Release Notes

for

OmniVista 2500 NMS Enterprise Version 4.3R2

January 2018

Revision B

Part Number 033381-10

READ THIS DOCUMENT

OmniVista 2500 NMS

for

VMware ESXi: 5.5, 6.0, 6.5, 6.7

VirtualBox: 5.2.x

MS Hyper-V: 2012 R2 and 2016

MS Hyper-V on Windows 10 Professional

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

Table of Contents

Table of Contents (continued)

Revision History

Release	Revision	Date	Description of Changes
4.3R2	B	01/21/19	Release Notes Update
4.3R2	A	11/27/18	GA Release
4.3R1	B	07/12/18	Release Notes Update
4.3R1	A	06/06/18	GA Release
4.2.2.R01	C	01/26/18	Maintenance Release 2
4.2.2.R01	B	12/11/17	Maintenance Release 1
4.2.2.R01	A	08/24/17	GA Release
4.2.1.R01	E	06/16/17	MR 2 Release Notes Update
4.2.1.R01	D	05/30/17	Maintenance Release 2
4.2.1.R01	C	02/02/17	Maintenance Release 1
4.2.1.R01	B	09/30/16	Release Notes Update
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 4.3R2 (OV 2500 NMS-E 4.3R2) is installed as a Virtual Appliance, and can be deployed to these hypervisors: VMware ESXi, VirtualBox, and MS Hyper-V:

- VMware ESXi: 5.5, 6.0, 6.5, and 6.7
- VirtualBox: 5.2.x
- MS Hyper-V: 2012 R2 and 2016
- MS Hyper-V on Windows 10 Professional.

This document details known problems and limitations in OV 2500 NMS-E 4.3R2, 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.

> **Important Note:** You must upgrade your Stellar APs to AWOS 3.0.4.2050. for OV 2500 NMS-E 4.3R2. **First** upgrade to OV 2500 NMS-E 4.3R2; then upgrade your APs to AWOS 3.0.4.2050. Please refer to the OV 2500 NMS-E 4.3R2 Installation Guide for details.

1.1 Technical Support Contacts

For technical support, contact your sales representative or go to the ALE Business Portal:

- https://businessportal2.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 4.3R2

Hardware/Release Support

OmniVista High-Availability Improvements

- **Support for Larger Networks -** OmniVista now supports up to 2,000 devices in a High-Availability Installation.
- **Layer 3 Configuration -** An OmniVista 2500 NMS High-Availability (Cluster) Installation can now be configured in a Layer 2 or Layer 3 configuration. In a Layer 2 Installation, which was supported in the previous release, both OmniVista Servers (Active and Standby) are installed on the same subnet. A virtual Cluster IP address is configured through which network devices can communicate with both servers. In a Layer 3 configuration, the OmniVista Servers can be installed on different subnets with a unique IP address for each server. Network devices can communicate with both VMs (Active and Standby Nodes). Network devices communicate with the Active Node. In the event of a failover, devices automatically communicate with the new Active Node. Note that **Stellar APs** are **only** supported in a **Layer 2** Installation.

- **Improved HA Installation Workflow -** In the previous release, a user had to decide during the initial installation process whether to configure a Standalone or High-Availability Installation. In the new workflow, a user configures a Standalone Installation; then, at any time, a user can convert the Standalone Installation into a High-Availability Installation by having a second OmniVista Server join in a Cluster configuration.
- **Failover Warning Banner –** When the Active Node fails in an HA Installation, a warning banner and link is displayed at the top of the screen prompting the user to redirect to the Standby Node if the user is in a Layer 3 HA configuration.

OmniVista Memory Footprint Reduction

- **Memory Service Profiles -** You can now configure Service Profiles specific to your network to save OmniVista memory. The profiles are configured in the Virtual Appliance Menu under the Run Watchdog Command set. These profiles can be applied to save memory if certain services are not required for your network (e.g., you are not using Stellar APs in your network, you are not using the Application Visibility application). By default, all services are started and run on OmniVista. By selecting a Service Profile for your network, those services that you do not need will not be started.

New Virtual Application Commands

- The following new commands have been added to the Virtual Appliance Menu:
  - **Convert to Cluster -** This command it used to convert a VM to Cluster (High-Availability) Mode. This command prepares the VM to be configured in a Cluster configuration. A VM in Cluster Mode can continue to run as a Standalone Installation and can be converted to an HA Installation at any time by adding a second Node using the Join Cluster command.
  - **Join Cluster -** This command is used to have a VM join with a VM in Cluster Mode. Once this command is completed, the two VMs will be configured as an Active Node and a Standby Node in an HA Configuration.
- The following new commands have been added to the HA Virtual Appliance Menu (Configure Cluster Menu):
  - **Remove Peer Node From Cluster -** This command is used to remove a Node from a Cluster. This command is issued on the Active Node and can be used if there is a problem with the Standby Node and you want to permanently delete it. Once the Node is removed from the Cluster, you can create a new Cluster on the Active Node using a different VM.
  - **Configure UPAM Portal Web IP -** This command is used to configure the UPAM Portal Web IP address.

VMware VMotion Support

- VMware VMotion is certified.

OS6900-C32

- OmniVista now supports the new OS6900-C32 running AOS 8.5R2.

OS6900-V72

- OmniVista now supports the new OS6900-V72 running AOS 8.5R2.

AP 1201H

- OmniVista now supports the AP 1201H Stellar AP running AWOS 3.0.4.2050.

Application Updates/Enhancements

The following section detail updates and enhancements to existing OmniVista applications.

UI Enhancements Across Applications

- The UI has been optimized to display more information:
  - Columns and text resized
  - Full-screen view option available for all screens.
  - Left-Hand Side Menus automatically close after a page is initially displayed to provide display more information on the screen. You can click on the arrows (>>) or hover the mouse over the area to temporarily display the menu, or lock the menu in place by clicking on the Pin Sidebar icon at the top of the menu.
- The navigation icon color scheme has been changed to a gray background for easier viewing.
- You can now copy/paste MAC addresses in the OmniVista UI in additional common formats (e.g., 00-80-0f-33-33-24 in addition to 00:80:0f:33:33:24).

AP Registration

- **Access Points**
  - **Reset APs -** A new "Reset APs" button has been added. When you reset an AP, the AP will reset to the factory default configuration and reboot. When an AP is rebooted as part of a reset, the latest configuration available on OmniVista is downloaded to the AP. If the AP is unable to connect to OmniVista, the AP will come up with the factory default configuration.
  - **Edit AP IP Address -** You can edit the IP address of an AP by selecting the AP and clicking on the Edit icon. Click on "Edit Mode" to edit the IP address. You can also set the AP to default DHCP Mode.
  - **Migrate an AP to a Different OmniVista Server -** You can release an AP from management on your system and make it available for management by another OmniVista Server. Select the AP in the Access Point List and select “Migrate to Other OV” from the Edit icon to specify the new OmniVista Server. The AP will be released from your OmniVista Server and migrate to the other server, where it will be displayed in the Unmanaged AP Tab. The Administrator of the other OmniVista Server can then license and configure the AP.
  - **View Port Information -** You can view port information on 1201H APs by selecting an AP(s) and selecting "Port Management" from the "Action" drop-down. The Ports page in the Inventory application will open with port information displayed for the selected AP(s).
- **AP Group**
  - **Enable SNMP -** This option allows third-party SNMP-based platforms to monitor APs in a group using SNMP. OmniVista Cirrus does not use SNMP to manage Stellar APs. With defined SNMP MIBs, an Administrator can monitor APs, configured services, and wireless clients and their traffic utilization.

Captive Portal

- **Redirect to FDQN -** Captive Portal can be configured to redirect to an FDQN as well as an IP address.
- **Captive Portal Certificates -** You can create Captive Portal Certificates to implement the HTTPs login when UPAM is used as a Captive Portal Server.

CLI Scripting

- **SSH/Telnet to a New Device -** SNMP users and community strings need to be configured on devices before they can be managed by OmniVista. You can now SSH/Telnet to a newly added device that is not yet reachable by SNMP to configure the device for OmniVista management.

Notifications

- **Resource Manager Backup Failure Trap -** A new trap has been added to the Notifications application (alaOperationTrap) for Resource Manager Backup Failure. A Trap Responder can be configured to automatically send an e-mail when this trap is triggered.

Topology

- **Virtual Chassis Configuration Change Warning/Trap -** For Virtual Chassis stacks (running AOS 8.5R2 or higher or 6.7.3. R04 higher), if you attempt to save a configuration to the Running Directory in the Topology (or Discovery) application and there has been a change in the Virtual Chassis stack topology since the last save, a warning prompt will appear listing the problem devices. You can proceed to save the configuration(s) on all devices, or make any necessary configuration updates to devices before saving. If you proceed with the save without addressing the changes, a trap will be generated (virtualchassisstatuschange) in the Notifications application.
- **Manual Link Display Option -** An “Ignore Manual Link” option has been added to the Topology Configuration Window. If enabled, manual links will be hidden when LLDP and manual links exist between a set of ports when hovering the mouse over the link; and the manual links will not be displayed in the Detail Panel after clicking on the link.

UPAM

- **Captive Portal Page/Language Customization -** Images and videos are customizable on the Captive Portal Page. In addition, when a user connects to an SSID with Guest/BYOD authentication, the user can change the language of the Captive Portal Page by clicking on a drop-down menu at the top-right-corner of the page.
- **Role Mapping Enhancements -** OmniVista Cirrus supports exact match of return attributes for role mapping. Partial string match (memberOf) is not supported at this time.

WLAN

- **Usage Reports –** New Usage Reports are available in the WLAN – Client application.
  - **The Client Summary Screen -** Provides a graphical view of the number of clients and system throughput on your network. You can view the information by AP/AP Group and WLAN; and can view information over different time periods (24 Hours,

Last 7 Days, 30 Days, 90 Days). You can also create printed reports of these screens using the Report application.

