Release Notes

for

OmniVista 2500 NMS Enterprise Version 4.3R1

June 2018

Revision A

Part Number 033326-00

READ THIS DOCUMENT

Includes OmniVista 2500 NMS for VMware ESXi: 5.5, 6.0, and 6.5

VirtualBox: 5.0.10

MS Hyper-V: 2012 R2 and 2016

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

Table of Contents

Table of Contents (continued)

Revision History

Release	Revision	Date	Description of Changes
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 4.3R1 (OV 2500 NMS-E 4.3R1) 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, and 6.5
- Virtual Box: 5.0.10
- MS Hyper-V: 2012 R2 and 2016.

This document details known problems and limitations in OV 2500 NMS-E 4.3R1, 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 3.0.3.x. for OV 2500 NMS-E 4.3R1. **First** upgrade to OV 2500 NMS-E 4.3R1; then upgrade your APs to AWOS 3.0.3.x. Please refer to the OV 2500 NMS-E 4.3R1 Installation Guide for details.

1.1 Technical Support Contacts

For technical support, contact your sales representative or go to the Support Site:

- 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 4.3R1

Hardware/Release Support

OmniVista High-Availability Feature

OmniVista 2500 NMS can now be deployed in a “High-Availability” configuration, with a redundant OmniVista Servers providing automatic failover if the Active server fails. The servers are synced and Standby server provides the same functionality as the Active server after failover. This feature requires a High-Availability License. Note that at this time the High-Availability Feature is only supported on small networks (“Low” - up to 500 devices). See Recommended System Configurations for more details on supported devices and required Hypervisor/VM configurations.

OS2220

OmniVista now supports the new OS2220 Light Manageability Switch. See Feature Set Support for details on supported OmniVista applications and features.

OS6465

OmniVista supports the new OS6465 Switch.

Stellar APs

- The AP1101-JP Stellar AP is now supported.
- OmniVista can now support up to 4,000 Stellar APs.
- The following new Stellar AP features are now supported:
  - **Bridge Mode -** Stellar APs can now be configured to act in Bridge Mode. Bridge Mode allows two Access Points from different networks to pair with each other to access shared resources.
  - **External Captive Portal Support -** You can now configure an External Captive Portal for authentication using the N2S Wi-Fi solution.
  - **Client Session Logging -** You can enable and configure logging for wireless client sessions as part of an Access Role Profile.
  - **Client Isolation -** Client isolation is a security feature to lock down your Wi-Fi clients to only access the internet. It is configured on the WLAN Service Screen.
  - **Smart Sticky Avoidance -** This feature is used to assist with client Wi-Fi roaming (e.g., 802.11k/802.11v protocol, Client Data Rate Controls, Minimum MGMT Rate Controls). It is configured on the WLAN Service Screen.

AOS and AWOS Upgrades

Refer to Section 2.0 - System Requirements for supported AOS/AWOS versions.

Application Updates/Enhancements

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

Topology

- **SPB –** Maps can be displayed to highlight all SPB-configured AOS Switches in an overlay. To view the SPB layout, click on **SPB Network** in the **Map Level Actions** drop-down button. Once in SPB Map mode, you can view link information for devices by BVLAN or SPT links between devices. You can also navigate to a new SPB Services Screen to view detailed information about all SPB Services. SPB is configured using the CLI.
- **ERP (Early Availability Feature) –** Maps can be displayed to highlight any configured ERP devices in an overlay. To view ERP configurations, click on **ERP Network** in the **Map Level Actions** drop-down button. Once in ERP Mode, all links for all ERP Rings are displayed. However, you can view information about links on a specific ERP Ring.

UI Enhancements

The OmniVista User Interface has been redesigned to improve user experience based on user feedback. The redesign includes

- Simplified menus
- Screen display optimization, targeting Network Operations Center (NOC) users, including:
  - Better use of screen real estate.
  - “At a Glance” Topology display, including Link Aggregation.
  - Improved navigation

