Installation Guide

for

**OmniVista 2500 NMS
Version 4.1.2.R01**

Alcatel·Lucent

December 2014

Revision B

Part Number 060403-10

READ THIS DOCUMENT

**Includes OmniVista 2500 NMS for
Windows Server 2012 R2
Windows 7 Professional SP1
Windows 8.1
Red Hat Linux 6.5
SUSE Linux 11**

Table of Contents

Installing OmniVista 2500 NMS

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* included with the OmniVista 2500 NMS Screen on line help.

Key applications in OmniVista 2500 NMS is 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 1.7 or 1.8 installed on the Client machine. OmniVista 2500 NMS includes Java 2 Runtime Environment (JRE) Version 1.8 (Update 25), which is required for the OmniVista Server. It is bundled with the installers for all supported platforms, and is automatically installed with OmniVista 2500 NMS. Because the bundled JRE is installed in the OmniVista 2500 NMS installation directory, it should NOT affect or conflict with any other JRE or Java Virtual Machine previously installed on your machine.

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

OmniVista 2500 NMS is installed from a file download. After installing OmniVista 2500 NMS, you must configure the java settings, install the OmniVista Security Certificates, and, if you are upgrading from a previous version of OmniVista, you should **backup the old database and restore it to the new installation**. Note that you can only upgrade from OmniVista 3.5.7, 4.1.1 GA, 4.1.1 Post-GA, 4.1.2.R01 GA.

The following sections detail the OmniVista 2500 NMS installation process.

- Installing the OmniVista 2500 NMS Software
- Configuring Java Settings
- Launching OmniVista 2500 NMS
- Installing the OmniVista Security Certificates

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.

4. The InstallAnywhere Introduction displays. Click **Next** to continue.
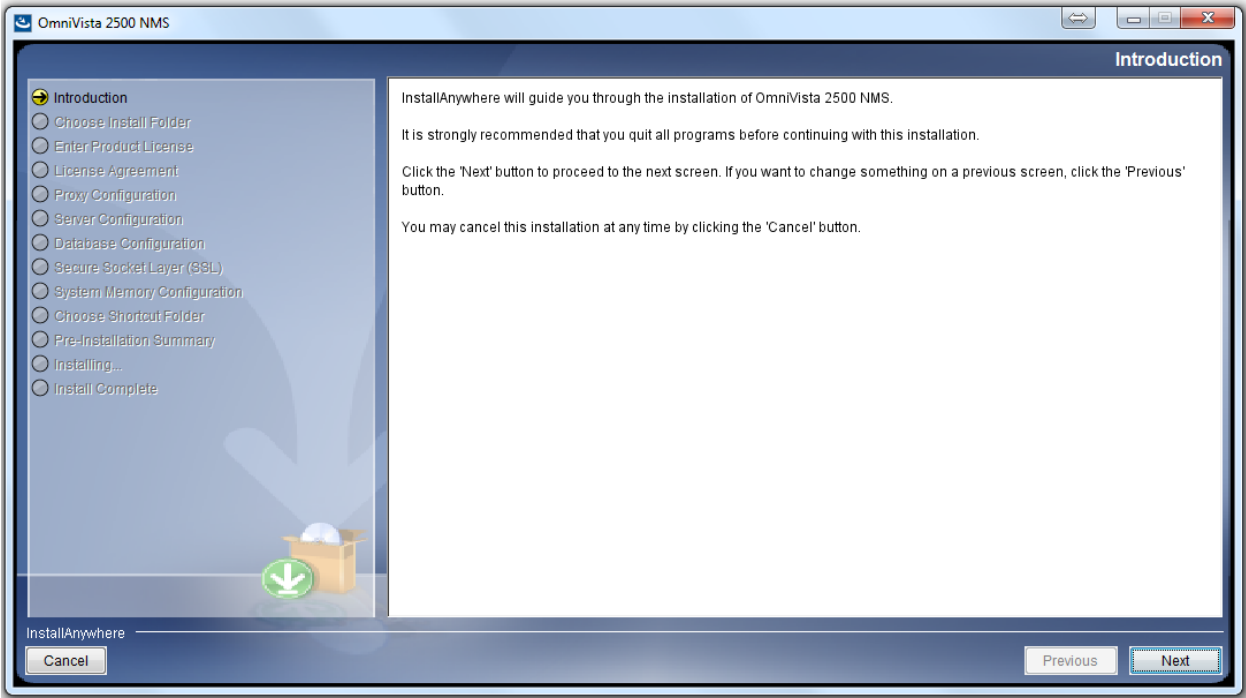
5. Choose Install Folder. Choose an Install Folder location. The default location automatically displays in the selection box (Windows - C:\Program Files\OmniVista 2500 NMS, Linux - /opt/OmniVista_2500_NMS). To change the location, select **Choose**. Click **Next** to continue.
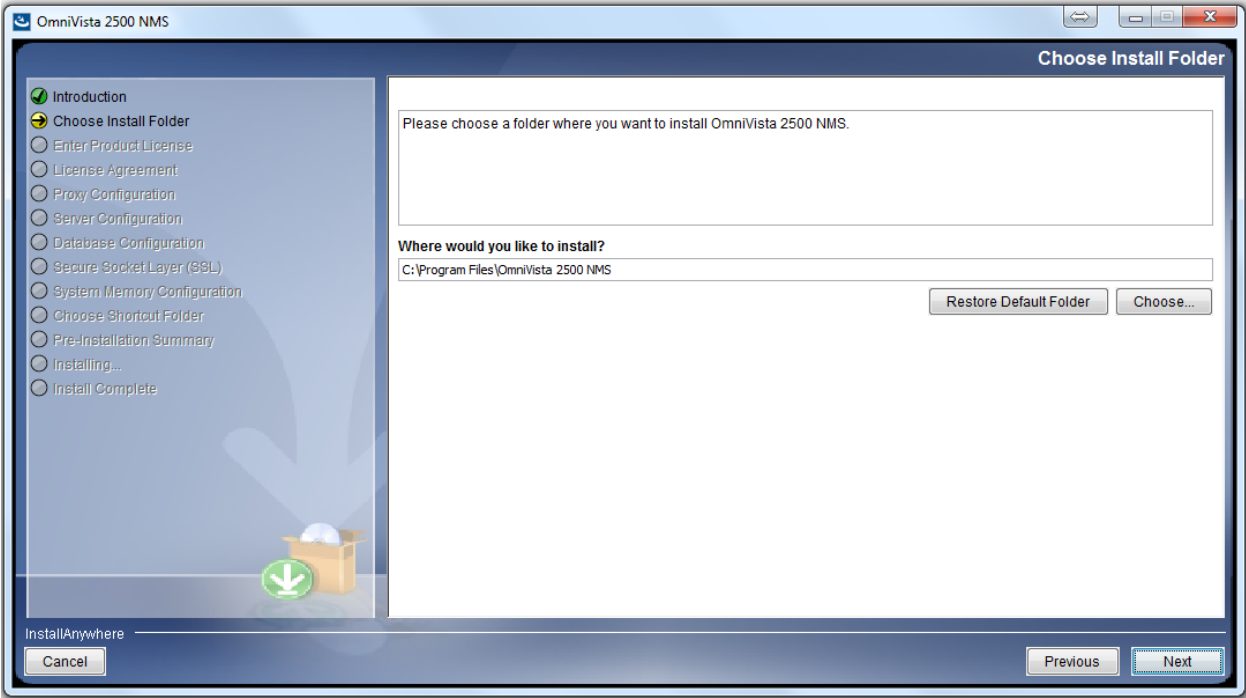
6. Enter Product License. OmniVista prompts for a Core license key. Enter the Core License Key received when you purchased the software. (The Core License is a required step.) Click **Next** to continue.
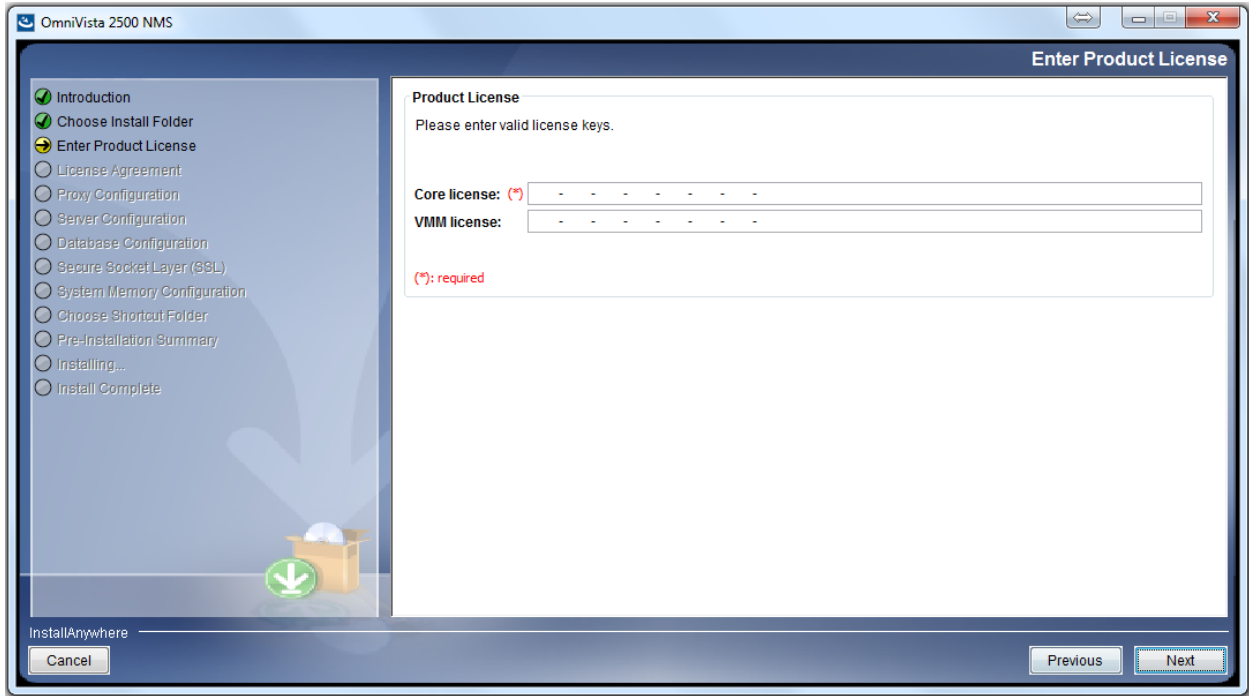
Note: The OmniVista 2500 NMS "Starter Pack" License is available for free. However, it will only enable you to manage 20 devices (10 AOS/10 Third-Party). If you are using a "Starter Pack" License, you can purchase an Evaluation or Production License at a later time and enable it using the License Application in OmniVista 2500 NMS.