- **The Client List Screens -** Provide real-time information about wireless and wired clients associated with APs in graphical and table format.
- **The Client Session Screens -** Provide session information about wireless and wired clients associated with APs.

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 independent 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
Web UI	• OS2200	Web UI Device Management
Web UI	• All supported Stellar APs	Web UI Device Management
Wireless Controller	• OAW-4030, OAW-4604, OAW-4704, IAP-105, IAP-205, IAP-225	OAW EMS
Third-Party	• Cisco, OmniAccess ESR, Aruba OS	Respective EMS

1.4.2 Device Feature Support

The following table details OV 2500 NMS-E 4.3R2 feature support by device.

Feature	OS10K 6900	OS6860/ OS6865	Other AOS	OS2220	Stellar APs	OA WLAN	OA ESR	3rd Party Switches
Application Visibility (1)	X	X			X			
Analytics (2)	X	X	X		X			
Basic MIB-2 Polling and Status Display	X	X	X	X		X	X	X (3)
ClearPass (BYOD) (4)	X	X	X					
CLI Scripting	X	X	X		X(5)	X	X	X
Discovery	X	X	X	X	X	X	X	X (3)
Locator	X	X	X	X	X	X		X (6)
mDNS		X	X (7)					
mDNS Gateway					X			
PolicyView-QoS	X	X	X		X	X		
Premium Service (BYOD)		X	X					

Feature	OS10K 6900	OS6860/ OS6865	Other AOS	OS2220	Stellar APs	OA WLAN	OA ESR	3rd Party Switches
ProActive Lifecycle Mgmt	X	X	X	X	X	X		
Quarantine Manager (8)		X	X			X		
Resource Manager BU/Restore/Upgrade	X	X	X		X			
SIP (9)		X	X					
SPB/ERP (10)	X	X	X					
Remote CLI	X	X	X			X	X	X
Topology Links (LLDP) (11)	X	X	X	X	X			
Trap Absorption	X	X	X	X	X	X		X
Trap Display/Trap Responder	X	X	X	X (12)	X	X	X	X
Trap Replay	X	X	X		X			
UPAM (Guest User, BYOD) (13)	X	X	X		X			
UNP (14)	X	X	X		X			
VLAN Configuration	X	X	X			X		
VM Manager	X	X	X					
VM Snooping	X (15)							
VXLANs	X (16)							
WLAN (SSID)					X			

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. It is also supported on the following Stellar APs OAW-AP1201, OAW-AP1221, OAW-AP1231, and OAW-AP1251.

2. The Analytics feature is supported on OS6250/6450 devices (6.7.1.R01 and later), OS6850/6855 devices (6.4.4.R01 and later, OS6860/6860E and OS6865 (8.3.1.R01 and later), OS6900 (8.3.1.R01 and later), OS9900 (8.3.1.R02 and later), and OS10K (7.3.4.R02 and later). It is also supported on Stellar APs (except for Top N Application and Clients – sFlow, and performance monitoring).

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/6855 Switches (AOS 6.4.6.R01 and later), OS6250, and OS6450 (6.7.1.R02 and later), and OS6860 (8.3.1.R01 and later).

5. CLI Scripting is not supported on Stellar APs, however you can connect (SSH) to a Stellar AP using the CLI Scripting application.

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

7. AOS 6.4.6.R01 and later Switches only.

8. The TAD feature in Quarantine Manager is only supported on OS6850, OS6855, OS9700 Switches running AOS 6.4.6.R01.

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. SPB is supported on OS6855, OS6860, OS6860E, OS9000, OS6900, and OS10K Switches. ERP is supported on OS OS6400, OS6850, OS6855, OS6860, OS6860E, OS9000, OS6900, and OS10K Switches.

11. 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.

LLDP Links for Third-Party Switches are supported and displayed in Topology maps. However, you must first add the Mibset for the device using the Third-Party Devices Support Feature in the Discovery application (Network – Discovery - Third Party Devices Support). Refer to the Discovery online Help for more details. Links between AOS and Third-Party devices as well as links between Third-Party devices are displayed in Topology maps. For this feature to work, the Third-Party device must support IEEE 802.1AB standard SNMP MIB “lldpMIB”.

12. Trap display is supported on OS2220 Switches. However, trap configuration must be performed on the device using the device’s web interface.

13. LDAP Role Mapping is supported with 802.1x Authentication only.

14. The UNP feature within Unified Access is supported on 6250, 6450, 6560, 6850E, 6855, 6860, 6900, OS10K devices, and Aruba OAW controller and OAW IAP.

15. 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.

16. VXLANs are supported on OS6900-Q32 and OS6900-X72 Switches (8.3.1.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 Discovery or Topology applications. Refer to the switch documentation for information on how to use the CLI.

> **Note:** To connect to Stellar APs, you must enable SSH at the AP Group level. If enabled, you will be able to connect (SSH) to all Stellar APs in the group. Telnet Scripting is not supported on Stellar APs.

2.0 System Requirements

The following builds are certified for OV 2500 NMS-E 4.3R2:

AOS

- OS6250 – 6.7.1.R02, 6.7.1.R03, 6.7.1.R04
- OS6350 – 6.7.2.R02, 6.7.2.R03, 6.7.2.R04
- OS6400 – 6.4.5.R01 (limited support, restricted to PALM)
- OS6450 – 6.7.2.R02, 6.7.2.R03, 6.7.2.R04
- OS6465 – 8.5R1, 8.5R2
- OS6560 – 8.4.1.R03, 8.5R1, 8.5R2
- OS6850 – 6.4.4.R01
- OS6850E – 6.4.6.R01
- OS6855 – 6.4.6.R01
- OS6860/E – 8.4.1.R03, 8.5R1, 8.5R2
- OS6865 – 8.4.1.R03, 8.5R1, 8.5R2
- OS6900 – 8.4.1.R03, 8.5R1, 8.5R2
- OS9700E– 6.4.6.R01
- OS9800E– 6.4.6.R01
- OS9900 – 8.4.1.R03, 8.5R1, 8.5R2
- OS10K – 7.3.4.R02, 8.3.1.R01

WebSmart

- OS2220 – 8.3.1.2, 8.3.1.3

OmniAccess WLAN

- OAW-4030 – OAW 6.5.1, 6.5.4
- OAW-4704 – OAW 6.5.1, 6.5.4
- OAW-4604 – OAW 6.5.1, 6.5.4
- OAW-4x50 – OAW 6.5.1, 6.5.4

OmniAccess WLAN IAP

- IAP-105 – OAW 6.5.1, 6.5.4
- IAP-205 – OAW 6.5.1, 6.5.4
- IAP-225 – OAW 6.5.1, 6.5.4
- IAP-325 – OAW 6.5.1, 6.5.4
- IAP-335 – OAW 6.5.1, 6.5.4

OmniAccess ESR

- OA 5710 – 11.00.00.02.05
- OA 5720 – 11.00.00.02.05
- OA 5725 – 11.00.00.02.05
- OA 5800 – 11.00.00.02.05

Stellar AP Series Wireless Devices

- OAW-AP1101 – AWOS 3.0.4.2050 (only)
- OAW-AP1101-JP – AWOS 3.0.4.2050 (only)
- OAW-AP1221 – AWOS 3.0.4.2050 (only)
- OAW-AP1201H – AWOS 3.0.4.2050 (only)
- OAW-AP1222 – AWOS 3.0.4.2050 (only)
- OAW-AP1231 – AWOS 3.0.4.2050 (only)
- OAW-AP1232 – AWOS 3.0.4.2050 (only)
- OAW-AP1251 – AWOS 3.0.4.2050 (only)
- OAW-AP1101-ME – AWOS 3.0.4.2050 (only)
- OAW-AP1221-ME – AWOS 3.0.4.2050 (only)
- OAW-AP1222-ME – AWOS 3.0.4.2050 (only)
- OAW-AP1251-ME – AWOS 3.0.4.2050 (only)

  Note: You cannot use older (or newer) AWOS with this OmniVista Release. If you are upgrading to OV 4.3R2 OmniVista from a previous release, you must upgrade AWOS devices to 3.0.4.2050 after the OmniVista upgrade.

  Note: Only the builds listed above are certified for this release.

OmniVista 2500 NMS-E 4.3R2 Upgrade Paths Certified

- 4.3R1 Standalone – 4.3R2 Standalone
- High-Availability (HÁ) Conversion/Upgrade:
  - You can only convert a **fresh** 4.3R2 Standalone Installation to a 4.3R2 HA Installation.
  - You **cannot** convert a 4.3R2 Standalone Installation to an HA Installation if the 4.3R2 Standalone Installation was upgraded from a 4.3R1 Standalone Installation.
  - You **cannot** upgrade a 4.3R1 HÁ Installation to a 4.3R2 HA Installation.

  Note: You can only perform a restore using a backup from the same release (e.g., you can only restore a 4.3R2 configuration using a 4.3R2 Backup File). OmniVista will not allow you to perform a restore using a backup from a previous release.