AP Registration

- **New Bridge Tab -** A new Bridge Tab has been added to the Access Points Table to display information on Stellar APs working in wireless Bridge Mode.
- **New Web UI Device Management Tool -** A Web UI Device Management Tool is now available to view configuration information and perform limited management on individual Stellar APs. To access the Web UI Device Management Tool, select an AP in the Access Points List and click on the **AP Web** option in the **Action** drop-down. Access Points Screen.
- **Access Heat Maps for Individual Stellar APs -** You can view a Heat map for a Stellar AP by selecting an AP in the Access Points List and clicking on the **Heat Map** option in the **Action** drop-down.
- **New Certificate Screen -** The Certificate Screen is used to create a Security Certificate to be used to establish a secure connection between OmniVista and APs when using the Web UI Device Management Tool.
- **New External Captive Portal Config File Screen -** The External Captive Portal Config File Screen has been added to create a custom External Captive Portal Configuration File. The file is used to establish a secure connection between OmniVista and an external captive portal server for authentication of Stellar APs.
- **New AP Group Configuration Fields -** “AP Web” configuration fields are used to enable the AP Web option to connect to APs through the Web UI Device Management Tool. “Client Behavior Tracking” configuration fields are used to enable and configure collection of client logs.

Analytics

- New options have been added to the Top N Applications Report:
  - A “Tabular View” link has been added to the widget to display Application Discovery and Application Count data in table view. In addition, you display the table information “By Device” (switch generating the data) or “By Source” (IP address/client generating the data).
  - In addition to a Summary View, 6860/AP Reports now display data by “Top Users by Application” and “Top Applications by User”. Currently supported on OS6860E Switches only.

Application Visibility

The following new Rainbow application signatures are included in the Signature File for OS6860/6860E Switches and Stellar APs:

- echo360
- canvas
- kahoot

Audit

- **New Collect Support Information Screen –** You can now collect log information from a network device that you can send to Alcatel-Lucent Enterprise (ALE) Technical Support to troubleshoot problems. The log files you specify are collected and downloaded to your OmniVista Client's "Download" Folder in a ZIP File that you can then send to Technical Support. Currently supported on AOS devices only.

PolicyView

- **ICMP Conditions –** ICMP Type and Code Conditions are now available in the PolicyView application. ICMP Conditions are not supported on Stellar APs.
- **Service Condition –** The following protocols are now available when configuring a Service Condition: ICMP, GRE, RDP. ICMP Conditions are not supported on Stellar APs.

Resource Manager

Filters have been added to the Backup/Restore Screen to enable the user to view customize the backups displayed in the Backup Table. You can view backups by map, device, or AP Group. You can also display only the most recent backup for each device, or display only backups performed for the last week or for a specific time range.

Unified Access

- **Access Role Profile –** Fields on the Access Role Profile configuration screen have been updated to support the "Walled Garden" feature for Stellar APs. This feature allows users to authenticate through social media login, and also enables you to configure "whitelist" domains to direct users to certain website without authentication. Also, you can now configure Client Session logging as part of an Access Role Profile.

WLAN

- **WLAN Service –** New Roaming Control fields have been added to the WLAN Service Screen to configure the Stellar AP Smart Sticky Avoidance Feature to assist with client Wi-Fi roaming (e.g., 802.11k/802.11v protocol, Client Data Rate Controls, Minimum MGMT Rate Controls).
- **Heat Map –** You can now create a new Heat Map by cloning an existing map.

UPAM

- **Access Policy –** An "AP Group" mapping attribute has been added.
- **Authentication Strategy –** Upstream/Downstream Bandwidth fields have been added as part of a Network Enforcement Policy. Also, you can now specify a location policy as part of a Web Direction Enforcement Policy.
- **Built-In Certificate for Captive Portal –** There is now a built in FDQN based re-direct URL (https://ov2500-upam-cportal.al-enterprise.com) for Guest Portal and BYOD Portal (HTTPS). For APs, OmniVista will directly resolve the FQDN to the OV/UPAM address. Note that you must apply the "upamGlobalConfiguration" to the AP Group in the Unified Access Application (Unified Access – Template - Global Configuration – Settings). Wired devices still require DNS configuration.

