Release Notes

for

OmniVista 2500 NMS Enterprise Version 4.2.2.R01

August 2017

Revision A

Part Number 033225-00

READ THIS DOCUMENT

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

VirtualBox: 5.0.10

MS Hyper-V: 2012 R2 and 2016

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

Table of Contents

Table of Contents (continued)

Revision History

Release	Revision	Date	Description of Changes
4.2.2.R01	A	08/24/17	GA Release
4.2.1.R01	E	06/16/17	MR 2 Release Notes Update
4.2.1.R01	D	05/30/17	Maintenance Release 2
4.2.1.R01	C	02/02/17	Maintenance Release 1
4.2.1.R01	B	09/30/16	Release Notes Update
4.2.1.R01	A	09/22/16	GA Release
4.1.2.R03	A	01/29/16	GA Release
4.1.2.R02	A	05/22/15	GA Release
4.1.2.R01	B	12/19/14	Maintenance Release
4.1.2.R01	A	10/24/14	GA Release
4.1.1	B	12/19/14	Maintenance Release
4.1.1	A	09/10/14	GA Release
3.5.7	B	04/21/14	Maintenance Release
3.5.7	A	01/27/14	GA Release

1.0 Introduction

OmniVista 2500 NMS Enterprise 4.2.2.R01 (OV 2500 NMS-E 4.2.2.R01) is installed as a Virtual Appliance, and can be deployed to these hypervisors: VMware ESXi, VirtualBox, and MS Hyper-V:

- VMware ESXi: 5.5, 6.0, and 6.5
- Virtual Box: 5.0.10
- MS Hyper-V: 2012 R2 and 2016.

This document details known problems and limitations in OV 2500 NMS-E 4.2.2.R01, and workarounds are included. Please read the applicable sections in their entirety as they contain important operational information that may impact successful use of the application.

1.1 Technical Support Contacts

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

- **NAR:** https://support.esd.alcatel-lucent.com/
- **EMEA and APAC:** https://businessportal2.alcatel-lucent.com

1.2 Documentation

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

1.3 New in 4.2.2.R01

Device/Release Support

AOS 8.4.1.R01/R02 and

OmniVista 2500 NMS now supports AOS 8.4.1.R01/R02 on all previously-supported OS9900, OS6865, and OS6860/6860E Switches, as well as OS6865-U12/U28.

Stellar AP Series Wireless Devices

OmniVista 2500 NMS now supports the following Stellar AP Series Wireless Devices:

- OAW-AP1101
- OAW-AP1221
- OAW-AP1222
- OAW-AP1251.

You can manage up to 512 Stellar Series Access Points (APs). Stellar APs are viewed and managed in the new AP Registration application, and are configured in the new UPAM and WLAN set of applications. These APs have the same level of support as existing wireless devices on OmniVista applications. However, when you configure Stellar APs in OmniVista (e.g., Application Visibility, Unified Access, Resource Manager), rather than apply the configuration to an individual AP, you apply the configuration to an AP Group, which applies the configuration to all APs in the group. When Stellar APs are present in the network, you will be

presented with both a device selection option and an AP Group selection when you apply the configuration.

New Applications

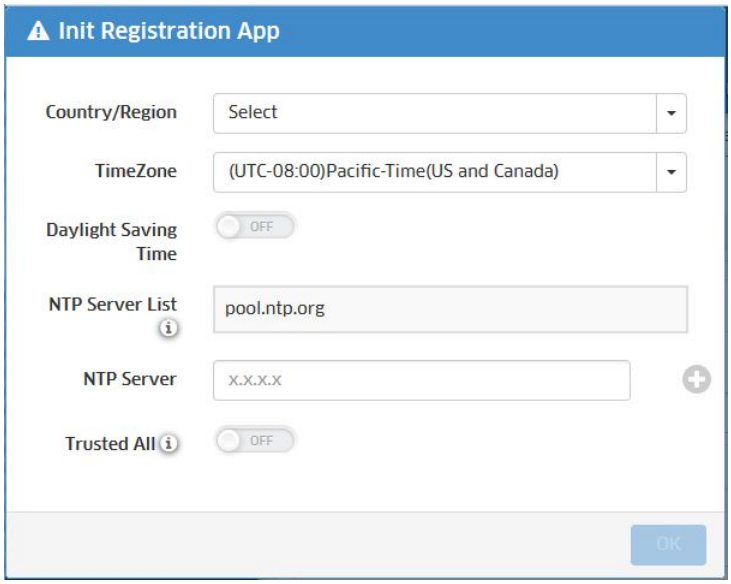
The following new applications have been added to OmniVista to manage the new Stellar AP Series Wireless Devices.