2.1 Proxy Requirements

OV 2500 NMS-E 4.3R2 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 4.3R2 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. The following URLs must be allowed to enable communication between the OmniVista Server and the ALE Central Repository, Application Visibility (AV) Signature Repository, and Proactive Lifecycle Management (PALM) Portal:

- **ALE Central Repository –** ovrepo.fluentnetworking.com
- **AV Repository –** ep1.fluentnetworking.com
- **PALM –** palm.enterprise.alcatel-lucent.com
- **Call Home Backend -** us.fluentnetworking.com

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/Net Device
Telnet	23	OV Client/Net Device
SNMP Request	161	OV Server/Net Device
SNMP Trap	162	Net Device OV Server
FTP	21	OV Server/Net Device
TFTP	69	Net Device OV Server
LDAP Server	5389	OV Server/Net Device
sFlow	6343	Net Device/OV Server
Web Server (HTTP)	80	OV Client/OV Server
Web Server (HTTPS)	443	OV Client/OV Server
Secure MQTT	1883	Stellar AP/OV Server
SMTP	25	UPAM/Third-Party Party SMTP Server
Log-MySQL	3306	UPAM/Log Server
Log-MSSQL	1433	UPAM/Log Server
LDAP	389	UPAM/LDAP Server
Active Directory (AD)	389	UPAM/AD Server
Syslog Listener	514	Net Device/OV Server, UPAM/Syslog Server
RADIUS Authentication	1812	Net Device/UPAM, UPAM/External RADIUS
RADIUS Accounting	1813	Net Device/UPAM, UPAM/External RADIUS
RADIUS CoA – UDP Port	3799	UPAM/Net Device
VMM	135	OV Server/Hyper-V Server
	49152-65535 (RPC Dynamic Port)	Hyper-V Server/OV Server
High-Availability	8000, 5405, 7801	Node 1/Node 2 Node 2/Node 1

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 4.3R2 (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 wired/wireless clients, the number of VLANs, applications open, etc. For more information, contact Customer Support.

	Network Size			
Configuration	**Low**	**Medium**	**High**	**Very High**
Total Number of Managed Devices (AOS, Third-Party, and Stellar APs)	500	2,000	5,000*	10,000*
Stellar AP Devices	500	2,000	4,000	4,000
Stellar AP Client Association	50,000	200,000	200,000	200,000
UPAM Authentication	15,000	30,000	100,000	100,000
Hypervisor Processor	2.4 GHz 8 Cores	2.4 GHz 8 Cores	2.4 GHz 12 Cores	2.4 GHz 12 Cores
OV VA RAM	16GB	32GB	64GB	64GB
HDD Provisioning	HDD1:50GB HDD2:256GB	HDD1:50GB HDD2:512GB	HDD1:50GB HDD2:2048GB	HDD1:50GB HDD2:2048GB

*****If there are 4,000 Stellar AP in a “High” network size, up to 500 AOS Switches can be supported. If there are 4,000 Stellar APs in a “Very Hight” network size, up to 1,000 AOS Switches can be supported.

Note: By default, OV 2500 NMS-E 4.3R2 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 4.3R2 Installation and Upgrade Guide* for instructions on extending the partition.

2.4 High-Availability Installation Limitations

The following features are not supported in a High-Availability (HA) Installation:

- Cluster IP configuration in L3 Cluster
- Two (2) NICs
- Configuring the UPAM Portal IP address on different subnet than the OmniVista IP address
- Upgrade from 4.3R1 HA to 4.3R2 HA
- Changing the OmniVista IP address and Hostname after creating the Cluster.
- Memory synchronization. When the active service is not available and failover happens, the data in memory of that service will be lost.
- Hostname in upper case. Also note that the Hostname can have a maximum of 15 characters

- Changing/configuring Timezone
- Configuring an NTP client.

3.0 Installation

OmniVista 2500 NMS is installed from a download file available on the Customer Support website. Note that you can only directly upgrade to OV 2500 NMS-E 4.3R2 from OV 2500 NMS-E OV 2500 NMS-E 4.3R2. See the *OmniVista 2500 NMS-E 4.3R2 Installation and Upgrade Guide* for upgrade paths from older builds.

3.1 Licensing

OmniVista 2500 NMS licensing is based on the license purchased. A user is allowed to manage up to the maximum number of devices allowed for that license. There are two types of licenses that can be purchased - Device Licenses and Service Licenses.

- **Device Licenses -** Licenses a user to manage a specific number of devices.
    - **Alcatel-Lucent Enterprise Devices -** Licenses a specific number of ALE devices (e.g., OS10K, 6900, 6860) that can be managed. OmniVista has been certified to manage up to 10,000 devices (includes AOS and Third-Party Devices).
    - **Third Party Devices -** Licenses third-party devices (e.g., Cisco).
    - **Alcatel Lucent Enterprise OmniAccess Stellar APs -** Licenses OmniAccess Stellar Wireless Devices (e.g., OAW-AP1101, OAW-AP1221). OmniVista has been certified to manage up to 512 Stellar APs.
- **Service Licenses -** Licenses a user to manage a specific number of devices for the following services:
    - **VMs -** Licenses Virtual Machines (VMs). 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.
    - **Alcatel Lucent Enterprise Guest Devices -** Licenses Guest Devices authentication through UPAM. The following licenses are available: 20, 50, 100, 500, or 1000 Guest Devices.
    - **Alcatel-Lucent Enterprise On-Boarding Devices -** Licenses BYOD Devices authentication through UPAM. The following licenses are available: 20, 50, 100, 500, or 1000 Guest Devices.
    - **High-Availability –** Licenses the High-Availability Feature.

There are three (3) types of OmniVista Licenses:

- **Starter Pack -** Is free and enables you to use OmniVista on a limited basis without expiration. You can manage up to 30 devices (10 AOS, 10 Third Party, 10 Stellar APs).
- **Evaluation -** Is free and gives you full use of OmniVista, but for a limited time (90 days). You can manage up to 60 devices (20 AOS, 20 Third Party, 20 Stellar APs)
- **Production -** Gives you full use of OmniVista without expiration.

Device License Types

	Starter Pack	Evaluation	Production
Device Count	30 (10 AOS, 10 Third Party, 10 Stellar AP)	60 (20 AOS, 20 Third Party, 20 Stellar AP) (full OV functionality)	Chosen at license generation (full OV functionality)
Expires	No	90 Days	No

Note: OAW (non-Stellar) Devices are counted as AOS Devices.

Service License Types

	Starter Pack	Evaluation	Production
VMs	10	100	Chosen at license generation (full VMM functionality)
ALE Guest Devices	10	20	Chosen at license generation (full VMM functionality)
ALE On-Boarding Devices	10	20	Chosen at license generation (full VMM functionality)
Expires	No	90 Days	No

Note: The High-Availability License is only available as a Production License. It does not expire.

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 4.3R2, go to Administrator – License, import the license, then select the license type you want to upgrade/relicense and enter the License Key.

See the *OmniVista 2500 NMS-E 4.3R2 Installation and Upgrade Guide* for instructions on generating an Evaluation License.

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 30 devices (10 AOS, 10 Third-Party, 10 Stellar APs) 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-E 4.3R2 License. You will receive a “Welcome Kit” e-mail that contains a Customer ID and Order Number.

2. Once you receive your e-mail, log onto the License Generation website at https://lds.al-enterprise.com/ov25411/enterLicenseData.jsp.

3. Enter your Customer ID and Order Number.

4. Complete the License Registration From and click **Submit**. A download prompt will appear.

5. Click **Save** at the confirmation prompt to download the license file to your computer.

6. Go to the **License – Add/Import License Screen** in OmniVista to import the license file you just downloaded.

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

OV 2500 NMS-E 4.3R2 is supported on the following browsers: Internet Explorer 11+ (on Windows client PCs), Chrome 68+ (on Windows and Redhat/SuSE Linux client PCs), and Firefox 62+ (on Windows and Redhat/SuSE Linux client PCs). To launch OmniVista), enter the IP address of the OmniVista 2500 NMS Server (e.g., *https://<OVServerIPaddress>*). The IP address entered depends on the type of installation:

- **Standalone -** Enter the IP address of the OmniVista Server.
- **High-Availability (Layer 2) -** Enter the Virtual Cluster IP address.
- **High-Availability (Layer 3) -** Enter the IP address of the Active Node.

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

  Note: The Watchdog Application, which enables all of the necessary OV 2500 NMS-E 4.3R2 Services must be started to launch OV 2500 NMS-E 4.3R2. By default, Watchdog should start automatically when OV 2500 NMS-E 4.3R2 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 4.3R2

After launching OV 2500 NMS-E 4.3R2 for the first time, log in using the Default Username and Password:

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

5.0 Known Problems

5.1 Known Analytics Problems

5.1.1 Modules Displayed Incorrectly in Performance Monitoring

When creating a profile in Performance Monitoring and selecting a module for a device, the modules displayed for 6.x Devices displays incorrectly. For 6x devices, the slot numbering scheme should be slot/port. However, OmniVista shows the Chassis number as the Slot number with a prefix of “Chassis=0”. That is, Chassis =1 is represented as Chassis 0 Slot 1, rather than “Chassis 1” or “Slot 1”.

Workaround: Chassis = 0 value is invalid and can be safely ignored by user when listed in the drop-down. The chassis number (or slot number) value is actually the Slot number.

PR# OVE-3033

5.2 Known Application Visibility Problems

5.2.1 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

5.2.2 Cannot Apply Signature and Classification to a Large Number of APs

Operation fails when attempting to apply an Application Visibility Profile or Access Classification Roles to a large number of APs at the same time.

Workaround: Apply profiles to no more than 500 APs at a time. Create AP Groups of no more than 500 APs and apply the Signature Profile or Access Classification Roles to the group. Create additional AP Groups and apply the Signature Profile or Access Classification Roles as needed.

PR# OVE-2256

5.3 Known AP Registration Problems

5.3.1 In 2,000 AP Setup, Many APs Cannot Register

When trying to register 2,000 APs at once, many APs do not register with OmniVista and remain in an “Unlicensed” State even though there are enough licenses for all of the APs.

Workaround: When registering a large number of APs, register them in AP Groups of 500. Bring up the first group of 500 APs and wait for them to be “Licensed” and “Trusted” before bringing up the next group. Repeat until all APs are registered.

PR# OV-5339

5.4 Known CLI Scripting Problems

5.4.1 Increase Buffer Size of Interactive SSH Terminal in Web UI

When you launch SSH session to a device from OmniVista from "CLI Scripting" application, the screen buffer size is only 300 lines. If the command output is long, then it is difficult to view the results. Also, the previously executed commands cannot be seen.