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 4.3R1 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					
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			

Feature	OS10K 6900	OS6860/ OS6865	Other AOS	OS2220	Stellar APs	OA WLAN	OA ESR	3rd Party Switches
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-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 4.3R1:

AOS

- OS6250 – 6.7.1.R02, 6.7.1.R03, 6.7.1.R04
- OS6350 – 6.7.1.R04, 6.7.2.R02, 6.7.2.R03
- OS6400 – 6.4.5.R01 (limited support, restricted to PALM)
- OS6450 – 6.7.1.R04, 6.7.2.R02, 6.7.2.R03
- OS6465 – 8.5R1
- OS6560 – 8.4.1.R02, 8.4.1.R03, 8.5R1
- OS6850 – 6.4.4.R01
- OS6850E – 6.4.6.R01
- OS6855 – 6.4.6.R01

- OS6860/E – 8.4.1.R02, 8.4.1.R03, 8.5R1
- OS6865 – 8.4.1.R02, 8.4.1.R03, 8.5R1
- OS6900 – 8.4.1.R02, 8.4.1.R03, 8.5R1
- OS9700E– 6.4.6.R01
- OS9800E– 6.4.6.R01
- OS9900 – 8.4.1.R01, 8.4.1.R02, 8.4.1.R03
- OS10K – 7.3.4.R02, 8.3.1.R01

WebSmart

- OS2220 – 8.3.1.2

OmniAccess WLAN

- OAW-4030 – OAW 6.4.4, 6.5.1
- OAW-4704 – OAW 6.4.4, 6.5.1
- OAW-4604 – OAW 6.4.4, 6.5.1
- OAW-4x50 – OAW 6.4.4, 6.5.1

OmniAccess WLAN IAP

- IAP-105 – OAW 6.4.4, 6.5.1
- IAP-205 – OAW 6.4.4, 6.5.1
- IAP-225 – OAW 6.4.4, 6.5.1
- IAP-325 – OAW 6.5.1
- IAP-335 – OAW 6.5.1

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 3.0.3.x (only)
- OAW-AP1101-JP – AWOS 3.0.3.x (only)
- OAW-AP1221 – AWOS 3.0.3.x (only)
- OAW-AP1222 – AWOS 3.0.3.x (only)
- OAW-AP1231 – AWOS 3.0.3.x (only)
- OAW-AP1232 – AWOS 3.0.3.x (only)
- OAW-AP1251 – AWOS 3.0. 3.x (only)
- OAW-AP1101-ME – AWOS 3.0.3.x (only)
- OAW-AP1221-ME – AWOS 3.0.3.x (only)
- OAW-AP1222-ME – AWOS 3.0.3.x (only)
- OAW-AP1251-ME – AWOS 3.0.3.x (only)

Note: You cannot use older (or newer) AWOS with this OmniVista Release. If you are upgrading to OV 4.3R1 OmniVista from a previous release, you must upgrade AWOS devices to 3.0.3.x after the OmniVista upgrade.

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

OmniVista 2500 NMS-E 4.3R1 Upgrade Paths Certified

- 4.2.2.R01 (MR 2) – 4.3R1 (Standalone only)

2.1 Proxy Requirements

OV 2500 NMS-E 4.3R1 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 4.3R1 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

Service	Port	Source/Destination
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	1814	UPAM/Net Device
VMM	135	OV Server/Hyper-V Server
	49152-65535 (RPC Dynamic Port)	Hyper-V Server/OV Server

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 4.3R1 (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 4.3R1 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 4.3R1 Installation and Upgrade 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 directly upgrade to OV 2500 NMS-E 4.3R1 from OV 2500 NMS-E 4.2.2.R01 (MR 2). See the *OmniVista 2500 NMS-E 4.3R1 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 4.3R1, 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 4.3R1 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 4.3R1 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

To launch OV 2500 NMS-E 4.3R1, enter the IP address of the OmniVista 2500 NMS Server (e.g., https://<OVServerIPaddress>) in a supported web browser (Explorer 11+, Firefox 53+, Chrome 58+).

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 4.3R1 Services must be started to launch OV 2500 NMS-E 4.3R1. By default, Watchdog should start automatically when OV 2500 NMS-E 4.3R1 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 4.3R1

After launching OV 2500 NMS-E 4.3R1 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 Cannot Collect Top N Clients Data for 6860 Switches Running AOS 8.5R1

Unable to collect Top N Clients data for 6860 Switches running AOS 8.5R1.

Workaround: This an AOS 8.5R1 issue. No workaround at this time. Expected to be fixed with the release of 8.5R2.

PR # OVE-1742

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# OV-5332

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: Change the default buffer size to about 1000 lines. Ensure that this does not impact performance issues. Also, provide a preference setting in the CLI Scripting application to configure the number of lines of the buffer: 300 to 10,000. Default = 1000. If it does not create memory issues, please allow up to 100,000.