7. License Agreement. OmniVista displays the End User License Agreement (EULA) in this panel. Read the agreement carefully and select "I accept the license agreement." Click **Next** to continue.

Note: You must accept the EULA License to continue to the next step.
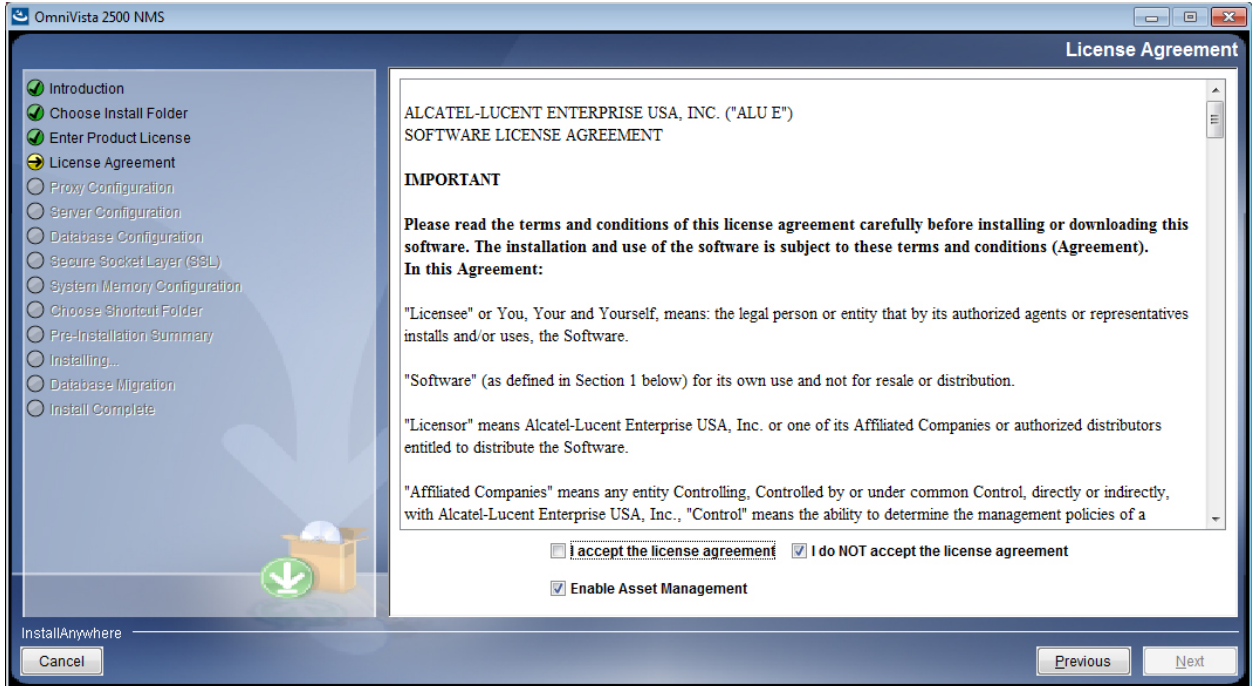
8. Proxy configuration. If using a proxy server, use this configuration screen to edit proxy settings for OmniVista 2500 NMS network connectivity. Click **Next** to continue.
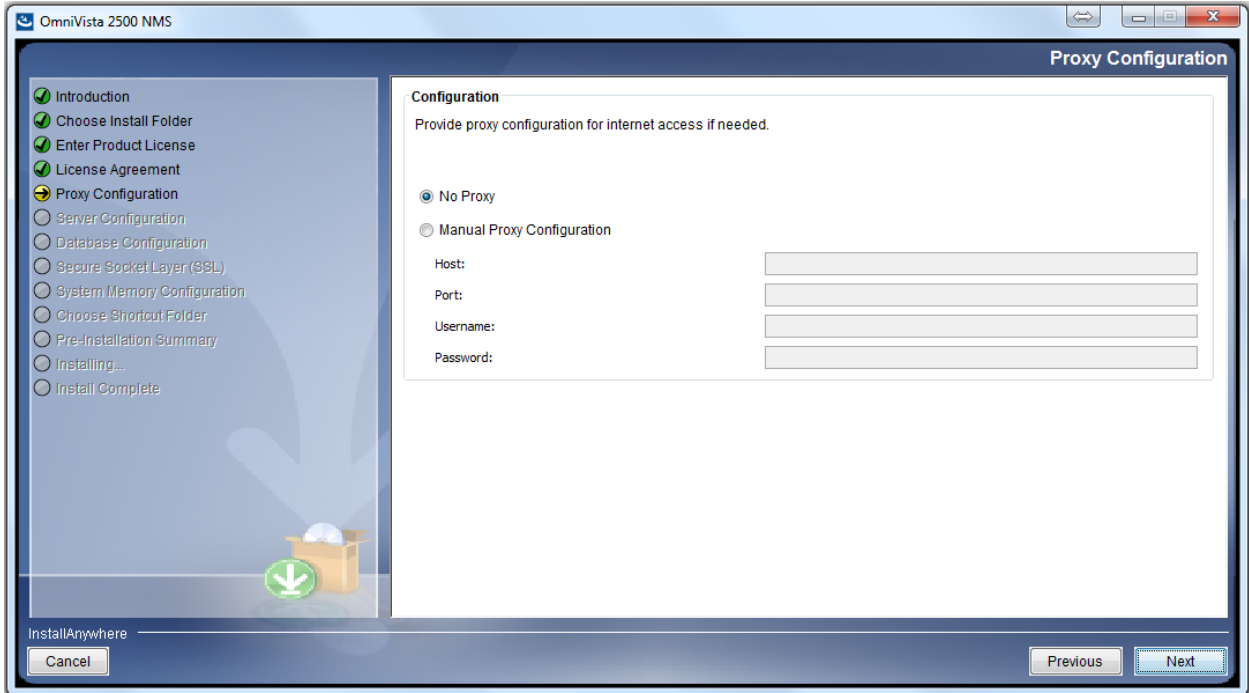
9. Server Configuration. This screen allows users to manually configure OmniVista 2500 NMS server information. Configure as required, or accept the default settings. Click **Next** to continue.

10. 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.

