Release Notes

for

OmniVista 2500 NMS Enterprise Version 4.2.1.R01

September 2016

Revision A

Part Number 033131-10

READ THIS DOCUMENT

Includes OmniVista 2500 NMS for VMware ESXi: 5.5 and 6.0

VirtualBox: 5.0.10

MS Hyper-V: 2012 R2

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

Table of Contents

Revision History

Release	Revision	Date	Description of Changes
4.2.1.R01	A	09/22/16	GA Release
4.1.2.R03	A	01/29/16	GA Release
4.1.2.R02	A	05/22/15	GA Release
4.1.2.R01	B	12/19/14	Maintenance Release
4.1.2.R01	A	10/24/14	GA Release
4.1.1	B	12/19/14	Maintenance Release
4.1.1	A	09/10/14	GA Release
3.5.7	B	04/21/14	Maintenance Release
3.5.7	A	01/27/14	GA Release

1.0 Introduction

OmniVista 2500 NMS Enterprise 4.2.1.R01 (OV 2500 NMS-E 4.2.1.R01) is installed as a Virtual Appliance, and can be deployed to these hypervisors: VMware ESXi, VirtualBox, and MS Hyper-V:

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

This document details known problems and limitations in OV 2500 NMS-E 4.2.1.R01, and workarounds are included. Please read the applicable sections in their entirety as they contain important operational information that may impact successful use of the application.

1.1 Technical Support Contacts

For technical support, contact your sales representative or refer to one of the support resources below. Alcatel-Lucent Enterprise Service and Support can be reached as follows:

- **North America:** 1-800-995-2696
- **Latin America:** 1-877-919-9526
- **European Union:** +800 00 200 100
- **Asia Pacific:** +65 6240 8484
- **Support E-Mail:** ebg_global_supportcenter@al-enterprise.com (non-critical technical questions)

  Support Site: https://support.esd.alcatel-lucent.com (customers with Alcatel-Lucent Enterprise service agreements can open cases 24 hours a day via this web page)

  Enterprise Site: http://enterprise.alcatel-lucent.com

1.2 Documentation

The user documentation is contained in the on-line help installed with this product. Click on the Help link (?) in the upper-right corner of a page to access the online help for the page.

1.3 New in 4.2.1.R01

Web Interface

OmniVista 2500 NMS now uses a web interface for all applications. The Web GUI is supported on the following browsers: Internet Explorer 10+ (on Windows client PCs), Firefox 26+ (on Windows and Redhat/SuSE Linux client PCs), and Chrome 26+ (on Windows and Redhat/SuSE Linux client PCs).

To launch OV 2500 NMS-E 4.2.1.R01, enter the IP address of the OmniVista Server in a supported web browser (e.g., *https://<OVServerIPaddress>*).

OmniVista 2500 NMS-E 4.2.1.R01 Installation

OV 2500 NMS-E 4.2.1.R01 is installed as a Virtual Appliance, and can be deployed on the following hypervisors: VMware ESXi, VirtualBox, and Hyper-V:

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

Detailed installation instructions are available in the *OmniVista 2500 NMS-E 4.2.1.R01 Installation Guide.*

> **Note:** OV 2500 NMS-E 4.2.1.R01 supports up to 10,000 managed devices (includes AOS, OAW, and Third Party devices).

OmniVista 2500 NMS-E 4.2.1.R01 External Repositories

OV 2500 NMS-E 4.2.1.R01 uses external repositories for Application Visibility Signature Files, ProActive Lifecycle Management (PALM), and the OmniVista 2500 NMS Software Repository which is used for OmniVista 2500 NMS software updates. The software update feature enables you to download the latest OmniVista 2500 NMS software upgrades directly from the repository. You can also configure an “update interval” to automatically notify you when an update is available.

> **Note:** If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.2.1.R01 to connect to the OmniVista 2500 NMS External Repository.

Applications

All of the OV 2500 NMS-E 4.2.1.R01 applications are now web-based (HTML 5). The following applications are included in OV 2500 NMS-E 4.2.1.R01:

Network

- Discovery
- Topology
- Locator
- Notifications
- VM Manager (VM Manager License required)
- Analytics
- Application Visibility

Configuration

- VLANs
- VxLANs
- IP Multicast
- CLI Scripting
- PolicyView

- SIP
- Captive Portal
- Groups
- Application Launch
- Report
- Resource Manager

Unified Access

- Unified Profile
- Unified Policy
- Multimedia Services (mDNS)
- Premium Services (BYOD)

Security

- Users and User Groups
- Authentication Servers
- Quarantine Manager

Administrator

- Control Panel
- Preferences
- Audit
- License

The following previously-supported Java applications are not included in OV 2500 NMS-E 4.2.1.R01:

- Access Guardian (now part of Unified Profile feature in Unified Access)
- Health
- Schedule
- Server Backup (perform a VM Snapshot to backup configuration)
- SecureView SA
- Statistics (Analytics application provides advanced analytics)

Application Changes

As mentioned earlier, all of the OmniVista 2500 NMS applications are now web-based (HTML 5). The following sections describe new application functions as well as application functions that have changed from previous releases.

Application Visibility

The Application Visibility Application is now included as part of the OV 2500 NMS-E 4.2.1.R01 Node Management License (Core License); and you no longer have to license individual devices. Supported devices are automatically licensed. Note that if you are upgrading from a

previous version of OmniVista 2500 NMS, Application Visibility and Analytics data will be retained.