PR# OVE-998

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# OV-3818

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# OV-4396

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# OV-4709

5.6 Known Notifications Problems

5.6.1 Configure Traps for Multiple Devices Failed on Some Devices

When configuring traps for a large number of devices, some of the device returned a “This target has been interrupted” error message.

Workaround: Configuring traps on a large number of devices takes a long time. The “This target has been interrupted” error message is caused by the Web Service timing out. The traps are configured. Ignore the error message. You can verify that the traps were configured by going to the Trap Configuration Wizard, selecting the devices and viewing the configured traps.

PR# OV-4768

5.7 Known PolicyView Problems

5.7.1 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

5.7.2 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

5.7.3 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

5.7.4 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

5.7.5 Cannot Apply Policy List to VC of 8 or VC of 5 Devices for AOS 8.5R1

Unable to push a Policy List to a VC of 8 or 5 containing AOS Switches running AOS 8.5R1.

Workaround: This an AOS 8.5R1 issue. No workaround at this time. Expected to be fixed with the release of 8.5R2.

PR # (OVE-1469)

5.8 Known Report Problems

5.8.1 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

5.9 Known Resource Manager Problems

5.9.1 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

5.9.2 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 Known Topology Problems

5.10.1 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 Known Unified Access Problems

5.11.1 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

5.11.2 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

5.11.3 Cannot Use UTF8 Characters in Unified Profile Name

You cannot use UTF-8 characters in a Unified Profile name, only ASCII characters.

Workaround: No workaround at this time.

PR# OV-4404

5.11.4 IAP SSID Generated a Default Role with the Same Name

In WLAN Service, when you apply a configuration to an IAP to create an SSID (e.g., "f1-wlan"), OmniVista automatically creates a default “Role” object on the IAP by the same name (e.g., "f1-wlan") and attaches this Role for the SSID. OmniVista does not allow the SSID to be created as unrestricted (without Role attachment). This Role denies all traffic on the SSID. In effect, all traffic is blocked on the SSID. The problem exists only on IAPs.

Workaround: There is a “Default access role profile” that you specify in WLAN Service. If you want to use this Profile as Role object for the SSID on an IAP, make sure that the name of Default Access Role Profile is same as the name of ESSID. That way, when OmniVista creates the Role object on the IAP, it will create the Role object with the QoS rules specified inside Default Access Role Profile.

If you specify any other Default Access Role Profile in WLAN Service, it will be ignored when creating the SSID on the IAP. OmniVista will continue with auto-creating a new Role object as described above.

PR# OV-4780

5.12 Known UPAM Problems

5.12.1 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# OV-4252

5.12.2 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# OV-4306

5.12.3 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# OV-4480

5.12.4 Unable to Configure OmniSwitch ASA Using UPAM as AAA Server

Configuration for AOS ASA is not available in UPAM.

Workaround: No workaround at this time.

PR# OV-4306

5.12.5 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# OV-4589

5.12.6 Expired Guest/BYOD Devices Not Removed from Remember Devices Tab

Guest/BYOD Devices are not removed from the Remembered Devices Tab after expiration.

Workaround: No workaround at this time.

PR# OV-5104

5.12.7 Guest Access Approval Setting Is Reset After Upgrade to MR 1

If the Self Registration Strategy Approval setting was set to “Enabled” in the GA build, it is reset to “Disabled” in the MR 1 Build after upgrade. If set to “Disabled”, wireless guests can get online without the approval of their employee sponsor.

Workaround: If Approval was “Enabled” on the GA build, it must be manually re-enabled after the upgrade. This issued will be resolved in the MR 2 release. Upgrade from GA or MR 1 to MR2 will not have this issue.

PR# OV-5182

5.12.8 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# OV-5380

5.12.9 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

5.12.10 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 Known Users and User Groups Problems

5.13.1 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

5.14 Known VM Manager Problems

5.14.1 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

5.14.2 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

5.14.3 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 Known Other Problems

5.15.1 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

5.15.2 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

5.15.3 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

5.15.4 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# OV-3993

5.15.5 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# OV-4602

5.15.6 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# OV-4618

5.15.7 Errors Displayed During OmniVista Upgrade

“Mount Failed” and “Ownership” errors regarding the “switchbackups” directory are displayed when performing an OmniVista upgrade.

Workaround: Ignore the errors. The upgrade will complete successfully.