AP Registration

The new AP Registration application supports the new Stellar AP Series Wireless Devices. The application displays all discovered Stellar APs as well as Stellar AP Groups. When Stellar APs are connected to the network, they contact the OmniVista Server and automatically register with OmniVista. The APs are initially placed into "Unmanaged" status by the AP Registration application. The APs can be viewed in the Access Points Screen. If there are no configuration problems with an AP, you can place the AP into "Managed" status. Once an AP is placed into "Managed" status, OmniVista initially places it in a Default AP Group, and creates a Default AP Group map in Topology. You can create custom AP Groups to include specific APs; however, an AP can belong to only one AP Group.

Once an AP is registered and placed into "Manageable" status, it can be configured in OmniVista. When you configure Stellar APs in OmniVista (e.g., Application Visibility, Unified Access, Resource Manager), rather than apply the configuration to an individual AP, you apply the configuration an AP Group, which applies the configuration to all APs in the group. When Stellar APs are present in the network, you will be presented with both a device selection option and an AP Group selection option when you apply the configuration.

> **Note:** The first time you open the AP Registration application, the Init Registration App window will appear (shown below). Complete the fields as described below and click **OK**.



- **Country/Region –** Select the country/region where the Stellar APs are installed.
- **Time Zone –** Select the timezone where the Stellar APs are installed.

- **Daylight Saving Time – I**ndicate whether or not Daylight Saving Time is in effect (On) or not (Off)
- **NTP Server List –** Enter the NTP Server List, if applicable.
- **NTP Server –** Enter the NTP Server IP address, if applicable.
- **Trusted All –** If enabled (On), all registered Stellar APs will automatically be placed into a “Trusted” state.

UPAM

The new Unified Policy Access Manager (UPAM) group of applications is used to configure and manage BYOD and Guest Access on AOS Switches and Stellar AP Series Wireless Devices.

Summary

The Summary application provides a graphical overview of UPAM activity on the network (e.g., License usage, authentication requests, device information).

Authentication

The Authenticating application is used to monitor and configure authentication for wired and wireless devices.

Guest Access

The Guest Access application is used to manage guest users accessing the network.

BYOD Access

The BYOD Access application is used to manage employee BYOD devices accessing the network.

Setting

The Setting application s used to configure UPAM components (e.g., Email Server, External Log Server, External RADIUS Server).

WLAN

The new Wireless LAN (WLAN) group of applications are used to configure AP Policies to prevent attacks on Stellar AP Series Wireless Devices, as well as configure RF Profiles for devices. It is also used to create Heat Maps and Floor Plans to design and troubleshoot Stellar AP networks.

WLAN Service

The WLAN Service Screen is used to configure wireless networks.

WIPS

The WIPS application is used to monitor the wireless radio spectrum for the presence of unsafe access points and clients, and is used to configure policies to classify rogue APs/wireless attacks and take countermeasures to mitigate the impact of foreign intrusions.

RF

The RF application is used to create wireless RF Profiles for Stellar APs and AP Groups. RF Profiles enable the user to ensure that transmit power and operating frequencies meet the requirements of global regulatory agencies and individual countries. A user can also use the profiles to adjust the wireless parameters and functions according to real network environment to improve the user experience of wireless network.

Heat Map

The Heat Map application is a design, verification, and troubleshooting tool for installed Stellar Wi-Fi networks. The application provides a way to create and organize Heat Maps from multiple locations, from Campus level to Building level and Floor level to give a comprehensive view of Wi-Fi coverage.

Floor Plan

The Floor Plan application is a design, verification, and troubleshooting tool for Stellar Wi-Fi networks. Floor Plan can be used to determine optimal placement of Stellar APs in a location. The application can also automatically determine AP placement and configurations for optimal set-up.

Client

The Client application displays real time information for clients associated with Stellar APs, as well as clients that have been blacklisted. The application can also be used to manually blacklist a client.

Application Updates/Enhancements

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

License

Licenses are now categorized as Device License and Service Licenses. A new Device License has been added for Stellar AP Series Wireless Devices, and new Service Licenses have been added for Stellar AP guest devices and Stellar AP on-boarding devices. The licenses are described below.

- **Device Licenses -** Licenses a user to manage a specific number of devices.
  - **Alcatel-Lucent Enterprise Devices -** Licenses a specific number of ALE devices (e.g., OS10K, 6900, 6860) that can be managed. OmniVista has been certified to manage up to 10,000 devices (includes AOS and Third-Party Devices).
  - **Third Party Devices -** Licenses a specific number of third-party devices (e.g., Cisco).
  - **Alcatel Lucent Enterprise OmniAccess Stellar APs -** Licenses a specific number of OmniAccess Stellar Wireless Devices (e.g.,OAW-AP1101, OAW-AP1221) that can be managed. The license enables a user to manage a specific number of Stellar Access Points (APs). The following licenses are available:
    - 1 AP
    - 10 APs

  - 20 APs
  - 50 APs
  - 100 APs
  - 500 APs.
- **Service Licenses -** Licenses a user to manage a specific number of devices for the following services:
  - **VMs -** Licenses Virtual Machines (VM) management from the OmniVista VM Manager application. Licenses are available for managing 200, 500, and 1,000 VMs.
  - **Alcatel Lucent Enterprise Guest Devices -** Licenses Guest Devices authenticated through UPAM. The following licenses are available: 20, 50, 100, 500, or 1000 Guest Devices.
  - **Alcatel-Lucent Enterprise On-Boarding Devices -** Licenses BYOD Devices authenticated through UPAM. The following licenses are available: 20, 50, 100, 500, or 1000 BYOD Devices.