> **Note:** Do **not** upgrade Signature Files directly on a switch. Always use OmniVista 2500 NMS to upgrade Signature Files.

Control Panel

The Control Panel application now includes a Scheduler feature that provides an overview of all currently Scheduled jobs (System Jobs and User-Defined Jobs), and is used to start/stop, edit, or delete a User-Defined Job. The Scheduler feature also provides a history of all completed Scheduler jobs. A new Session Management feature displays a list of all OmniVista 2500 NMS Client login sessions, and can be used to log out a session.

> **Note:** If you are upgrading from a previous installation, scheduled jobs will not be migrated. You must re-create any old scheduled jobs.

Discovery

The Discovery application uses Discovery Profiles to discover devices. A Discovery Profile contains the parameters that are used by OV 2500 NMS-E 4.2.1.R01 when performing a discovery (e.g., SNMP version used to discover devices, CLI/FTP passwords needed to connect to a device). The application now includes a list of all discovered devices, and an Inventory Screen that displays inventory information for any discovered network device (e.g., Model Type, Serial Number, AOS version, Firmware version). You can also create manual links between devices, and perform device operations (e.g., Poll, CLI Scripting, Reboot) in the Discovery application.

OmniVista 2500 NMS now supports SNMPv3 advanced authentication and privacy protocols.

Health and Statistics

The Health and Statistics applications have been discontinued. Users cannot monitor custom SNMP OIDs and their historical trends. However, the Analytics application provides advanced analytics, including Top N Ports based on utilization ratio, Predictive Analytics, Top N Applications, and Top N Clients.

Locator

Locator has the same level of support as in previous releases with the following changes:

- If you are upgrading from a previous installation, note that historical data will not be retained. History will start from day OV 2500 NMS-E 4.2.1.R01 is installed. The automatic Locator Poll will discover the latest data from the network.
- The Port Selection function in Browse is not available. The endstation search is performed on all ports of selected devices.

License

OV 2500 NMS-E 4.2.1.R01 has a single installer and single license. The Node Management License (Core License) licenses all OmniVista applications except Virtual Machine Manager (VMM). OmniVista has been certified to manage up to 10,000 devices (includes AOS and Third-Party Devices).

The VMM License licenses the OmniVista 2500 NMS Virtual Machine Manager (VMM) application. VMs can be deployed on VMware vCenters, Citrix XenServers, and MS Hyper-V Servers. OV 2500 NMS-E 4.2.1.R01 supports a mixture of Hypervisor types with no limit on the number of Hypervisors. However, the VM Manager application supports a maximum of 5,000 VMs from all Hypervisors. More than 5,000 VMs are allowed, however a warning message will be displayed and an entry will be written to the VMM Log File.

Preferences

The following preferences can be configured in the Preferences application:

- **User Settings -** These settings can be configured for each user.
  - **Locale -** Used to set a system-wide language and time/date format.
  - **Theme -** Used to set the color scheme and look of OmniVista 2500 NMS.
  - **Inactivity Timeout -** Used to set the Inactivity Timer. If there is no user activity within this timeframe, the user is logged off.
  - **Table/List View Mode -** Used to set the default display layout for all table/list screens in OmniVista 2500 NMS.
  - **Temperature Unit -** Used to set the temperature unit that will be displayed, when applicable, in OmniVista 2500 NMS (e.g., Centigrade or Fahrenheit).
  - **Device Naming -** Used to specify how devices are identified and displayed in OmniVista 2500 NMS (e.g., IP address, Device Name, DNS Name).
  - **Colors -** Used to configure the colors displayed in Dashboard Widgets for Network Status, Alarms, Quarantine Manager, and ProActive Lifecycle Management.
- **System Settings -** These settings are system-wide settings that are configured by a Network Administrator for all users.
  - **Branding -** Used to change the logo displayed on the OmniVista 2500 NMS user interface and the logo displayed on reports created in the Report application.
  - **Proxy -** Used to configure a Proxy for the OmniVista 2500 NMS Client.
  - **ProActive Lifecycle Management -** Used to enable/disable ProActive Lifecycle Management and manually upload information.
  - **Videos -** Used to specify the Alcatel-Lucent Enterprise YouTube Demo Playlist that will play when the "Videos" link at the top of the OmniVista 2500 NMS Screen is clicked.
  - **Email -** Used to specify the Simple Mail Transfer Protocol (SMTP) mail server that you want to use to send e-mails generated by OmniVista 2500 NMS.
  - **Install Zulu CEK-** Used to install the Zulu Cryptography Extension Kit (CEK). Required for SNMPv3 advanced encryption.

Application-specific preference settings (e.g., Locator, Notifications, Resource Manager), have been moved to a “Settings” screen within the application.

Resource Manager

If you are upgrading from a previous installation note that images are not retained. You will need to re-import the images. Also note that Inventory Reports and Auto Configuration Profiles are not retained. You will need to re-create them.

SIP

Historical call records data will not be retained after an upgrade. The latest network data will begin on the next automatic poll.

