Release Notes

for

OmniVista 2500 NMS
Version 4.9R2

September 2025
Revision C
Part Number 033792-10
READ THIS DOCUMENT

OmniVista 2500 NMS

for

VMware ESXi: 6.5, 6.7, 7.0.2, 8.0
MS Hyper-V: 2012 R2, 2016, 2019, 2022
MS Hyper-V on Windows 10 Professional
Linux KVM/Ubuntu 22.04

ALE USA Inc.
2000 Corporate Center Drive
Thousand Oaks, CA 91320
+1 (818) 880-3500

Table of Contents

Revision History

Release	Revision	Date	Description of Changes
4.9R2	C	9/4/25	Release Notes Update
4.9R2	B	6/5/25	Release Notes Update
4.9R2	A	4/25/25	GA Release
4.9R1	A	9/30/24	GA Release
4.8R2	A	1/16/24	GA Release
4.8R1	B	8/11/23	Release Notes Update
4.8R1	A	6/30/23	GA Release
4.7R1	D	05/18/23	Updated section 6.1.1 with patch 2 (build 30) information
4.7R1	C	01/09/23	Release Notes Update
4.7R1	B	10/21/22	Release Notes Update
4.7R1	A	10/11/22	GA Release
4.6R2	C	03/30/22	Release Notes Update
4.6R2	B	03/04/22	Release Notes Update
4.6R2	A	02/18/22	GA Release
4.6R1	C	11/01/21	Release Notes Update
4.6R1	B	10/22/21	Release Notes Update
4.6R1	A	09/28/21	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

1. Introduction

This document details known problems and limitations in OmniVista 2500 NMS 4.9R2 (OV 2500 NMS 4.9R2), 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 4.9R2 is installed as a Virtual Appliance, and can be deployed on the following hypervisors:

- Vmware ESXi 6.5, 6.7. 7.0.2, 8.0
- MS Hyper-V: 2012 R2, 2016, 2019, and 2022
- MS Hyper-V on Windows 10 Professional
- Linux KVM/Ubuntu 22.04

1.2 Technical Support Contacts

Alcatel-Lucent Enterprise technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	1-800-995-2696
Latin America	1-877-919-9526
Europe Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: https://myportal.al-enterprise.com/.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1 – Production network is down resulting in critical impact on business—no workaround available.

Severity 2 – Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 – Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 – Information or assistance on product feature, functionality, configuration, or installation.

1.3 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.

1.4 New in this Release

Hardware/Release Support

AOS Switches

The following new switch models are now supported:

- OS6870

Stellar APs

There were no new OmniAccess Stellar AP models introduced with this release:

Software

- **AOS 5.2R7** – OmniVista 2500 NMS now supports AOS 5.2R7 for the OS2260 and OS2360 Series Switches.
- **AOS 8.9R4 MR** – OmniVista 2500 NMS now supports AOS 8.9R4 MR on all previously supported AOS Switches.
- **AOS 8.10R2** – OmniVista 2500 NMS now supports AOS 8.10R2 on all previously supported AOS Switches.
- **AOS 8.10R3** – OmniVista 2500 NMS now supports AOS 8.10R3 on all previously supported AOS Switches.
- **AWOS 5.0.2** – OmniVista 2500 NMS now supports AWOS 5.0.2 on all previously supported Stellar APs.

New Features and Functions

This section details new features introduced in this release.

OmniSwitch 6870 Support

The OmniSwitch 6870 (OS6870) is supported with this release. Consider the following guidelines for supporting this platform:

- OmniVista does not support performing CPLD upgrades. To upgrade the CPLD version, refer to the AOS Release Notes for the CPLD procedure on ONIE-based switches.
- Application Monitoring is now supported on an OS6870 running AOS 8.10R3 or higher. Application Enforcement is not yet supported.

Pro Active LifeCycle Management Replaced with Fleet Supervision

The ProActive LifeCycle Management (PALM) application is no longer available as a service and support option. OmniVista now provides Fleet Supervision as a PALM replacement for monitoring Service and Support entitlement, hardware status, and software versions, etc. Go to https://myfleet.ovcirrus.com/ for more information.

Application Updates/Enhancements

This section details updates and enhancements to existing OmniVista applications.

- **Password Enhancements for OmniVista User Logins**
    - **Enforce Strong Password Setting** – New Password Expiry policy now configurable. You can specify the number of days during which a password remains valid. By default, Password Expiry is set to "Never". Changes to this setting apply immediately to new users, but do not affect existing users until they change their password on or after the current password expires.
    - **Password Recovery for CLI Admin** – If a user enters an incorrect password when logging into OmniVista 2500, the message "Forget your password? Use the VA menu to reset it." appears on the login screen. The user can go to the “Change Password” option in the VA Menu for the OmniVista 2500 instance to change the password.
- **Provisioning Encryption Strengthening** – Support added for all Auth & Priv protocols when configuring SNMPv3 access in the default or custom Management Users Template.