11. 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.
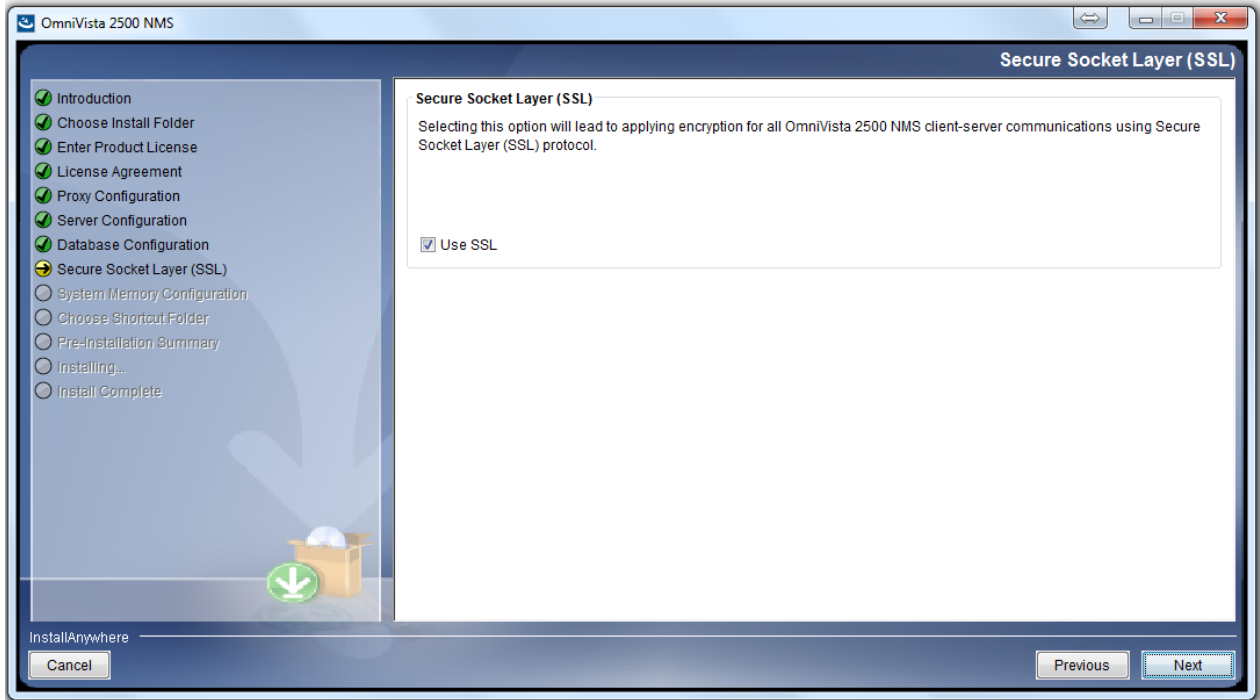
12. System Memory Configuration. This screen allows users to configure the maximum memory usage for OmniVista Core and Client Core Services. OmniVista displays minimum values in the recommended ranges. After configuring memory settings, click **Next** to continue.
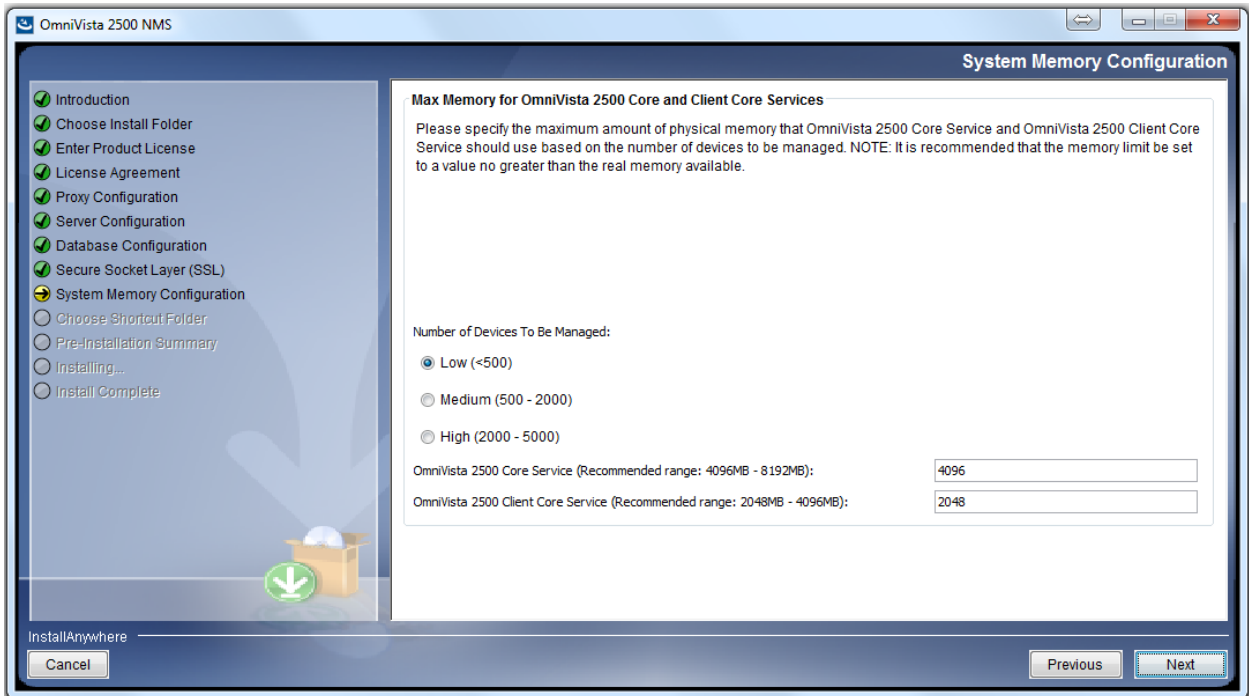
13. Choose Shortcut Folder. Select an option and click **Next** to continue.
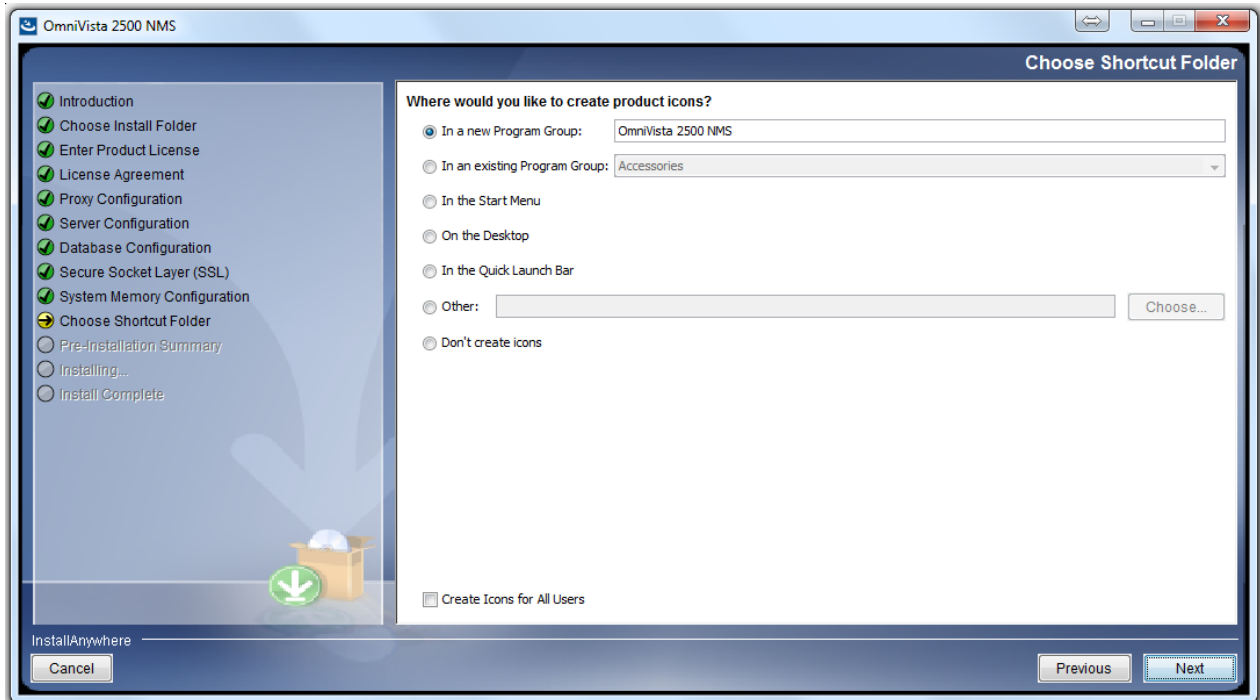
The "Choose Shortcut Folder" Screen **above** is displayed in a **Windows** installation. The screen **below** is displayed in a **Linux** installation.
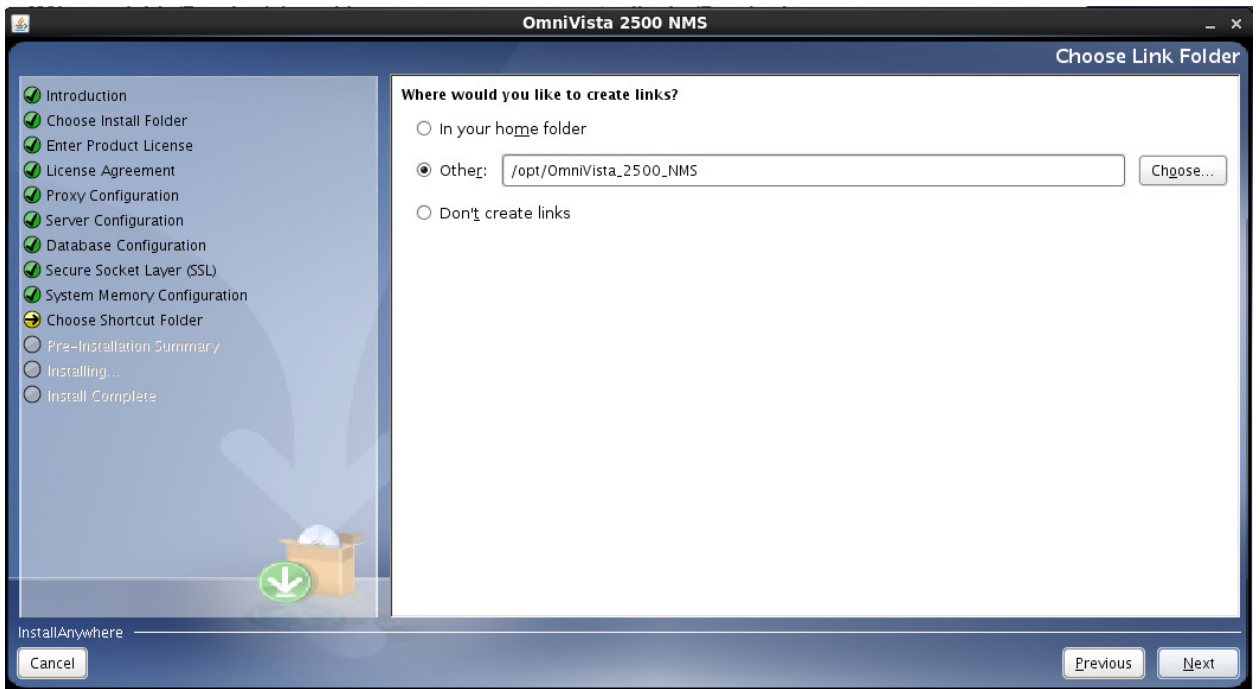
14. Pre-Installation Summary. The Pre-Installation Summary screen displays the configuration that will install on the OmniVista Server. Review the configuration summary carefully before clicking **Install**. If settings require revisions, click the **Previous** button to go back and edit the settings as needed.
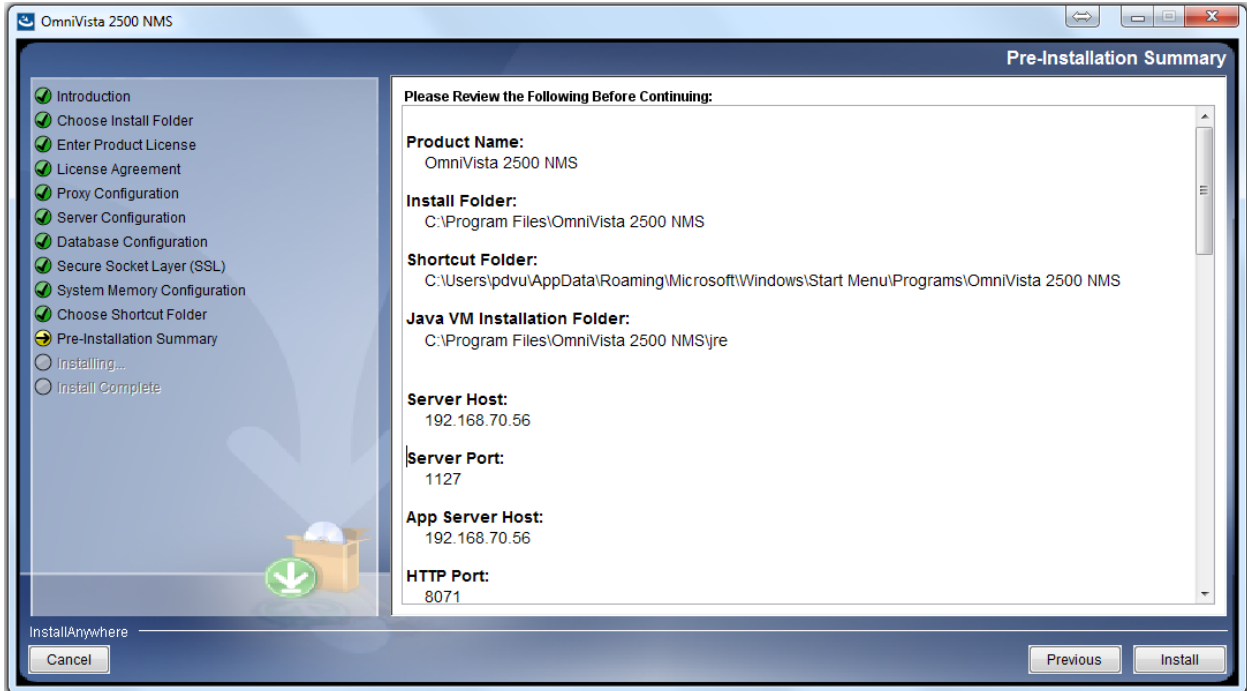
15. A progress bar displays as the installation begins. Note that it can take several minutes to finish the installation.
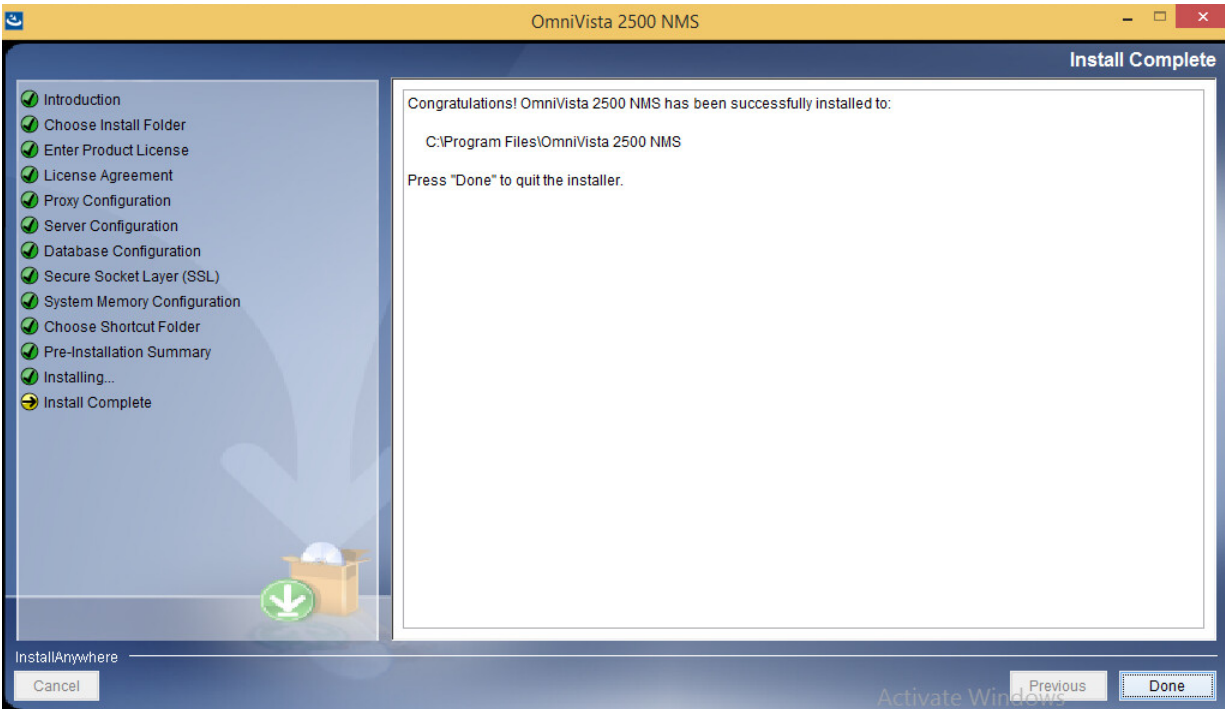
16. Configure the java settings as described below.