Topology

Like all applications, the Topology application is now web-based (HTML 5). Discovered devices are displayed in map view only (a List of Discovered Devices can now be viewed in the Discovery application). Pop-up menu functions that were available in the List of Discovered Devices and in maps (e.g., Poll, CLI Scripting, Reboot) are now performed by clicking on a device in the map and selecting a function from an Operations Panel on the right side of the map.

By default, all discovered devices are shown in the Physical Map. You can manually create custom maps and create dynamic maps that automatically update based on filters you create. Map layouts can be configured, and devices and links can be isolated/highlighted by device status, link type, and alarm type.

The following Topology features/functions have changed in this release.

- **List of Discovered Devices –** Discovered devices are displayed in map view only (a List of Discovered Devices can now be viewed in the Discovery application).
- **Device View Tabs –** Device View Tab information and functions are now available using the Topology map.
  - **Device Information –** Basic device information can now be accessed by selecting a device on the Topology map and viewing device information in the Details Panel on the right side of the screen. Functions such as saving and loading configuration files, are available by selecting a device and then selecting an operation from the Operations Panel in the right side of the screen.
  - **Device Module Information –** Device module information can now be accessed on the Inventory Screen in the Discovery application.
  - **Link Information –** Link information can now be accessed by clicking on a link in the Topology map and viewing information in the Details panel
  - **Additional Information –** You can also connect to a device for additional information by selecting a device and launching a webpage element manager (e.g., WebView). Select a device, then click on the “Webpage” operation.
  - **Ethernet OAM –** Not supported in this release.
  - **DCB –** Not supported in this release.
  - **SAA –** Not supported in this release.
  - **SPB –** Not supported in this release.
- **Pop-Up Menu Functions –** Pop-up menu functions that were available in the List of Discovered Devices and in maps (e.g., Poll, CLI Scripting, Reboot) are now performed by selecting a device in the Topology map and selecting a function from an Operations Panel on the right side of the map.
- **Built-In MIB Browser –** The built-in MIB Browser is no longer available in Web UI. If necessary, use an external MIB Browser.

Users and User Groups

The Users and User Groups application now enables you to configure role-based access to OmniVista 2500 NMS and network resources. A User Role specifies access/rights to specific OmniVista 2500 NMS applications and network devices. You can also limit user access to specific devices for VLAN and VXLAN configuration. For the most part, configuring Users and User Groups is all that will be required. However, User Roles enable you to configure very specific access for a user.

Unified Access

All AOS devices and OAW devices are now supported in Unified Access. The Access Guardian 1.0 application functionality (Java application) has been moved to the Unified Profile feature of the Unified Access application. UNP Profile Templates are configured and assigned to network devices. A “Device Config” Screen has been added to display UNP Profile configuration on specific devices. A user can also edit UNP Profiles on specific devices, and delete profiles from specific devices. In addition to mapping Access Role Profiles and Access Classification Profiles to VLAN’s, users can now map those profiles to an SPB Profile, a VXLAN Profile, or a Static Service Profile.

> **Note:** Host Integrity Check (HIC) server configuration has been discontinued. SPB Information and configuration is not available. Customize Access Guardian Policy is not available, OV 2500 NMS-E 4.2.1.R01 only supports authentication flows in Unified Access Workflows.

VM Manager

VM Manager now supports the following Hypervisors for Virtual Machines: VMware ESXi, Citrix XenServer, and Hyper-V:

- VMware ESXi: 5.5 and 6.0
- Citrix XenServer 6.2 and 6.5
- MS Hyper-V: 2012 R2.

VM Manager now supports a mixture of Hypervisors (vCenters, XenServer , Hyper-V Servers) in the same configuration.

> **Note:** If you are upgrading from a previous installation, historical VM data is not retained. The automatic poll will discover all latest data from the network.

Device/Release Support

AOS 6.7.1.R02

OmniVista 2500 NMS now supports AOS 6.7.1.R02 on all previously supported OS6250, OS6350, and OS6450 Switches, plus the following new switches:

- OS6450-M/X/MX.

AOS 7.3.4.R02

OmniVista 2500 NMS now supports AOS 7.3.4.R02 on OS10K and OS6900 Switches.

AOS 8.2.1.R01

OmniVista 2500 NMS now supports AOS 8.2.1.R01on OS6860 and OS 6860E Switches.

AOS 8.3.1.R01

OmniVista 2500 NMS now supports AOS 8.3.1.R01 on all previously-supported OS10K, OS6860/6860E, and OS6900 Switches, as well as on the following new switches:

- OS9900
- OS6865-P16.

OAW 6.4.3

OmniVista 2500 NMS now supports OAW 6.4.3 on OAW-4030, OAW-4704, and OAW-4604 devices.

OAW 6.4.3.1

OmniVista 2500 NMS now supports OAW 6.4.3.1 on IAP-105 and IAP-205 devices.

OAW 6.3.2.6

OmniVista 2500 NMS now supports 6.3.2.6 on IAP-225 devices.

1.4 Feature Set Support

1.4.1 Element Manager Integration

To provide additional support for supported devices with different architectures, OmniVista 2500 NMS can integrate with independent Element Managers to provide direct access to devices. Element Managers enable you to access, configure, and gather statistics from individual devices. The Element Managers currently supported in OmniVista 2500 NMS are listed below.

Element Managers are platform independently and are interfaced through a web browser. They can be accessed in the **Topology** application by selecting a device in a Topology map and clicking on the **Webpage** operation in the Operations Panel on the right side of the screen.