Workaround: Up to 300 lines can be displayed. No workaround at this time.

PR# OVE-998

5.4.2 Using “show log swlog” in OV Client Window Causes Window to Crash

If you run “show log swlog” from the CLI Scripting Terminal, the OmniVista Client window crashes due to the large amount of data returned by the command output.

Workaround: This command should be avoided in OmniVista. To view the switch swlog, use the “Collect Support Info" feature in the Audit application to download the log files from the switch.

PR# CRNOV-645

5.5 Known Discovery Problems

5.5.1 AP Reason Down Field is Updated Slowly System with 500 APs

The “Reason Down” field is blank if an AP is UP. If and AP goes down and then returns to an UP state, the “Reason Down” field does not return to a blank field.

Workaround: If an AP goes down, the "Reason Down" field may not update to "Blank" when the AP returns to an "Up" state. For APs, ignore this field if the AP Status is "Up". No workaround at this time.

PR# OVE-2131

5.5.2 “Save to Running” on Large Number of APs Is Slow

Performing a “Save to Running” action on a large number of APs in the Discovery application takes a long time (it takes approximately 10 seconds for each AP).

Workaround: No workaround at this time.

PR# OVE-2264

5.5.3 Unable to Discover Additional Devices Once 7,000 Devices Is Reached

When performing a discovery on a large network, once approximately 7,000 devices were discovered, OmniVista could not discover additional devices.

Workaround: Discover no more than 5,000 devices at a time. Perform additional discoveries as needed to discover remaining devices.

PR# OVE-2198

5.5.4 Missing Device Info After Re-Discovering Multiple APs

When a user attempts to rediscover more than two APs, the UI displays incorrect information on the Results page.

Workaround: No workaround at this time.

PR# OVE-2978

5.6 Known Locator Problems

5.6.1 Cannot Locate End Stations Connected to OS2220

Unable to locate end stations connected to OS2200 Switch.

Workaround: The Locator application is not supported on OS2200 Switches.

PR# OVE-1226

5.7 Known Notifications Problems

5.7.1 Backup Failure Trap Not Working on System Upgraded From OV422 MR2 - OV43R2

The Backup Failure Trap (alaOvOperationTrap) does not work properly on a system upgraded from OmniVista 4.2.2.R01 (MR2) to 4.3R2. Trap Severity should be “Major”. It is “Normal”.

Workaround: Restart the ovclient service from the Watchdog UI in OmniVista (Administrator – Control Panel – Watchdog); then correct the severity (from Normal to Major) in the Notifications application (Notifications – Trap Definition).

PR# OVE-3031

5.8 Known PolicyView Problems

5.8.1 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

5.8.2 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

5.8.3 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

5.8.4 Problems When Applying Unsupported Attributes in Policy List to AOS 8.x Switches After Upgrade from OV 4.2.2 GA

The “Send Trap” attribute is present in default policies but is not supported in AOS 8.x Switches. If you upgrade to OV 4.3R1 from OV 4.2.2 GA and configured policy lists in OV 4.2.2 GA containing this attribute, you will not be able to push that policy list to devices. This is not a problem if you are upgraded from OV 4.2.2 (MR2) or are working with a fresh install of OV 4.3R1.

Workaround: Create new policies/policy lists to replace the old policy lists containing the attribute.

PR# OVE-653

5.8.5 Layer 3 “Accept All” and “Deny All” Policies Fail

OV-L3-AcceptAllPolicy and OV-L3-DenyAllPolicy Policies Fail.

Workaround: Create new policies with the same conditions (“Accept All. “Deny All”), but set the trap attribute to “ignore”. Re-apply the policies to the devices.

PR # OVE-2753

5.9 Known Report Problems

5.9.1 Cannot Add Widget to Report if Current Data is More Than 16 MB

Cannot create a report containing more than 16 MB of data.

Workaround: A report can contain a maximum of 16MB of data (for a table report, such as Discovery - Inventory List, this is approximately 1,000 rows of data). If you are unable to generate a larger report, reduce the number of devices/rows in the report.

PR# OV-4463

5.10 Known Resource Manager Problems

5.10.1 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

5.10.2 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

5.10.3 Upgrade APs Shows Wrong Error Message

When upgrading an AP, a “Failed” error message is displayed because of the amount of time it takes to upgrade the software (< 5 minutes).

Workaround: Contact Customer Support.

PR# OVE-3018

5.10.4 Resource Manager Failed to Upgrade OS6350/6450 Switches

When upgrading OS6350 and OS6450 Switches, the upgrade times out and fails because of the amount of time it takes to remove older images files.

Workaround: Retry the upgrade in OmniVista. If unsuccessful, upgrade the image using the CLI. ALE is working on a patch for this issue.

PR# OVE-3160

5.10.5 “Restore” Must Be From The Same Release

You can only perform a restore using a backup from the same release (e.g., you can only restore a 4.3R2 configuration using a 4.3R2 Backup File). OmniVista will not allow you to perform a restore using a backup from a previous release.

Workaround: Informational

PR# CRNOV-675

5.11 Known Topology Problems

5.11.1 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

5.11.2 SPT Available Links Are Not Shown When More than 2 Devices Selected

SPT Available links are not shown when more than 2 devices are selected using 'Multiple Selection'.

Workaround: SPB Topology will only display SPT links between 2 nodes. If more than 2 nodes are selected, the "Show SPT Available Links" function is disabled.

PR# OVE-1491

5.11.3 Slow Discovery of Links of Newly Discovered Devices

SPB links do not appear in Topology when there are too many entries in the SPB SNMP tables.

Workaround: There is no workaround at this time. You can manually poll the switch, but the poll can take 10-20 minutes.

PR# OVE-3147

5.12 Known Unified Access Problems

5.12.1 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

5.12.2 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

5.13 Known UPAM Problems

5.13.1 Authentication Fails with Secret Key as "alcatel" Instead of "123456”

MAC and 1x authentication may fail if the NAS Client is using a different IP address than the Management IP address for RADIUS authentication.

Workaround: Configure the NAS Client to use the Management IP address for RADIUS authentication

PR# OVE-2025

5.13.2 No Way to configure OmniSwitch ASA using UPAM as AAA Server

UPAM does not support import of RADIUS dictionary.

Workaround: No workaround at this time.

PR# OVE-2187

5.13.3 Cannot Fully Customize UPAM Captive Portal Page

Full HTML customization is not available when creating UPAM Captive Portal Page in OmniVista.

Workaround: No workaround at this time. OmniVista does not support HTML-level customization.

PR# OVE-834

5.13.4 UPAM Authentication with an External LDAP Server Does Not Work with an Encryption Password Configured for the User

UPAM authentication does not work if you are using an external LDAP with an Encryption Password (e.g., MD5, SHA) configured for the user.

Workaround: If using an external LDAP Server for UPAM authentication, use a plain text password.

PR# OVE-818

5.13.5 Unable to Activate Old Certificate After Upgrade to OV Build 115

If you uploaded and activated a new certificate for UPAM RADIUS on the OV 422R01 GA build, after upgrading to 422R01 MR 2, OmniVista falls back to the default certificate. The new certificate is displayed in UPAM – Settings - RADIUS Server Certificate, but it is not activated.

This was only observed when upgrading from OV 422R01 GA to OV 422R01 MR 2. It did not occur when upgrading from OV 422R01 MR 1 to OV 422R01 MR 2.

Workaround: After the upgrade, go to UPAM- Settings - RADIUS Server Certificate. Remove the certificate that you used earlier, upload it again, and activate it.

PR# OVE-833

5.13.6 UPAM Does Not Work with LDAP if We Use Encryption Password for User

UPAM does not work with an External LDAP Server if the user password in encrypted.

Workaround: If UPAM is configured to use an External LDAP Server for user authentication, the user password must not be encrypted in the LDAP.

PR # OVE-818

5.13.7 CP/Guest-Authentication Fails with UPAM as RADIUS Server

CP/Guest-Authentication fails with UPAM as RADIUS Server. Client is unable to open redirect-url portal because 'hotspot login cannot open the page because it is not connected to internet'.

Workaround: There must be a DNS Server in the Customer Network for Captive Portal user authentication for wired devices if AOS is the network authenticating device. The DNS must resolve to the secondary OV IP address (UPAM address). This is not required for wireless devices authenticating through an AP.

PR # OVE-1693

5.13.8 802.1X Authentication with External Windows LDAP Failed When Logging in with User Credential

802.1X Authentication using an external Windows LDAP Server fails when Logging in with user credentials.

Workaround: Currently, UPAM does not work when using a Windows LDAP server for external LDAP Authentication. Use OpenLDAP on a Linux machine or AD on Windows Server.

PR # OVE-3000

5.13.9 Unable to Save AD Configuration

Unable to save the AD configuration on the OV2500 but test connect LDAP & AD is successful. Sometimes the RADIUS Service cannot bind to port 80 after it is stopped and restarted. This causes an error when applying an LDAP/AD configuration in UPAM.

Workaround: Reboot the VM.

PR # OVE-2438

5.13.10 No Tier 2 DFS Channel Support for US Domain

Tier 2 for US regulatory domain is not supported.

Workaround: NA

PR # OVE-819

5.13.11 HTTPs Traffic is Not Redirected to Portal Page for an HSTS Website

The first time a user opens an HSTS website, they are redirected to the portal page, as expected. The second time a user opens an HSTS website, the redirection will not work. If the user clears browser cache and retries connecting to the HSTS website, it will work. The behavior depends on the browser used. Chrome is very strict, so the problem is always seen, Firefox is not as strict; the problem will still happen but not as frequently.

Workaround: There is no workaround at this time.

PR # OVE-779

5.13.12 UPAM Web Portal Is Not Updated on OV After Changing

After reconfiguring the UPAM Web Portal IP with another IP address, the UI Does not update to display the new UPAM Web Portal IP address.

Workaround: Create a new Global Setting Profile with the new UPAM Web Portal IP address and apply it to devices.