Discovery

The Discovery application now supports Stellar AP Series Wireless Devices. These devices have the same level of support as existing APs in OmniVista; however, there are some differences in how these devices are discovered in the Discovery application. When these devices are connected to the network, they contact the OmniVista Server and automatically register with OmniVista. The APs are initially placed into “Unmanaged” status by the AP Registration application. The APs can be viewed in the Access Points Screen. If there are no configuration problems with an AP, you can place the AP into “Managed” status. Once an AP is placed into “Managed” status, the device will appear in the Discovery and Topology applications and you will be able to configure it using OmniVista.

> **Note:** When a Stellar AP reboots, it reboots from the last saved configuration. It is recommended that users regularly perform a “Save to Running” operation on Stellar APs to save the most recent configuration in the event an AP reboots but is unable to connect to OmniVista to retrieve the latest configuration.

Additional new Discovery application features include:

- The Managed Devices Screen now has two tabs: The “ALL” tab displays all discovered devices. The “OAW” tab displays all discovered wireless devices, including Stellar APs.
- There is also a new “Clone LLDP Link” feature in the Discovery application. A “Clone LLDP to Manual” button has been added to the Discovery - Links Screen that can be used to clone an existing LLDP link to create a manual link. This can be helpful if an LLDP link goes down. If an LLDP link goes down, a "Link Down" Trap is sent, but the link disappears from the Topology map on the next poll because it no longer exists. However, if you clone an LLDP link to create a manual link, the manual link will continue to display (in Red) on the Topology map. You can also clone and edit an LLDP link to quickly create a new manual link on different ports on a device.

Topology

The Topology application now supports the Stellar AP Series Wireless Devices. Stellar APs have the same level of support as existing APs in OmniVista; however, there are some differences in how these devices are viewed/configured in the Topology application. As with all discovered devices, you can view information on these devices, search for these devices, and perform operations on the devices.

- Stellar APs are displayed in the Physical topology map, as well as in a new AP Group Map. When these devices register with OmniVista and are placed in "Managed" status, they are placed into a Default AP Group Map, automatically created by OmniVista. You can also create custom AP Groups containing different APs. When these groups are created, OmniVista automatically creates a map for this new AP Group.
- A new operation has been added for these devices – AP/Node Relationship Overlay View. Similar to the existing Overlay View operation, this overlay view displays information about the AP and the switch to which it is connected.
- "AP Group" has been added to the search criteria, enabling you to search for devices in a specific AP Group; and a new AP Group condition has been added to use when creating filters for Dynamic Maps.
- In AP Group maps, links from Stellar APs to switches are not displayed because switches are not part of this map. You can view links using the "Overlay" view. Or you can create a custom map and add switches and Stellar APs to view the links.

Additional new Topology application features include:

- You can now hover the mouse over a device or link in a map to display pop-up information for the device or link (in addition to clicking on a device or link to display information in the Detail Panel).
- Manual Links are now displayed in maps as a dashed line.
- "MAC Address" has been added to the Search Criteria available when searching on a map.
- You now have the option of adding gridlines to a Topology Map. Gridlines are enabled/disabled in the "Show Grid" field on the Topology Configuration window.
- You can now set a minimum number of devices that must be displayed on a map to trigger the Clustering Feature. The number is set in the "Min. No. of Devices to Enable Clustering" field on the Topology Configuration window. Clustering will not be enabled unless there is this minimum number of devices in a map.

Notifications

The Notifications application has been updated for Stellar AP Series Wireless Devices, and AP Series Device traps have been added to the application. Also, the Notifications Home Screen, "View By" option is now presented as a series of filters, which includes a new "AP Group" filter. As in previous releases, traps are displayed based on the filers selected.

Additional new Notifications application enhancements include:

- The user interface on the Notifications Screen has been improved to display more information in the Notifications Table. The Detail View for each trap is now displayed

directly beneath the trap (rather than on the right sided as in previous releases) so you see all of the basic trap information in addition to the detailed information.

- You can also now acknowledge individual traps by hovering over a trap in the Notifications Table and clicking on an ACK pop-up button.

Locator

The Locator application supports the new Stellar APs; and enables you to view wireless clients connected to Stellar APs.

Resource Manager

Resource Manager is supported on Stellar APs. You can perform a configuration backup of a Stellar AP and use the Backup File to compare configurations or perform troubleshooting. Stellar APs are not restored from a backup file; rather they are restored to the most recent saved configuration automatically on re-boot. Image upgrades are also supported on both Stellar AP Groups and individual Stellar APs. Resource Manager Inventory is not supported on Stellar APs.