Element Manager	Supported Devices	Description
WebView	• All supported AOS OmniSwitch Devices	WebView
Wireless	• OAW-4030, OAW-4604, OAW-4704, IAP-105, IAP-205, IAP-225	OAW EMS
Third-Party	• Cisco, Extreme, OmniAccess ESR, Aruba OS	Respective EMS

1.4.2 Device Feature Support

The following table details OV 2500 NMS-E 4.2.1.R01 feature support by device.

Feature	OS10K 6900	OS6860	Other AOS	OA WLAN	OmniAccess ESR	3rd Party Switches
Application Visibility (1)	X	X				
Analytics (2)	X	X	X			
Basic MIB-2 Polling and Status Display	X	X	X	X	X	X (3)
ClearPass (BYOD) (4)	X	X	X			
CLI Scripting	X	X	X	X	X	X
Discovery	X	X	X	X	X	X (3)
Locator	X	X	X	X		X (5)
mDNS		X	X (6)			
PolicyView-QoS	X	X	X	X		
Premium Service (BYOD)		X	X			
ProActive Lifecycle Mgmt (8)	X	X	X	X		
Quarantine Manager		X	X	X		
Report	X	X	X			
Resource Manager BU/Restore/Upgrade	X	X	X			
SIP (9)		X	X			
Telnet	X	X	X	X	X	X
Topology Links (LLDP) (10)			X			
Trap Absorption	X	X	X (11)	X		X
Trap Display/Trap Responder	X	X	X	X	X	X
Trap Replay	X	X	X			
UNP (12)	X	X	X			
VLAN Configuration	X	X	X	X		
VM Manager	X	X	X			
VM Snooping	X (13)					
VXLANs	X (14)					

1. The Application Visibility feature is supported on OS10K Switches (AOS 7.3.4.R02 and later), OS6900 Switches (AOS 7.3.4.R02 and later), and OS6860E Switches (AOS 8.2.1.R01 and later). It is also supported in a virtual chassis of OS6860/OS6860E Switches where at least one OS6860E is present.

2. The Analytics feature is supported on OS6250/6450 devices (6.6.1.R01 and later), OS6850/6855 devices (6.4.1.R01 and later, OS6860/6860E (8.1.1.R01 and later), OS6900 (7.3.2.R01 and later), OS9900 (8.3.1.R01 and later), and OS10K (7.3.1.R01 and later).

3. Third-Party devices, such as Cisco and Extreme are supported; however you must manually provide OIDs and map the OIDs to the mib-2 directory from the Third Party Device Support feature in the Discovery application. Refer to online Discovery help for details.

4. ClearPass (BYOD) is supported on OS6850E Switches (AOS 6.4.6.R01 and later), OS6850E, OS6855, OS6250, and OS6450 (6.6.5.R01 and later), and OS6860 (8.1.1.R01 and later).

5. Requires MIB-2 support for 3rd-party devices.

6. AOS 6.4.6.R01 and later Switches only.

7. MIB browser support is no longer available.

8. The ProActive Lifecycle Management feature is supported on the following devices: OS10K, OS9900, OS6900, OS6860/E, OS6865, OS6850/E, OS6855, OS6250, OS6350, OS6450, OAW-4005, OAW-4010, OAW-4030, OAW-4504, OAW-4604, OAW-4704, OAW-4550,OAW-4650,and OAW-4750.

9. The SIP feature is only supported on the following devices running 6.4.6.R01 and later: 6850E (C24/24x/48/48X, P24/24X/48/48X, U24X), 6855 (U24x), 9700E (C-24/48, P24, U2/6/12/24), 9800E (C24/48, P24, U2/6/12/24).

10. LLDP is supported on OS10K/OS6900 Devices (7.x.x and later), AOS Devices (6.3.1.R01 and later), and IPD SR7x50 devices (version 9.x and later). Links to Third-Party devices are not supported. Also note that OmniVista 2500 NMS does not display LLDP links reported by a single device. For a link to be displayed, both devices must be supported devices and LLDP MIB interface from each must have the Link.

11. Trap absorption feature is already built into AOS devices.

12. The UNP feature within Unified Access is supported on 6250, 6450, 6850, 6850E, 6855, 6900, OS10K devices, and Aruba OAW controller and OAW IAP.

13. VM Snooping is supported on OS6900 and OS10K Switches 7.3.4.R02 and later). Note that on OS10K Switches, VM Snooping is only supported on OS10K-XNI-U16E NIs. VM Snooping is supported on a port/linkagg, fixed bridge port, UNP bridge port, service access port, and UNP Service Access Point. VM Snooping is not supported on eVB, SDP, or VXLAN service ports.

14. VXLANs are supported on OS6900-Q32 and OS6900-X72 Switches (7.3.4.R02 and later).

1.4.3 SSHv2/Telnet Element Management

Many devices provide element management through a user interface accessible through SSHv2/telnet. For example, you can perform element management for most Alcatel-Lucent Enterprise devices via telnet using the device's CLI (Command Line Interface). You can use OmniVista 2500 NMS to access and configure telnet capable devices. This is generally not recommended if these tasks can also be performed using OmniVista 2500 NMS. If you change device configurations without using OmniVista 2500 NMS, configuration information stored by OmniVista 2500 NMS must then be refreshed to reflect the current device configuration, using manual or automatic polling.

