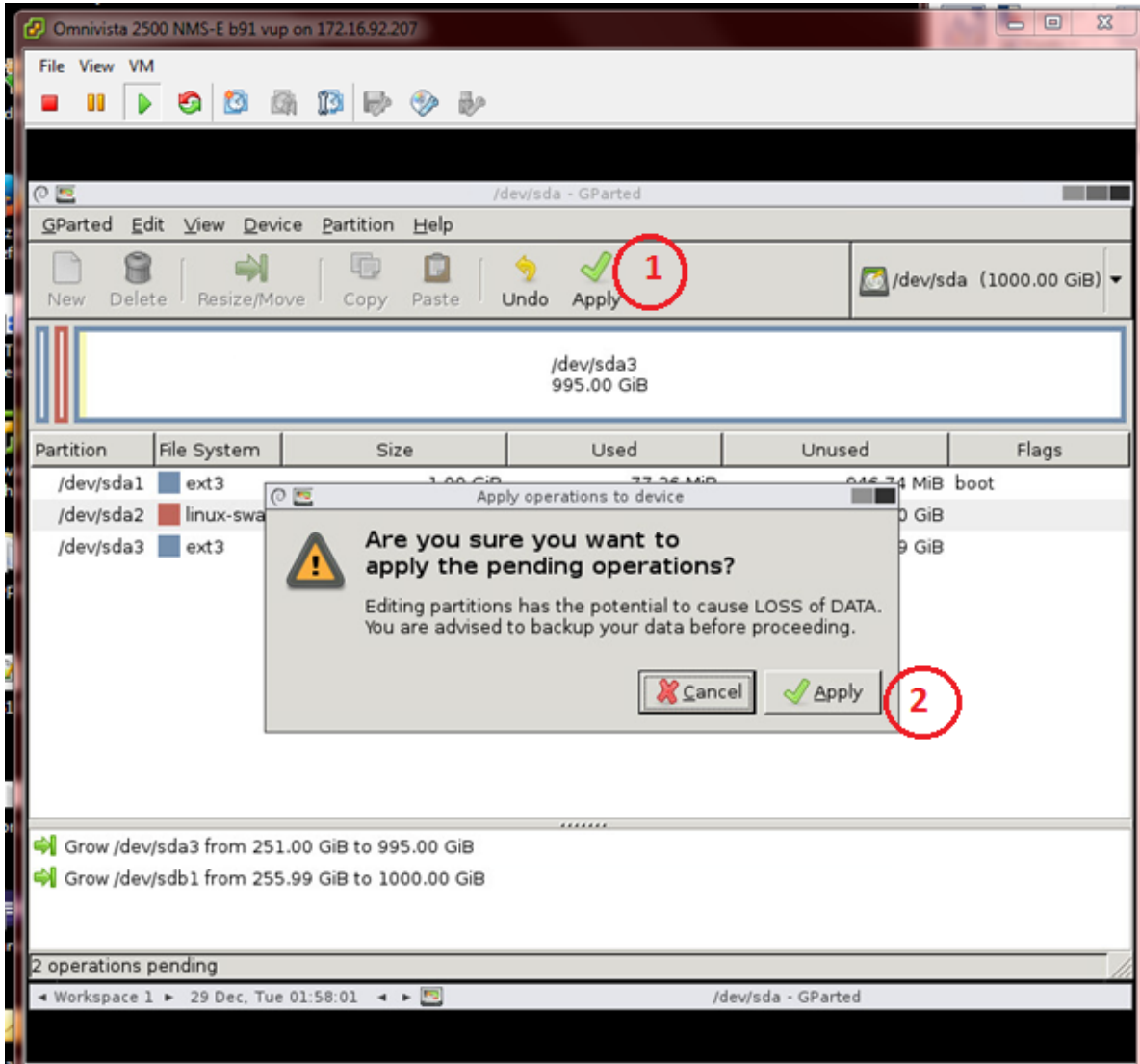


## OmniVista 2500 NMS Installation Guide (4.1.2.R03)

**Step 9:** Extend the