The Backup Summary Screen now displays only the latest backup status for each device.

Dashboard

The Dashboard now has two tabs – a Global Tab and a WLAN Tab. The Global Tab displays all of the previously available widgets with the addition of new widgets for Stellar APs. The WLAN Tab displays new widgets created specifically for Stellar APs. The new widgets are listed below:

- **Global Tab**
  - **AP Groups -** Displays information for all configured Stellar AP Groups. This widget automatically displays information for all configured groups.
  - **AP Management -** Displays information for all registered Managed and Unmanaged Stellar APs. This widget automatically displays information for all registered APs.
  - **Client Health -** Displays information about all clients currently connected to Stellar APs, including Blacklisted Clients. This widget automatically displays information for all registered APs.
  - **Intrusive AP -** Displays the number of Intrusive Stellar APs detected on the network by category (e.g., Rouge AP, Interfering AP). This widget displays information based on policies configured in the WIPS application.
  - **UPAM Status -** Displays the administrative status of the UPAM Service in OmniVista. This widget automatically displays status information.
  - **Wireless Attacks -** Displays information about wireless attacks on the Stellar wireless network. This widget displays information based on policies configured in the WIPS application.
- **WLAN Tab**
  - **AP -** Displays information for all registered Stellar APs. This widget automatically displays information for all registered APs.
  - **AP Group -** Displays information for all configured Stellar AP Groups. This widget automatically displays information for all configured groups.

- **Client -** Displays information about all clients currently connected to Stellar APs, including Blacklisted Clients. This widget automatically displays information for all registered APs.
- **Monitoring Band -** Displays radio band information for all clients currently connected to Stellar APs. This widget automatically displays information for all registered APs.
- **Monitoring Client -** Displays information for all clients currently connected to Stellar APs. This widget automatically displays information for all registered APs.
- **Monitoring Client Health -** Displays health information for all clients currently connected to Stellar APs. This widget automatically displays information for all registered APs.
- **Monitoring Throughput -** Displays information about data throughput for all clients currently connected to Stellar APs. This widget automatically displays information for all registered APs.
- **SSID -** Displays all configured WLAN Services.

  Note: By default, the WLAN Tab displays information on all registered Stellar APs. You can also filter the view to display information by specific SSID, AP Group, AP, or Client. Click on the “View by” link at the top of the Dashboard to filter the display.

User Interface

The Main Menu at the top of the OmniVista Screen has been updated to display all of the applications and their configuration screens under each drop-down (e.g., Network, Configuration, Unified Access). You can click on any application or screen in the drop-down to go directly to that screen in OmniVista.

The device selection process for Application Wizards in OmniVista has been improved for all applications that are used to configure Stellar AP Series Wireless Devices (e.g., Application Visibility, Unified Access, Resource Manager). Devices are now displayed in detailed table format (rather than listed in a single column). This enables you to sort devices by column in the table or page through larger tables to select devices. You then select devices in the table and click on an **ADD** button to choose devices. You can also click on an **EDIT** button to add/remove devices. Application Wizards that are not used to configure AP Series Wireless Devices (e.g., PolicyView) retain the old device selection process.

To improve performance, applications with larger tables (e.g., VLANs, Unified Access Device Config) do not display all data by default. You must select the devices/AP Groups you want to display in the table. These applications feature a Device Selection Bar at the top of the table. You click on an **ADD** button and selects the devices to display. You can also click on an **EDIT** button to add/remove devices. The device selection remains persistent until it is changed or you log out of OmniVista . When you log out, the default setting (no display) returns.

Analytics

The Top N Switches Report has been replaced with the Network Health Report. The Network Health Report displays the health of all discovered network devices in terms of CPU, Memory, Temperature. The widgets on the page provide a status overview for all network devices for each health category. You can hover over an area in the widget for more information; and click on a widget to bring up an overview screen for a specific health category (CPU, Memory,

Temperature), where you can view detailed information on each network device and set health thresholds for devices.

Unified Profile

The Unified Profile application has been updated with some new Workflows, Templates, and Device Configuration Screens, and the left-hand menu has been re-organized.

- **Workflows -** The following new Workflows have been added to the Unified Profile application:
  - **MAC Authentication –** Use RADIUS Servers to authenticate users using MAC Address.
  - **MAC Authentication and Captive Portal with UPAM –** Use the 802.1x, MAC Authentication and Captive Portal with UPAM.
  - **Setting Up Edge Infrastructure for WLAN –** Classify AP traffic (management and client) to edge devices using Access Auth Profile and Classification Rules.
- **Templates –** The following new Templates have been added to the Unified Profile application:
  - **WLAN Service –** Used to configure wireless networks.
  - **Access Policies**
    - **Location Policy –** Defines a specific location where a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.
    - **Period Policy –** Specifies the days and times during which a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.
  - **Legacy Wireless Profiles (Non-Stellar Devices)**
    - **802.1x Authentication Profile –** Create an 802.1X Profile to use Radius Servers to authenticate users using 802.1x. An 802.1X Profile can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.
    - **MAC Authentication Profile –** Create a MAC Authentication Profile to use Radius Servers to authenticate users using MAC address. A MAC Authentication Profile can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.
- **Device Config Screens –** The following Device Configuration Screens have been added/re-organized in the Unified Profile application. Device Config Screens enable you to edit and delete Unified Profiles on specific network devices.
  - WLAN Service (SSID)
  - Access Policies
    - Location Policy
    - Period Policy
  - Legacy Wireless Profiles
    - 802.1x Authentication Profile
    - MAC Authentication Profile