You can telnet to a device using the CLI Scripting application or the Topology application. Refer to the switch documentation for information on how to use the CLI.

2.0 System Requirements

The following builds are certified for OV 2500 NMS-E 4.2.1.R01:

AOS

- OS6250 – 6.6.5.R02, 6.7.1.R02
- OS6350 – 6.7.1.R02
- OS6450 - 6.6.5.R02, 6.7.1.R02
- OS6850E – 6.4.6.R01
- OS6855 – 6.4.6.R01
- OS6860/E – 8.1.1.R01, 8.2.1.R01, 8.3.1.R01
- OS6865 – 8.3.1.R01
- OS6900 – 7.3.4.R02, 8.3.1.R01
- OS10K –7.3.4.R02, 8.3.1.R01

OmniAccess WLAN

- OAW 6.3.1, 6.4.2, 6.4.3

OmniAccess WLAN IAP

- OAW 6.4.3, 6.4.3.1, 6.3.2.6

OmniVista 2500 NMS-E 4.2.1.R01 Upgrade Paths Certified

- 4.1.2.R03 to 4.2.1.R01
- 3.5.7 to 4.2.1.R01

2.1 Proxy Requirements

OV 2500 NMS-E 4.2.1.R01 uses external repositories for Application Visibility Signature File updates, ProActive Lifecycle Management (PALM), and the OmniVista 2500 NMS Software Repository, which is used for software updates/upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.2.1.R01 to connect to the OmniVista 2500 NMS External Repository. .

2.2 Firewall Requirements

The OmniVista 2500 NMS Web Client, OmniVista 2500 NMS Server and network devices communicate over an IP network. You must configure the firewall appropriately for OmniVista 2500 NMS to run properly.

2.2.1 OmniVista 2500 NMS Ports

The following table lists the default ports used to communicate between the OmniVista 2500 NMS Server and Client, and the OmniVista 2500 NMS Server and network devices.

Service	Port	Source/Destination
SFTP/SSHv2	22	OV Server/OV Client
Telnet	23	OV Client/Net Device
SNMP Request	161	OV Server/Net Device
SNMP Trap	162	OV Server/Net Device
FTP	21	OV Server/Net Device
TFTP	69	OV Server/Net Device
LDAP Server	5389	OV Server/Net Device
sFlow	6343	OV Server/Net Device
Syslog Listener	514	OV Server/Net Device
Web Server (HTTP)	80	OV Server/OV Client
Web Server (HTTPS)	43	OV Server/OV Client

2.3 Recommended System Configurations

The table below provides recommended Hypervisor configurations based on the number of devices being managed by OV 2500 NMS-E 4.2.1.R01 (500, 2,000, 5,000, and 10,000 devices). These configurations should be used as a guide. Specific configurations may vary depending on the network, the number of clients, the number of VLANs, applications open, etc. For more information, contact Customer Support.

Number of Managed Devices	Hypervisor Processor	Hypervisor RAM	HDD Provisioning
500	2.4 GHz 8 Cores	16GB	HDD1:50GB HDD2:256GB
2,000	2.4 GHz 8 Cores	32GB	HDD1:50GB HDD2:512GB
5,000	2.4 GHz 12 Cores	64GB	HDD1:50GB HDD2:2048GB
10,000	2.4 GHz 12 Cores	64GB	HDD1:50GB HDD2:2048GB

Note: By default, OV 2500 NMS-E 4.2.1.R01 is partitioned as follows: HDD1:50GB and HDD2:256GB. If you are managing more than 500 devices it is recommended that you go to the Virtual Appliance Menu on the VA to the increase the HDD2 provision. See the *OmniVista 2500 NMS-E 4.2.1.R01 Installation Guide* for instructions on extending the partition.

3.0 Installation

OmniVista 2500 NMS is installed from a download file available on the Customer Support website. Note that you can only upgrade to OV 2500 NMS-E 4.2.1.R01 from OmniVista 2500 NMS 3.5.7 or 4.1.2.R03.

3.1 Licensing

OV 2500 NMS-E 4.2.1.R01 has a single installer and single license. The Node Management License (OV2500-NM) licenses all OmniVista 2500 NMS applications except Virtual Machine Manager (VMM). OmniVista 2500 NMS has been certified to manage up to 10,000 devices (includes AOS and Third-Party Devices).

The VMM License (OV2500-VMM) licenses the OmniVista 2500 NMS Virtual Machine Manager (VMM) application. VMs can be deployed on VMware vCenters, Citrix XenServers, and MS Hyper-V Servers; and OmniVista 2500 NMS supports a mixture of Hypervisor types with no limit on the number of Hypervisors. However, the VM Manager application supports a maximum of 5,000 VMs from all Hypervisors. More than 5,000 VMs are allowed, however a warning message will be displayed and an entry will be written to the VMM Log File.

"Starter Pack" Node Management and VMM Licenses provide full functionality, but for a limited number of devices. The following tables provide an overview of the different license types.

Node Management License Types

	Starter Pack	Evaluation	Production
Device Count	20 (10 AOS, 10 Third Party)	Chosen at license generation (full OV functionality)	Chosen at license generation (full OV functionality)
Expires	No	60 Days	No

Note: OAW Devices are counted as AOS Devices.