Configuring Java Settings

You must configure Java Control Settings as described below to launch OmniVista 2500 NMS java-based applications (e.g., Discovery, Topology) on an OmniVista Client. Note that Java v1.7 and v1.8 are both supported on OmniVista Clients. The screens in the instructions below are from a client with Java v1.8 installed. Most of the Java Windows are the same for v1.7 and v1.8. 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.
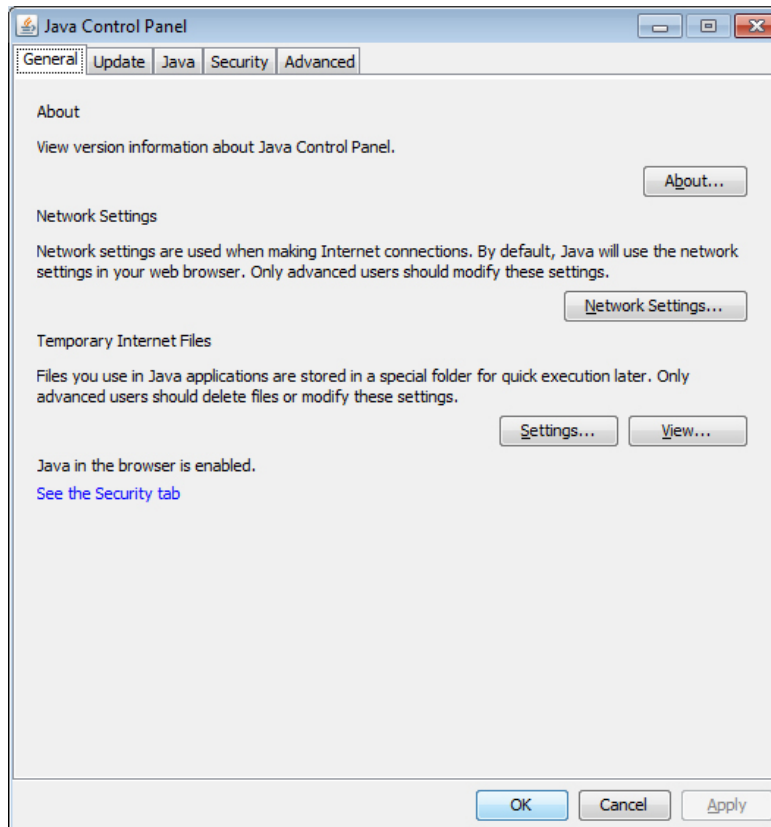
2. On the **General** Tab, click on the **Network Settings** button and configure the java-based application connection to the OmniVista Server.
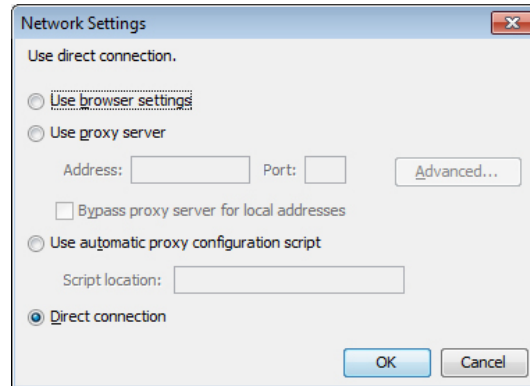
- **Use Browser Settings:** Select to use the browser default browser settings.

- **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 want to use a Proxy 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 1.7 Clients -** Set the Security Level Slider to **Medium**.

