

**Release Notes
for
OmniVista 2500 NMS
Version 4.6R1**



**October 2021
Revision C
Part Number 033620-00
READ THIS DOCUMENT
OmniVista 2500 NMS
for
VMware ESXi: 6.5, 6.7, 7.0
MS Hyper-V: 2012 R2, 2016, and 2019
MS Hyper-V on Windows 10
Professional
Linux KVM on Centos 7.8/Ubuntu 20.04**

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

Table of Contents

1.0 Introduction	1
1.1 Technical Support Contacts	1
1.2 Documentation	1
1.3 New in this Release	1
1.4 Feature Set Support.....	3
2.0 System Requirements	7
2.1 Proxy Requirements	9
2.2 Firewall Requirements	9
2.3 Required Minimum System Configurations.....	11
2.4 High-Availability Installation Limitations	12
3.0 Installation	13
3.1 Licensing.....	13
3.2 Upgrading a Starter Pack or Evaluation License to a Production License.....	14
4.0 Launching OmniVista 2500 NMS	15
4.1 Logging Into OmniVista 2500 NMS 4.6R1	15
5.0 Known Problems	15
5.1 Known AP Registration Problems	15
5.2 Known CLI Scripting Problems	16
5.3 Known Discovery Problems	16
5.4 Known Locator Problems	17
5.5 Known mDNS Problems	17
5.6 Known Notifications Problems	18
5.7 Known PolicyView Problems.....	19
5.8 Known Resource Manager Problems	19
5.9 Known Topology Problems	20
5.10 Known Unified Access Problems	20
5.11 Known UPAM Problems.....	21
5.12 Known Users and User Groups Problems	23
5.13 Known VM Manager Problems	24
5.14 Known Web Content Filtering Problems	24
5.15 Known WLAN Problems.....	25
5.16 Known Other Problems	27
6.0 Release Notes PRs Fixed	31
6.1 PRs Fixed Since 4.5R3.....	31
6.2 PRs Fixed Since 4.5R2.....	35

OmniVista 2500 NMS 4.6R1 Release Notes

6.3 PRs Fixed Since 4.5R1	37
6.4 PRs Fixed Since 4.4R2	44
6.5 PRs Fixed Since 4.4R1	49
6.6 PRs Fixed Since 4.3R3	52
6.7 PRs Fixed Since 4.3R2	55
6.8 PRs Fixed Since 4.3R1	56
6.9 PRs Fixed Since 4.2.2.R01 (MR 2)	58
6.10 PRs Fixed Since 4.2.2.R01 (MR 1)	59
6.11 PRs Fixed Since 4.2.2.R01 GA	60
6.12 PRs Fixed Since 4.2.1.R01 (MR 2)	60
6.13 PRs Fixed Since 4.2.1.R01 (MR 1)	61
6.14 PRs Fixed Since 4.2.1.R01 GA	61
6.15 PRs Fixed Since 4.1.2.R03	62
6.16 PRs Fixed Since 4.1.2.R02	62
6.17 PRs Fixed Since 4.1.2.R01 Maintenance Release	62
6.18 PRs Fixed Since 4.1.2.R01	62
6.19 PRs Fixed Since Release 4.1.1	63
6.20 PRs Fixed Since 3.5.7 Maintenance Build	63
6.21 PRs Fixed Since Release 3.5.7 GA	63
Appendix A – Enabling DCOM on Hyper-V	1
Enable DCOM on Hyper-V (Standalone Installation)	1
Enable DCOM on Hyper-V (High-Availability Installation)	2

Revision History

Release	Revision	Date	Description of Changes
4.6R1	A	09/28/20	GA Release
4.5R3	B	04/21/20	Release Notes Update
4.5R3	A	03/30/20	GA Release
4.5R2	A	11/23/20	GA Release
4.5R1	C	06/05/20	Release Notes Update
4.5R1	B	04/29/20	Release Notes Update
4.5R1	A	04/21/20	GA Release
4.4R2	A	11/14/19	GA Release
4.4R1	C	09/09/19	Release Notes Update
4.4R1	B	07/24/19	Release Notes Update
4.4R1	A	07/15/19	GA Release
4.3R3	A	03/15/19	GA Release
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

1.0 Introduction

This document details known problems and limitations in OmniVista 2500 NMS 4.6R1 (OV 2500 NMS 4.6R1), 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.

OmniVista 2500 NMS 4.6R1 (OV 2500 NMS 4.6R1) is installed as a Virtual Appliance, and can be deployed on the following hypervisors:

- VMware ESXi 6.5, 6.7. 7.0
- MS Hyper-V: 2012 R2, 2016, and 2019
- MS Hyper-V on Windows 10 Professional
- Linux KVM on Centos 7.8/Ubuntu 20.04.

1.1 Technical Support Contacts

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

- <https://myportal.al-enterprise.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 this Release

Hardware/Release Support

Switches

- **OS2260 Series Switches** - The new OS2260 Series Switch is now supported. The following models are available: OS2260-10, OS2260-P10, OS2260-24, OS2260-P24, OS2260-48, and OS2260-P48. See [Device Feature Support](#) for a list of supported features.
- **OS2360 Series Switches** - The new OS2260 Series Switch is now supported. The following models are supported: OS2360-24, OS2360-48, OS2360-P24, OS2360-P48, OS2360-P24X, and OS2360-P48X. See [Device Feature Support](#) for a list of supported features.
- **New OS6900 Switch Model** - OS6900-V48C8 switches are now supported.

Stellar APs

- **OAW-AP1351** - OAW-AP1351 is now supported in OmniVista.

Software

- **AOS 5.1R1** - OmniVista 2500 NMS now supports AOS 5.1R1 for the new OS2260 and OS2360 Series Switches.
- **AOS 8.7R3** - OmniVista 2500 NMS now supports AOS 8.7R3 on all previously supported AOS Switches.
- **AWOS 4.0.3** - OmniVista 2500 NMS now supports AWOS 4.0.3 on all supported Stellar APs.
- **ESXi 7.0** - ESXi 7.0 is now supported for OmniVista Hypervisor and RAP Hypervisor installations.

New Applications

The following section details new applications introduced in this release.

- **Introducing OmniVista Cirrus 10.1**
A “teaser” version of OmniVista 10.1 is now available. OmniVista Cirrus 10.1 is a cloud-based Network Management System (NMS) that simplifies monitoring and troubleshooting of Stellar Access Points through detailed QoE Measurements and WiFi Analytics in an easy-to-read dashboard display. An existing installation of OmniVista 2500 NMS 4.6R1 or OmniVista Cirrus 4.6.1 is required to initially discover, register, and manage Stellar Access Points. Once discovered, the Access Points are then configured to send events to OmniVista Cirrus 10.1, where the data is gathered and can be analyzed by a Network Administrator. For more information see [Getting-Started](#) with OmniVista Cirrus 10.1.

To access OmniVista Cirrus 10.1, use the following URL:

<https://manage.ovcirrus.com>

Application Updates/Enhancements

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

Audit

- **User Activity Report Purge Settings Can Now Be Controlled from the UI.**
 - User can control how long they want to retain the user activity history. Range: 7 days to 365 days, Default = 90 days.

CLI Scripting

- **Tabs Added to the CLI Terminal Screen**
 - If you open multiple CLI Terminal sessions, the IP address of each device is displayed in a tab at the top of the Terminal Screen for easy access.

Discovery

- When you get a warning status for a device, the word “warning” now provides a link to the SNMP Traps for that device.

Resource Manager

- **Restoring an RMA Switch from a Golden Config or Resource Manager Backup**
 - OmniVista now supports RMA use case via Golden Config and Resource Manager Backup features.

SSID

- **Option to Enable/Disable UAPSD**
 - You can now enable/Unscheduled Automatic Power Save Delivery (UAPSD) on an SSID. The UAPSD field is located in the “Advanced WLAN Service Configuration” section when configuring an SSID. The field is also available on the WLAN (Expert) page. (Default = Enabled)
 - SSID UI is now enhanced to differentiate AP groups that advertise SSIDs according to a configured schedule versus those that advertise SSIDs all the time.

UPAM

- You can now disable multiple accounts at the same time.

WLAN

- **RF Profile Support for 160 MHz Channel Width.**
- **Kick-off Client is now allowed from the Wireless Client List page.**
- **AP Support Roaming RSSI Threshold for non-802.11K/V Clients**

OmniVista Framework Improvements

Performance

- **New Performance Improvements**
 - OmniVista now supports polling of large SNMP tables using REST API for switches running greater or equal to AOS 8.7R3. Enabled by default; go to Managed Devices settings to disable polling.
 - Topology improved to handle large number of devices and links in the network.

1.4 Feature Set Support

1.4.1 OmniVista REST API Management

You can use REST APIs for scripting or integration with any third-party systems in your management network. Available OmniVista REST APIs can be found here:

<https://ovcirrus.com/api>.

1.4.2 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	<ul style="list-style-type: none"> All supported AOS OmniSwitch Devices, including OS2260 and OS2360 	WebView
Web UI	<ul style="list-style-type: none"> OS2200 	Web UI Device Management
Web UI	<ul style="list-style-type: none"> All supported Stellar APs 	Web UI Device Management
Wireless Controller	<ul style="list-style-type: none"> OAW-4030, OAW-4604, OAW-4704, IAP-105, IAP-205, IAP-225 	OAW EMS
Third-Party	<ul style="list-style-type: none"> Cisco, OmniAccess ESR, Aruba OS 	Respective EMS

1.4.3 Device Feature Support

The following table details OmniVista 2500 NMS 4.6R1 feature support by device:

Feature	OS6900	OS6860/OS6865	Other AOS	OS2220	OS2260 OS2360	Stellar APs	Legacy WLAN	3rd Party Switches
Application Visibility (1)		X				X		
Analytics (2)	X	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			X		
CLI Scripting	X	X	X		X	X (5)	X	X
Discovery	X	X	X	X	X	X	X	X (3)
IoT (6)	X	X				X		
Locator	X	X	X	X	X	X	X	X (7)
mDNS		X	X (8)					
mDNS Gateway (9)	X	X	X			X		
mDNS Responder (10)	X	X	X			X		
Provisioning (11)	X	X	X		X			
PolicyView-QoS	X	X	X			X	X	
Premium Service (BYOD)		X	X					
ProActive Lifecycle Mgmt (PALM)	X	X	X	X	X	X	X	
Quarantine Manager (12)		X	X				X	

OmniVista 2500 NMS 4.6R1 Release Notes

Feature	OS6900	OS6860/OS6865	Other AOS	OS2220	OS2260 OS2360	Stellar APs	Legacy WLAN	3rd Party Switches
Resource Manager BU/Restore/Upgrade	X	X	X		X	X		
SIP (13)		X	X					
SPB/ERP (14) (15)	X	X	X					
Remote CLI	X	X	X				X	X
Topology Links (LLDP) (16)	X	X	X	X	X	X		
Trap Absorption	X	X	X	X	X	X	X	X
Trap Display/Trap Responder	X	X	X	X (17)	X	X	X	X
Trap Replay	X	X	X		X	X		
UPAM (Guest User, BYOD) (18)	X	X	X			X		
UNP (19)	X	X	X			X		
VLAN Configuration	X	X	X		X (20)		X	
VM Manager (21)	X	X	X		X			
VM Snooping	X (22)							
VRF	X	X	X					
VXLANS	X (23)							
Web Content Filtering (24)						X		
WLAN (SSID)						X		

1. The Application Visibility feature is supported on 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 all Stellar APs models except AP1101 and AP1201H. (AP132x and AP136x models require minimum Signature Kit version of 3.6.11.) Application Visibility is supported on OS6860N Switches (8.7R2 and later).

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), OS6860N (8.7R1 and later), OS6900 (8.3.1.R01 and later), and OS9900 (8.3.1.R02 and later). It is also supported on Stellar APs (except for Top N Ports, Top N Application and Clients – sFlow, and performance monitoring). Top N Clients are not supported on OS2260 and OS2360.