VMM License Types

	Starter Pack	Evaluation	Production
VMM Count	10	200	Chosen at license generation (full VMM functionality)
Expires	No	60 Days	No

The maximum number of devices allowed and the current number being managed is displayed in License Application (Administrator – License). This enables the user to determine if more devices can be added for management. Trying to discover new devices after the allowed limit will result in an Audit log and Status message.

Note: Licenses are imported/upgraded in the License Application. After installing OV 2500 NMS-E 4.2.1.R01, go to Administrator – License, import the license, then select the license type you want to upgrade/relicense and enter the License Key.

Procedures for generating an Evaluation License are available in the *OmniVista 2500 NMS-E 4.1.2.R01 Installation Guide*.

3.2 Upgrading a Starter Pack or Evaluation License to a Production License

A Starter Pack License of the OmniVista 2500 NMS Application allows you to manage up to 20 devices (10 AOS and 10 Third-Party) with no expiration date. An Evaluation license of OmniVista 2500 NMS is valid only for a limited period of time. To gain permanent use of the OmniVista 2500 NMS software, you must order a Permanent Node Management License. The following procedure describes how to obtain an OmniVista 2500 NMS license key.

1. Purchase a permanent OmniVista 2500 NMS Node Mangement License. You will receive an e-mail that contains a Customer ID and Order Number.

2. Once you receive your e-mail, log onto the Customer Support website at http://service.esd.alcatel-lucent.com/portal/page/portal/EService/LicenseGeneration and select **OmniVista 2500 NMS/VMM Release 4.1.x & 4.2.1**.

3. Select the product from the drop-down menu for which you want a key.

4. Enter your Site Name, Company Name, Phone, and E-Mail in the required fields. The e-mail address will be used to send a valid license key to you.

5. Click **Submit**. An e-mail will be sent to you with a valid license key. A text file with the license keys will also get downloaded to your browser's default Downloads directory.

6. Make a note of the License Key.

7. Go to the **License** Application and select **Node Management License**.

8. Click **Relicense**.

9. Enter the license key and click **OK**. The new license will take effect immediately.

If you have questions or encounter problems upgrading your OmniVista 2500 NMS License, please contact Alcatel-Lucent Enterprise Customer Support.

4.0 Launching OmniVista 2500 NMS

To launch OV 2500 NMS-E 4.2.1.R01, enter the IP address of the OmniVista 2500 NMS Server in a supported web browser (e.g., *https://<OVServerIPaddress>*.

> **Note:** The Watchdog Application, which enables all of the necessary OV 2500 NMS-E 4.2.1.R01 Services must be started to launch OV 2500 NMS-E 4.2.1.R01. By default, Watchdog should start automatically when OV 2500 NMS-E 4.2.1.R01 is installed. However, if you are having trouble launching OmniVista 2500 NMS, check to make sure that the Watchdog Service is enabled. If it is not, enable it. It will launch the remaining OmniVista 2500 NMS Services.
>
> Open a Console on the VA, and select the **Run Watchdog Command** option to display the status of Services or launch Services.

4.1 Logging Into OmniVista 2500 NMS-E 4.2.1.R01

After launching OV 2500 NMS-E 4.2.1.R01 for the first time, log in using the Default Username and Password:

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

5.0 Known Problems

5.1 Known Application Visibility Problems

5.1.1 User Allowed to Use the Same Application Group Name for Monitoring and Enforcement

A user should not be able to use the same Application Group Name for Monitoring and Enforcement.

Workaround: Do not create a Monitoring Group and Enforcement Group with the same name.

PR# 221096

5.2 Known CLI Scripting Problems

5.2.1 CLI Scripting Built-In Variable Value Contains Extra Space

OmniVista 2500 NMS CLI Scripting built-in variables replaced by their value with extra " " (space)

Workaround: These spaces help many java scripts work in field. If you do not want the spaces around built-in variable values, you can use JavaScript to strip them off as follows:

<js>

var ipAddr = "$IP_ADDRESS";

ipAddr = ipAddr.substring(1);

cli.sendCmd("show running-config tftp://10.10.110.251/"+ipAddr);

</js>

PR# 163776

The following guidelines should be kept in mind when creating scripts for the CLI Scripting application:

- You must always use semicolons to mark the end of a line/statement.
- Multi-line comments are supported. Single-line comments ('//') are not.
- The dollar sign being used to identify user-defined variables, if you need to use it in another context, you need to go through a variable. For instance, to use it in a JavaScript variable called 'dollar': var dollar = String.fromCharCode(36)
- The <tapps>...</tapps> tags are not meant to be used for proper scripting; they are only commodity methods, allowing you to execute one command at a time. In other words, each tapps command must to have its own <tapps> tags.

For example:

<tapps>import file1</tapps>

<tapps>import file2</tapps>

Rather than:

<tapps>

import file1

import file2

</tapps>

PR# N/A

5.3 Known Locator Problems

5.3.1 User Cannot Navigate to Diagnostic Screen in Locator

User cannot navigate to the Diagnostic Screen when clicking on " Show ClearPass Authentication" in Locator.

Workaround: Go to Unified Access – Premium Services – BYOD - Diagnostics and input the IP/MAC to query data.