- **Java 1.8 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 1.7 Client
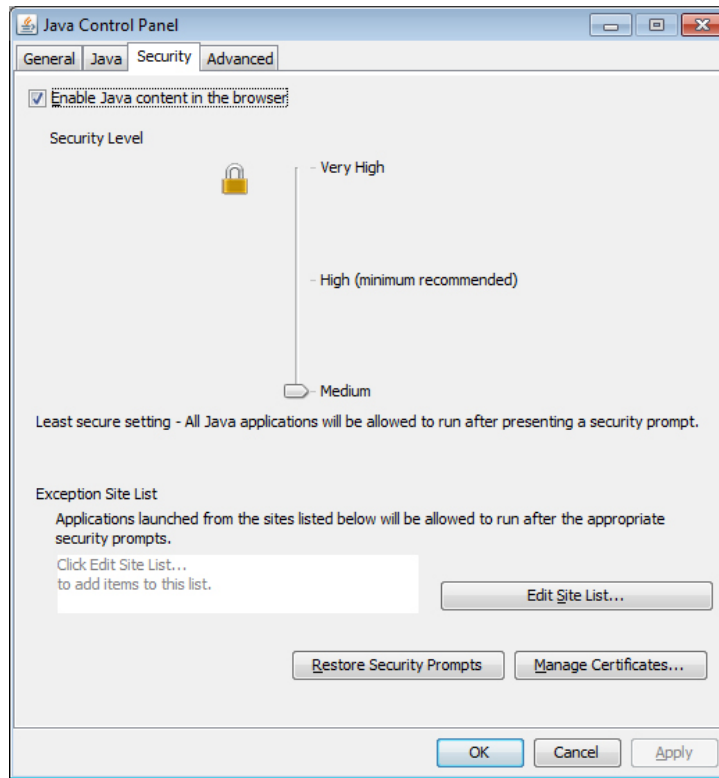
Security Tab - Java 1.8 Client
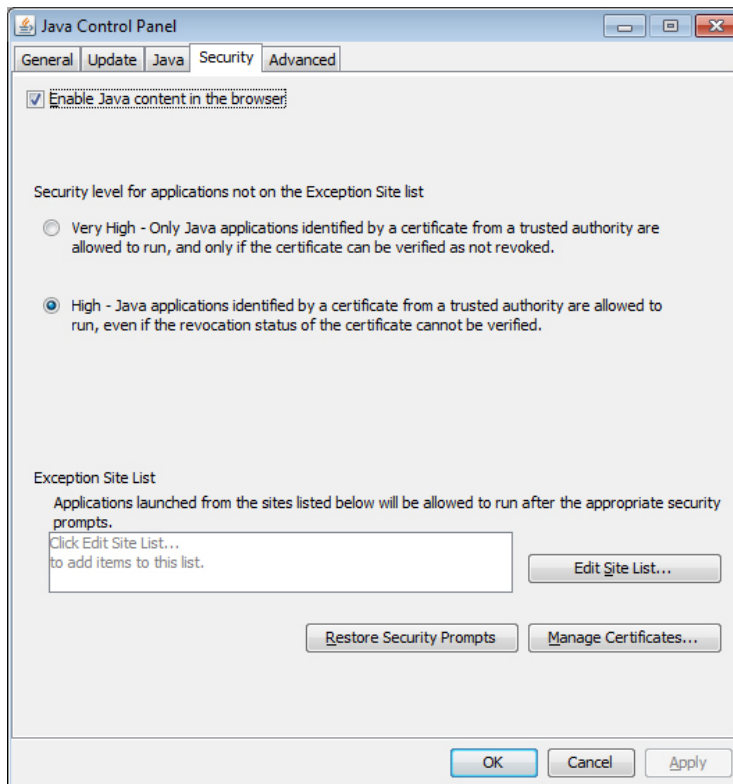
Launching OmniVista 2500 NMS

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

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 described below.

Installing Security Certificates (Windows)

Install the Web Security Certificate and the Java Security Certificate as described below.

Installing the Web Security Certificate

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. Browse to the following directory on your system: \OmniVista 2500 NMS\ThirdParty\openssl\bin.

2. Right-click on the **bin** folder and select **Properties** from the list of options to bring up the bin Properties Window, then click the **Security** tab.
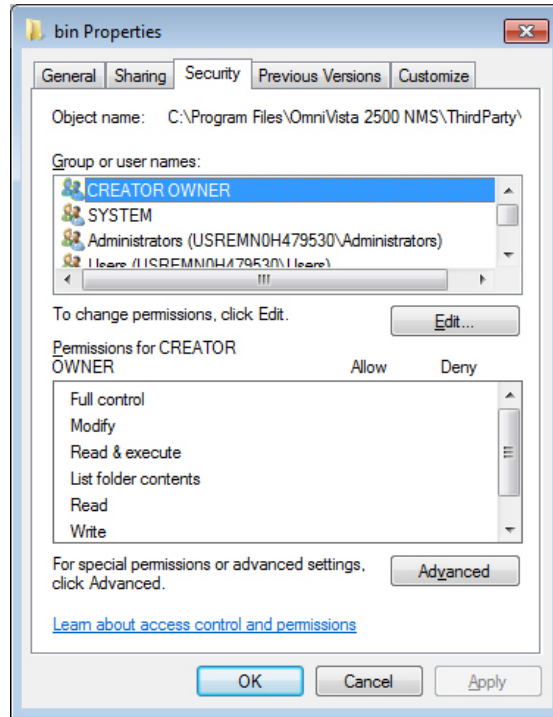
3. Select **Users** in the "Group or user names" list and click **Edit**. The Permissions for bin Window appears.
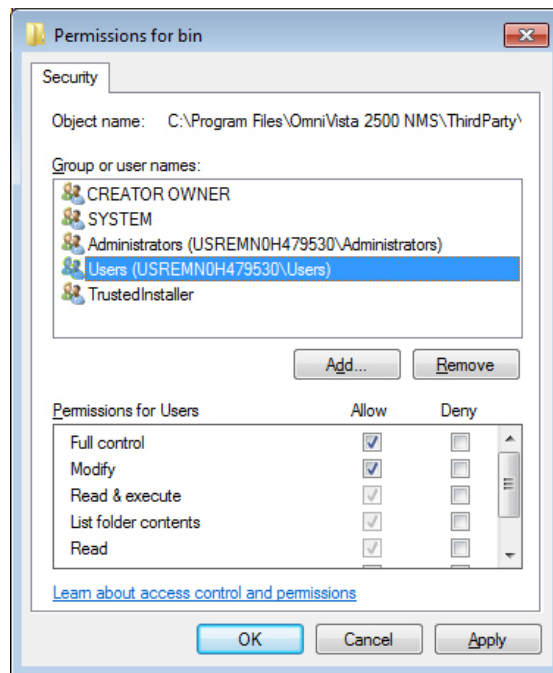
4. Make sure "Users" is still selected. In the "Permissions for Users" list, click on the **Allow** box next to **Full control**, and click **Apply**. Note that "Allow" is also automatically selected for **Modify**.

5. Click **OK** to exit the **bin Properties** window.

6. 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*

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

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

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

9. Generate a self-signed certificate:

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

10. Once you have created the certificate, continue to Importing the Certificate.

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. Start by opening an OpenSSL utility on your system. If you require the utility, downloads are available online.

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 scripts directory, located in the **OmniVista 2500 NMS** Program File folder. Run it with Administrator privilege.

2. Input the location of the SSL certificate.

3. Input the location of the private key.
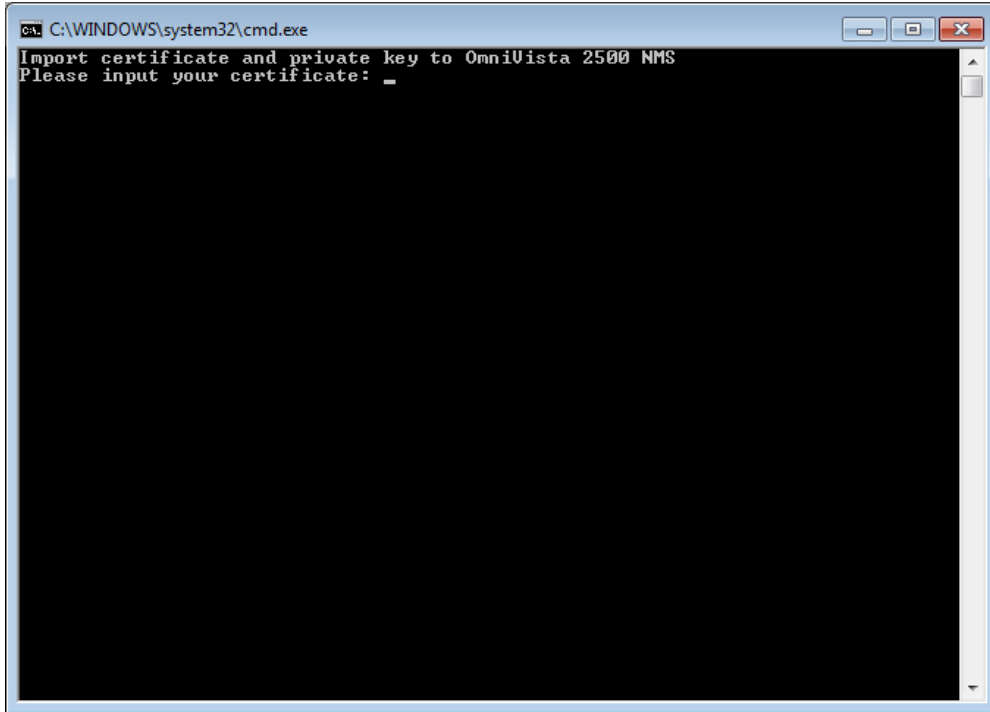
4. Stop Apache Tomcat using the Watchdog CLI.

The Watchdog CLI command is available inside Watchdog directory under the install directory base (chosen during Installation).

   watchdog-cli stopservice –n ovtomcat

5. Restart Apache Tomcat using the Watchdog CLI.

   watchdog-cli startservice –n ovtomcat

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

Installing the Java Security Certificate

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 1.8**. The Certificate is not required on clients running Java 1.7; 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 1.7**.

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.

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 1.7 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**.

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. Use Explorer to locate the Certificate file (ov.cer) that you downloaded in Step 3, and double click on the file.

12. The certificate's General Information window appears.
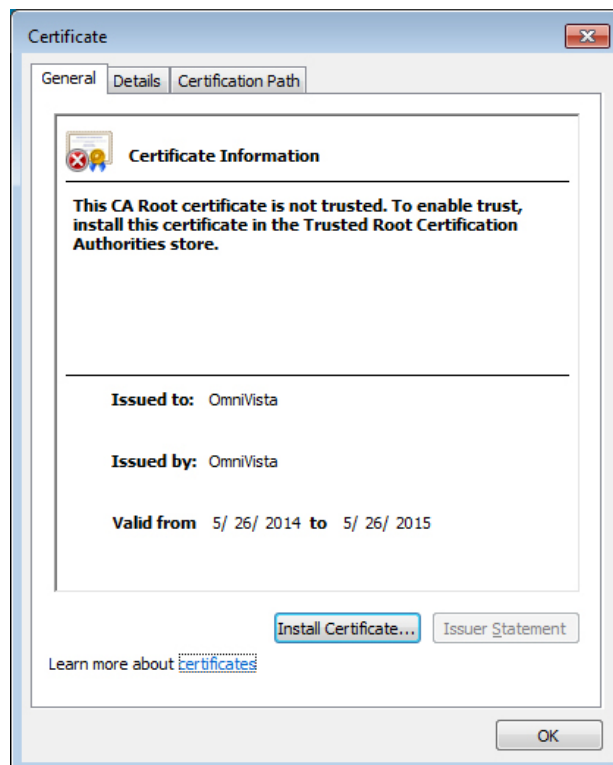
13. Click the **Install Certificate** button. The first screen of the Certificate Import Wizard appears.

Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

< Back   Next >   Cancel

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

Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

◉ Place all certificates in the following store

Certificate store:

[   ]   Browse...

Learn more about certificate stores

< Back   Next >   Cancel

15. Select the "Place all certificates in the following store" radio button, then click **Browse**. The Select Certificate Store window appears.
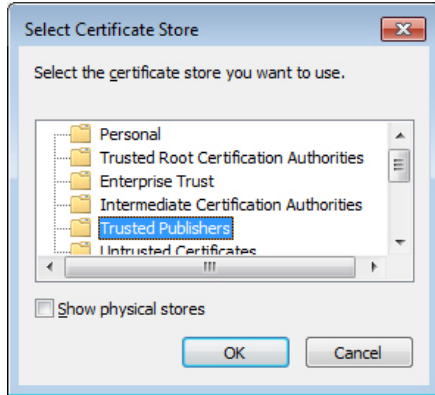
16. Select the **Trusted Publishers** Folder and click **OK**, then click **Next**. The final Wizard screen appears.
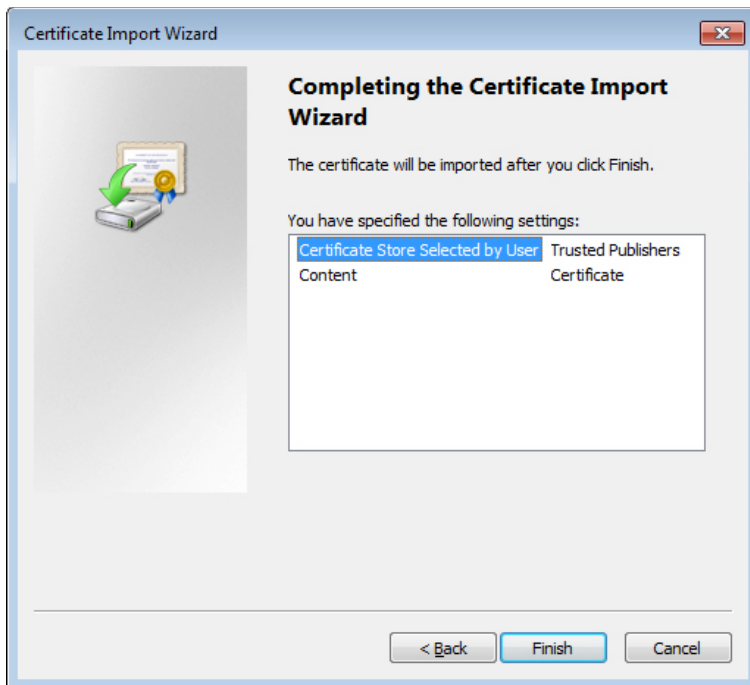
17. Click the **Finish** button.

Installing Security Certificates (Linux)

Install the Web Security Certificate and the Java Security Certificate as described below.

Installing the Web Security Certificate

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 <u>Importing the Certificate</u>, 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. 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. Generate a self-signed certificate:

> *openssl x509 -req -days 365 -in server.csr -signkey server.key –out server.crt*

5. Once you have created the certificate, continue to <u>Importing the Certificate</u>.

### *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. Start by opening an OpenSSL utility on your system. If you require the utility, downloads are available online.

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 <u>Importing the Certificate</u>.

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** Program File folder. Run it with root privilege.

2. Input the location of the SSL certificate.

3. Input the location of the private key.
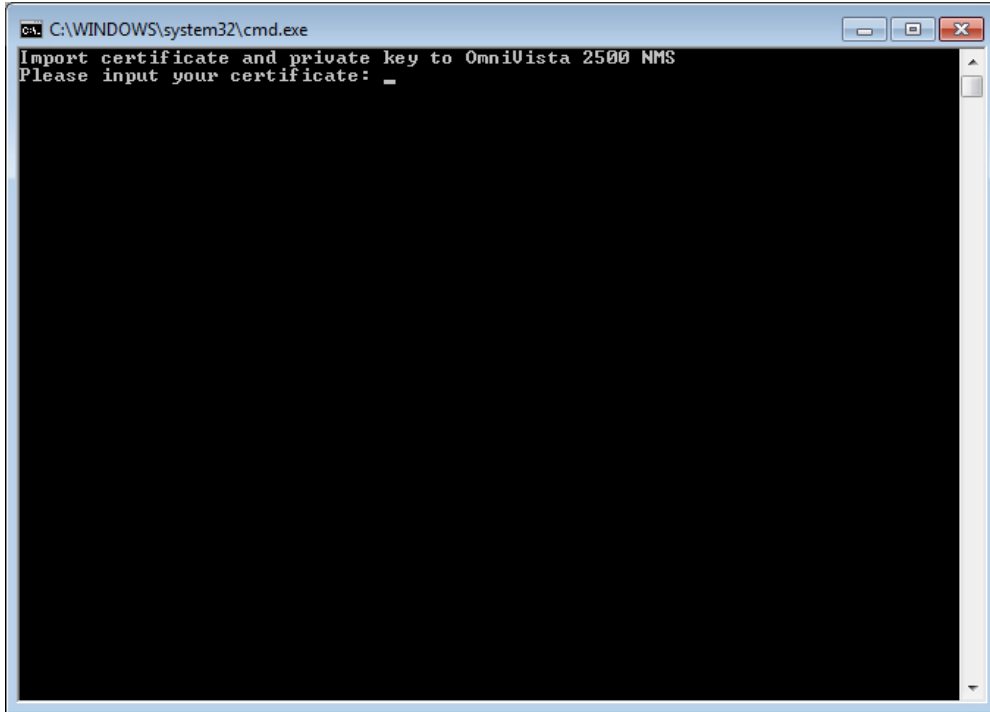
4. Stop Apache Tomcat using the Watchdog CLI.

The Watchdog CLI command is available inside Watchdog directory under the install directory base (chosen during Installation).

watchdog-cli.sh stopservice –n ovtomcat

5. Restart Apache Tomcat using the Watchdog CLI.

watchdog-cli.sh startservice –n ovtomcat

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

Installing the Java Security Certificate

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 1.8**. The Certificate is not required on clients running Java 1.7; 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 1.7**.
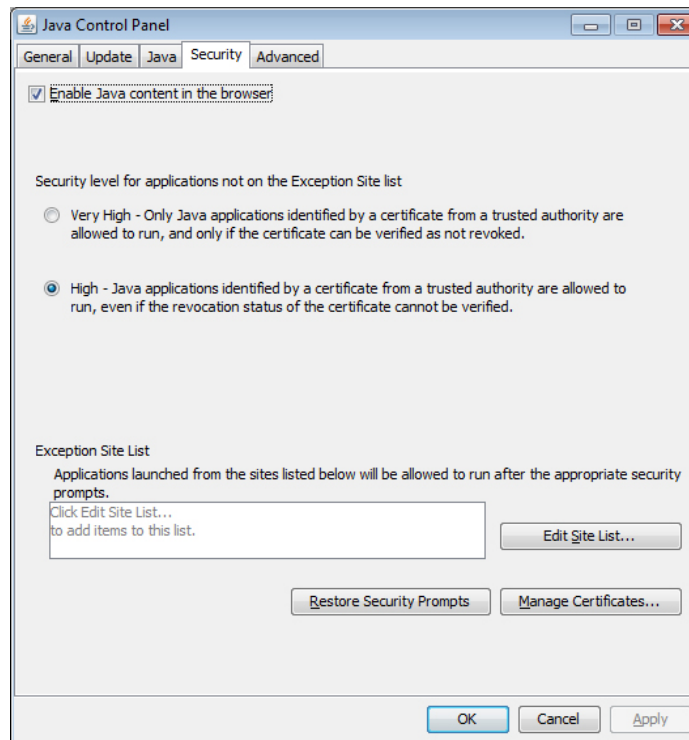
1. Log into OmniVista 2500 NMS.

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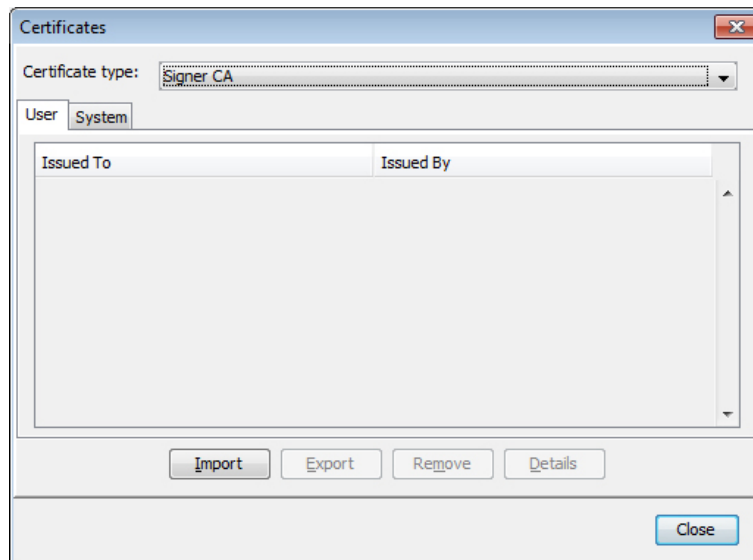
3. Press **Enter** to download the certificate.