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), OS6860N (8.7R1 and later), OS6250, and OS6450 (6.7.1.R02 and later), and OS6860 (8.3.1.R01 and later), and Stellar APs.

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

6. IoT is supported on AOS switches running AOS 8.6R1 and higher and Stellar APs running AWOS 4.0.0.42 and higher. IoT Enforcement is only supported on OS6560-P48Z16 models with part number 904044-90. Models with part number 903954-90 are not supported.

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

8. AOS 6.4.6.R01 and later switches only.

9 mDNS Gateway is supported on OS6450 switches running AOS 6.7.2.R02 or higher; and OS6860E, OS6865, and OS6900 switches running 8.4.1.R02 or higher, and OS6860N (8.7R1 and later).

10. The following devices can be configured as Responder Devices: OS6860/E, OS6865, OS6900, OS9900, running AOS 8.7R1 and higher. The following devices can be configured as Edge Devices: OS6465, OS6560, OS6860/E, OS6865, OS6900, and OS9900, running AOS 8.5R1 and higher; and Stellar APs running 4.0.1.44 and higher (except for OAW-AP1101).

11. The Provisioning application is supported on OS6350, OS6450 (running AOS 6.7.2.R06 and higher); and OS6465, OS6560, OS6860, OS6860E, OS6865, and OS6900 switches (running AOS 8.4.1.R03 and higher), and OS6860N (8.7R1 and later).

12. The TAD feature in Quarantine Manager is only supported on OS6850, OS6855, OS9700 switches running AOS 6.4.6.R01. Quarantine Manager is supported on OS6250, OS6350, OS6450, OS6850, OS6855, OS6860, and OS6900 switches, as well as OA WLAN Devices.

13. 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).

14. SPB is supported on OS6860, OS6860E, OS6860N, OS6865, OS9000, OS6900, and OS9900 switches. You can view SPB configurations in the Topology application. SPB Services can be configured in the Services application (Configuration – Services)

15. ERP is supported as “early availability” feature on OS6465, OS6560, OS6860N, OS6850, OS6855, OS6860, OS6860E, OS6865, OS9000, OS6900 (excluding C32 and V72 models), and OS9900 switches. You can view ERP configurations in the Topology application.

16. 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”.

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

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

19. The UNP feature within Unified Access is supported on 6250, 6450, 6560, 6850E, 6855, 6860, OS6865, 6900, OS9900, devices, and OAW Controller and OAW IAP.

20. Dynamic VLAN configuration is not supported on OS2260 and OS2360 switches; only static VLAN configuration is supported.

21. The VM Manager application is not supported if OmniVista is deployed on Hyper-V 2019. In addition, only the English version of third-party software (VMware's vSphere, Citrix XenServer, or Microsoft Hyper-V) that VM Manager interfaces with is tested and certified; other languages may work, but they are not certified.

22. VM Snooping is supported on OS6900 switches (7.3.4.R02 and later). 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.

23. VXLANs are supported on OS6900-Q32/X72/C32/V72 switches.

24. Web Content Filtering is supported on Stellar APs running AWOS 4.0.2 and higher (except AP1101, AP1201H, AP1201L, and AP1201HL models).

1.4.4 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.

You can also connect to a device using a custom SSH client installed on your computer (SecureCRT®). Select a device in the Managed Devices List, click on the **Actions** button and select **SSH Custom**. You can also select a switch in a topology map, click on the CLI Scripting action, and select the **SSH Custom** option. This has been certified using SecureCRT®.

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 4.6R1:

AOS

- OS2260 – 5.1R1
- OS2360 – 5.1R1
- OS6250 – 6.7.1.R02, 6.7.1.R03, 6.7.1.R04
- OS6350 – 6.7.2.R06, 6.7.2.R07, 6.7.2.R08
- OS6360 – 8.7R2, 8.7R3
- OS6450 – 6.7.2.R06, 6.7.2.R07, 6.7.2.R08
- OS6465 – 8.7R1, 8.7R2, 8.7R3
- OS6560 – 8.7R1, 8.7R2, 8.7R3
- OS6850 – 6.4.4.R01
- OS6850E, OS6855 – 6.4.6.R01
- OS6860/E – 8.7R1, 8.7R2, 8.7R3
- OS6860N – 8.7.R1, 8.7R2, 8.7R3
- OS6865 – 8.7R1, 8.7R2, 8.7R3

OmniVista 2500 NMS 4.6R1 Release Notes

- OS6900 – 8.7R1, 8.7R2, 8.7R3
- OS6900 X48C4E - 8.7R2, 8.7R3
- OS6900 V48C8 – 8.7R3
- OS9700E, OS9800E– 6.4.6.R01
- OS9900 – 8.7R1, 8.7R2, 8.7R3

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 6.5.4, 8.3.0
- IAP-205 – OAW 6.5.4, 8.3.0
- IAP-225 – OAW 6.5.4, 8.3.0
- IAP-325 – OAW 6.5.4, 8.3.0
- IAP-335 – OAW 6.5.4, 8.3.0

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

The following AP models are supported. The recommended AWOS version is 4.0.3.

- OAW-AP1101
- OAW-AP1201
- OAW-AP1201L (available for China/Brazil only)
- OAW-AP1201HL (available for China only)
- OAW-AP1201H
- OAW-AP1201BG
- OAW-AP1221, OAW-AP1222
- OAW-AP1231, OAW-AP1232
- OAW-AP1251
- OAW-AP1301
- OAW-AP1311
- OAW-AP1321, OAW-AP1322

OmniVista 2500 NMS 4.6R1 Release Notes

- OAW-AP1351
- OAW-AP1361, OAW-AP1361D, OAW-AP1362

Note: If you are upgrading to OV 4.6R1 OmniVista from a previous release, it is recommended that you upgrade AWOS devices to AWOS 4.0.3 after the OmniVista upgrade.

Note: See the *AWOS 4.0.3 Release Notes* for more information on Stellar APs and details on any known issues.

OmniVista 2500 NMS 4.6R1 Upgrade Paths Certified

- Standalone Upgrade
 - 4.5R3 Standalone Installation to 4.6R1 Standalone Installation
 - To upgrade from older releases, you must first upgrade to 4.5R3.
- High-Availability (HA) Upgrade
 - 4.5R3 HA Installation to 4.6R1 HA Installation
 - To upgrade from older releases, you must first upgrade to 4.5R3 HA.
- Standalone to High-Availability (HA) Conversion
 - You can convert a 4.6R1 Standalone Installation to a 4.6R1 HA Installation if the 4.6R1 Standalone installation was upgraded from a 4.3R2 or newer Standalone Installation.

Note: Detailed upgrade instructions are available in the *OmniVista 2500 NMS 4.6R1 Installation and Upgrade Guide*.

Note: Backup and Restore is supported on both 4.6R1 Standalone and 4.6R1 HA. However, you can only perform a restore using a backup from the same release and build number (e.g., you can only restore a 4.6R1 GA configuration using a 4.6R1 GA Backup File). OmniVista will not allow you to perform a restore using a backup from a previous release or different build of the same release.

2.1 Proxy Requirements

OV 2500 NMS 4.6R1 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 4.6R1 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, the Proactive Lifecycle Management (PALM) Portal, and the Cloud-Based Device Fingerprinting Service:

- **ALE Central Repository** - ovrepo.fluentnetworking.com
- **AV Repository** - ep1.fluentnetworking.com

OmniVista 2500 NMS 4.6R1 Release Notes

- **PALM** - palm.al-enterprise.com
(Note that the PALM URL was changed from the previous release.)
- **Call Home Backend** - us.fluentnetworking.com
- **Device Fingerprinting Service** - api.fingerbank.org
- **Web Content Filtering** – api.bcti.brightcloud.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
SFTP	22	SFTP Client/OV Server (via "cliadmin" user)
SSHv2	2222	SSH Client/OV Server (via "cliadmin" user)
Telnet	23	OV Server/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
Policy (QoS) 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 OV Server/Net Device (REST API Polling)
Secure MQTT	1883	Net Device/OV Server
SMTP	TLS: 25 SSL: 465	OV Server/Third-Party Party SMTP Server
Log-MySQL	3306	UPAM/Log Server
Log-MSSQL	1433	UPAM/Log Server
LDAP	389	UPAM/LDAP Server or AD Server
LDAPS	636	UPAM/LDAP Server or AD 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

OmniVista 2500 NMS 4.6R1 Release Notes

Service	Port	Source/Destination
High-Availability	8000, 5405, 7801	Node 1/Node 2 Node 2/Node 1

2.3 Required Minimum System Configurations

The table below provides required minimum Hypervisor configurations based on the number of devices being managed by OV 2500 NMS 4.6R1 (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.

Configuration	Network Size			
	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
Authenticated UPAM Clients	20,000	50,000	75,000	100,000
Hypervisor Processor	2.4 GHz 8 Logical Processors	2.4 GHz 8 Logical Processors	2.4 GHz 12 Logical Processors	2.4 GHz 12 Logical Processors
Minimum Reserved OmniVista VA RAM	20GB	32GB	64GB	64GB
HDD Provisioning	HDD1:50GB HDD2:512GB	HDD1:50GB HDD2:1024GB	HDD1:50GB HDD2:2048GB	HDD1:50GB HDD2:2048GB

*OmniVista allocates memory based on the network size selected during installation.

**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 High” network size, up to 1,000 AOS switches can be supported.

Notes:

- When provisioning RAM for a new VM for OmniVista, never allocate more memory than is available on the Host Server. For example, if you are running a Host Server with 128GB of memory and have already allocated 96GB of memory to your existing VMs, accounting for the Host Server’s own memory use, you are not left with enough memory to run OmniVista without incident. VM RAM is configured from the Hypervisor.
- Allocate the recommended amount of RAM for the OmniVista VM based on your network size as shown in the above table. In addition, it is recommended that you **reserve** that RAM for the OmniVista VM to prevent performance issues. VM RAM, including reserving VM RAM is configured on the Hypervisor.

OmniVista 2500 NMS 4.6R1 Release Notes

- Set CPU Shares to “High”.
- Do not exceed the number of Logical Processors recommended for your network size as shown in the above table. Hypervisor Processors are configured from the Hypervisor.
- By default, OV 2500 NMS 4.6R1 is partitioned as follows: HDD1:50GB and HDD2:512GB. If you are managing more than 500 devices it is recommended that you go to the Virtual Appliance Menu on the VA to increase the HDD2 provision. See the *OmniVista 2500 NMS 4.6R1 Installation and Upgrade Guide* for instructions on extending the partition.
- OmniVista can be configured to use SNMPv3 to communicate with devices. When editing this configuration, you can specify which algorithms should be used. A recommended algorithm is AES (“Advanced Encryption Standard”). To get the best performance from your hypervisor, we recommend that you use Intel processors with the AES-NI instruction set enabled.
- AES-NI was introduced by Intel in 2010 in its Westmere family of processors and allows your hypervisor and its VMs to manage AES-related workloads natively. To realize the full benefits of AES-NI, you need to ensure that it is made available to the VM running OmniVista. To do this:
 - Your hypervisor's CPUs must be newer CPUs (> 2010)
 - AES-NI must be enabled in your hypervisor's BIOS
 - The AES-NI feature must not be “masked” by your hypervisor.
- By default, VMWare and Hyper-V are “pass-through” meaning that OmniVista's VM will be able to use AES acceleration. When using VirtualBox, please verify that “Nested paging” is enabled.
- The High-Availability Feature supports up to 4,000 devices.

Important Note: For OV 2500 NMS 4.6R1, Stellar APs in your network should be running a minimum AWOS version of 4.0.1 (AWOS 4.0.3 is recommended). **First** upgrade to OV 2500 NMS 4.6R1; then upgrade your Stellar APs. Please refer to the *OmniVista 2500 NMS 4.6R1 Installation Guide* for details.