PR # OVE-2973

5.14 Known Users and User Groups Problems

5.14.1 When You Configure the Analytics Application for a Role, the Performance Monitoring Application is also Configured

In OV 4.3R1, Performance Monitoring is a new feature and you can configure permissions of Analytics and Performance Monitoring application separately. However, if you upgrade to OV 4.3R1 from OV 422 MR2, the default permissions for the Performance Monitoring application are automatically derived from Analytics application permissions because the Performance Monitoring application is a sub-application of the Analytics application. This is expected behavior.

Workaround: NA

PR # OVE-1847

5.15 Known VM Manager Problems

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

VLAN notification 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

5.15.2 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

5.15.3 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

5.15.4 Live Search Does Not Work for VM IP Address/Switch IP Address

Live Search does not work when searching for VM IP address or Switch IP address.

Workaround: No workaround at this time.

PR# OVE-1908

5.16 Known Other Problems

5.16.1 Apostrophe Is an Invalid Character in SNMP Community String

Apostrophe Is an Invalid Character in SNMP Community String.

Workaround: Remove Apostrophe from the SNMP community string.

PR# 195715

5.16.2 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

5.16.3 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

5.16.4 Some OmniVista Features Do Not Work if the System Port is Changed

If a user changes the System Port using the VA Menu on a system that has been running, the system will not be able to reach the internet (for PALM, upgrades, etc.) via the network proxy since the port has been changed.

Workaround: Change the Proxy Port back to correct network Proxy Port. Go to Preferences - System Settings - Proxy.

PR# OVE-2127

5.16.5 OmniVista Cannot be Accessed by Web Client

OmniVista became unavailable to web clients, displaying the following error message on the browser: "OmniVista Error Fail to get current user".

Workaround: Restart ovclient or tomcat service.

PR# OVE-2220

5.16.6 Packet Drops When Roaming with OKC Enabled

When a client roams between APs with OKC enabled, some packets are lost. However, there is no disconnection or re-authentication.

Workaround: No workaround at this time.

PR# OVE-2218

5.16.7 WMA/UPAM Memory Not Updated After Upgrade

If you are upgrading from a previous build (not a fresh installation), the VA memory settings will not be upgraded for OV 2500 NMS-E 4.2.2.R01 (MR 2). This can cause problems in installations with more than 256 Stellar APs.

Workaround: If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply the VA memory settings. Go to the VA Menu, re-apply the memory settings, and reboot the VA.

This is not required if you have fewer than 256 Stellar APs, or if you are performing a fresh installation.

PR# OVE-1993/2048

5.16.8 Cannot Activate Old Certificate After upgrading to OV Build 115

If OmniVista had certificates (UPAM RADIUS Server Certificate) prior to MR 2, they are lost when upgrading to MR 2 and hence not available in 4.3R1.

Workaround: Re-import the certificate.

PR# OVE-833

5.16.9 Update Firewall Rules and Script to Enable DCOM When Creating Hyper V Profile

Error messages are displayed when trying to add a Hyper-V Hypervisor in the VM Manager Hypervisor Systems Screen.

Workaround: Make sure that the VMM Ports are configured as shown in Section 2.2.1 OmniVista 2500 NMS Ports. If the problem persists, follow the applicable DCOM procedure as detailed in Appendix A.

PR # OVE-1568

5.16.10 OV Nginx Service Does Not Start After Updating OmniVista Web Server SSL Certificate (OV 4.2.2 Build 115 MR-2)

If you update the OmniVista SSL Web Certificate using the VA Menu option, The OmniVista Nginx Service does not start up even if the VM is restarted.

Workaround: OmniVista does not support importing a Web Server SSL certificate with private key that was encrypted with password. Import a new SSL certificate with a private key not protected with a password and reboot OmniVista.

PR # OVE-1776

5.16.11 Unsupported Features in High-Availability (HA) Installation

The following features are not supported in a High-Availability (HA) Installation:

- Cluster IP configuration in L3 Cluster
- Two (2) NICs
- Configuring the UPAM Portal IP address on different subnet than the OmniVista IP address
- Upgrade from 4.3R1 HA to 4.3R2 HA
- Changing the OmniVista IP address and Hostname after creating the Cluster.
- Memory synchronization. When the active service is not available and failover happens, the data in memory of that service will be lost.
- Hostname in upper case.
- Changing/configuring Timezone
- Configuring an NTP client.

Workaround: NA

PR # OVE-2327

5.16.12 During OV Upgrade, User Must “Press Any Key” When Prompted

When a user is upgrading from OV 4.3R1 to OV 4.3R2, if the user does not “press any key” when prompted to continue the upgrade, the upgrade will fail.

Workaround: If this happens, perform the upgrade again and “press any key” when prompted to complete the upgrade

PR # OVE-2291

5.16.13 Cannot Upgrade from 4.3R1 Download Package After Selecting the “Download Only” Option

When upgrading from OV 4.3R1 to OV 4.3R2, if a user selects the option "To 4.3R1 (Upgrade to Latest patch of Current Release, if any)", then selects “Download Only”, and “Upgrade from downloaded package”, the following message is displayed “4.3R1 has not been yet downloaded on system”.

Workaround: Select option "Download and Upgrade" or select option "To new release".

PR # OVE-3112

5.16.14 Failover Banner Warning Redirects User to Inoperable Standby Node

If a user manually stops/restarts all services on the Active Node in an HA Installation, the Failover Banner will appear, directing the user to the Standby Node. Since a failover did not actually occur, the Standby Node will be inoperable.

Workaround: Ignore the Banner Warning. The Active Node will return once all services are restarted.

PR # OVE-3313

5.16.15 OVUPAM and OVRadius Services Do Not Start After OV Restore

When you perform a restore of OmniVista using the VA Menu, the ovupam and ovradius services may not start.

Workaround: After the restore is complete, reboot the VM.

PR # OVE-3142

5.16.16 Failover During VM Sync in HA Installation

Although extremely rare, there could be a case when a failover occurs during a sync between the Active and Standby Nodes in a High-Availability Installation. Since the failover interrupts the data sync, the Standby Node will not come up as the Active Node because it does not have the latest data.

Workaround: If it was a temporary problem with the Active Node that caused the failover, the Active Node may come up again and complete the sync. If the Active Node is permanently down, SSH to the Standby Node. On the HA Virtual Appliance Menu select **3 – Configure**

Cluster, then select **14 – Cluster Error Check**. When the error check is complete, the Standby Node will come up as the Active Node. Note that it may not have the most recent data since the sync was interrupted.

PR # OVE-1629

5.16.17 OV Hostname Cannot Be More than 15 Characters

When configuring the OmniVista Hostname in the VA Menu, the name can contain a maximum of 15 characters.

Workaround: Informational

PR # CRNOV-793

6.0 Release Notes PRs Fixed

6.1 PRs Fixed Since 4.3R1

- IAP SSID Generated a Default Role with the Same Name (OVE-795)
- Configure Traps for Multiple Devices Failed on Some Devices (OVE-838)
- Stellar APs do not show up after upgrade of OV from 4.2.1 to 4.2.2-build 115 (OVE-1023)
- Cannot Apply Policy List to VC of 8 or VC of 5 Devices for AOS 8.5R1 (OVE-1469)
- Cannot Collect Top N Clients Data for 6860 Switches Running AOS 8.5R1 (OVE-1742)
- “Cannot topology.msg.getMap” OmniVista 2500 NMS 4.2.2.R01 MR-2 (Build 115, 01/22/2018) (OVE-1783)
- Sorting Report List by Date does not sort by chronological order (OVE-1789)
- Some Stellar APs upgrade via OV failed (OVE-1806)
- OmniVista Not Displaying OS6560, OS9900 Switches When Mapping Tunnels in Unified Profile application (OVE-1816)
- OV server time (time zone) is not getting updated properly (OVE-1834)
- Unable to re-discover the switches after deleting them in Managed Devices using IP range (OVE-1872)
- OV doesn't display Trap Name for alaLldpTrustViolation of OS 6860 (OVE-1909)
- Group permission is changed when the user add/remove the user in Administrators group (OVE-1938)
- Monitoring Band Widget do not show up in the WLAN Dashboard (OVE-1943)
- OV Should allow SSH/Telnet to a Newly Added Device That Is Unreachable by SNMP (OVE-1949)
- OV2500: Unable to update the CLI/FTP user name and password for existing discovered switches. (OVE-1966)
- Error when sending test email with SMTP Authentication in Home > UPAM > Settings > Email Server (OVE-1973)
- Remove quota option in mongodb.cfg (OVE-2000)
- OV2500 SMTP/ Mail server communication issue port 25 (OVE-2288)
- Link between the Stellar AP and OS6860 switch is missing in the Topology tab (OVE-2294)