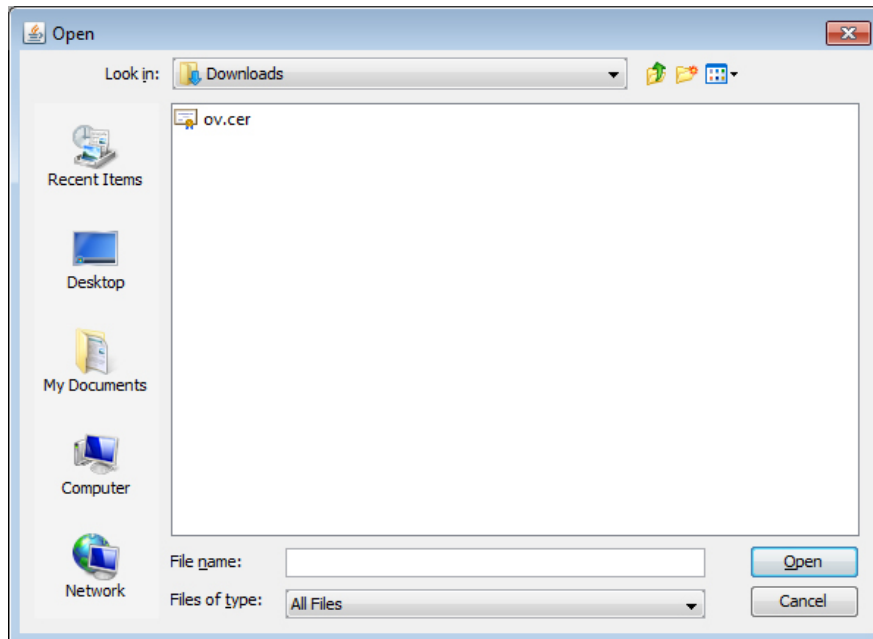**4.** Open the **Java Control Panel** - Start > Control Panel > Java.

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 1.7 clients is slightly different. However, you will still click on the **Manage Certificates** button to bring up the Certificates window.*
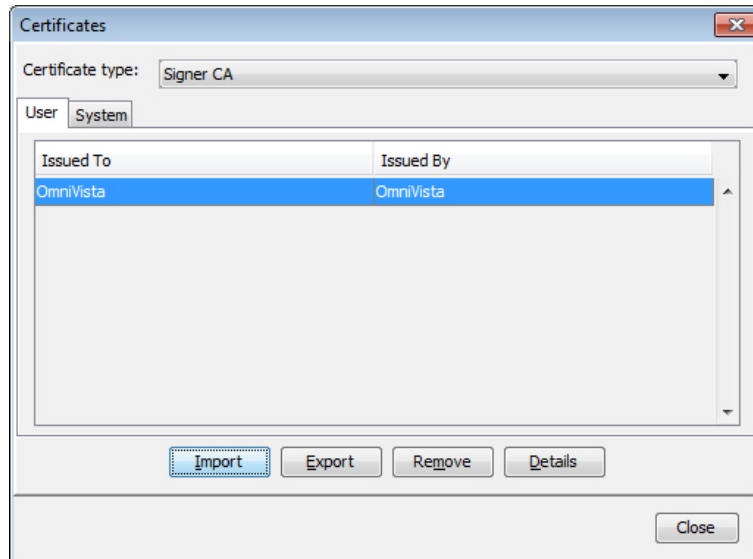

7. In the **Certificate Type** pull-down, select **Signer CA**, then click **Import**.

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. Use the "ca-certificates" package to install the Certificate (ov.cer) to the Trusted Source Directory.

1. Make sure you have the "ca-certificates" package installed.

   rpm –qa | grep certificate

2. If you **do** have the package installed, **go to Step 3**. If not, install it using the following command.

   yum install ca-certificates

3. Enable the dynamic CA configuration feature:

   update-ca-trust enable

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

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

5. Extract the file:

   update-ca-trust extract

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.

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.

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 for 3.5.7 and 4.1.1 GA – 4.1.2.R01 GA.

Upgrading from 3.5.7

Follow the steps below to upgrade from OmniVista 3.5.7. 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. See the Server Backup Application On-Line Help for more information.

3. Login to the OmniVista 2500 NMS 4.1.2.R01 Web UI.

4. Open the Server Backup application (**Administrator > Server Backup**). Keep this application window open.

5. Open the Watchdog application **(Administrator > Control Panel > Watchdog)**.

6. On the Watchdog Screen, click on **OmniVista Client Core Service** to open the service's details panel, then click on the **Stop Service Tree** button.

   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, perform a restore using the OmniVista 3.5.7 backup file you created. See the Server Backup Help for information on performing the backup.

8. 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

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

Upgrading from 3.5.7 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. 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.

4. Perform a fresh Installation of OmniVista 2500 NMS 4.1.2.R01 VA.

5. Login to the OmniVista 2500 NMS 4.1.2.R01.Web UI.

6. Open the Server Backup application (Administrator > Server Backup). Keep this application window open.

7. Open the Watchdog application (Administrator > Control Panel > Watchdog).

8. On the Watchdog Screen, click on **OmniVista Client Core Service** to open the service's details panel, then click on the Stop Service Tree button.

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.

9.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 /home/admin/omnivista/ng_shared/ temp/admin Directory. See the Server Backup Help for information on performing the restore.

10. After the OmniVista Services startup, you will be able to login to the Web UI of OmniVista 2500 NMS VA again.

Upgrading from 4.1.1 GA – 4.1.2.R01 GA

Follow the steps below to upgrade from OmniVista 4.1.1 GA - 4.1.2.R01 GA. If you are upgrading to a Virtual Appliance installation, click here for procedures.

1. On the existing installation of OmniVista 2500 NMS, navigate to the following directory: <OmniVista installation path>/scripts.

2. Run the "backup.sh" or "backup.bat" (in case of Windows installations) file found in that directory.

3. Enter the output path and file name for the backup file. Wait for a successful backup to complete.

4. Perform a fresh Installation of OmniVista 2500 NMS. If you are installing OmniVista 2500 on the same system as the one that had the previous version, uninstall the previous version first.

5. Copy the backup file to the new installation of OmniVista 2500 NMS and navigate to the <OmniVista installation path>/scripts Directory.

6. Run the "restore.bat" (Windows) or "restore.sh" (Linux) file found in that directory.

7. Enter the path of the backup file saved at Step 3 above.

8. After the OmniVista Services startup, you will be able to login to the Web UI of OmniVista 2500 NMS VA again.

Upgrading from a VA Installation to a VA Installation

To upgrade from an old VA installation to a new VA installation, backup the previous OmniVista 2500 NMS VA installation and restore it to the new OmniVista 2500 NMS VA installation. Click here for backup/restore procedures. After a successful restore, reboot the Virtual Appliance from console.

Deploying OmniVista 2500 NMS as a Virtual Appliance

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

- VMware ESXi 5.0 and above
- 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.

Deploying the Virtual Appliance

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

1. Log into vCenter and open the vSphere client.

2. Select **File > Deploy OVF Template**. The Deploy OVF Template Wizard appears.
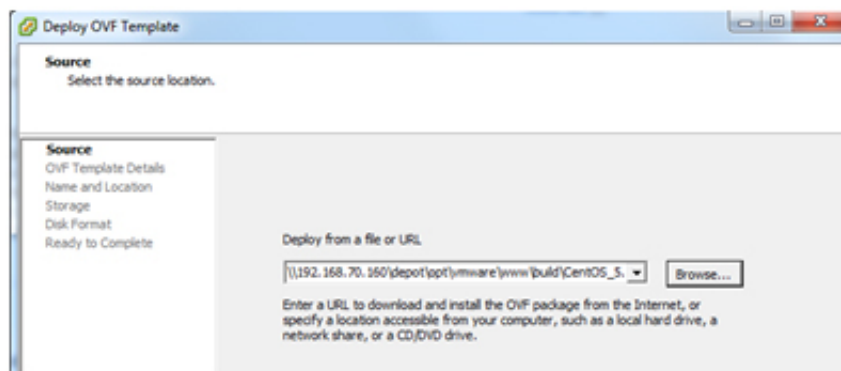
3. Follow additional steps in the Virtual Appliance deployment wizard. The wizard may prompt the following steps:

- Review VM details.
- Review and accept end user license agreement.
- Specify a name and location for the deployed template.
- Select the host or cluster where the template is to be deployed
- Storage location of VM files.
- Disk formatting (Thin or Thick Provision). (**Thick** provision is recommended.)
- Network mapping.

4. If the new Virtual Appliance was not powered on via the deployment wizard, power on the VM now.

Launching the Console and Setting a Password

1. Launch the Console for the new Virtual Appliance. (In vCenter, this can be done by right-clicking on the OVF file from the navigation tree and selecting **Open Console**.)