Also note that when upgrading Stellar APs in a Mesh Network, you must upgrade them starting from the last node and proceeding hop-by-hop. You cannot use OmniVista Resource Manager for the upgrade since Resource Manager upgrades Stellar APs by AP Group simultaneously. You must use Stellar AP Express Mode for the upgrades.

See the *AWOS 4.0.3 Release Notes* for more information on Stellar APs and details on any known issues.

2.4 High-Availability Installation Limitations

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

- Cluster IP configuration in L3 Cluster
- Converting 4.6R1 Standalone to 4.6R1 HA if the 4.6R1 Standalone was upgraded from 4.3R1 Standalone. (You can convert 4.6R1 Standalone to 4.6R1 HA if the 4.6R1 Standalone was upgraded from 4.3R2 Standalone.)
- Changing the OmniVista IP address and Hostname after creating the Cluster.
- Hostname in upper case.

- Memory synchronization. When the active service is not available and failover happens, the data in memory of that service will be lost.
- Failover while re-syncing between nodes.

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 4.6R1 from OV 2500 NMS 4.4R2. See the *OmniVista 2500 NMS 4.6R1 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., 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 4,000 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.
 - **Alcatel Lucent Enterprise Web Content Filtering** - Licenses a user to enable Web Content Filtering on Stellar APs.

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)
High Availability Feature	NA	NA	NA
Web Content Filtering	NA	NA	NA
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 4.6R1, 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 4.6R1 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 4.6R1 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/ARB/loadOmniVistaLicGeneration.action>.
3. Enter your Customer ID and Order Number.
4. Complete the License Registration Form 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 4.6R1 is supported on Chrome, Firefox, and Microsoft Edge browsers. (See the Browser Support section).

Note: Internet Explorer is not recommended and has been deprecated.

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 OmniVista Virtual 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 4.6R1 Services must be started to launch OV 2500 NMS 4.6R1. By default, Watchdog should start automatically when OV 2500 NMS 4.6R1 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 4.6R1

After launching OV 2500 NMS 4.6R1 for the first time, log in using the Default Username and Password:

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

5.0 Known Problems

5.1 Known AP Registration Problems

5.1.1 Some Charts in the Statistics Application Do Not Support Chinese

Some charts in the Statistics application do not support Chinese characters. If the display is changed to Chinese, some items will be displayed in English. This is also seen in the VA Health application.

Workaround: No workaround at this time.

PR# OVE-7596

5.1.2 I/E v11 Does Not Work with Stellar AP Web Management Tool

Internet Explorer, Version 11 does not work when connecting to a Stellar AP using the AP Web Management Tool.

Workaround: Set another web browser as your default browser.

PR# OVE-2096

5.2 Known CLI Scripting Problems

5.2.1 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 500 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 500 lines can be displayed. No workaround at this time.

PR# OVE-11170

5.3 Known Discovery Problems

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

The "Reason Down" field is blank if an AP is UP. If an 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

5.3.2 "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

5.3.3 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

5.3.4 Timeout Issue when the “Use GetBulk” Option is Enabled

The Discovery “Use GetBulk” operation (enabled by default) may cause a delay between OmniVista and some AOS switches that can trigger a timeout state when attempting to communicate with the switch. As a result, OmniVista may not have up-to-date information for the switch.

Workaround: Disable the “Use GetBulk” option by selecting the switches to edit from the Discovery -> Managed Devices list and disabling this option under the “Advanced Settings” section of the “Edit Discovery Manager Entry” screen.

PR# OVE-11112

5.4 Known Locator Problems

5.4.1 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

5.5 Known mDNS Problems

5.5.1 Video Source Unable to Discover Chromecast on Different VLAN

With the mDNS feature you can setup and configure service sharing rules for your services across wireless and wired networks. However, when sharing services with a Chromecast device, if your video source (e.g., Chromebook, laptop) is connected to wired or wireless network in VLAN x, and the Chromecast device is in VLAN Y, the video source cannot see Chromecast device and cannot cast video.

Workaround: For service sharing to work, the Chromecast device must be on same VLAN as the video source; and it must be connected to an Access Point that is configured as an mDNS Edge Device connected to an mDNS Responder. Problem will be fixed on AOS 8.7R2.

PR# OVE-8941

5.5.2 Services Not Shared if Client Connects to SSID on an AP Before Responder and Edge Devices Configured

If a client connects to an SSID on an AP and starts sharing mDNS services before the OmniVista Administrator configures Responder and Edge Devices, services will not be shared with other users.

Workaround: Follow the expected mDNS Responder configuration sequence: Configure Responder Switch and Edge Devices first. Then, let users join the network and share mDNS Services. If this sequence is not followed, users must share services again after the Responder and Edge Devices are configured for mDNS Services.

PR# OVE-9848

5.5.3 Video Source Able to Cast Video After mDNS Responder Disabled

Even after the MDNS Responder and mDNS Edge Device are administratively disabled, the MAC Book Client (video source) connected to SSID1(VLAN 121) is able to cast the video to an Apple TV connected to SSID2 (VLAN 201) on the same AP. This behavior gives the impression to the user that even after disabling the services (mdns-edge and mdns-responder admin-disabled), the desktop mirroring and casting services are working. However, when mDNS Responder is administratively disabled, there are no response packets from MDNS Responder to the client who is sending the mDNS query. But the mirroring continues to work for MAC Book Pro and Apple TV until they are aged out or until they are disconnected and reconnected to the network.

Workaround: Informational.

PR# OVE-9112

5.5.4 AP Not Added to the Edge List when Deploying mDNS on Eth1 Port

Connecting AP1351/AP1301 to the switch only on Eth1 port does not support mDNS service deployment.

Workaround: When deploying mDNS, use either the Eth0 port only or link aggregation (Eth0 and Eth1) on AP1351/AP1301 to connect to the switch.

PR# OVE-11033

5.5.5 Deleting a Responder Device Fails

When attempting to delete a Responder Device, you might see the following error message when you click on “Result” to check the progress of the delete action:

“The device was ignored or is blocked by another process.”

Workaround: Restart the mDNS service to bypass this issue.

PR# OVC-8876

5.6 Known Notifications Problems

5.6.1 SNMP “Up/Down” Traps Are Not Showing After Upgrade from OV422MR2 to OV43R3

SNMP “Up/Down” Traps (“alasnmpdown” and “alasnmpup”) are not displayed after upgrading from OV422MR2 to OV43R3 via multiple releases.

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-3759

5.6.2 Trap Configuration Fails when the Switch Name Contains a “#” Character

When a switch name contains the “#” character (for example, “Switch10.1.1.10##”), configuring traps on that switch will fail.

Workaround: Do not include the “#” character in the switch name.

PR# OVE-10558

5.7 Known PolicyView Problems

5.7.1 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

5.7.2 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

5.7.3 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# OVE-678

5.8 Known Resource Manager Problems

5.8.1 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

5.9 Known Topology Problems

5.9.1 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

5.9.2 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

5.10 Known Unified Access Problems

5.10.1 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

5.10.2 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

5.10.3 Unified Policy Sometimes Works Abnormally

When a user configured a Layer 3 Destination IP address Unified Policy to "Drop" traffic with the Reflexive option, some packets were not dropped.

Workaround: Do not turn on the Reflexive option.

PR# OVE-10083

5.10.4 Source MAC Address Condition Not Supported in Policy List on OS6465/OS6560

Policy lists containing a rule with a source MAC address condition are not supported on OS6465/OS6560 switches. This is an AOS restriction on these switches.

Workaround: Do not include a source MAC address condition in a policy list rule. Source MAC address conditions are supported on OS6465/OS6560 switches when they are not part of a policy list rule.

PR# OVE-10696

5.11 Known UPAM Problems

5.11.1 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

5.11.2 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

5.11.3 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

5.11.4 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

5.11.5 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

5.11.6 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

5.11.7 802.1X 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

5.11.8 Guest User Account Names Are Not Case-Sensitive in OVE 4.4R1

In previous OVE releases, the Guest Account Name in UPAM was case-sensitive (e.g., "Account1" and "account1" are seen as two different accounts). In OVE 4.4R1 Guest Accounts are not case-sensitive (e.g., "Account1" and "account1" are seen as the same account by OmniVista). In OVE 4.4R1, if two accounts have the same name (e.g., "Account1 and "account1"), UPAM will authenticate the first account received for authentication. The other account will not be authenticated.

Workaround: Guest Account names must be different in OVE4.4R1. If necessary, change any existing account names to avoid this problem.

PR# OVE-4999

5.11.9 No IPv4 or IPv6 Value Displayed in UPAM Authentication Record

Client IP address is not displayed in UPAM Authentication Record.

Workaround: No workaround at this time.

PR# OVC-6061

5.11.10 Radius Service Cannot Start After Secure LDAP Server is Stopped

If the LDAPs Server is shut down, the freeradius service goes down and cannot be restarted. This is not an issue for unsecure LDAP, the issue exists only for Secure LDAP.

Workaround: Enable the LDAP Server or Disable LDAP/AD Server on the LDAP/AD Configuration Screen (UPAM – Settings – LDAP/AD Configuration).

PR# OVE-8986

5.11.11 Client Disconnects on First Authentication if UPAM Fails Over to Backup External Radius Server

If you upgrade to OVE 4.5R2 and re-use the default RADIUS Server Timeout setting from the previous release, you may experience client connectivity problems during an external RADIUS Server failover.

Workaround: The default Timeout Settings on previous releases was 5 seconds. The new default setting is 2 seconds. If you have authentication failover client connectivity problems, change the Timeout Setting to 2.

PR# OVE-9528

5.11.12 Guest Account Status Still Displays “Enabled” After Validity Period Has Expired

The Guest Account status in the UPAM Guest Account List still displays “Enabled” after the Validity Period for the account has expired.

Workaround: Set the Guest Account Deletion Policy on the UPAM Guest Access Global Configuration page to delete accounts after they expire. Accounts will automatically be deleted and removed from the Guest Account List when they expire. You can set expired accounts to be deleted immediately upon expiration, or set a number of days before deletion (1 – 90 days).

PR# OVE-10128

5.11.13 WiFi4EU not Connected to Captive Portal

The validity period for Captive Portal authentication defaults to 30 days, but WiFi4EU requirement is maximum 24 hours.

Workaround: Is there a workaround.

PR# OVE-11164

5.12 Known Users and User Groups Problems

5.12.1 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 4.22 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

5.13 Known VM Manager Problems

5.13.1 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

5.13.2 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

5.13.3 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 Known Web Content Filtering Problems

5.14.1 End User Should be Notified When a Page Is Blocked by WCF

When a client tries to access a website restricted by Web Content Filtering (WCF), the page will fail to load, and the browser will display an error. However, the error message is a generic connection error message. It does not explain why the page failed to load (e.g., "Access to this Website is restricted").

Workaround: Connect to a known unrestricted site to verify the reason the connection failed. In a future release, if a client attempts to access a restricted site, OmniVista will redirect the client to a specific block page.

PR# OVE-10205

5.15 Known WLAN Problems

5.15.1 Two Tunnel Profiles with Same Remote IP & VPN-ID But Different Entropy Status Will Not Take Effect Correctly

You can create two tunnel Profiles with the same Remote IP address and VPN-ID and a different Entropy Status for each (one is Enabled and one is Disabled) and apply it to an AP, but the configuration will not work.

Workaround: If you create two tunnel profiles with the same Remote IP and Tunnel ID, the "Support of Entropy" status **must** be the same on both tunnels (both must be "enabled" or "disabled"). Choose the value based on what use case you plan to deploy. The following are the four possible use cases that are supported:

- 1. GRE Tunnel from AP to AOS Switch** - This is the typical Guest Tunnel uses case where AOS acts as the Guest Tunnel Termination Switch. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".
- 2. GRE Tunnel from AP to Non-AOS Switch/Server (e.g., Nokia 7750 SR/Standard Linux Tunnel Server)** - This is the Guest Tunnel use case with a non-AOS switch. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by the Switch/Server.
- 3. GRE Tunnel Between AP and OV VPN Server Appliance** - This is the regular Data VPN tunnel use case between Remote APs and OV VPN Server acting as the Data VPN Server. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by OV VPN Server.
- 4. GRE Tunnel from AP to AOS Switch, Over the Data VPN tunnel Between AP and OV VPN Server Appliance** - This is a rare use case of using the Data VPN tunnel to reach from a Remote site where the AP is located, to the Central Site where the AOS Switch is located. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".