- Registration Status message on AP Registration Page is not descriptive of the underlying issue (OVE-2305)
- Topology Search Map Is Case Sensitive (OVE-2308)
- SSH Terminals in New Browser Tabs Do Not Show Device Name (OVE-2309)
- The list port of Access Auth Profile does not sort (OVE-2310)
- The item "OmniAccess Stellar APs" in Device Type in Topology should be changed as "WLAN" (OVE-2318)
- OV 4.3.51.R1 UPAM Captive Portal Authentication. Switch responding CoA NAK Unsupported attribute (OVE-2321)
- Don't allow the user to perform a restore using a backup from a previous release. (OVE-2326)
- The password is showed on the Captive Portal page after register the guest user by Phone Number (OVE-2336)
- CLI Scripting: Parameter should be moved "$" to display friendly at the last step when sending a scripting file (OVE-2426)
- OV 4.3.51.R1/UPAM Guest Access with Self-Registration, receipt contains some errors (OVE-2436)
- Resource Manager does not recognize OS6560_8.5.164.R01 ISSU zip package as an ISSU image set (OVE-2456)
- Resource Manager can't run backup after upgrading OV to 4.3R1 (OVE-2480)
- OV2500 4.3 Trap responder issue (OVE-2535)
- Settings of Managed Devices are not saved (OVE-2571)
- Need to customize the captive portal login page (OVE-2591)
- OV2500 sees OAW-AP1251 as down; device is reachable from OV via ICMP (OVE-2600)
- Resource Manager page is stuck and does not response (OVE-2647)
- Guest Account table content removed by the system all 2 hours (OVE-2735)
- KEC international. ; OV 2500 integrated with stellar AP (OVE-2749)
- [Locator] Change column headers of Netforward results (OVE-2895)
- [Locator] Allow Copy function in the MAC address field of the locator result (OVE-2896)
- [Locator] Should persist the sort setting in the locator result (OVE-2897)
- Support one new command "Show tech-support eng complete" in Collect Support Info app (OVE-2907)
- OV2500 unable to discover complete VM machines by the VM manager and license issue (OVE-2938)
- Remove auto trap config feature when discovering a new device in OV Enterprise (OVE-2945)
- AP coverage from Floor Plan application is very different from the actual coverage. (OVE-2948)
- The Compare page of Resource Manager could not load switch snapshots (OVE-2968)
- Operator available in OV2500 UPAM (OVE-2970)
- OV 2500 - display issue regarding the “changes” status of Stellar AP which is seen as « unsaved (OVE-2971)
- Cannot Use UTF8 Characters in Unified Profile Name (OV-4404)

- Errors Displayed During OmniVista Upgrade (OV-4752)
- Expired Guest/BYOD Devices Not Removed from Remember Devices Tab (OV-5104)
- Guest Access Approval Setting Is Reset After Upgrade to OV 422-MR 1 (OV-5182)
- OmniVista 2500 NMS 4.3 Extend Data Partition Issue and High CPU Usage (CRNOV-534)
- Customer OV2500 4.3R1 Issue with High CPU on the VM (CRNOV-561)
- Authenticating Record Module Is Not Responding on OV2500 4.3R01 B51 (CRNOV-572)
- Cannot delete a map in Topology, Button is Greyed Out (CRNOV-575)

6.2 PRs Fixed Since 4.2.2.R01 (MR 2)

- OV makes SSH connections to OS6860 switches every 15 minutes even though no AV profiles have been assigned to those switches (OVE-679)
- AP Stellar - Up Time received in the trap from AP is incorrect (OVE-727)
- HTTPs traffic is not redirected to Portal page (OVE-779)
- IAP SSID generated a default role with the same name (OVE-795)
- Add a Serial Number column in Managed Devices table (OVE-829)
- LAG member ports: No way to know which are members of a given LAG (OVE-843)
- Guest username does not support hyphen (OVE-845)
- Error message "Fail to load data from server" after waiting a long time to get the data in Top N port report (OVE-846)
- Backup Files table should show backup files by device and by latest time periods (OVE-856)
- OV does not support showing a serial number with the prefix 00 in Configuration > Resource Manager > Inventory (OVE-879)
- The associated time in WLAN Client list shows the incorrect time (OVE-989)
- User-installed OV Web Server SSL certificate was lost after upgrading from OV422GA to OV422 MR-2 (OVE-1065)
- Enhance TTS template configuration to input arbitrary IP (OVE-1151)
- 4.2.2.115.R01 – Vulnerabilities (OVE-1157)
- Initializing OV Cluster stops at "Synchronizing activemq data". Cannot go further because of unstable network (OVE-1302)
- CRAOS8X-1165 Notifying "one touch data" policy fails on 0S6465 8.5R01 (OVE-1457)
- Copy-Paste on Terminal (OVE-1482)
- The "Device DNS Name" on Netforward Result and "End station Name" on ARP Results are missing in OV 4.3R1 (OVE-1552)
- Analytics for AV (App count) is not showing data for Top User per application and Top Application per user after upgrade from OV42 MR2 (OVE-1593)
- Script triggering without considering the scheduled start time (OVE-1633)
- OV2500: Read and Write community strings are the same after OV discovers the switches (OVE-1762)
- The Locator polling was broken when receiving “disposition=null” from the switch (OVE-1785)

- Update Help pages/Release Notes for Preferred Node in HA configuration (OVE-1875)
- Upgrade from 422_115_MR to 431_42R1 failed during OV43R1 FAT (OVE-1886)
- Users are unable to authenticate after OV2500 reboot (ALEISSUE-156)
- UPAM/ Updated Guest/BYOD Device Validity Period options (ALEISSUE-166)
- Not able to manage the right side of the map/image when running "Heat Map" (ALEISSUE-168)
- Latvia country not configurable in the RF profile in OV enterprise (ALEISSUE-194)

6.3 PRs Fixed Since 4.2.2.R01 (MR 1)

- OmniVista Takes More Than One Hour to Boot Up (227970)
- UPAM authentication with and External RADIUS server will fail if the shared secret between UPAM and AP are different than the shared secret between UPAM and the External RADIUS server (OV-4242)
- UPAM External RADIUS Server Certificate Fails When Importing .der, .pfx Certificates (OV-4490)
- LLDP Link disappeared between OS6450 and Stellar AP (OV-4706)
- Monitoring and Enforcement CSV Files are not Getting Populated in OmniVista (OV-4751)
- Errors Displayed During OmniVista Upgrade (OV-4752)
- Unsecure Host Key Algorithm Used in VA for SFTP on Port 22 (OV-4765)
- UPAM Does Not Support NAS Clients with Different Keys (OV-4786)
- OmniVista Does Not Show Correct LLDP Port Numbers for 9900 Devices (OV-4886)
- Unable to Create Multiple Manual Links to the Same Port (OV-4913)
- SSH/SSL Security Vulnerabilities - CVE-2016-2183, CVE-2016-2183 (OV-5003)
- Application Visibility Stats in Summary View and Details View Not Updated Though There Are Flows (OV-5056)
- Account and Device Validity Period Set to 1 Day, But Device Displayed in Remembered Devices After 2 Days. Client Can Still Connect after 24 Hours (OV-5062)
- Not able to modify the Guest Access Strategy (OV-5063)
- Unable to Delete Expired Blacklist Client (OV-5084)
- UPAM External Log Server configuration is not saved (OV-5123)
- Guest username does not support hyphen (“-“) (OV-5146)
- UPAM Does Not Validate AOS Device Shared Secret (OV-5159)
- AOS Switches Frequently Show as “Down” (OV-5197)
- Issue with “Associated time” with WLAN Client – AM/PM Not Displayed (OV-5328)

6.4 PRs Fixed Since 4.2.2.R01 GA

- External RADIUS Users Cannot Utilize the Template Function (228018)
- Imported Floor Plan Does Not Display in Heat Map (OV-4640)

6.5 PRs Fixed Since 4.2.1.R01 (MR 2)

- Backup files are disordered by date (226863)
- Backup fail_operation failed on the device (226999)
- Some Switches are missing from PALM summary reports (227209)
- Boot up takes more than an hour (227704)
- Two folders switchbackups and switchBackups are displayed in cliadmin folder (228220)
- Update MIB for OS9900 from OV because this device displays type incorrectly as OS9907 (OV-2142)
- The value of " Last Known Up At" field between 2 features (Discovery and Topology) is mismatched (OV-2808)
- CLI Scheduled CLI Script Fails to Run (OV-2883)
- Report file for Discovery is empty (OV-2961)
- Display serial number in topology view (OV-3066)
- Support send scripts for Cisco devices (OV-3248)
- Hardware Inventory does not show Miniboot version and Firmware Version correctly for OS6450 device (OV-3283)
- OS6860 8.4.1.R02 cannot get IP from DHCP Server (Auto Configuration) (OV-3853)
- Topology does not react to link down trap sent from switches (OV-4007)
- New switches within the discovery range are not being discovered when full auto discovery polling is run (OV-4133)
- OV cannot get statistics if the devices are using SNMPv3 except MD5+DES (OV-4144)
- OV cannot send the script with long command (OV-4321)
- OV shouldn't use OID to display the info of Module-name and Description for OS6350 (OV-4557)
- Schedule reload the switch does not work (OV-4605)
- Failed to login to OV after upgrade if the previous system using external radius server (OV-4660)
- Schedule Configuration backup device with Incremental ON does not work (OV-4664)
- SNMP settings revert to default value if users provide FTP user/password at CLI scripting terminal (OV-4676)
- Filtering doesn’t work for the List view in Discovery/Range List (OV-4681)
- Cannot see Alarm widget data if OV using external radius server and users belongs to groups "Network Administrator", "Writers" and "Default" (OV-4683)
- Got the error "Failed to load data" from server when sending a long script to the device (OV-4684)
- Auto configuration entries do not display after restoring (OV-4700)

6.6 PRs Fixed Since 4.2.1.R01 (MR 1)

- User allowed to use the same Application Group Name for monitoring and enforcement. (PR 221096)
- User cannot navigate to Diagnostic Screen in Locator. (PR 220966)
- Certain Operations in Topology Fail Using I/E Browser (220967)

- OV421 GA to MR 1 upgrade failed the first time, and subsequent attempts to upgrade to MR 1 build were not successful because VA could not detect the new build in the Repository. (OV-2556)
- It takes a long time to load large log files in the Audit application. (OV-2623)
- Topology Map List sort order is not persistent. Sort order is now retained for the current OmniVista login session. (OV-2632)
- Not enough information in the Scheduler application for schedule Resource Manger Backup Jobs. Need job description and list of devices being backed up. (OV-2665)
- It takes a long time to re-discover existing switches in Discovery application. (OV-2672)
- When importing Third Party MIBs, if MIB Files are not sorted in the correct order, some MIB file imports failed because of dependencies on other MIB files. (OV-2680)
- A CLI Script scheduled to run periodically would fail with "STOPPING" status in Scheduler Jobs but show as "Running" in Scheduler History. (OV-2883)
- Analytics Port Utilization job in Scheduler application displays incorrect device list. (OV-2909)
- After performing an image upgrade of multiple devices, the “Install Upgrade Result Wizard” Results Screen is usually very long, forcing the webpage scroll-bar to display. As a result, users might not see the “Go to Topology to Reboot Device**”** link at the bottom of the screen, and know that they need to reboot the devices to complete the upgrade. The link has been moved to the top of the Results Screen. (OV-2990)
- In the Report application, the Backup Report does not include a Date Column. (OV-3195)
- The Role Based Access Control (RBAC) feature does not work for Discovery - Ports. (OV-3427)