disk size for /dev/sdb and /dev/sdb1.

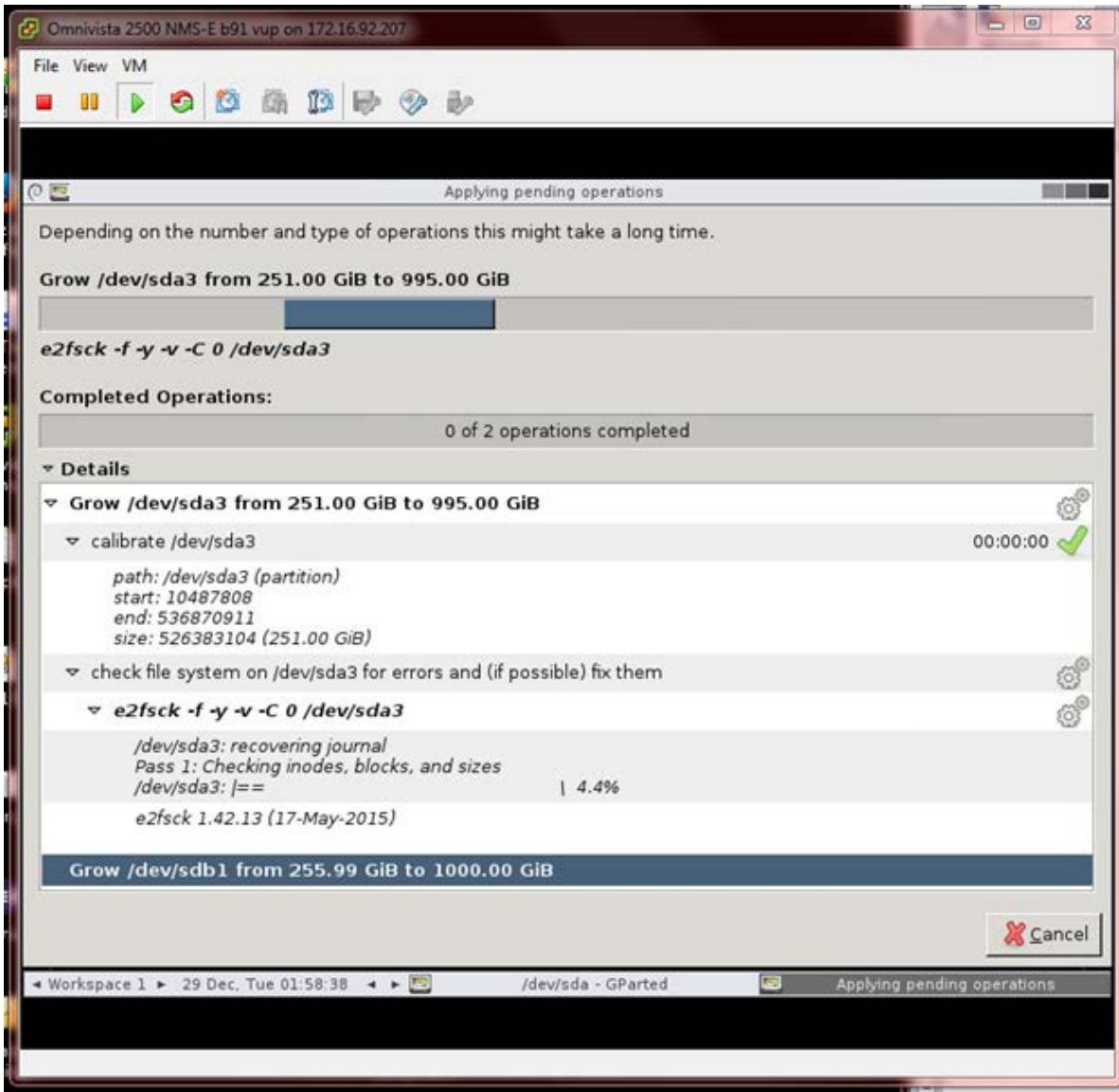


Step 10: Select **Apply** and confirm.