The following combinations of values are not supported:

- Tunnel ID > 0 and Support of Entropy = Disabled
- Tunnel ID = 0 and Support of Entropy = Enabled.

5.15.2 AP1321 Advertises Incorrect SSID Name in Some Cases

Stellar OAW-AP1321 displays the SSID Name incorrectly in some cases in the Managed Devices List.

Workaround: No workaround at this time.

PR# OVE-9545

5.15.3 Client Name Field Blank for Clients Running iOS 14

The Client Name field in the “List of All Client on All APs” is not displayed for devices running iOS 14.

Workaround: No workaround at this time. The problem occurs on devices running iOS 14 as they do not send Option 12 in the DHCP message.

PR# OVC-8287

5.15.4 Intrusive AP Page and Widget Time Out When Loading Data

There are around 20000 intrusive APs on the customer side. WMA needs 65 seconds to query the completed data. However, the policy queries timeout is 50 seconds, causing the timeout error.

Workaround: No workaround at this time.

PR# OVE-9693

5.15.5 RF Profile Not Supported on AP1201BG

Stellar OAW-AP1201BG does not support RF profiles, as it is a BLE gateway.

Workaround: No workaround at this time.

PR# OVE-10781

5.15.6 WMA in a Not Responding State on the Standby Node

Sometimes WMA will stay in a “Not Responding” state on the Standby node. This has no impact to OmniVista or network operations when this occurs.

Workaround: When the Standby node becomes Primary, the WMA status will automatically change to “Running”.

PR# OVE-10513

5.15.7 Social Login Fail with Google Account

The default list of URLs shown when selecting Social login vendors (Google, Facebook...) does not include country specific URLs.

Workaround: Manually add/append the required URLs to the list of “Whitelist Domains” when you configure the SSID.

PR# OVC-8901

5.16 Known Other Problems

5.16.1 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

5.16.2 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 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

5.16.4 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

5.16.5 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

5.16.6 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

5.16.7 OV Nginx Service Does Not Start After Updating OmniVista Web Server SSL Certificate

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

5.16.8 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 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

5.16.9 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

5.16.10 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

5.16.11 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
- You cannot convert a 4.5R2 Standalone installation to an HA installation if the 4.5R2 Standalone installation was upgraded from a 4.3R1 Standalone installation.
- 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.
- Failover while re-syncing between nodes.

Workaround: NA

PR# OVE-2327

5.16.12 Failover Banner Directs User to Inoperable HA Standby Node

If you are restarting services on the Active Node in an HA Installation, the Failover Banner will appear informing the user to redirect to the Standby Node. Failover does not occur when services are manually restarted, only when the Active Node is unreachable. Ignore the message when it appears due to services being manually restarted. The Active Node should become available again when all of the services are “Up”.

Workaround: Informational.

PR# OVE-3113

5.16.13 Offline Upgrade from 4.3R3 to 4.4R1 Failed

Offline Upgrade from 4.3R3 to 4.4R1 Failed due to invalid upgrade location.

Workaround: Contact Customer Support for Offline Upgrades

PR# OVE-5006

5.16.14 Cannot Push Policy with IPv6 Conditions to AOS 6.4.6

User cannot push policies with IPv6 Conditions to AOS 6.4.6 switches. IPv6 is not supported on AOS 6.4.6 switches. It is only supported on AOS 6.7.2R7 and later, and AOS 8.6R2 and later.

Workaround: Upgrade to a supported build.

PR# OVE-5793

5.16.15 Problem Connecting to Switch with OV Assistant When Multiple Bluetooth Dongles Present

The OmniVista Assistant uses the Bluetooth dongle MAC address to initiate a connection to a switch. If multiple Bluetooth dongles are active at the same time, OmniVista Assistant may initiate a connection to an unexpected dongle.

Workaround: Make sure there are no other active Bluetooth dongles in the area. And make sure the correct model and serial number appear under "Paired Devices" before initiating a connection to a switch.

PR# OVC-7240

5.16.16 Download Package Failed When Choosing "Download Only" Option in OV44R2 Build 50 Patch 1

When upgrading the OmniVista VA from 4.4R2 to 4.5R1 or from 4.5R1 to 4.5R2, the VA displays an error and the download fails when choosing the "Download only" option during the upgrade.

Workaround: You must use the 'Download and Upgrade' option during the upgrade process when upgrading from 4.4R2 to 4.5R1 or from 4.5R1 to 4.5R2.

PR# OVE-8050

5.16.17 Warning Message Appears in Firefox Browser When Displaying a Large Number of Managed Devices

A warning message appears when using a Firefox Browser to view a large number of devices on the Managed Devices Screen – "A webpage is slowing down your browser". This occurs when the response returned from the server exceeds 1MB.

Workaround: Use the latest versions of Chrome or Microsoft Edge Browsers. For Firefox, you modify the following settings: Type about:config in the Address Bar and search for the following:

- devtools.netmonitor.responseBodyLimit: Set it to **0** to disable the limit.
- dom.max_script_run_time: Set it to **20** to let the script run longer.

PR# OVE-8019

5.16.18 Database Connection Stuck at "Connecting/Standalone" Status on HA System

User database connection got stuck at Connecting/Standalone Status on OmniVista 4.5R1 HA System.

Workaround: Do not perform any export/checkpoints/snapshots while the VM is running. These operations should only be done after shutting down watchdog and stopping the VM.

PR# OVE-8874

5.16.19 OV Restore Fails with Error "Failed to Start ovdap Service

While restoring Customer backup file, a timeout error occurred when recovering (starting) ovdap.

Workaround: If you cannot start the ovdap service without a timeout error, delete most of the log files manually (keep only one file - log.0000000001).

1. Restore the backup file.
2. If the ovdap service fails to start after 15 minutes (check it via Watchdog), check if there are multiple recovery log files (the files with prefix "log.0000000...") in the OV directory: "/opt/OmniVista_2500_NMS/data/openIdapdb". If yes, delete these specific log files except the oldest one (log.0000000001).
3. Restart OmniVista from Watchdog, or reboot the OV VM. You do not have to retry the restore.

PR# OVE-9782

5.16.20 VA Console Displays Error Message when Joining Cluster

While joining the peer node, the message "WARN: stdin/stdout is not a TTY; using /dev/console" may be displayed. This happens because OmniVista opens an internal session to a DRBD service for synchronizing data between two nodes.

Workaround: You can ignore this message; it does not impact the Join Cluster process.

PR# OVE-10576

5.16.21 Backup/Restore on HA System Can't Restore on System Upgrade to OV46R1 Build 44

Performing a Backup/Restore on HA system when upgrading to OV 4.6R1 build 44 triggers a permission error. This only occurs on an HA system upgrade; works fine on a fresh HA system.

Workaround:

- Step 1: Open the backup file by using 7-zip (Right-click on the backup file -> Open archive).
- Step 2: Navigate to "logs" folder then delete "ha_failover_handler.log" file.
- Step 3: Use the backup file to restore.

PR# OVE- 11172

6.0 Release Notes PRs Fixed

6.1 PRs Fixed Since 4.5R3

6.1.1 Customer PRs

CR/PR Number	Description
Case: 00559299 <i>OVE-10635</i>	Summary: OV 2500: Fresh installation in 4.5R03 - Installing VMWARE tools failed Click for Additional Information
Case: 00542487 <i>ALEISSUE-1009</i>	Summary: OmniAccess Stellar – Wifi Users unable to login to Employee sponsor page with Windows Active Directory credentials. Explanation: Customer expects restrict access to Employee sponsor page based on Windows AD. Click for additional information
Case: 00553521 <i>OVE-3051</i>	Summary: OV 2500: Issue when doing backup of OmniSwitches running in Version AOS8 if the SSH Preference on Managed Device is set to Telnet Click for Additional Information
Case: 00556157 <i>OVE-10933/ OVE-10061</i>	Summary: OV 2500: High resource usage while creating manual links on discovery tool Click for Additional Information
Case: 00558241 <i>OVE-10333</i>	Summary: OV 2500: Locator fails to load the Netforward table of few switches

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
	Click for Additional Information
Case: 00548874 <i>ALEISSUE-1066</i>	Summary: OV 2500: Email server settings set to TLS - exchange fails with error "TLS Alert: unknown certificate" Click for Additional Information
Case: 00548841 <i>OVE-10748</i>	Summary: OV 2500: "Scheduled devices backup using MAP" is not working Click for Additional Information
Case: 00549435 <i>OVE-10651</i>	Summary: OV 2500: Error "Failed to connect to the device. Please check the user name and password" Click for Additional Information
Case: 00550500 <i>OVE-10787</i>	Summary: OV 2500: User with "Network Admin" role does not have access to view "Schedulers" Click for Additional Information
Case: 00550675	Summary: OV 2500: Cannot add vCenter 7.0.1 server in OV2500 using VM Manager application Click for Additional Information
Case: 00545399 <i>OVE-10760 and</i> <i>OVE-10762</i>	Summary: OV 2500: IP of devices/switches disappear in "Policy Roles" (Policy View-Expert Mode) Click for Additional Information
Case: 00545307 <i>OVE-10756</i>	Summary: OV 2500: HA cluster unstable after the active OV server reboot Click for Additional Information
Case: 00546230 <i>OVC-8492</i>	Summary: OV 2500 / OV Cirrus: IoT classification fails or is not displayed Click for Additional Information
Case: 00546094 <i>OVE-10707</i>	Summary: OV 2500: If running in Cluster mode, the UPAMRadiusServer object in Authentication Servers -> Radius must be greyed out Click for Additional Information
Case: 00542968 <i>OVE-10690</i>	Summary: OV 2500: Trap-Filter with Mac-Address on the SnmpVariable returns Invalid Syntax Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00541800 <i>OVE-10614</i>	<p>Summary: OV 2500: After upgrade from 4.5R01 to 4.5R02 the services ovav and ovwma are not Running</p> <p>Click for Additional Information</p>
Case: 00541177 <i>OVE-10385</i>	<p>Summary: OV 2500: VLAN Type is displayed as "Standard" instead of "Dynamic" for a VLAN which has been learned through MVRP.</p> <p>Click for Additional Information</p>
Case: 00541178 <i>OVE-10385</i>	<p>Summary: OV 2500: The "Type" and "Device Type" are blank on the "Configuration -> VLAN Manager"</p> <p>Click for Additional Information</p>
Case: 00543643 <i>OVE-10645</i>	<p>Summary: OV Cirrus / OV 2500: Application Visibility - We cannot remove AP Group from Signature profiles</p> <p>Click for Additional Information</p>
Case: 00540266 <i>OVE-10639</i>	<p>Summary: OV 2500: Since we added Web Server IP address, when OV is rebooting we have message "your network configurations have some changes, please re-check"</p> <p>Click for Additional Information</p>
Case: 00538815 <i>OVE-10613</i>	<p>Summary: OV Cirrus / OV 2500: Guest Operators are unable to generate Guest Accounts using option Batch Creation</p> <p>Click for Additional Information</p>
Case: 00524131 <i>OVE-10577</i>	<p>Summary: OV Cirrus / OV 2500: Not showing LLDP link on some switches</p>
Case: 00524129 <i>OVE-10385</i>	<p>Summary: OV Cirrus / OV 2500: Changing a VLAN configuration on one switch causes all other switches which have the same VLAN, learned dynamically via MVRP, are changed to an Unsaved state.</p> <p>Click for Additional Information</p>
Case: 00527168 <i>OVE-10614</i>	<p>Summary: OV 2500: High memory issue</p>
Case: 00529945 <i>ALEISSUE-971</i>	<p>Summary: OV Cirrus / OV 2500: Portal users still have internet access after clicking on logout</p> <p>Click for Additional Information</p>
Case: 00531174 <i>ALEISSUE-961</i>	<p>Summary: OV Cirrus / OV 2500: Captive portal Logo does not maintain right aspect ratio</p>