        - SSID Profile
        - AP Group
        - Virtual AP
        - AAA Profile
        - AAA Server Group
    - Global Configuration
        - Setting
        - AAA
        - Redirect Allowed Profile

Audit Application

The following new logs have been added to the Audit application:

- Network Log
    - WMA
- System Log
    - Telegraph
    - VA Config
    - VA Upgrade
- UPAM Logs
    - Jetty
    - Radius
    - UPAM

The following logs have been removed from the Audit application:

- Security Logs
    - SecureView SA
    - Security Configuration

Multimedia Services (mDNS)

The original mDNS application (Legacy mDNS) has been retained. However, a new Gateway Device Screen has been added to configure mDNS Gateway Switches. A Gateway mDNS Switch replaces the Wireless Controller used in Legacy mDNS, and can be used if there are Stellar Access Points (APs) in the network. A new Poll Screen has also been added to poll Gateway Switches for updates to the mDNS configuration in the OmniVista Database.

VLAN Manager

In addition to the previous method of creating VLANs by selecting devices, you can now create VLANs by Topology Map. Two new buttons have been added to the top of the VLAN Manager Screen – **Create VLAN by Devices** and **Create VLAN by Map**. When you click on **Create VLAN by Devices**, the Create VLAN Wizard presents a Device Selection screen. When you select **Create VLAN by Map**, Create VLAN Wizard presents a Map Selection screen. When you

create VLANs using a Topology Map, you configure the VLAN(s) on all of the devices contained in the selected map.

Also, a “VLAN Overwrite” option has been added to the Create VLAN Wizard. If enabled, currently-configured VLANs are replaced with new VLAN Configuration, including devices or ports configured with the VLANs.

VA Menus

The following new menus have been added to the “Configure the Virtual Appliance” Menu:

- **Configure UPAM Portal IP and Ports –** Used to configure the UPAM IP address and port.
- **Change Screen Resolution –** Used to configure the VA screen resolution.
- **Configure the Other Network Cards –** Used to configure additional network cards on the VA.

The following menu has been deleted from the “Configure the Virtual Appliance” Menu:

- **Configure JRE Certificate –** A certificate can now be imported using the Preferences – CA Certificate Import Screen.

1.4 Feature Set Support

1.4.1 Element Manager Integration

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

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

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

Note: This feature is not supported on Stellar APs.

1.4.2 Device Feature Support

The following table details OV 2500 NMS-E 4.2.2.R01 feature support by device.

Feature	OS10K 6900	OS6860	Other AOS	Stellar APs	OA WLAN	OmniAccess ESR	3rd Party Switches
Application Visibility (1)	X	X		X			
Analytics (2)	X	X	X	X			
Basic MIB-2 Polling and Status Display	X	X	X		X	X	X (3)
ClearPass (BYOD) (4)	X	X	X				
CLI Scripting	X	X	X	X(5)	X	X	X
Discovery	X	X	X	X	X	X	X (3)
Locator	X	X	X	X	X		X (6)
mDNS		X	X (7)				
mDNS Gateway				X			
PolicyView-QoS	X	X	X	X	X		
Premium Service (BYOD)		X	X				
ProActive Lifecycle Mgmt	X	X	X	X	X		
Quarantine Manager		X	X		X		
Report	X	X	X	X			
Resource Manager BU/Restore/Upgrade	X	X	X	X			
SIP (8)		X	X				
Telnet	X	X	X		X	X	X
Topology Links (LLDP) (9)			X	X			
Trap Absorption	X	X	X (10)	X	X		X
Trap Display/Trap Responder	X	X	X	X	X	X	X
Trap Replay	X	X	X	X			
UPAM (Guest User and BYOD)	X	X	X	X			
UNP (11)	X	X	X	X			
VLAN Configuration	X	X	X		X		
VM Manager	X	X	X				
VM Snooping	X (12)						
VXLANs	X (13)						
WLAN				X			

1. The Application Visibility feature is supported on OS10K Switches (AOS 7.3.4.R02 and later), OS6900 Switches (AOS 7.3.4.R02 and later), OS6560 (AOS 8.4.1.R02 and later), and OS6860E and OS6865 Switches (AOS 8.2.1.R01 and later). It is also supported in a virtual

chassis of OS6860/OS6860E Switches where at least one OS6860E is present. It is also supported on the following Stellar APs OAW-AP1221, OAW-AP1222, and OAW-AP1251.