6.7 PRs Fixed Since 4.2.1.R01 GA

- OmniVista should display ifAlias in addition to ifDescr in port pickers (PR 214448)
- In the Application Visibility application, the default option for Data Unit should be "Bytes" instead of "MB" for Counter Type/Byte Count (PR 220623) Create ClearPass Roles matching the names of the standard Enforcement Profiles (PR 220825)
- Tomcat shuts down on a system running for a long time (PR 220833)
- OmniVista using 127.0.0.1 as the NAS-IP instead of using the physical address in the RADIUS request sent (PR 221385)
- BYOD Diagnostics - Search for IP address for authenticated endpoint in ClearPass fails (PR 221798)
- BYOD fails to update Access Role Profile if it is associated with an Enforcement Policy (PR 221857)
- Read and Write community string are the same after OV discovers switches (PR 222203)
- OmniVista Scheduled reboot is not working (PR 222520)
- Backup Tab in Resource Manager is not responding. Screen takes a long time to load or never responds when there are a large number of backups. (PR 222706)
- Repetitive proxy message displayed when YouTube is not reachable from the OmniVista Server (PR N/A)

6.8 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)

6.9 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)

6.10 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)

6.11 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)

6.12 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)

6.13 PRs Fixed Since 3.5.7 Maintenance Build

- Live Search for IP Phones Issue (PR 187956)

6.14 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)

Appendix A – Enabling DCOM on Hyper-V

Follow the applicable procedures below to enable DCOM on a Standalone or High-Availability installation.

Enable DCOM on Hyper-V (Standalone Installation)

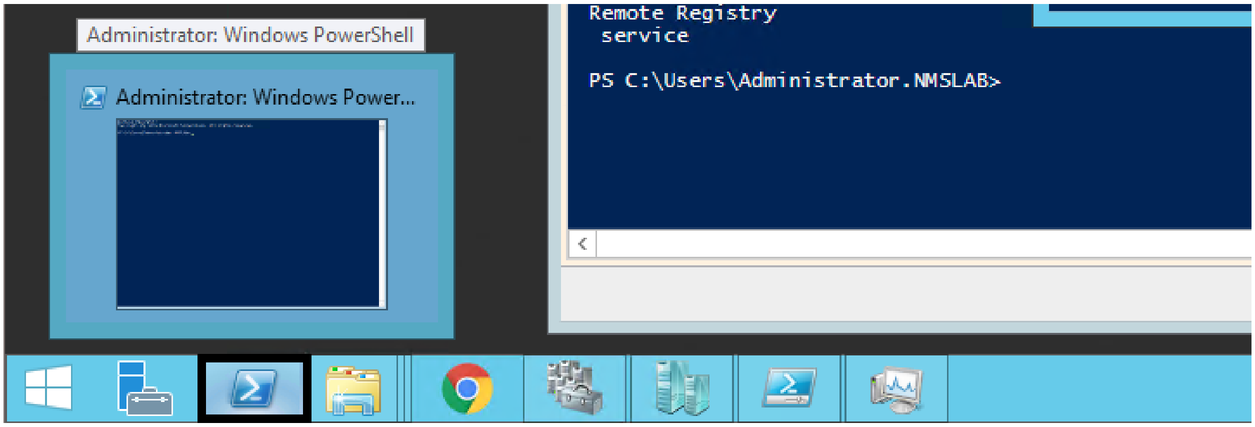
The following steps are specific to Windows 64 bit only.

1. Log in Hyper-V Server

2. Get the Powershell script from attachment: HyperV_Enable_DCOM_x64.ps1

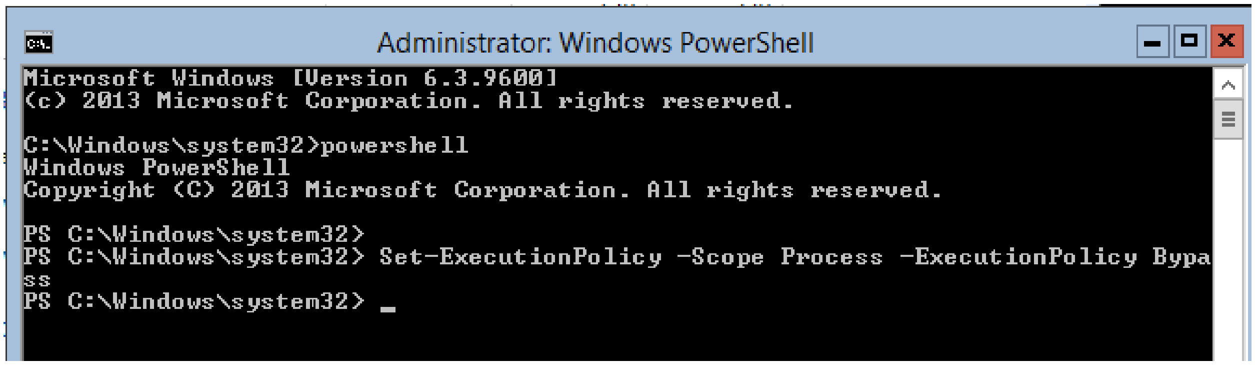
HyperV_Enable_DCOM_x64.ps1

3. Run Powershell.


Administrator: Windows PowerShell
Administrator: Windows Power...

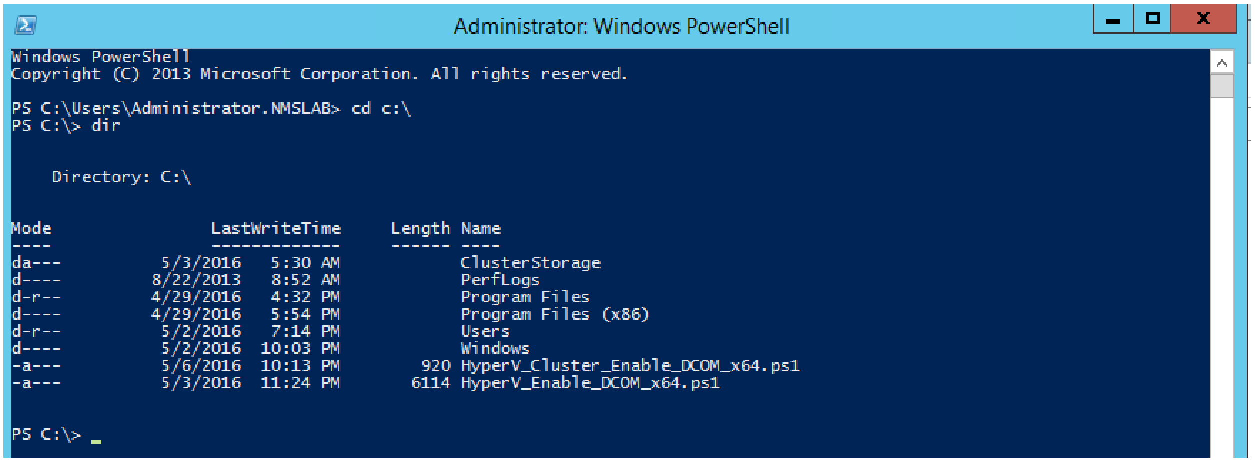
```
Remote Registry
 service

PS C:\Users\Administrator.NMSLAB>
```

4. Run Set-ExecutionPolicy -Scope Process - ExecutionPolicy Bypass.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
PS C:\Windows\system32> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypa
ss
PS C:\Windows\system32> _
```

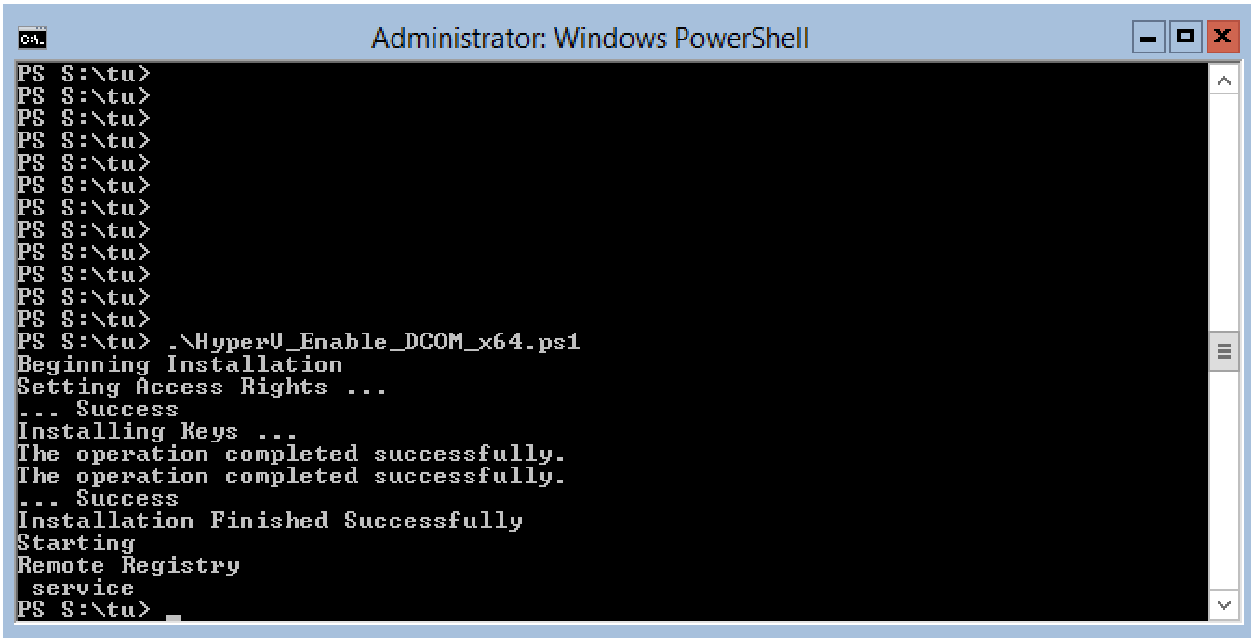
5. Change to the directory that contains the downloaded script from Step 2.



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.NMSLAB> cd c:\
PS C:\> dir


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
da---          5/3/2016   5:30 AM            ClusterStorage
d----         8/22/2013   8:52 AM            PerfLogs
d-r--         4/29/2016   4:32 PM            Program Files
d----         4/29/2016   5:54 PM            Program Files (x86)
d-r--          5/2/2016   7:14 PM            Users
d----          5/2/2016  10:03 PM            Windows
-a---          5/6/2016  10:13 PM        920 HyperV_Cluster_Enable_DCOM_x64.ps1
-a---          5/3/2016  11:24 PM       6114 HyperV_Enable_DCOM_x64.ps1


PS C:\> _
```