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
	Click for Additional Information
Case: 00531597 <i>OVE-10514</i>	Summary: OV Cirrus / OV 2500: Cannot create a new topology map when lot of child maps Click for Additional Information
Case: 00531221 <i>OVE-10481</i>	Summary: OV Cirrus / OV 2500: Stops receiving traps after user changes Trap Port from 162 to another value Click for Additional Information
Case: 00513237 <i>OVE-11112</i>	Summary: OV 2500: Link between 6450 & core OS10K switch are not shown in topology map Click for Additional Information
Case: 00531818 <i>OVE-10553</i>	Summary: OV 2500: High CPU and Web GUI not responding when using Top N PoE Analytics Click for Additional Information
Case: 00556303 <i>ALEISSUE-741</i>	Summary: OV 2500/OV Cirrus: wifi4eu banner shall be displayed full size
Case: 00547689 <i>OVC-8746</i>	Summary: OV 2500/OV Cirrus: Stellar AWOS 4.0.x // WPA3-Enterprise is doing fallback in WPA2-Enterprise whatever we select Authentication type WPA3_AES or WPA3_AES_256 Click for Additional Information
Case: 00542453 <i>OVC-8703</i>	Summary: OV 2500/OV Cirrus: IoT device remains into Pending state after IoT enforcement Click for Additional Information
Case: 00538748 <i>OVC-8634 and OVE-10608</i>	Summary: OV 2500/OV Cirrus: It takes a long time to load "Geo Location View" on Topology app Click for Additional Information

6.1.2 Release Note PRs Fixed

- Cannot Download Radius Server Certificates (OVC-8405)
- Cannot Live Search by Auth User for OS6360 Devices (OVE-10550)
- Sflow Consumes Large Amount of Disk Space on OV Server (OVE-9145)
- Cannot Apply Signature and Classification to a Large Number of Aps (OVE-2256)
- Unified Policies Are Lost on Certain Switches After Reboot (CRAOS8X-26272)
- When Upgrading Stellar APs in Mesh Network Start From Last Node (OVE-4015)

OmniVista 2500 NMS 4.6R1 Release Notes

- OV Hardware Inventory Fails When Selecting All Devices (OVE-10342)
- Device Start Time Is Incorrect in IoT Inventory List (OVE-5658)
- IoT Inventory List Displays Active/Online Endpoints as Offline (OVC-6788)
- IoT Client Continuously Re-Connects After Category Enforcement (OVE-7648)
- mDNS Server and Client Policy: UI Offers Policy Lists in "Access Role Profile" Drop-Down (OVE-10559)
- Problems with RAP Deployment on ESXi 5.5 (OVE-8484)
- "Restore" Must Be From The Same Release (CRNOV-675)
- Device Address Column Sorted Incorrectly in Device Backup/Restore Table (OVE-1861)
- Potential Problems with Backup/Restore of OS6860E with AOS 8.7R1 (OVE-8581)
- Cannot Push Unified Policy to AOS Switches (OVE-5794)
- Redirect Allowed Profile IPv6 Does Not Work for AOS Devices (OVE-6214)
- Client Blacklisting Does Not Work on AP1320/AP1360 (OVE-9544)
- Cloning SSID Works Incorrectly (OVE-9775)
- BMF File Upgrade Failed on OS6360 When Master Chassis ID is 2 or Higher (OVE-10463)
- Cannot Restore HA Installation Using a Backup Taken From a Freshly-Installed 4.5R3 GA Build (OVE-10579)

6.2 PRs Fixed Since 4.5R2

6.2.1 Customer PRs

CR/PR Number	Description
Case: 00526846 <i>OVE-10388</i>	<p>Summary: OV 2500: No option to input VLAN information in "Filter Data".</p> <p>Click for Additional Information</p>
Case: 00522580 <i>OVE-10299</i>	<p>Summary: OV 2500 Enterprise: IOT problems on wired and wireless clients.</p> <p>Click for Additional Information</p>
Case: 00479752 <i>OVE-9228</i>	<p>Summary: OV 2500 Scheduled backups with dynamic maps.</p> <p>Click for Additional Information</p>
Case: 00491445 <i>OVE-9581</i>	<p>Summary: OV 2500 Stellar AP are unable to register or disappear from registration after a while.</p> <p>Click for Additional Information</p>
Case: 00492353 <i>OVE-9497</i>	<p>Summary: OV 2500 configuration save issue from Notifications tab.</p> <p>Click for Additional Information</p>
Case: 00481162 <i>OVE-9483</i>	<p>Summary: OV 2500 Login activity not displayed for guest operator.</p>

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
	Click for Additional Information
Case: 00481748 <i>OVE-9053</i>	Summary: OV 2500 - failed to push the Policy List config to the OS6860 switch. Click for Additional Information
Case: 00494007 <i>OVE-9556</i>	Summary: OV 2500 APs upgrade status is not shown in managed tab. Click for Additional Information
Case: 00496811 <i>OVE-10200</i>	Summary: OV 2500 fails to configure policies with multiple conditions to AOS 6x and AOS 8x. Click for Additional Information
Case: 00508695 <i>OVE-9949</i>	Summary: OV 2500 Generating a report is blank in "Managed Devices". Click for Additional Information
Case: 00501928 <i>ALEISSUE-853</i>	Summary: OV 2500 Spellcheck for Swedish translation of OmniVista UPAM Captive Portal. Click for Additional Information
Case: 00508643 <i>OVE-10155</i>	Summary: OV 2500 External Radius Server changes updated to switch automatically. Click for Additional Information
Case: 00511547 <i>OVE-10077</i>	Summary: OV 2500 Telnet connections are seen from OV2500 to switch. Click for Additional Information
Case: 00511432 <i>OVE-10025</i>	Summary: OV 2500: ovtomcat service consumes high CPU Utilization. Click for Additional Information
Case: 00512076 <i>OVE-9198</i>	Summary: OV 2500 - Application Visibility - Signature Profiles stuck to Loading. Click for Additional Information
Case: 00512305 <i>OVE-10039</i>	Summary: OV 2500 - Data sync error in HA - DRBD diskless status on standby after partition extended. Click for Additional Information
Case: 00512405 <i>OVE-10034</i>	Summary: OV 2500 while generating CSV for Home - WLAN - Client - Summary, nothing displayed for last 30 or 90 days. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00514612 <i>OVE-10159</i>	<p>Summary: OV 2500 Wireless Clients fail to authenticate.</p> <p>Click for Additional Information</p>
Case: 00517044 <i>OVE-10167</i>	<p>Summary: OV 2500 Tomcat error in the GUI.</p> <p>Click for Additional Information</p>
Case: 00517438 <i>OVE-10203</i>	<p>Summary: OV 2500 / OV Cirrus - Policy list updating is failing after removed device from devices list.</p> <p>Click for Additional Information</p>
Case: 00518955 <i>OVE-10255</i>	<p>Summary: OV 2500 Unable to recreate the disk with new copied virtual disk file while upgrading the VPN VA server.</p> <p>Click for Additional Information</p>
Case: 00521123 <i>OVE-10281</i>	<p>Summary: OV 2500 UPAM services is in out of memory.</p> <p>Click for Additional Information</p>

6.2.2 Release Note PRs Fixed

- Detailed Inventory Report Can Take a Long Time to Complete (OVE-9231)
- ovtomcat Is Out Of Memory (OVE-10468)
- Unified Policy List Notify Failed on OS6360 When Using Default Policies (OVE-10476)
- Fail to Notify Unified Policy with TOS Condition on OS6900 and OS6860/E Devices (OVE-10495)

6.3 PRs Fixed Since 4.5R1

6.3.1 Customer PRs

CR/PR Number	Description
Case: 00467107 <i>OVE-8482</i>	<p>Summary: OV Cirrus - Filter with attribute Geo Location does not work on Managed Devices page.</p> <p>Click for Additional Information</p>
Case: 00465793 <i>OVC-7659</i>	<p>Summary: OV Cirrus Freemium - Cannot manage the Network ID in System Settings.</p> <p>Click for Additional Information</p>