PR# 220966

5.4 Known PolicyView Problems

5.4.1 LDAP Policy with 'TCP Flags' Condition Fails in Notify

LDAP Policy with 'TCP Flags' Condition Fails in Notify because the "tcpflags" attribute is not getting processed in switch properly.

Workaround: No workaround at this time.

PR# 196666

5.4.2 OS6900-Q32 Does Not Support Port Type in Expert Mode Policy Action

OS6900-Q32 Does Not Support Port Type in Expert Mode Policy Action.

Workaround: No workaround at this time.

PR# 201688

5.4.3 Problems Re-Caching When Port Policy Applied to Both OS6900-X32 Switches and Non-OS6900-X32 Switches

If you mix OS6900-Q32 and other switches in a policy that contains an action on a physical port, the configuration can be applied on the wrong port on some switches. You can mix switches in a policy only if the policy does not contain any physical port in the policy action.

Workaround: If you want to create a policy with a Policy Action on a physical slot/port of OS6900-Q32 switches, do not include any switch that is not an OS6900-Q32 switch in the same policy. Create separate policies.

PR# 202737

5.5 Known Resource Manager Problems

5.5.1 BMF Upgrade Fails on OS6250 Switch

BMF upgrade (u-boot, miniboot and FPGA) fail on OS6250 Switch.

Workaround: Use the CLI to upgrade BMF manually.

PR# 210056

5.5.2 SSH Key and User Table Missing after Full Backup of OS6900 8.3.1

The SSH Key and User Table are missing after performing a full backup of OS6900 Switch running AOS 8.3.1.R01. User Table cannot be backed up.

Workaround: No workaround at this time.

PR# 219688

5.6 Known Topology Problems

5.6.1 AMAP Entries for ERP-RPL Links Are Not Always Displayed

AMAP is a proprietary protocol and has been deprecated, so AMAP Entries for ERP-RPL Links are not always displayed.

Workaround: AMAP Adjacency Protocol functionality on the switch does not work properly with ERPv2 in case of ERP-RPL link, which may affect ERPv2 functionality. Use LLDP as the adjacency protocol when working with ERPv2.

PR# 177202

5.6.2 Certain Operations in Topology Fail Using I/E Browser

The Save to Running, Copy Certified to Working/Running, and Copy Working/Running to Certified operations fail when launched from the Topology application using I/E Browser.

Workaround: Perform the above operations in the Discovery application.

PR# 220967

5.7 Known Unified Access Problems

5.7.1 Cannot Find End Station Using Upper Case MAC Address in Diagnostics

Cannot find end station using upper case MAC address when trying to locate a device on the Diagnostics Screen.

Workaround: Specify MAC address in lower case only.

PR# 205365

5.7.2 Device Config - Port and Dynamic Service Access Auth Profile Displayed Incorrectly for OS6900-Q32/X72

Device Config - Port and Dynamic Service Access Auth Profile Displayed Incorrectly for OS6900-Q32/X72 Switches.

Workaround: Switch issue. No workaround at this time.

PR# 219133

5.7.3 Device Config - Cannot View Access Role Profile of AOS 8.2.1 Devices

Cannot view Access Role Profiles on Device Config Screen.

Workaround: No workaround at this time.

PR# 220259

5.8 Known VM Manager Problems

5.8.1 VLAN Notification Does Not Generate a Notification When Default UNP of LAG Port Is Deleted

VLAN notifications does not come up when the default UNP of a Link Agg Port is deleted

Workaround: This is a switch issue. When the default UNP is taken away from the LAG, the switch takes longer than usual to populate the MAC Learning Table. For a period of time, the MAC Address belong to the VM disappears and hence cannot even be located. Both commands 'show unp user' and 'show mac-learning' have no entry of the VM's MAC address. This behavior is not observed on the standard port. Notification eventually gets raised as the switch populates its table.

PR# 174181

5.8.2 VMM Locator VM Count Can Be Greater Than VMM License VM Count or Reported by vCenter

If VMs are using multiple Physical NIC Interfaces, the same VM will be bound to different MAC Addresses and OmniVista 2500 NMS will display multiple rows for the VM in VMM Locator search and browse applications. However, this will not affect VM Manager Licensing. The VMM License Manager will count multiple references as single Virtual Machine its UUID and the count will match the number of Virtual Machines reflected in vCenter.

Workaround: N/A

PR# 163885

5.8.3 OmniVista 2500 NMS Treats a VM Template as a Virtual Appliance

This is working as designed. vCenter treats Virtual Machine Templates and Virtual Machines in a similar manner. A MAC address is assigned to templates and they can be converted to a Virtual Machine in a single click. vCenter returns VM Template in the list of Virtual Machines like any other VM, and OmniVista 2500 NMS treats VM Templates like any other Virtual Machine.

Workaround: N/A

PR# 163314

5.9 Known Other Problems

5.9.1 VC Takeover Affects Inventory Reporting if Switch is Added in Topology with IP Address of the EMP Port

Change of a device's Management IP address due to VC takeover causes problems with inventory reporting in the ProActive Lifecycle Management application. This happens when a VC is added in Topology with a Management IP Address that is assigned to the EMP interface on the slave chassis. This typically happens after a VC takeover scenario. The problem does not occur on a VC of 1.