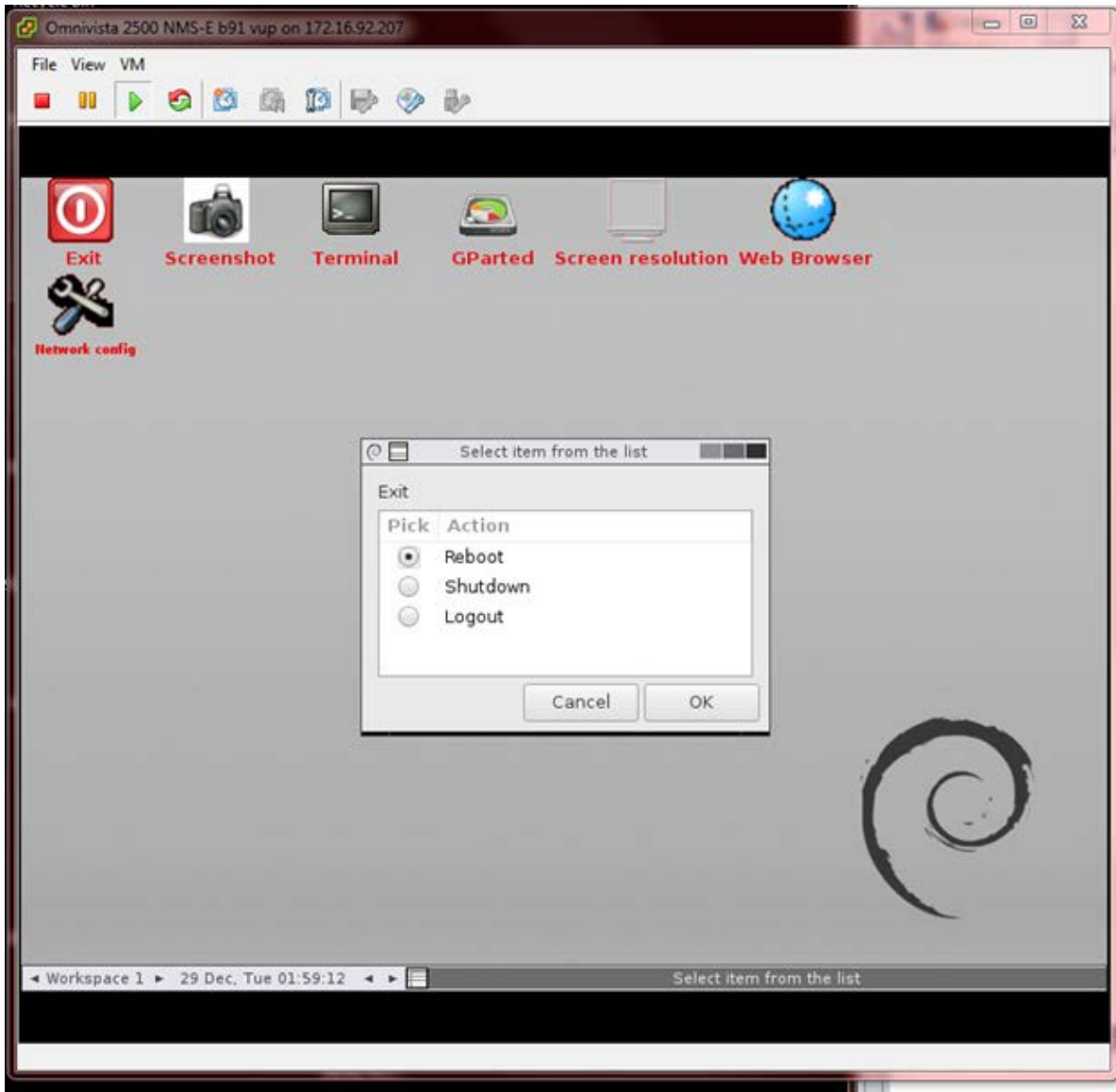




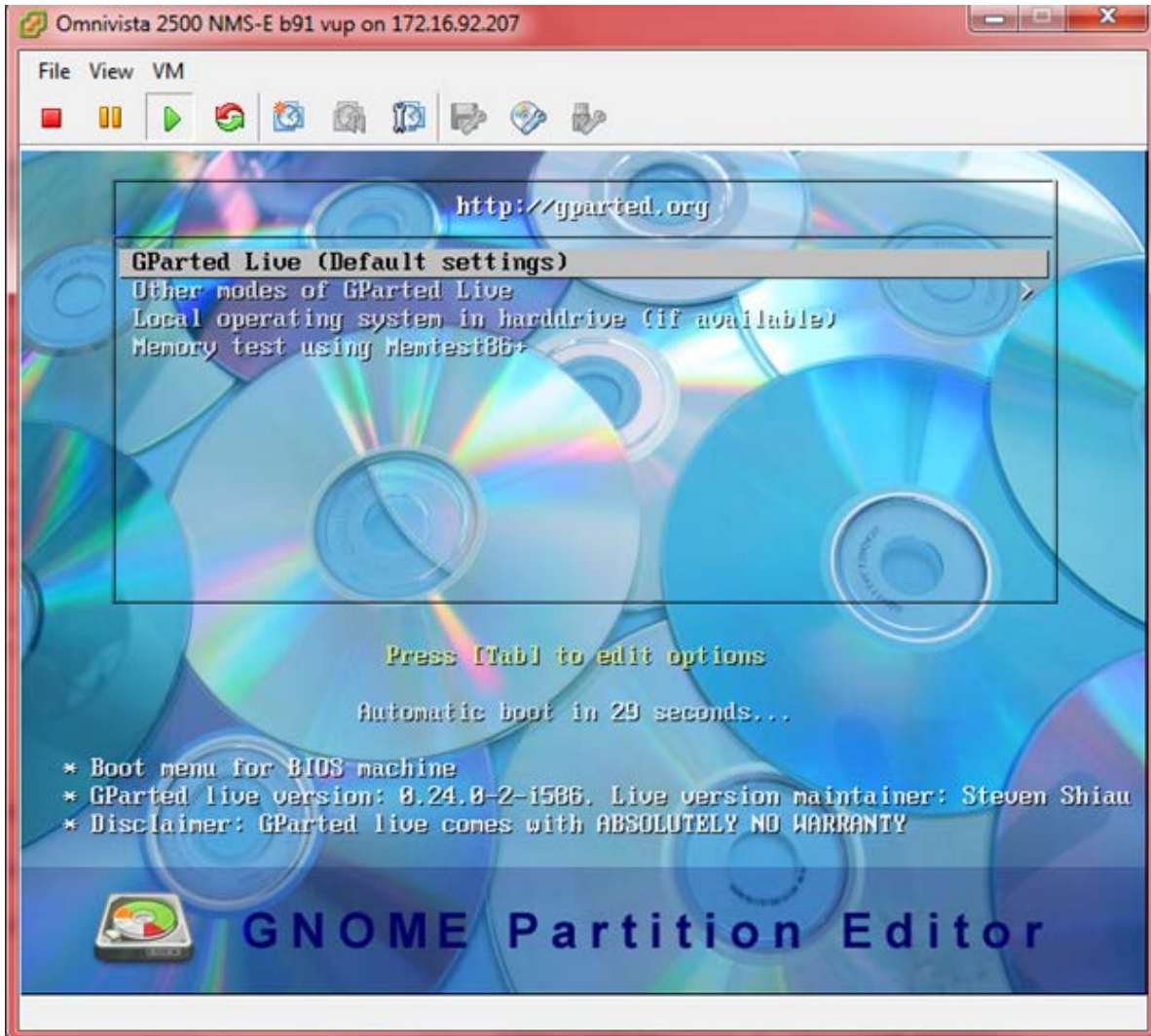
Step 11: Wait for the process to finish, then reboot the VA.



## OmniVista 2500 NMS Installation Guide (4.1.2.R03)



Once the VA is rebooted, the main GParted Screen will appear.



**Step 12.** Reboot from the local drive. Select **Local operating system in hard drive**, and press **Enter**. The system will reboot from the local drive and the new disk partition size will take effect.

**Note:** To prevent the VA from loading from GParted on the next reboot, can change the boot order from the BIOS as shown in steps 4 – 5 above; or reset the CD/DVD drive 1 Device Type to **Host Device** by right-clicking on the VA to bring up the Virtual Machine Properties Screen.