PR# OV-4752

5.15.8 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# OV-5378/5379

5.15.9 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

5.15.10 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

5.15.11 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

6.0 Release Notes PRs Fixed

6.1 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)

6.2 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)

6.3 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)

6.4 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)

6.5 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)

6.6 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)

6.7 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)

6.8 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)

6.9 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)

6.10 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)

6.11 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)

6.12 PRs Fixed Since 3.5.7 Maintenance Build

- Live Search for IP Phones Issue (PR 187956)

6.13 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)

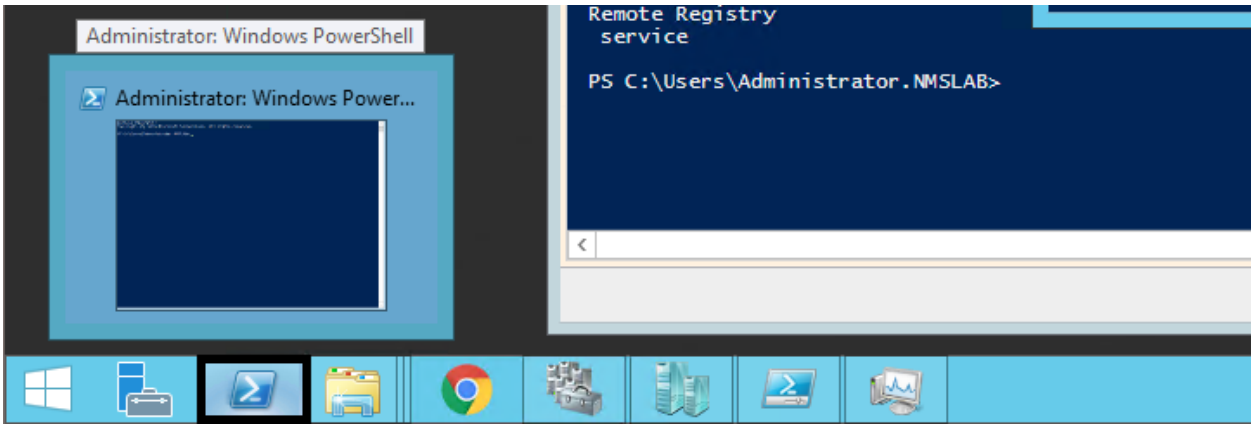
The following steps are specific to Windows 64 bit only.

1. Log in Hyper-V Server

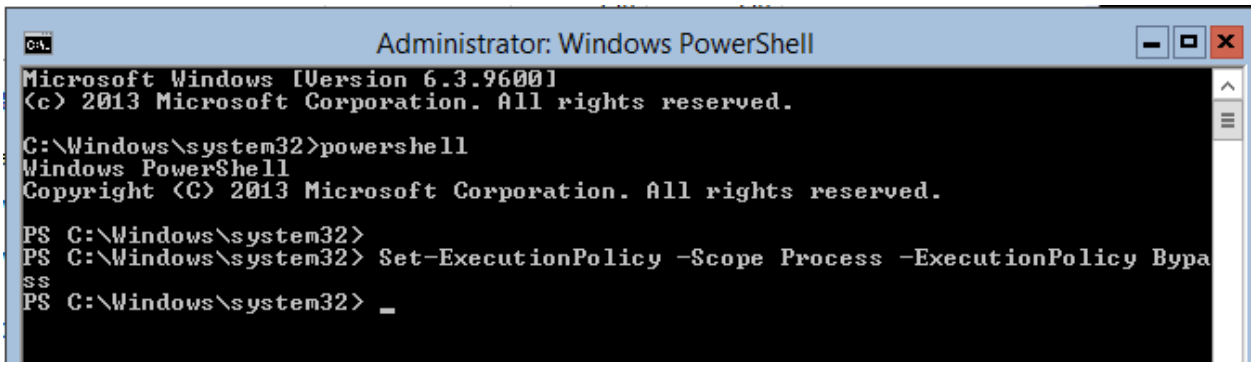
2. Get the Powershell script from attachment: HyperV_Enable_DCOM_x64.ps1