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

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

4. ClearPass (BYOD) is supported on OS6850E/6855 Switches (AOS 6.4.6.R01 and later), OS6250, and OS6450 (6.7.1.R02 and later), and OS6860 (8.3.1.R01 and later).

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

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

7. AOS 6.4.6.R01 and later Switches only.

8. The 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).

9. LLDP is supported on OS10K/OS6900 Devices (7.3.4.R02 and later), AOS Devices (6.4.4.R01 and later), and IPD SR7x50 devices (version 9.x and later). It is also supported on links between AOS switches and Stellar APs. Links to Third-Party devices are not supported. Also note that OmniVista 2500 NMS does not display LLDP links reported by a single device. For a link to be displayed, both devices must be supported devices and LLDP MIB interface from each must have the Link.

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

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

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

13. VXLANs are supported on OS6900-Q32 and OS6900-X72 Switches (8.3.1.R02 and later).

1.4.3 SSHv2/Telnet Element Management

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

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

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

2.0 System Requirements

The following builds are certified for OV 2500 NMS-E 4.2.2.R01:

AOS

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

OmniAccess WLAN

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

OmniAccess WLAN IAP

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

OmniAccess ESR

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

Stellar AP Series Wireless Devices

- OAW-AP1101 – SOS 3.0.0
- OAW-AP1221 – SOS 3.0.0
- OAW-AP1222 – SOS 3.0.0
- OAW-AP1251 – SOS 3.0.0

OmniVista 2500 NMS-E 4.2.2.R01 Upgrade Paths Certified

- 4.2.1.R01 (MR 2) – 4.2.2.R01

2.1 Proxy Requirements

OV 2500 NMS-E 4.2.2.R01 uses external repositories for Application Visibility Signature File updates, ProActive Lifecycle Management (PALM), and the OmniVista 2500 NMS Software Repository, which is used for software updates/upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.2.2.R01 to connect to the OmniVista 2500 NMS External Repository.

2.2 Firewall Requirements

The OmniVista 2500 NMS Web Client, OmniVista 2500 NMS Server and network devices communicate over an IP network. You must configure the firewall appropriately for OmniVista 2500 NMS to run properly. The following URLs must be allowed to enable communication between the OmniVista Server and the ALE Central Repository, Application Visibility (AV) Signature Repository, and Proactive Lifecycle Management (PALM) Portal:

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

2.2.1 OmniVista 2500 NMS Ports

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

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

2.3 Recommended System Configurations

The table below provides recommended Hypervisor configurations based on the number of devices being managed by OV 2500 NMS-E 4.2.2.R01 (500, 2,000, 5,000, and 10,000 devices). These configurations should be used as a guide. Specific configurations may vary depending on the network, the number of wired/wireless clients, the number of VLANs, applications open, etc. For more information, contact Customer Support.

Total Number of Managed Devices (AOS, Third-Party, and Stellar APs)	Total Number of Wireless Clients (Corporate, Guest, and BYOD)	Hypervisor Processor	Hypervisor RAM	HDD Provisioning
500	5,000	2.4 GHz 8 Cores	16GB	HDD1:50GB HDD2:256GB
2,000	10,000	2.4 GHz 8 Cores	32GB	HDD1:50GB HDD2:512GB
5,000	20,000	2.4 GHz 12 Cores	64GB	HDD1:50GB HDD2:2048GB
10,000	25,000	2.4 GHz 12 Cores	64GB	HDD1:50GB HDD2:2048GB

Note: The maximum number of Stellar APs supported is 512.

Note: By default, OV 2500 NMS-E 4.2.2.R01 is partitioned as follows: HDD1:50GB and HDD2:256GB. If you are managing more than 500 devices it is recommended that you go to the Virtual Appliance Menu on the VA to the increase the HDD2 provision. See the *OmniVista 2500 NMS-E 4.2.2.R01 Installation and Upgrade Guide* for instructions on extending the partition.

3.0 Installation

OmniVista 2500 NMS is installed from a download file available on the Customer Support website. Note that you can only upgrade to OV 2500 NMS-E 4.2.2.R01 from OmniVista 2500 4.2.1.R01 (MR2).