Workaround: Always configure an EMP-VC IP address on the VCs (*ip interface master emp address*) or configure an "ip interface" on the device. Then, make sure that the VC is displayed with one of these IP addresses in Topology. If the VC is displayed with any physical chassis IP address (EMP-CMMA-CHAS1 or EMP-CMMA-CHAS2), change the IP Address by right clicking the device and selecting "Edit".

PR# 205556

5.9.2 OmniVista 2500 NMS Does Not Display Application Visibility DPI Statistics on Switches Running AOS 8.1.1

Application Visibility DPI Statistics are generated with incorrect format after upgrade from 811GA build to 811postGA build and OmniVista 2500 NMS does not display DPI statistics.

Workaround: Login to the switch CLI and delete the files "/flash/switch/afn/dpi/dpi_flow_records.csv" and "/flash/switch/afn/dpi/dpi_flow_records.csv.old." The files will get created again with the correct format after the deletion.

PR# 197850

5.9.3 Apostrophe Is an Invalid Character in SNMP Community String

Workaround: Remove Apostrophe from the SNMP community string.

PR# 195715

5.9.4 Unable to Access Web UI Using IP Address on I/E

Unable to access Web UI using IP address on Internet Explorer browser, locally on a Windows 2012 R2 system.

Workaround: Have the correct mapping for 'localhost' in the hosts file and use 'localhost' instead of IP address to access the Web UI locally.

PR# 194913

5.9.5 U-Boot Version for OS6450 Devices Shows as "NA" in Inventory Report

U-Boot Version for OS6450 Devices Shows as "NA" in OmniVista 2500 NMS Inventory Report.

Workaround: This is a hardware issue with the OS6450. No workaround at this time.

PR# 181085

5.9.6 Help in VA Menu is Not Complete

The help in the VA Menus is not complete. Help is only available for main menus, not sub-menus.

Workaround: Detailed help is available in the Installation Guide.

PR# N/A

6.0 Release Notes PRs Fixed

6.1 PRs Fixed Since 4.1.2.R03

- The Modules tab in the Topology application is displaying incorrect information for transceivers connected to OS-XNI-U12E daughter cards on OS6900-X20 devices (PR 187119)
- SIP does not display Active Call Records on devices running AOS 6.4.6.R01 even when SIP call is running successfully on device (PR 189041)
- Cannot find end station using upper case MAC address when trying to locate a device on the Diagnostics Screen (PR 205365)
- If the sFlow Receiver is configured on a switch in the CLI as Receiver “1” and a user applies an Analytics Profile to the switch OmniVista 2500 NMS overwrites the CLI-configured sFlow receiver with its own IP address as Receiver “1” (PR 205843)
- "Failed to activate signature file" error on OS6860E-P48 (AOS 8.2.1.256.R01 GA) (PR 211504)

6.2 PRs Fixed Since 4.1.2.R02

- No Traps Generated on 7.x/8.x when Trap Port Set to Number Other Than 162 (PR 198919)
- UA Policy Re-Caches Incorrectly with Policies on AOS Switch (PR 205481)

6.3 PRs Fixed Since 4.1.2.R01 Maintenance Release

- When linkagg removed via CLI, UNP linkagg is deleted on switch, but not in OmniVista 2500 NMS (PR 195702)
- Installation of OmniVista 2500 NMS Fails with “Error: Mongo couldn’t be started” and the installation rolls back (PR 197900)

6.4 PRs Fixed Since 4.1.2.R01

- VA Upgrade - Error "The SNMP trap listener could not be created on port 162" when notification app opened (PR 201406)
- OmniVista 2500 NMS Discovery issue for Juniper switches in VC configuration (PR 190524)
- Clarification in color status change for Link Aggregate link status (PR 196909)

- Issue with the SPB One Touch Feature (PR 197937)
- "Max Timeout" script error seen when sending SPB Configuration Telnet Script through OmniVista 2500 NMS (PR 199393)
- Unable to assign ClearPass Server for AOS device (6.4.4.R01) (PR 199978)
- OmniVista 2500 NMS Tomcat Service does not start if database backup is imported from 3.5.7 through a RADIUS Server (PR 200009)
- SSLv3 vulnerability issue (PR 200391)
- OmniVista 2500 NMS Server in a VA installation should be able to bind to a port lower than 1024 (e.g., 162, 514) (PR 201007)
- OmniVista 2500 NMS should not show stack split warning icon when the stack does not support SSP and is not in loop (PR 201483)

6.5 PRs Fixed Since Release 4.1.1

- Even if GetBulk is disabled in the SNMP Settings of the java UI, OmniVista 2500 NMS 411 services such as Unified Access, Application Visibility, and BYOD ignore this setting and still use GetBulk (PR 196768)

6.6 PRs Fixed Since 3.5.7 Maintenance Build

- Live Search for IP Phones Issue (PR 187956)

6.7 PRs Fixed Since Release 3.5.7 GA

- "Set Row" displays error when user logs into OV Server with multiple browser windows (PR 188220)
- Status "In Active" of Statistics profile is not correct; and the Calendar does not work when scheduling a Statistics profile (PR 188827)
- Error in vmm.log if the VM name contains "/" character and the VM name in VM Manager is not correct (PR 188876)
- Unable to start OV Server if LDAP server is not running (PR 191084)
- 64-bit OmniVista 2500 NMS 3.5.7 does not detect the previously installed version during upgrade (PR 192354)