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00469644 OVC-7838	Summary: OV Cirrus - Newly-added Stellar AP moves to "Provisioning Failed" status. Click for Additional Information
Case: 00479330 CRNOV-2172	Summary: OV Cirrus - Stellar RAP inner IP address is changed and tunnel is down Click for Additional Information
Case: 00465789 OVC-7685	Summary: OV Cirrus - Freemium - Nothing is listed in Export VPN Settings until the AP performs a new call home. Click for Additional Information
Case: 00468024 OVC-7743	Summary: OV Cirrus - Tunnel Profile creation failed on OV Cirrus. Click for Additional Information
Case: 00440153 OVE-8105	Summary: OV 2500 - Quarantine Manager not blocking the intruder MAC Click for Additional Information
Case: 00467694 OVE-8495	Summary: OV 2500 - Unable to install the VMware tools Click for Additional Information
Case: 00456536 OVE-8161	Summary: OV 2500 - OS10K is not displayed in hardware inventory. Click for Additional Information
Case: 00469761 OVE-8535	Summary: OV 2500 - Unlimited Device Validity Period in Guest Access / Global Configuration is not possible. Click for Additional Information
Case: 00473765 OVE-8633	Summary: OV 2500 - Missing Symlink to switch backups for cliadmin. Click for Additional Information
Case: 00469781 CRNOV-2044	Summary: OV 2500/OV Cirrus - WiFi4EU portal template support in Greek language Click for Additional Information
Case: 00449971 OVE-8181	Summary: OV 2500 - Not receiving the traps from the third-party devices Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00418540 <i>OVE-8279</i>	Summary: OV 2500 -Fails to provide Captive portal page every week Click for Additional Information
Case: 00461255 <i>OVE-8459</i>	Summary: OV 2500 - Report only shows the parent pie-chart statistics not the sub-tree statistics Click for Additional Information
Case: 00460570 <i>CRNOV-1925</i>	Summary: OV Cirrus - Issues adding the OV Cirrus Captive portal URL on the WiFi4EU Portal. Click for Additional Information
Case: 00461232 <i>OVE-8210</i>	Summary: OV 2500 - Firmware version cannot be set for AOS 8.x devices in the Auto Configuration's instruction file Click for Additional Information
Case: 00447382 <i>OVE-8888</i>	Summary: OV 2500 - External web session from OV Click for Additional Information
Case: 00462741 <i>CRNOV-1967</i>	Summary: OV 2500/OV Cirrus - WiFi4EU Captive Portal does not display correctly. Click for Additional Information
Case: 00426224 <i>OVE-8279</i>	Summary: OV 2500 - UPAM crash and no more 802.1x Authentication processed Click for Additional Information
Case: 00478884 <i>CRNOV-2143</i>	Summary: OV 2500 - Bulk Notification AP Stopped/Resumed Responding to OV Click for Additional Information
Case: 00480606 <i>OVE-8171</i>	Summary: OV 2500 - 100% Disk space. Click for Additional Information
Case: 00434325 <i>OVE-8382</i>	Summary: OV 2500 - Report failures. Click for Additional Information
Case: 00465897 <i>OVE-8316</i>	Summary: OV 2500 - ASA requests are not proxied by OV to external RADIUS Server Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00466510 <i>CRNOV-2063</i>	Summary: OV 2500 - High CPU and synchronization issue with HA peer node Click for Additional Information
Case: 00454490 <i>OVE-8848</i>	Summary: OV 2500 - Opening Notifications results in error message "Communication failure" Click for Additional Information
Case: 00457434 <i>OVE-7937</i>	Summary: OV 2500 - Screen object changes when doing Logout and login. Click for Additional Information
Case: 00471352 <i>OVE-8407</i>	Summary: OV 2500 - OV GUI and CLI slowness issue. Click for Additional Information
Case: 00457582 <i>OVE-8043</i>	Summary: OV 2500 - Topology does not work. It returns the following error after 20-30 minutes: "?Cannot topology.msg.getMap." Click for Additional Information
Case: 00464031 <i>OVE-8279</i>	Summary: OV 2500 - ovupam service down. Click for Additional Information
Case: 00431484 <i>OVE-7454</i>	Summary: OV 2500 - netadmin user not able to create AP Groups and manage AP association. Click for Additional Information
Case: 00423181 <i>OVE-7007</i>	Summary: OV 2500 - Policies ACL/QOS "notified all" and "notified selected" does not work all the time. Click for Additional Information
Case: 00450497 <i>OVE-8204</i>	Summary: OV 2500 - experiencing slowness while accessing GUI. Click for Additional Information
Case: 00470058 <i>OVC-7688</i>	Summary: OV 2500 - Duplicate IP leasing issue in RAP Data VPN configuration. Click for Additional Information
Case: 00475712 <i>OVE-8671</i>	Summary: OV 2500 - Wired users MAC authentication failing after upgrade to 4.5 R01. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00477543 <i>OVE-8860</i>	Summary: OV 2500 - Time Period in Wireless Client List is always 24h Click for Additional Information
Case: 00478110 <i>OVE-8675</i>	Summary: OV 2500 - Backup is not working after upgrade to 4.5R1. Click for Additional Information
Case: 00463967 <i>OVE-8269</i> <i>OVE-8105</i>	Summary: OV 2500 - Quarantine Manager Rule - Add restriction for OS6560 and OS6465 Click for Additional Information
Case: 00470560 <i>OVE-8171</i>	Summary: OV 2500 - Unable to upgrade to 4.5R01 due to space issue. Click for Additional Information
Case: 00483504 <i>OVC-8056</i>	Summary: OV 2500 / OV Cirrus – Wifi4EU language flag overlaps logo. Click for Additional Information
Case: 00484663 <i>OVE-8627</i>	Summary: OV 2500 - High disc utilization when using Top N Applications analytics Click for Additional Information
Case: 00485017 <i>CRNOV-2262</i>	Summary: OV 2500 - Most of the services in OV were continuously restarting and the HA sync was stuck. Click for Additional Information
Case: 00486274 <i>OVE-8279</i> <i>OVE-8407</i> <i>OVE-8627</i>	Summary: OV 2500 - High Availability failed to work. Click for Additional Information
Case: 00489662 <i>CRNOV-2292</i>	Summary: OV 2500 - Channel 144 is missing in OV with Singapore country code. Click for Additional Information
Case: 00465552 <i>OVE-8309</i>	Summary: OV 2500 - Mismatched AP license count. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00481748 <i>OVE-8627</i>	Summary: OV 2500 - Failed to push the Policy List configuration to OS6860 switch.
Case: 00482002 <i>OVE-8406</i>	Summary: OV 2500 - "ovldap" service failed to start. Click for Additional Information
Case: 00470905 <i>ALEISSUE-692</i>	Summary: OV 2500 – Captive Portal customization issue. Click for Additional Information
Case: 00453284 <i>OVE-7902</i>	Summary: OV 2500 - Unable to execute Action (Copy Certified to working/ Running) on 8x switches.
Case: 00451799 <i>OVE-7873</i>	Summary: OV 2500 – Not possible to create an Unified Policy with condition source IP and Tricolor marking on OS6450 Click for Additional Information
Case: 00490777 <i>OVE-9294</i>	Summary: OV 2500 – There was a JMS Request timeout error noticed when we enable IoT on Stellar AP Click for Additional Information
Case: 00494012 <i>OVE-9490</i>	Summary: OV 2500 – AP Group is not visible for 40 minutes after creating it Click for Additional Information
Case: 00497999 <i>OVE-8475</i>	Summary: OV 2500 – Top N PoE Switches Utilization Summary widget/report stuck to "Loading" Click for Additional Information
Case: 00475299 <i>OVE-8407</i>	Summary: OV 2500 – Not possible perform a OmniVista backup after upgrade to 4.5R01 Click for Additional Information
Case: 00474701 <i>OVE-8658</i>	Summary: OV 2500 – After power on/off the VPN-VA all Stellar RAPs are down Click for Additional Information
Case: 00461567 <i>OVE-9586</i>	Summary: OV 2500 – Down devices are listed as "unsaved" devices on Notifications bell icon Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00467006 <i>OVE-7405</i>	Summary: OV 2500 – Dummy stellar AP called "no-name" in OV2500 Managed devices cannot be deleted Click for Additional Information
Case: 00496113 <i>CRNOV-2387</i>	Summary: OV 2500 /OV Cirrus – On Notifications home we still receive apRogueAPDiscovery traps whereas WIPS Traps is set to off in Settings Click for Additional Information
Case: 00496811 <i>OVE-9622</i>	Summary: OV 2500 /OV Cirrus – “Condition mismatch...” displayed when user is creating policy with multiple conditions Click for Additional Information
Case: 00499118 <i>OVE-9581</i>	Summary: OV 2500 - AP not able to register on OV, maximum MQTT connections were reached Click for Additional Information
Case: 00499753 <i>OVE-8702</i>	Summary: OV 2500 – Core pool size of each thread pool is too high and should be decreased to avoid performance issue Click for Additional Information
Case: 00491463 <i>OVE-9487</i>	Summary: OV 2500 – /dev/mapper/vgdata-lvdata into linked to /opt is getting full disk space because services were writing logs to deleted files Click for Additional Information
Case: 00503755 <i>OVE-9487</i>	Summary: OV 2500 – service ovclient stuck to “starting” Click for Additional Information

6.3.2 Release Note PRs Fixed

- Unregistered Stellar APs Discovered as “Down” Cannot Be Deleted (OVE-7405)
- LDAP Policy with 'TCP Flags' Condition Fails in Notify (OVE-3020)
- After Changing Languages, Report Still Printed in Previous Language (OVE-4960)
- Error Message When Backing Up Stack of 6x Switches (OVE-4211)
- Cannot Select WPA3 Encryption via Unified Profile Workflow (OVE-4950)
- Failed to Assign ClearPass Server to AOS Switches (OVE-5882)
- Packet Drops When Roaming with OKC Enabled (OVE-2218)
- HA 4.5R1 Disk Space Filled Up Writing Logs to Deleted Files (OVE-9487)
- Tomcat Security Vulnerabilities (OVE-9236)
- Endpoints Are Not Getting Profiled (OVE-9294)

OmniVista 2500 NMS 4.6R1 Release Notes

- Clean Up Scheduled Reports After OV User Is Deleted (OVE-7488)
- ovclient Service Memory Issue Problem (OVE-8776)
- ovclient OutOfMemoryError - GC Overhead Limit Exceeded (OVE-8876)
- AP Poller Change Events Keeping System Too Busy (OVE-8157)
- The Current Core Pool Size of Each Thread Pool Too High (OVE-8702)
- VMM Service Out of Memory (OVE-8939)
- Service Memory Limit Should Be Increased in Medium Setup (OVE-1921)
- Cluster Sync Progress Errors on HA System (OVE-8627)
- Cannot Access System After Manual Failover of HA System (OVE-8732)
- HA System Upgrade From 4.5R1GA to 4.5R2 Build 3 Failed (OVE-8539)
- Total Number of Rows Shown in Locator Browse Is Different from REST API (OVE-7959)
- No Data Response When Running API /rest-api/locator/browse for Many Devices with a Large amount of Locator Data (OVE-9225)
- Calling Locator/Browse REST APIs Every 2 Minutes Caused OOM Issue in Tomcat (OVE-9626)
- Failed to Update uboot on OS6350 (OVE-8588)
- Resource Manager Showing Error when upgrade CPLD/FPGA for OS6350, Although the Switch is Upgraded to New Version Successfully (OVE-8737)
- Cluster System Missing Switch Backup Folder for Resource Manager (OVE-8633)
- "Export VPN Setting" Issue in RAP Workflow (OVE-7685)
- "Export VPN Settings" Issue in RAP Workflow for Data VPN Servers (OVE-7688)
- Unable to specify VPN Server Setting Name when Importing APs into Device Catalog (OVE-7793)
- Many Python Processes Running in 5k System (OVE-8624)

6.4 PRs Fixed Since 4.4R2

6.4.1 Customer PRs

CR/PR Number	Description
Case: 00436946 OVC-6861	Summary: Print tickets time differs + Account Validity Period exceeds in Guest-Operator login - OV Cirrus 3.1.0 GA. Click for Additional Information
Case: 00435963 OVC-7114	Summary: Access to Captive portal fail with "Reject Reason = "Receive time out"" in Captive Portal records. Click for Additional Information
Case: 00440399 OVC-7426	Summary: OV Cirrus CLI Scripting log page stuck "Loading" for 3 minutes. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00434606 <i>OVC-5400</i>	Summary: OV Cirrus Guest access portal is not working. Click for Additional Information
Case: 00434966 <i>OVC-7167</i>	Summary: OV Cirrus If the admin password is different than the default one, the provisioning fails. Click for Additional Information
Case: 00452519 <i>CRNOV-1790</i>	Summary: OVC - Provisioning Failed state. Click for Additional Information
Case: 00447389 <i>OVE-7712</i>	Summary: OV 2500 4.4R2 / OV Cirrus 3.1.0 Duplicate SSID on WLAN -> SSIDs page. Click for Additional Information
Case: 00443735 <i>OVE-6775</i>	Summary: OV Cirrus Managed Inventory Ports, Wrong PoE Status and Wattage for OS6860E-P24. Click for Additional Information
Case: 00436366 <i>OVC-6861</i>	Summary: Wrong expiration date for Guest Accounts in UPAM. Click for Additional Information
Case: 00430474 <i>OD-894</i>	Summary: OVC - AP and switch are down. Click for Additional Information
Case: 00437271 <i>OVC-7154</i>	Summary: OV Cirrus 3.1 Adding or removing a device from device catalog causes an issue on Data Pond. Click for Additional Information
Case: 00439730 <i>OVC-7364</i>	Summary: OV Cirrus LDAP server management not taken into account when "Admin name" changed. Click for Additional Information
Case: 00419713 <i>OVE-6470</i>	Summary: OV 2500 4.4R2 GA (Build 37) issue when we select Unified Profile -> Workflow -> MAC Authentication. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00405472 <i>CRNOV-1251</i>	Summary: OV2500 NGINX service Stopped and do not restart. Click for Additional Information
Case: 00411920 <i>CRNOV-1425</i>	Summary: OV2500 VLAN Manager misbehavior. Click for Additional Information
Case: 00423209 <i>CRNOV-1555</i>	Summary: Guest Access Service Level is ignored when using Access Code. Click for Additional Information
Case: 00423292 <i>CRNOV-1508</i>	Summary: OV2500 objects are flickering when we are zooming. Click for Additional Information
Case: 00423298 <i>CRNOV-1506</i>	Summary: Editing existing AAA Server Profile in Simplified SSID App fails. Click for Additional Information
Case: 00423036 <i>ALEISSUE-515</i>	Summary: If account name is empty chosen Service Level does not affect settings. Click for Additional Information
Case: 00423038 <i>ALEISSUE-514</i>	Summary: UPAM Guest - Service Level - Level 4 - *Device Validity Period cannot not be changed! Click for Additional Information
Case: 00427821 <i>OVC-7003</i>	Summary: Unable to add the captive portal server in the ARP profile. Click for Additional Information
Case: 00429261 <i>ALEISSUE-534</i>	Summary: UPAM Guest: Verification Code not working on IOS devices. Click for Additional Information
Case: 00432688 <i>OVE-7084</i>	Summary: OV 2500 Add the command lsblk on the CLIADMIN Advanced Menu for HA troubleshooting. Click for Additional Information
Case: 00432778 <i>OVE-7089</i>	Summary: OV 2500 Enhance logs for OV HA Troubleshooting (during upgrade and normal operation). Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00431484 <i>OVE-7217</i> <i>OVE-7454</i>	Summary: OmniVista user Access rights. Click for Additional Information
Case: 00439743 <i>OVE-7210</i>	Summary: Unable to delete L:DAP server in OV Cirrus - An exception was encountered while accessing the database or while processing the database object. See the log file for details. Click for Additional Information
Case: 00447572 <i>CRNOV-1779</i>	Summary: Captive portal IP config issue - OV2500. Click for Additional Information
Case: 00448845	Summary: OV2500 Version 4.4R2: Scheduled Backup Not Working. Click for Additional Information
Case: 00431586 <i>OVE-7927</i>	Summary: The application bandwidth usage and application flow count widget not showing correct data. Click for Additional Information
Case: 00455156 <i>CRNOV-1779</i>	Summary: CRNOV-1894: OV2500 Error: IP Unavailable. Click for Additional Information
Case: 00451633 <i>CRNOV-1779</i>	Summary: OV2500 IP-Add Configuration Keeps On Appearing. Click for Additional Information
Case: 00454512 <i>CRNOV-1877</i>	Summary: HTTPS certificate of UPAM (Radius -Captive portal auth) expiring on March 15, 2020: Extension of validity period required. Click for Additional Information
Case: 00439901 <i>OVE-6983</i>	Summary: Error message while changing SSID password on stellar WIFI managed by OV-Cirrus. Click for Additional Information
Case: 00419855 <i>CRNOV-1467</i>	Summary: Unable to delete whole employee account at once. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00441376 <i>CRNOV-1725</i>	Summary: OV2500: Scheduler job task concurrently failed. Click for Additional Information
Case: 00435316 <i>CRNOV-1662</i>	Summary: OV2500: Unable to Apply the Signature Profile. Click for Additional Information
Case: 00444773 <i>ALEISSUE-625</i>	Summary: Machine auth issue - OV2500. Click for Additional Information
Case: 00444226 <i>OVE-7906</i>	Summary: OV2500_Managed Devices Menu Options Not Working. Click for Additional Information
Case: 00445322 <i>CRNOV-1737</i>	Summary: OV2500 as internal Radius server to authenticate switch login. Click for Additional Information
Case: 00445718 <i>OVE-6598</i>	Summary: OV2500: OV CPU utilization is high on VM-ESXI. Click for Additional Information
Case: 00437236 <i>CRNOV-1718</i>	Summary: Telegraf Logs in OV2500 with Error. Click for Additional Information
Case: 00444164 <i>CRNOV-1768</i>	Summary: Unable to take the Backup of the OV2500. Click for Additional Information
Case: 00446941 <i>ALEISSUE-584</i>	Summary: Stellar Enterprise with OV2500: device limitation fur Guest User with access-code not working. Click for Additional Information
Case: 00450766 <i>OVE-1817</i>	Summary: CLI script issue- OV2500 4.4R2. Click for Additional Information
Case: 00454040 <i>CRNOV-1834</i>	Summary: OmniVista services stopped after IP change. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00458796 <i>CRNOV-1913</i>	Summary: OV2500: SSL Error Message. Click for Additional Information
Case: 00459196 <i>OVE-6983</i>	Summary: Changes made on OV SSID template is not pushed to the AP group. Click for Additional Information
Case: 00442743 <i>CRNOV-1739</i>	Summary: OV2500 - OV is not accessible through GUI. Click for Additional Information