3.1 Licensing

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

- **Device Licenses -** Licenses a user to manage a specific number of devices.
  - **Alcatel-Lucent Enterprise Devices -** Licenses a specific number of ALE devices (e.g., OS10K, 6900, 6860) that can be managed. OmniVista has been certified to manage up to 10,000 devices (includes AOS and Third-Party Devices).
  - **Third Party Devices -** Licenses third-party devices (e.g., Cisco).
  - **Alcatel Lucent Enterprise OmniAccess Stellar APs -** Licenses OmniAcess Stellar Wireless Devices (e.g.,OAW-AP1101, OAW-AP1221). OmniVista has been certified to manage up to 512 Stellar APs.
- **Service Licenses -** Licenses a user to manage a specific number of devices for the following services:
  - **VMs -** Licenses Virtual Machines (VMs). VMs can be deployed on VMware vCenters, Citrix XenServers, and MS Hyper-V Servers; and OmniVista 2500 NMS supports a mixture of Hypervisor types with no limit on the number of Hypervisors. However, the VM Manager application supports a maximum of 5,000 VMs from all Hypervisors. More than 5,000 VMs are allowed, however a warning message will be displayed and an entry will be written to the VMM Log File.
  - **Alcatel Lucent Enterprise Guest Devices -** Licenses Guest Devices authentication through UPAM. The following licenses are available: 20, 50, 100, 500, or 1000 Guest Devices.
  - **Alcatel-Lucent Enterprise On-Boarding Devices -** Licenses BYOD Devices authentication through UPAM. The following licenses are available: 20, 50, 100, 500, or 1000 Guest Devices.

There are three (3) types of OmniVista Licenses:

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

Device License Types

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

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

Service License Types

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

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

Note: Licenses are imported/upgraded in the License Application. After installing OV 2500 NMS-E 4.2.2.R01, go to Administrator – License, import the license, then select the license type you want to upgrade/relicense and enter the License Key.

See the *OmniVista 2500 NMS-E 4.2.2.R01 Installation and Upgrade Guide* for instructions on generating an Evaluation License.

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

A Starter Pack License of the OmniVista 2500 NMS Application allows you to manage up to 30 devices (10 AOS, 10 Third-Party, 10 Stellar APs) with no expiration date. An Evaluation license of OmniVista 2500 NMS is valid only for a limited period of time. To gain permanent use of the OmniVista 2500 NMS software, you must order a Permanent Node Management License. The following procedure describes how to obtain an OmniVista 2500 NMS license key.

1. Purchase a permanent OmniVista 2500 NMS-E 4.2.2.R01 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 http://service.esd.alcatel-lucent.com/portal/page/portal/EService/LicenseGeneration and select **OV 411/422**.

3. Enter your Customer ID and Order Number.

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

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

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

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

4.0 Launching OmniVista 2500 NMS

To launch OV 2500 NMS-E 4.2.2.R01, enter the IP address of the OmniVista 2500 NMS Server in a supported web browser (e.g., *https://<OVServerIPaddress>*.

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

Note: The Watchdog Application, which enables all of the necessary OV 2500 NMS-E 4.2.2.R01 Services must be started to launch OV 2500 NMS-E 4.2.2.R01. By default, Watchdog should start automatically when OV 2500 NMS-E 4.2.2.R01 is installed. However, if you are having trouble launching OmniVista 2500 NMS, check to make sure that the Watchdog Service is enabled. If it is not, enable it. It will launch the remaining OmniVista 2500 NMS Services.

Open a Console on the VA, and select the **Run Watchdog Command** option to display the status of Services or launch Services.

4.1 Logging Into OmniVista 2500 NMS-E 4.2.2.R01

After launching OV 2500 NMS-E 4.2.2.R01 for the first time, log in using the Default Username and Password:

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

5.0 Known Problems

5.1 Known Application Visibility Problems

5.1.1 Monitoring and Enforcement CSV Files are not Getting Populated in OmniVista

Monitoring and Enforcement CSV Files are intermittently not getting populated in OmniVista.

Workaround: Re-start the Application Visibility Service. Go to Administrator – Control Panel – Watchdog to restart the service.

PR# OV-4751

5.2 Known Discovery Problems

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

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

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

PR# OV-3818

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

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

Workaround: No workaround at this time.

PR# OV-4396

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

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

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

PR# OV-4709

5.3 Known Heat Map Problems

5.3.1 Imported Floor Plan Does Not Display

The imported floor plan image file does not display when creating a Heat Map.

Workaround: No workaround at this time.

PR# OV-4640

5.4 Known Locator Problems

5.4.1 External RADIUS Users Cannot Utilize the Template Function

Users who log into OmniVista using an External RADIUS Server cannot Utilize the Template Function in the NetForward Results Table. The “Template 1” and “Template 2” buttons will be labeled “Custom” but will not have any functionality.

Workaround: No workaround at this time.

PR# 228018

5.5 Known Notifications Problems

5.5.1 Configure Traps for Multiple Devices Failed on Some Devices

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

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

PR# OV-4768

5.6 Known PolicyView Problems

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

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

Workaround: No workaround at this time.

PR# 196666

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

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

Workaround: No workaround at this time.

PR# 201688

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

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

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

PR# 202737

5.7 Known Report Problems

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

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

Workaround: A report can contain a maximum of 16MB of data (for a table report, such as Discovery - Inventory List, this is approximately 1,000 rows of data).

PR# OV-4463

5.8 Known Resource Manager Problems

5.8.1 BMF Upgrade Fails on OS6250 Switch

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

Workaround: Use the CLI to upgrade BMF manually.