2. Specify a new password for the administrative password, then re-enter to confirm the new password.

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

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

```
* IPv4 Address: 192.168.70.101                                                 *
* NetMask: 255.255.255.0                                                        *
*                                                                              *
* IPv6 Address: 2001::101                                                       *
* Prefix: 64                                                                    *
*                                                                              *
* HTTP Port: 8071                                                              *
* HTTPS Port: 8072                                                             *
* Data Port: 1127                                                              *
*                                                                              *
* Default gateway v4: 192.168.70.1                                             *
* Default gateway v6: 2001::1                                                   *
*                                                                              *
* Hostname: hostnameva                                                         *
*                                                                              *
* DNS Server 1: 192.168.1.3                                                    *
* DNS Server 2: 192.168.1.11                                                   *
*                                                                              *
* Proxy Server 1: http_proxy=http://tma.com.vn:8080                           *
*                                                                              *
* Timezone: Asia/Ho_Chi_Minh                                                   *
*                                                                              *
********************************************************************************
Press Enter to continue. . .
```

Configuring OmniVista 2500 NMS

1. Enter **2** at the prompt 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, skip 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 [172.17.2.161]: 192.168.70.101
Please input Netmask [255.255.255.0]:
Do you want to use IPv6 (y/n) [y]: y
Please input IPv6 []: 2001::101
Please input Prefix [64]:

Are you sure to set:
        IPv4: 192.168.70.101
        Netmask: 255.255.255.0
        IPv6: 2001::101
        Prefix: 64
(y/n): _
```

7. Enter **y** to confirm the settings. Press **Enter** to access the next option.

8. 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 keep default values. New port values must be unique (i.e., they must differ from any previously-configured ports).

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

Configuring the Default Gateway

1. At the Main Menu prompt, enter **Option 3** 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 []: 192.168.70.1
Please input IPv6 Default Gateway []: 2001::1

Are you sure to set:
        Default Gateway v4: 192.168.70.1
        Default Gateway v6: 2001::1
(y/n): _
```

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

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

Configuring the Hostname

1. At the Main Menu prompt, enter Option **4** to configure the hostname.

2. Enter a hostname.

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

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

3. Enter **y** 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 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 [192.168.2.3]: 192.168.1.11

Are you sure to set:
        DNS Server 1: 192.168.1.3
        DNS Server 2: 192.168.1.11
(y/n): _
```

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

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

Setting the Time Zone

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

```
========================================================================
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.

```
Please select a country.
 1) Afghanistan          18) Israel              35) Palestine
 2) Armenia              19) Japan               36) Philippines
 3) Azerbaijan           20) Jordan              37) Qatar
 4) Bahrain              21) Kazakhstan          38) Russia
 5) Bangladesh           22) Korea (North)       39) Saudi Arabia
 6) Bhutan               23) Korea (South)       40) Singapore
 7) Brunei               24) Kuwait              41) Sri Lanka
 8) Cambodia             25) Kyrgyzstan          42) Syria
 9) China                26) Laos                43) Taiwan
10) Cyprus               27) Lebanon             44) Tajikistan
11) East Timor           28) Macau               45) Thailand
12) Georgia              29) Malaysia            46) Turkmenistan
13) Hong Kong            30) Mongolia            47) United Arab Emirates
14) India                31) Myanmar (Burma)     48) Uzbekistan
15) Indonesia            32) Nepal               49) Vietnam
16) Iran                 33) Oman                50) Yemen
17) Iraq                 34) Pakistan
#? _
```

4. If prompted, enter the numeric value for the specific time zone within the country.

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

Configuring a Route

1. At the Main Menu prompt, enter option **8** to begin configuring a route.

2. Configure an IPv4 route by entering **1** at the command prompt.

```
=================================================================================
Configuring Route...
=================================================================================
*********************************************************************************
*  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** to confirm the settings. Press Enter to return to the Configure Route menu. (To exit, select option 0.)

```
Please input Subnet: 1.1.1.0
Please input Netmask: 255.255.255.0
Please input Gateway: 192.168.70.2

Are you sure to set:
        Route V4: 1.1.1.0/255.255.255.0 via 192.168.70.2
(y/n): _
```

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** to confirm the settings. Press **Enter** to return to the Configure Route Menu.

8. Enter **0** to exit to the Main Menu.

Activating the Software License

All users are required to have a valid Core License and must accept the Alcatel-Lucent end user license agreement (EULA). (VMM and Application Visibility licenses are optional).

1. Once the OmniVista 2500 NMS has been configured, users are prompted for the Core License number. Enter the license at the prompt and press **Enter**.

```
================================================================================
License for OmniVista 2500 NMS...
================================================================================


Please input Core License:
```

2. Accept the Core License terms and conditions. (Press **Enter** or the down arrow to scroll through the terms and conditions. Press **Enter** to display the "Accept End user license agreement" prompt, then enter **y** to accept.)

```
ALCATEL-LUCENT ENTERPRISE USA, INC. ("ALU E")
SOFTWARE LICENSE AGREEMENT

IMPORTANT

Please read the terms and conditions of this license agreement carefully before
installing or downloading this software. The installation and use of the softwar
e is subject to these terms and conditions (Agreement).
In this Agreement:

"Licensee" or You, Your and Yourself, means: the legal person or entity that by
its authorized agents or representatives installs and/or uses, the Software.

"Software" (as defined in Section 1 below) for its own use and not for resale or
 distribution.

"Licensor" means Alcatel-Lucent Enterprise USA, Inc. or one of its Affiliated Co
mpanies or authorized distributors entitled to distribute the Software.

"Affiliated Companies" means any entity Controlling, Controlled by or under comm
on Control, directly or indirectly, with Alcatel-Lucent Enterprise USA, Inc., "C
ontrol" means the ability to determine the management policies of a company or o
ther entity through ownership of a majority of shares, by control of the board o
f management, by agreement or otherwise
52_
```

Configuring Asset Management Settings

1. Asset Management posts periodic switch inventory information to the Asset Management web portal. To enable this feature, enter **y** at the command prompt.

2. To enable a Proxy for the Asset Management feature, enter **y** at the "enable Proxy" at the command prompt. Otherwise, enter **n** to bypass Proxy configuration and skip to "Activating Optional Software Licenses."

3. If configuring a Proxy, enter the host name, port, user name and password.

```
Copyright 2014 Alcatel-Lucent Enterprise USA, Inc.

Accept End user licensing agreement (y/n): y
New Core license is updated

Would you like to enable Asset Management feature (y/n) [n]: y

Would you like to enable Proxy for Asset Management feature (y/n) [n]: y
Please input Asset Management proxy Host: omnivista
Please input Asset Management proxy Port: 5678
Please input Asset Management proxy Username: admin
Please input Asset Management proxy Password:
Proxy for Asset Management feature is saved
Do you want to add VMM License [y/n] (y): n
```

Activating Optional Software Licenses

You can also activate optional VMM and Application Visibility licenses via the command prompt.

- To activate a VMM license, enter **y** at the command prompt and enter the VMM license key in the command line. To skip this step, enter **n** at the command prompt.

- To activate an Application Visibility license, enter **y** at the command prompt and enter the license key in the command line. To skip this step, enter **n** at the command prompt.

    Note: Application Visibility is being introduced with this release as an **early availability feature**. It is available for demonstration purposes only but is not officially supported. Contact the OmniVista Product Line Manager for an Application Visibility Evaluation License. Contact Customer Support for the AOS 7.3.3.R01 and AOS 8.1.1.R01 Builds that support this application.

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.

Using the VM Appliance Menu

Following memory configuration, an installation summary screen displays, followed by the OmniVista 2500 NMS VM installation diagnostics.

```
********************************************************************************
* Deploying the appliance...please wait                                       *
********************************************************************************
* Product Name: OmniVista 2500 NMS                                            *
* Revision: 4.1.2                                                             *
* Build Number: 10                                                            *
* Build Date: 08/29/2014                                                      *
*                                                                             *
* Server IPv4: 192.168.70.196                                                 *
* Server IPv6: 2001::196                                                      *
*                                                                             *
* HTTP Port: 8071                                                             *
* HTTPS Port: 8072                                                            *
* Data Port: 1127                                                             *
********************************************************************************
Press any key within 12s to continue...
```

Following diagnostics, the Virtual Appliance menu displays. The menu provides the following options:

- 1: Configure the Virtual Appliance
- 2: Run Watchdog CLI command
- 3: Update the Virtual Appliance
- 4: Backup/Restore OmniVista 2500 NMS
- 5: Log out of the Virtual Appliance
- 6: Reboot the Virtual Appliance
- 0: Power off the Virtual Appliance

```
********************************************************************************
* 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? _
```

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 an option to **Configure the Swap File**. For menu options 1 through 8, refer to the sections above. To configure a Swap file, begin by entering **9** at the command prompt.

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. User needs to input version.
- Option 0: Exit menu

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

```
Type your option? 1

Current version of Virtual Appliance:
Version - Build 87
Description - Enterprise OmniVista 2500 NMS
```

```
Type your option? 2

Available updates of Virtual Appliance:

Checking for available updates, this process can take a few minutes.......
Available Updates -
   No available updates found
```

```
Type your option? 3

Please type version to update and press <Enter>:
```

Backing Up or Restoring OmniVista 2500 NMS

Follow the steps below to backup or restore OmniVista 2500 NMS.

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

Option 1: Backup OmniVista 2500 NMS

```
Enter base name (default is "ov2500nms"):
Stopping services...
Backing up data...
Generating backup file...
Starting services...

Finish ov2500nms_2014-09-05--11-03
```

1. Enter the base name of the backup files. If no base name is specified, "ov2500nms" will be used as the default base name.

2. Stop all services.

3. Create the backup files. The backup filename is combination of the base name and time, with the following format <base name>_yyyy-MM-dd--HH-mm. A backup includes OV2500 data backup (.osb), MongoDB data backup (.mgb) and license data backup (.lic).

4. Start all services.

Option 2: Restore OmniVista 2500 NMS

```
Type your option? 2

Backups available:
        [1] ov2500nms_2014-09-05--11-03
Choose a backup file to restore (choose 0 to exit): 1
Are you sure to restore from
        [1] ov2500nms_2014-09-05--11-03
(y/n): y
Stopping services...
Extracting backup file...
Restoring data...
Do you want to restore license information? (y/n): y
Restoring license...
Starting services...
Finish ov2500nms_2014-09-05--11-03
```

1. Enter "Backups available" to display the list of available backups.

2. Enter the backup number (choose 0 to exit).

3. Enter **y** to confirm the restore.

Part No. 060403-10, Rev. B

4. Enter **y** to confirm the license information restore.

5. Start all services.

If OV2500 data backup (.osb) or MongoDB data backup (.mgb) is missed, a warning will be shown and you will have to confirm one more time.

Note that you can access the VA via FTP for copying backup files from/to the VA:

- FTP User: admin
- FTP Password: admin
- FTP Port: 8888
    Note: Includes data from OmniVista and mongodb servers.

Logging Out Of the Virtual Appliance

To log out of the VM and return to the admin login prompt, enter **5** at the command line. Confirm logout by entering **y**. Note that OmniVista functions continue following logout.

Rebooting the Virtual Appliance

To reboot the VM, enter **6** at the command line. 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.

Powering Off the Virtual Appliance

To power off the VM, enter 0 at the command line. 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.