6.5 PRs Fixed Since 4.4R1

6.5.1 Customer PRs

CR/PR Number	Description
Case: 00413013 <i>OVE-6300</i>	Summary: Topology still showed AMAP links after disabling AMAP in all of the switches. Click for Additional Information
Case: 00402884 <i>OVE-6225</i>	Summary: Third-Party device licenses consumed count is incorrect after upgrading to 4.4R01. Click for Additional Information
Case: 00403449 <i>OVE-6220</i>	Summary: Downloading backup set file does not use Proxy. Click for Additional Information
Case: 00408143 <i>OVE-6201</i>	Summary: Route configured on VA is not working after system upgraded from 4.3R03 to 4.4R1. Click for Additional Information
Case: 00404524 <i>OVE-6173</i>	Summary: OmniVista did not show scripting files after clicking "Cancel" many times while sending a script to many switches. Click for Additional Information
Case: 00413273 <i>OVE-6172</i>	Summary: sFlow data grew too fast and caused High CPU and Mongo Exception Error. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00409665 <i>OVE-6088</i>	Summary: APs still kept "Warning" status after doing ACK/CLEAR for all traps. Click for Additional Information
Case: 00406679 <i>OVE-5962</i>	Summary: 4.4R1GA displays 40G/100G ports of OS9900 incorrectly. Click for Additional Information
Case: 00405981 <i>OVE-5871</i>	Summary: Cannot import both upgrade files of OS6560 normal/ISSU. Click for Additional Information
Case: 00400606 <i>OVE-5844</i>	Summary: Unable to view historic trap files. OmniVista keeps only one file "traps_xxx_.bak". Click for Additional Information
Case: 00404120 <i>OVE-5807</i>	Summary: Inaccurate error message is displayed when performing switch upgrade with wrong CLI/FTP credentials. Click for Additional Information
Case: 00402735 <i>OVE-5718</i>	Summary: Data migration issue after upgrading from 4.3R2 to 4.3R3 HA. Click for Additional Information
Case: 00400606 <i>OVE-5661</i>	Summary: Audit application does not show "Historical" logs. Click for Additional Information
Case: 00393203 <i>OVE-5522</i>	Summary: Help page is missing info on the usage of "Export" button in Resource Manager Backup/Restore screens. Click for Additional Information
Case: 00395408 <i>OVE-5442</i>	Summary: Unable to create service condition for Policy Rule. Click for Additional Information
Case: 00391775 <i>OVE-5362</i>	Summary: Topology Sites do not display on UI due to missing "Location" field. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00391416 <i>OVE-5358</i>	Summary: The list of IP interfaces of a switch does not update immediately after rediscovering. Click for Additional Information
Case: 00379740 <i>OVE-5275</i>	Summary: After Upgrading collection "ovproperties" was missing in MongoDB. Click for Additional Information
Case: 00386659 <i>OVE-5244</i>	Summary: Scheduler jobs should have timeout. Click for Additional Information
Case: 00390146 <i>OVE-5234</i>	Summary: Policy List should exclude rules that contain "source mac" condition when pushing to Policy List to OS6560. Click for Additional Information
Case: 00404905 <i>OVE-5171</i>	Summary: Telnet/SSH is connecting to google maps first when in Topology traditional view. Click for Additional Information
Case: 00388154 <i>OVE-5097</i>	Summary: Documentation Issue with OV2500 cluster in L3 mode. Click for Additional Information
Case: 00374278 <i>OVE-5053</i>	Summary: Add option Daylight Saving Time (DST) to Period Policy. Click for Additional Information
Case: 00353713 <i>OVE-3960</i>	Summary: Setting up Resource Allocation for OV VM is necessary. Click for Additional Information
Case: 00414788 <i>OVE-3958</i>	Summary: Top N Clients data is not displayed. Click for Additional Information
Case: 00351286 <i>OVE-3822</i>	Summary: The time zone between user 'root' and 'cliadmin' should be synchronized. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 00416898 <i>OVE-6088</i>	Summary: Mismatched AP license count. Click for Additional Information
Case: 00403073 <i>OVC-6525</i>	Summary: OmniVista Cirrus Trap responder not able to put special character in the SnmpVariable's filter. Click for Additional Information

6.5.2 Release Note PRs Fixed

- Cannot Edit Health Threshold Report for Devices In 4K AP System (OVE-1944)
- Process Stops When Trying to Create Top N Ports Profile (OVE-4946)
- "Last Known Up At" Field in Managed Devices Empty for Down AP (OVE-3159)
- Adding Heavily-Configured Device Takes Additional Time (OVE-4145)
- Backup Failure Trap Not Working on System Upgraded From OV422 MR2 - OV43R2 (OVE-3031)
- Cannot Notify Policy List with Accept All | Deny All Policy on AOS 6x Devices (OVC-6133)
- Unable to Create a Floor Plan in OVE 4.4R1 (OVE-5414)
- Unable to upload Captive Portal Certificate on UPAM (ALEISSUE-410, SR# 00392907)
- Unable to change "Account Validity Period" While Creating Guest Access Code with Service Level (ALEISSUE-459, SR# 00408173)
- APs were UP, however showed DOWN in OmniVista (ALEISSUE-383)

6.6 PRs Fixed Since 4.3R3

6.6.1 Customer PRs

CR/PR Number	Description
Case: 379841 <i>CRNOV-1000</i>	Summary: UPAM LDAP / AD AUTH No UPN support. Click for Additional Information
Case: 372065 <i>CRNOV-913</i>	Summary: Custom Radius Server certificate ineffective after upgrade to OV 4.3.R3 or service restart. Click for Additional Information
Case: 292909 <i>OVE-1777</i>	Summary: OmniVista should allow importing Web Server SSL Certificate with encrypted private key. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 314628 <i>OVE-2529</i>	Summary: Increase "Max Open Files" to limit the error "too many open files" of influxdb. Click for Additional Information
Case: 314452 <i>OVE-2549</i>	Summary: METRA SPA:OV2500:Unable to add the license. Click for Additional Information
Case: 346874 <i>OVE-2583</i>	Summary: Conflicting AP's IP. Click for Additional Information
Case: 322701 <i>OVE-2740</i>	Summary: Email trap responder is not working properly. Click for Additional Information
Case: 331841 <i>OVE-2941</i>	Summary: IAP-215 Management Login via UPAM Radius Proxy not possible. Click for Additional Information
Case: NA <i>OVE-3182</i>	Summary: The "Device DNS Name" on Netforward Result and "End station Name" on ARP Results are missed in OV 4.3R2. Click for Additional Information
Case: 345626 <i>OVE-3277</i>	Summary: OV2500 - Need API for Guest & BYOD users for UPAM. Click for Additional Information
Case: 356522 <i>OVE-3905</i>	Summary: Traps should be displayed consecutively from the first page when searching by trap name. Click for Additional Information
Case: 379239 <i>OVE-3925</i>	Summary: OmniVista kept the old Memory values (Xms, Xmx) of wrapper.conf. Click for Additional Information
Case: 356499 <i>OVE-4229</i>	Summary: Update help info about audit settings. Click for Additional Information
Case: 363763 <i>OVE-4351</i>	Summary: The template of browser page works incorrectly when changing the order of columns. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 371694 <i>OVE-4385</i>	Summary: Add a note in discovery online help that LLDP links cannot be manually edited/delete. Click for Additional Information
Case: 322800 <i>OVE-4466</i>	Summary: Settings of Managed Devices are not saved. Click for Additional Information
Case: 375237 <i>OVE-4513</i>	Summary: DNS configuration missing after changes to hostname in OmniVista. Click for Additional Information
Case: 375760 <i>OVE-4539</i>	Summary: In Topology page, the map node missed the IP address information. Click for Additional Information
Case: 372645 <i>OVE-4567</i>	Summary: OmniVista terminal command output is misaligned for the command 'ssudo sta_list'. Click for Additional Information
Case: 372645 <i>OVE-4567</i>	Summary: OmniVista terminal command output is misaligned for the command 'ssudo sta_list'. Click for Additional Information
Case: 358719 <i>OVE-4667</i>	Summary: OmniVista needs to push Trust-tag configuration to AP. Click for Additional Information
Case: NA <i>OVE-4708</i>	Summary: Some code flows of Application Visibility did not close connection after using. Click for Additional Information
Case: 380331 <i>OVE-4712</i>	Summary: Update Help document: Failure Policy - The authentication method used for 802.1X authentication is not supported on AOS 6.x devices. Click for Additional Information
Case: 380433 <i>OVE-4808</i>	Summary: Trap Responder - Email notification is not functioning. Click for Additional Information