HyperV_Enable_DCOM_x64.ps1

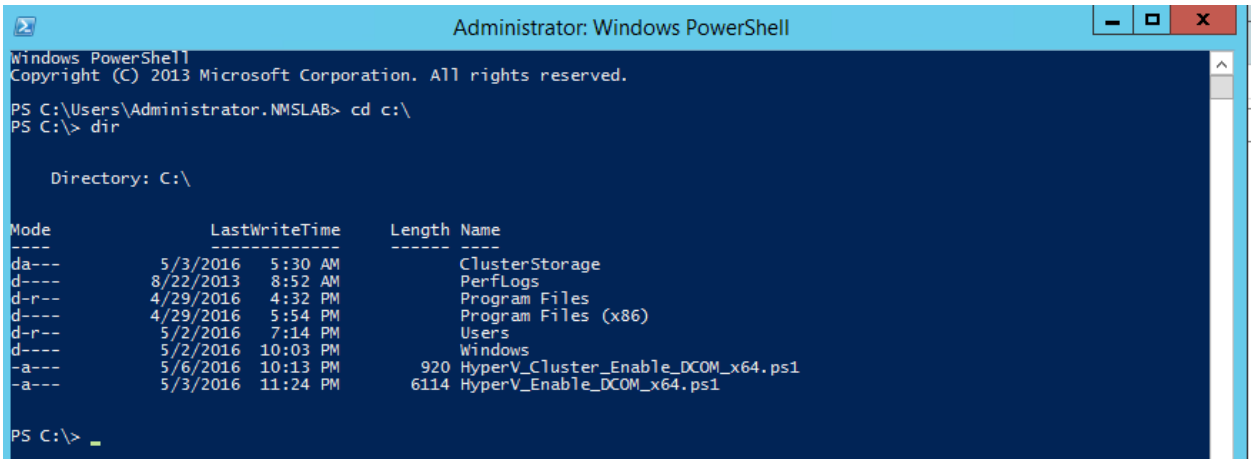
3. Run Powershell.