6. Open Registry Editor (regedit.exe) > create a backup by using Export.

7. Run .\HyperV_Enable_DCOM_x64.ps1.



```
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu>
PS S:\tu> .\HyperV_Enable_DCOM_x64.ps1
Beginning Installation
Setting Access Rights ...
... Success
Installing Keys ...
The operation completed successfully.
The operation completed successfully.
... Success
Installation Finished Successfully
Starting
Remote Registry
 service
PS S:\tu> _
```

Enable DCOM on Hyper-V (High-Availability Installation)

1. Log in the Active Hyper-V (Node 1) using the Cluster IP Address.

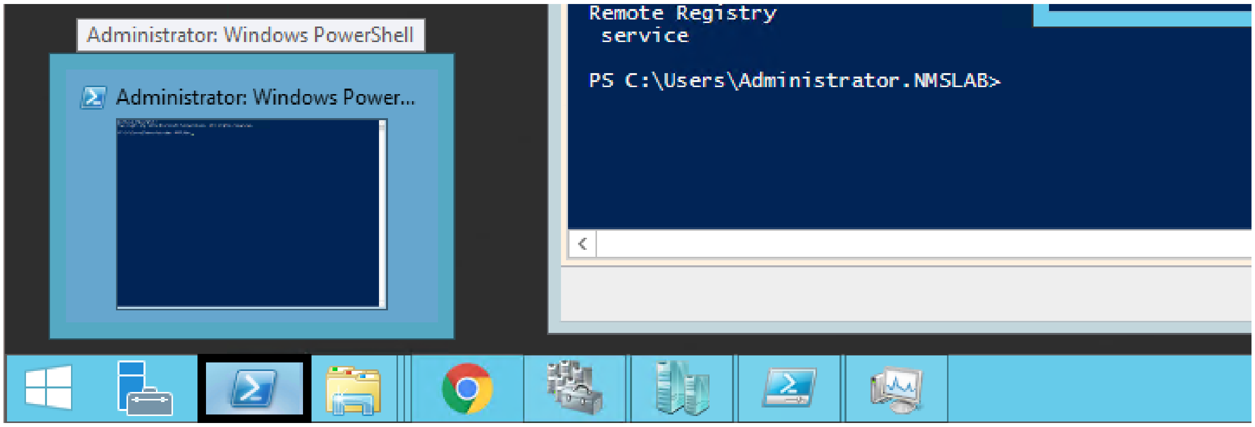
2. Download both files from the attachment and place them on the same directory:
HyperV_Cluster_Enable_DCOM_x64.ps1

HyperV_Cluster_Enable_DCOM_x64.ps1

HyperV_Enable_DCOM_x64.ps1

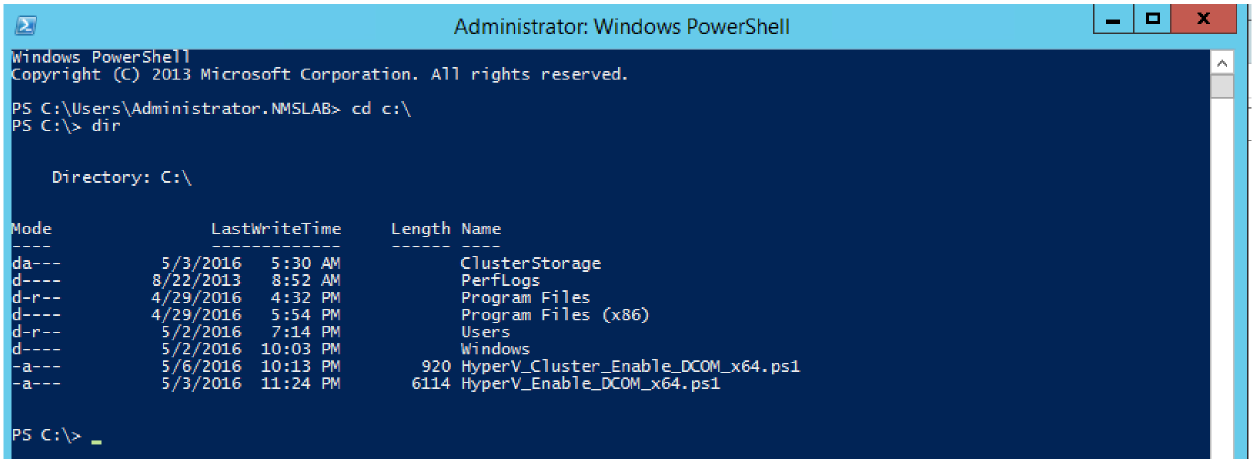
HyperV_Enable_DCOM_x64.ps1

3. Run Powershell.


Administrator: Windows PowerShell
Administrator: Windows Power...

```
Remote Registry
 service

PS C:\Users\Administrator.NMSLAB>
```

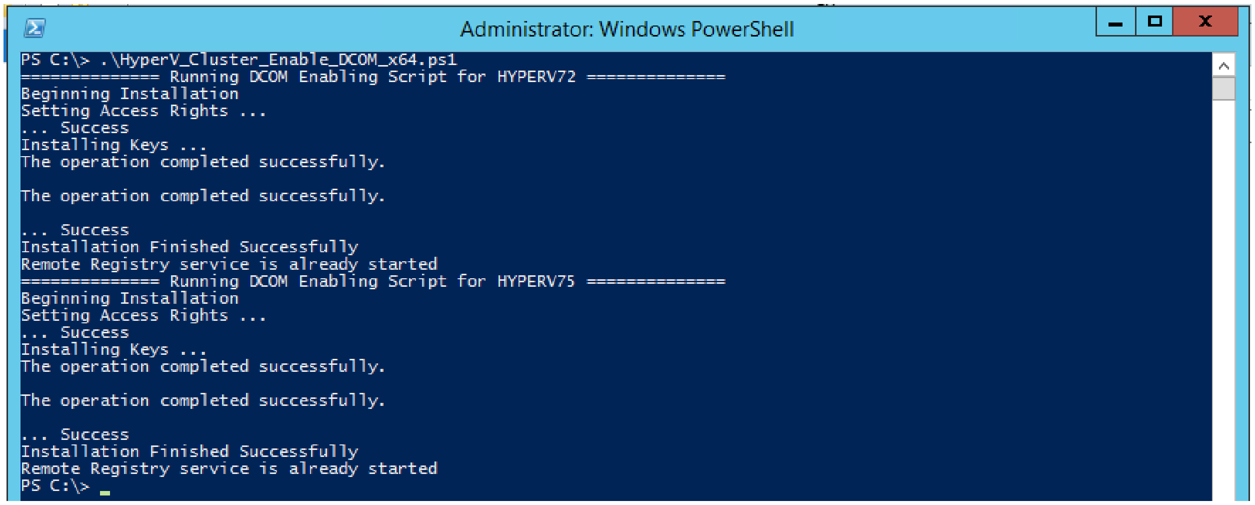
4. Change to the directory that contains the downloaded scripts from Step 2.



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.NMSLAB> cd c:\
PS C:\> dir


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
da---          5/3/2016   5:30 AM            ClusterStorage
d----         8/22/2013   8:52 AM            PerfLogs
d-r--         4/29/2016   4:32 PM            Program Files
d----         4/29/2016   5:54 PM            Program Files (x86)
d-r--          5/2/2016   7:14 PM            Users
d----          5/2/2016  10:03 PM            Windows
-a---          5/6/2016  10:13 PM        920 HyperV_Cluster_Enable_DCOM_x64.ps1
-a---          5/3/2016  11:24 PM       6114 HyperV_Enable_DCOM_x64.ps1


PS C:\> _
```

5. Open Registry Editor (regedit.exe) > create a backup by using Export.

6. Execute HyperV_Cluster_Enable_DCOM_x64.ps1.



```
PS C:\> .\HyperV_Cluster_Enable_DCOM_x64.ps1
============== Running DCOM Enabling Script for HYPERV72 ==============
Beginning Installation
Setting Access Rights ...
... Success
Installing Keys ...
The operation completed successfully.

The operation completed successfully.

... Success
Installation Finished Successfully
Remote Registry service is already started
============== Running DCOM Enabling Script for HYPERV75 ==============
Beginning Installation
Setting Access Rights ...
... Success
Installing Keys ...
The operation completed successfully.

The operation completed successfully.

... Success
Installation Finished Successfully
Remote Registry service is already started
PS C:\> _
```