PR# 210056

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

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

Workaround: No workaround at this time.

PR# 219688

5.9 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

5.10 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 Cannot Use UTF8 Characters in Unified Profile Name

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

Workaround: No workaround at this time.

PR# OV-2201

5.11 Known UPAM Problems

5.11.1 UPAM Authentication with External RADIUS Fails if Secret Between UPAM and AP are Different than UPAM and External RADIUS

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.

Workaround: The shared secret between the AP and UPAM should be the same at the shared secret between UPAM and the external RADIUS.

PR# OV-4242

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

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

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

PR# OV-4252

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

UPAM does not support import of RADIUS dictionary.

Workaround: No workaround at this time.

PR# OV-4306

5.11.4 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# OV-4480

5.11.5 LDAP Role Mapping Does Not Work with MAC Authentication

LDAP Role Mapping works with 802.1x Authentication, not with MAC Authentication.

Workaround: LDAP Role Mapping is supported with 802.1x Authentication, not with MAC Authentication. No workaround at this time.

PR# OV-4284

5.11.6 Unable to Configure OmniSwitch ASA Using UPAM as AAA Server

Configuration for AOS ASA is not available in UPAM.

Workaround: No workaround at this time.

PR# OV-4306

5.11.7 UPAM External RADIUS Server Certificate Fails

Importing a .der or .pfx certificate fails when importing a certificate for the UPAM External RADIUS Server.

Workaround: The imported certificate file must be a ".pem" file. No other file formats are supported.

PR# OV-4490

5.11.8 UPAM Does Not Support NAS Clients with Different Keys

UPAM does not support NAS Clients with different Shared Secret keys. All NAS clients **must** have the same key. If one does not, any Access-Request will be silently discarded. There will be no authentication record and no error on the summary reports. The only way to know would be to view the UPAM Audit Log. .

Workaround: All NAS clients **must** have the same Shared Secret key.

PR# OV-4490

5.12 Known VM Manager Problems

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

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

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

PR# 174181

5.12.2 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

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

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

Workaround: N/A

PR# 163314

5.13 Known Other Problems

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

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

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

PR# 197850

5.13.2 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

5.13.3 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

5.13.4 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

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

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

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

PR# OV-3993

5.13.6 OmniVista Cannot be Accessed by Web Client

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

Workaround: Restart ovclient or tomcat service.

PR# OV-4602

5.13.7 Packet Drops When Roaming with OKC Enabled

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

Workaround: No workaround at this time.

PR# OV-4618

5.13.8 Errors Displayed During OmniVista Upgrade

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

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

PR# OV-4752

6.0 Release Notes PRs Fixed

6.1 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 back 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)

6.2 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)

6.3 PRs Fixed Since 4.2.1.R01 GA

- OmniVista should display ifAlias in addition to ifDescr in port pickers (PR 214448)
- In the Application Visibility application, the default option for Data Unit should be "Bytes" instead of "MB" for Counter Type/Byte Count (PR 220623)Create ClearPass Roles matching the names of the standard Enforcement Profiles (PR 220825)
- Tomcat shuts down on a system running for a long time (PR 220833)
- OmniVista using 127.0.0.1 as the NAS-IP instead of using the physical address in the RADIUS request sent (PR 221385)
- BYOD Diagnostics - Search for IP address for authenticated endpoint in ClearPass fails (PR 221798)
- BYOD fails to update Access Role Profile if it is associated with an Enforcement Policy (PR 221857)

- Read and Write community string are the same after OV discovers switches (PR 222203)
- OmniVista Scheduled reboot is not working (PR 222520)
- Backup Tab in Resource Manger 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)

6.4 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)

6.5 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)

6.6 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)

6.7 PRs Fixed Since 4.1.2.R01

- VA Upgrade - Error "The SNMP trap listener could not be created on port 162" when notification app opened (PR 201406)
- OmniVista 2500 NMS Discovery issue for Juniper switches in VC configuration (PR 190524)
- Clarification in color status change for Link Aggregate link status (PR 196909)
- Issue with the SPB One Touch Feature (PR 197937)
- "Max Timeout" script error seen when sending SPB Configuration Telnet Script through OmniVista 2500 NMS (PR 199393)

- Unable to assign ClearPass Server for AOS device (6.4.4.R01) (PR 199978)
- OmniVista 2500 NMS Tomcat Service does not start if database backup is imported from 3.5.7 through a RADIUS Server (PR 200009)
- SSLv3 vulnerability issue (PR 200391)
- OmniVista 2500 NMS Server in a VA installation should be able to bind to a port lower than 1024 (e.g., 162, 514) (PR 201007)
- OmniVista 2500 NMS should not show stack split warning icon when the stack does not support SSP and is not in loop (PR 201483)

6.8 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)

6.9 PRs Fixed Since 3.5.7 Maintenance Build

- Live Search for IP Phones Issue (PR 187956)

6.10 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)