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

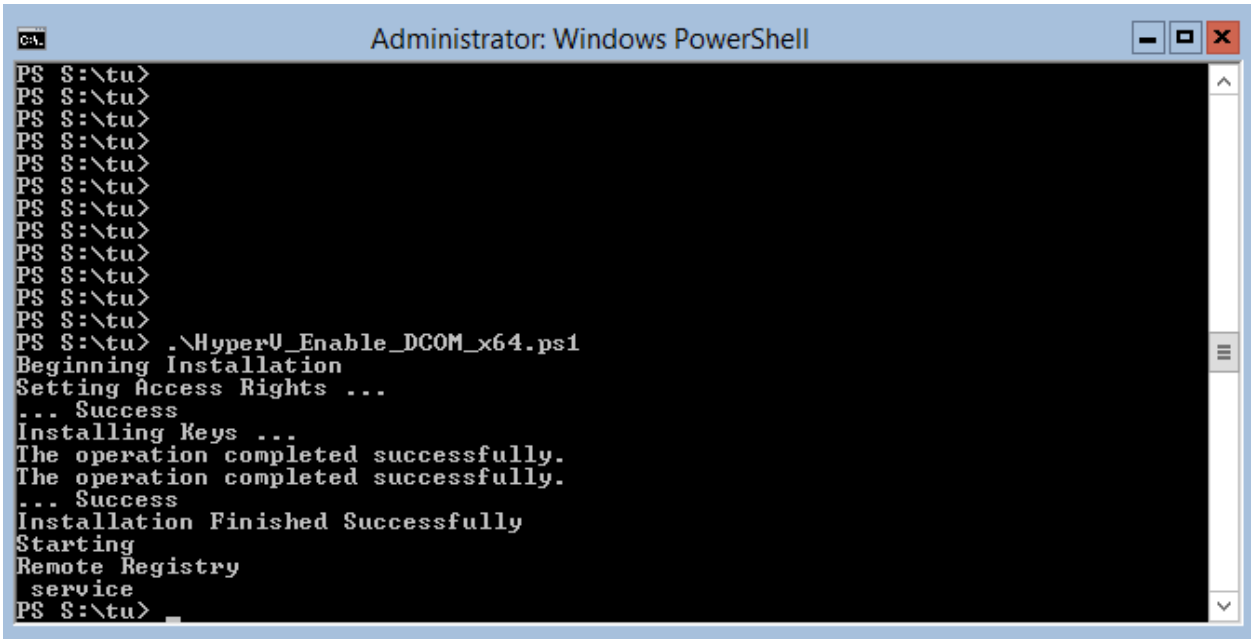


5. Change to the directory that contains the downloaded script from Step 2.



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

7. Run .\HyperV_Enable_DCOM_x64.ps1.



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

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

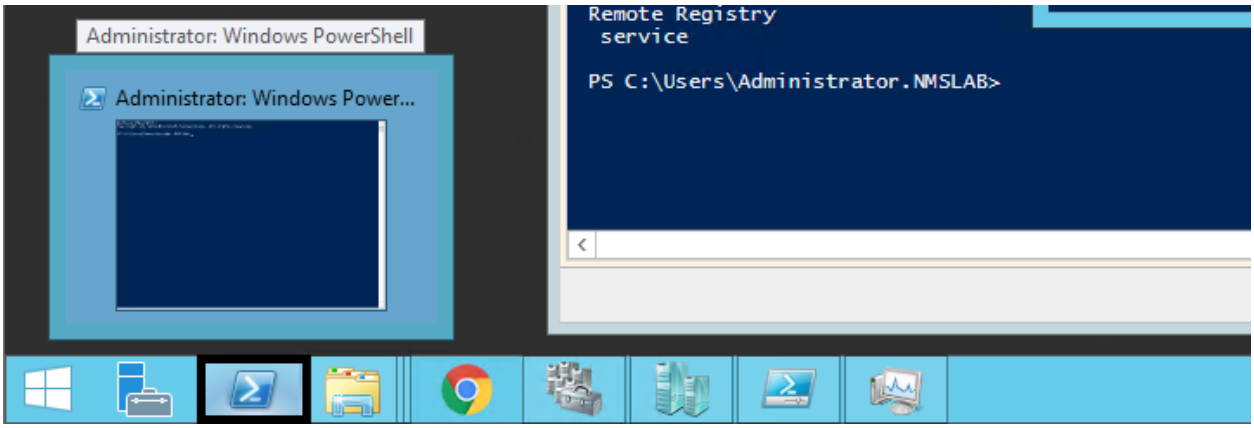
2. Download both files from the attachment and place them on the same directory:
HyperV_Cluster_Enable_DCOM_x64.ps1

HyperV_Cluster_Enable_DCOM_x64.ps1

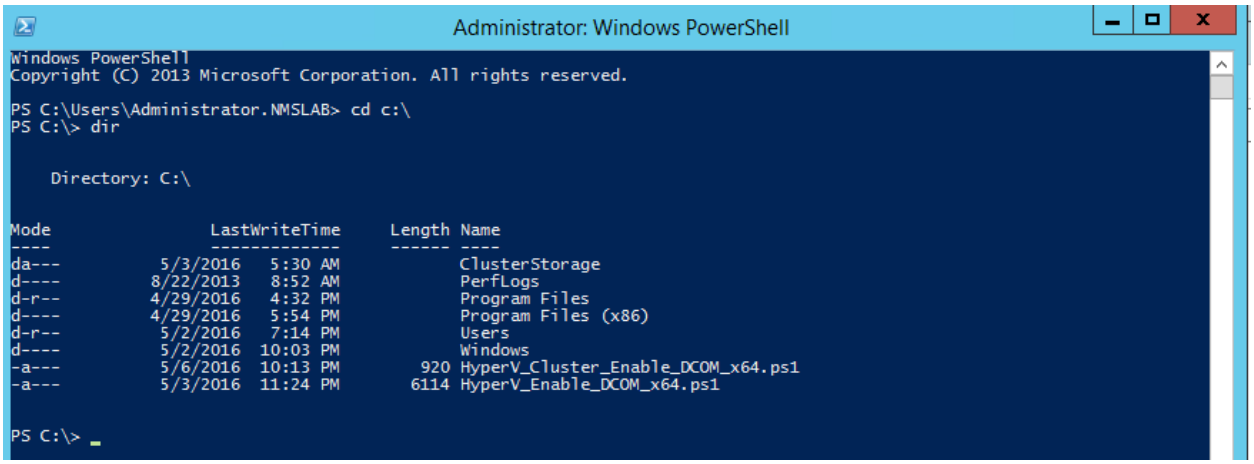
HyperV_Enable_DCOM_x64.ps1

HyperV_Enable_DCOM_x64.ps1

3. Run Powershell.



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



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

6. Execute HyperV_Cluster_Enable_DCOM_x64.ps1.