OmniVista 2500 NMS 4.6R1 Release Notes

CR/PR Number	Description
Case: 381830 <i>OVE-4829</i>	Summary: Error in plugin [inputs.snmp]: agent 10.1.20.95:161: performing get on field healthDeviceRxTxLatest: Request timeout. Click for Additional Information
Case: 385881 <i>OVE-5056</i>	Summary: Topology map with background image does not save device's position. Click for Additional Information
Case: 386993 <i>OVE-5109</i>	Summary: Update the help-on-line page - Widget WLAN Client Health, what are the defined thresholds to determine Best/Good/Fair client health. Click for Additional Information
Case: 391867 <i>OVE-5292</i>	Summary: Resource Manager Backup/Restore page stuck at Loading due to corrupted data in MongoDB. Click for Additional Information

6.6.2 Release Note PRs Fixed

- No Tier 2 DFS Channel Support for US Domain (OVE-819)
- Live Search Does Not Work for VM IP Address/Switch IP Address (OVE-1908)
- During OV Upgrade, User Must “Press Any Key” When Prompted (OVE-2291)
- Layer 3 “Accept All” and “Deny All” Policies Fail (OVE-2753)
- UPAM Web Portal Is Not Updated on OV After Changing (OVE-2973)
- Missing Device Info After Re-Discovering Multiple APs (OVE-2978)
- Upgraded Stellar APs Display Incorrect Error Message (OVE-3018)
- Slow Discovery of Links of Newly Discovered Devices (OVE-3147)
- Switch Responding “Unsupported-Attribute” After Successful Guest/BYOD Authentication on 8.5R2 Switch (OVE-4189)

6.7 PRs Fixed Since 4.3R2

- Using “show log swlog” in OV Client Window Causes Window to Crash (CRNOV-645)
- OV Should Allow to Reset AP to Factory Settings (OVE-2162)
- AP Records Are Not Received by OmniVista in L2 HA Mode (OVE-2292)
- UPAM Authentication Log Issue with External Syslog Log Server (OVE-2699)
- Issue No Auth Radius Possible Between UPAM and RADIUS (OVE-3041)
- Stellar Clients Connected to AP1231 in Enterprise Mode Are Mapped to the Wrong VLAN (OVE-3042)
- Trap Description Does Not Show In OmniVista If Trap Is Defined as a V2 trap (OVE-3105)
- Cannot Upgrade from 4.3R1 Download Package After Selecting the “Download Only” Option (OVE-3112)

OmniVista 2500 NMS 4.6R1 Release Notes

- Performance Monitoring Does Not Support OS9900 (OVE-3151)
- Resource Manager Failed to Upgrade OS6350/6450 switches (OVE-3160)
- Edit RADIUS shared key it automatically synchronizes to all the switch – no way to revert (OVE-3166)
- “Synchronized status” field in OV 2500 under “managed devices” is not correct for switches on R8 (OVE-3181)
- Topology child maps order (OVE-3347)
- OV fails to create policy conditions of MAC group along with service group (OVE-3359)
- Need to improve the work flow to limit the error “failed to stop all services, proceed to exit ov restore flow” (OVE-3537)
- If Data Migration process is failed, OV needs to have a mechanism to inform the result of upgrade to the user (OVE-3538)
- If Backup/restore operation is failed, OV needs to have a mechanism to inform exactly the result to the user (OVE-3862)
- Authentication Server doesn’t support RADIUS Server that has Shared Secret > 16 characters (OVE-3878)
- Unable to change Discovery polling frequencies in OV 4.3R2 (OVE-3909)
- Add more some info of OV system when collecting OV log via VA Menu (OVE-3934)
- CLI Scripting’s Scheduler jobs have wrong start time when schedule the same script in the second time (OVE-3935)
- Guest can register account with long mail-address (OVE-3994)
- AP Registration - Access Point: Cannot change AP name + RF Profile at the same time (OVE-4005)

6.8 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)

OmniVista 2500 NMS 4.6R1 Release Notes

- 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)

OmniVista 2500 NMS 4.6R1 Release Notes

- 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)
- BMF Upgrade Fails on OS6250 Switch (210056)

6.9 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)
- 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)

OmniVista 2500 NMS 4.6R1 Release Notes

- CRAOS8X-1165 Notifying "one touch data" policy fails on OS6465 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)

6.10 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)

6.11 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)

6.12 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)

6.13 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)

6.14 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)

OmniVista 2500 NMS 4.6R1 Release Notes

- 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)

6.15 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)

6.16 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)

6.17 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)

6.18 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 4.6R1 Release Notes

- 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)

6.19 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)

6.20 PRs Fixed Since 3.5.7 Maintenance Build

- Live Search for IP Phones Issue (PR 187956)

6.21 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)

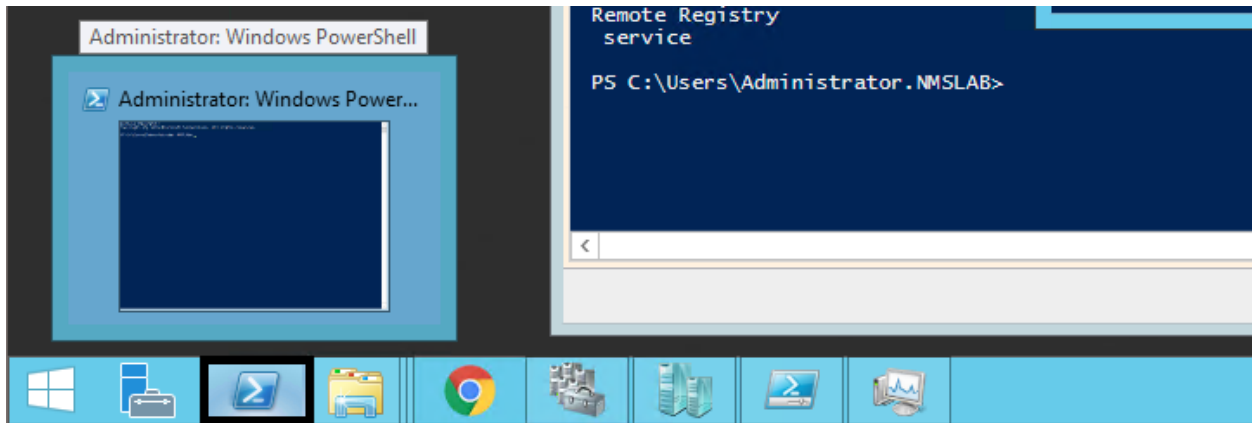
The following steps are specific to Windows 64 bit only.

1. Log in Hyper-V Server.
2. Get the Powershell script from attachment: HyperV_Enable_DCOM_x64.ps1.

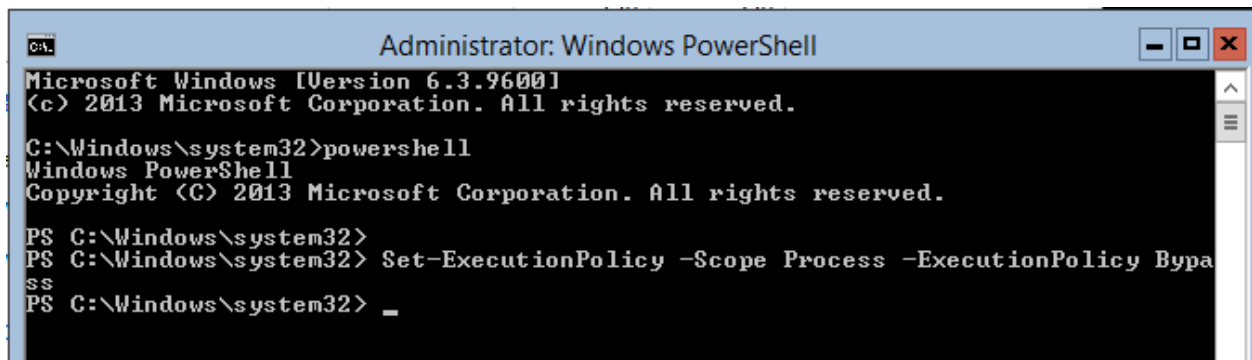


HyperV_Enable_DCOM_x64.ps1

3. Run Powershell.

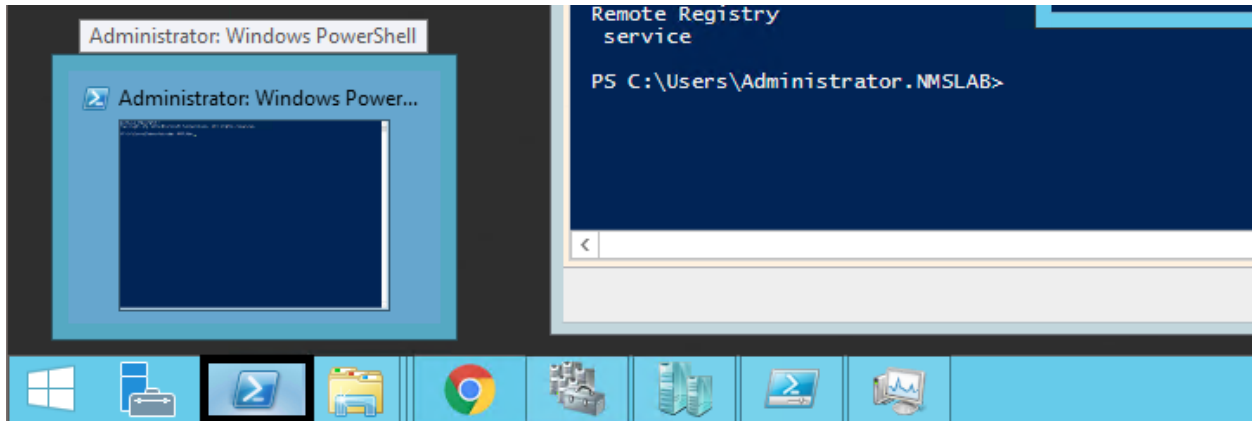


4. Run Set-ExecutionPolicy -Scope Process - ExecutionPolicy Bypass.

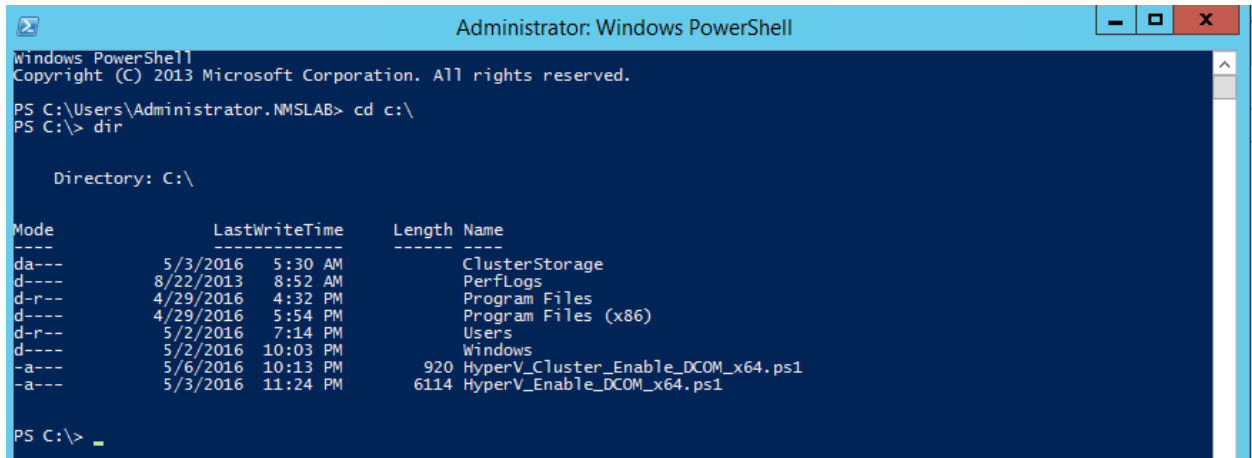


5. Change to the directory that contains the downloaded script from Step 2.

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.