MD5	SHA+AES192	SHA224+AES192	SHA256+AES192
SHA	SHA+AES256	SHA224+AES256	SHA256+AES256
MD5+DES	SHA+3DES	SHA224+3DES	SHA256+3DES
SHA+DES	SHA224	SHA256	SHA384
SHA+AES	SHA224+AES	SHA256+AES	SHA384+AES

- **SSID**
    - **Wi-Fi Enhanced Open Transition Mode** – Support added to enable Enhanced Open Transition Mode for an SSID.
        - When this mode is enabled, the AP broadcasts two different types of BSSID: one legacy Open SSID on 2.4GHz/5.0GHz band and one Enhanced Open SSID on 2.4GHz/5.0GHz/6.0GHz band. This allows both Enhanced Open and Non-Enhanced Open clients to connect to the same open SSID without adversely impacting the end user experience.
        - The Enhanced Open setting is available when the SSID usage is set to Guest Network (Open or Captive Portal) or Employee BYOD Network.
        - Note that the Enhanced Open Transition Mode is supported only on APs running AWOS 4.0.8 or above. Enabling this mode for APs running older AWOS versions may cause the SSID to revert to an open SSID after a reboot. Upgrading your network is highly recommended.
    - **Backward Compatibility** – Support for 2.4/5GHz devices when 6GHz band is selected.
        - Enables/disables using WPA3_PSK_SAE_AES encryption on 2.4GHz and 5.0GHz bands when encryption is automatically set to WPA3_SAE_AES for the 6.0GHz band.

        - When the 6.0GHz band is selected for the SSID, the other bands inherit using WPA3_SAE_AES encryption, which some legacy devices cannot use to connect to the SSID.
        - When Backward Compatibility is enabled, the WPA3_PSK_SAE_AES Encryption Type is automatically used for the 2.4GHz and 5.0GHz bands, and the 6.0GHz band continues to use WPA3_SAE_AES.
        - The Backward Compatibility setting is available when the SSID usage is set to Protected Network (Pre-Shared Key & an Optional Captive Portal) or Protected Network for Employees (Pre-Shared Key & BYOD Registration Portal) and the Allowed Band is 6.0GHz.
        - Note that if the MLO Band setting includes 6.0GHz, then the Backward Compatibility option is automatically disabled.

- **UPAM Check for Message-Authenticator RADIUS Attribute** – A new Require Message Authenticator flag is now available to specify whether to check RADIUS packets for the Message-Authenticator attribute. This flag is configurable for the following use cases and resolves CVE-2024-3596 (#Blast-RADIUS):
    - **UPAM as RADIUS Server for AP/OmniSwitch** – UPAM RADIUS server accepts RADIUS requests from clients within a specified IP range.
        - Access Points always include the Message-Authenticator attribute in RADIUS request packets.
        - The OmniSwitch does not include the Message-Authenticator attribute in RADIUS requests or checks for that attribute in RADIUS responses. To ensure that the OmniSwitch includes that attribute in all RADIUS packets sent and also enforces validation of the attribute in all RADIUS server responses, use the **aaa radius message-authenticator** CLI command on the switch. This CLI command is a global command supported on AOS 8.10R2 or higher.
    - **External Radius server for AP/OmniSwitch (No UPAM)** – An Access Point or OmniSwitch sends RADIUS AAA requests directly to a RADIUS server (on-premises or hosted elsewhere); UPAM is not involved. OmniVista configures the AAA RADIUS settings on the AP or OmniSwitch through the AAA Server Profile.
        - The Require Message Authenticator flag in the AAA Server configuration on Access Points running AWOS >= 5.0.2 enforces that the RADIUS response packets from the RADIUS server contain the Message-Authenticator attribute. Access Points running AWOS < 5.0.2 do not verify the attribute in RADIUS server response packets.
        - The OmniSwitch does not include the Message-Authenticator attribute in RADIUS requests or checks for that attribute in RADIUS responses. To ensure that the OmniSwitch includes that attribute in all RADIUS packets sent and also enforces validation of the attribute in all responses received from any RADIUS server, use the **aaa radius message-authenticator** CLI command on the switch. This CLI command is a global command supported on AOS 8.10R2 or higher.

- **UPAM as Proxy between AP/OmniSwitch and External Radius** – UPAM proxies incoming RADIUS requests from an Access Point or OmniSwitch to an external RADIUS server.
  - When the Require Message Authenticator flag is enabled for the external RADIUS server, UPAM checks for the Message-Authenticator attribute in response packets received from the external RADIUS server. UPAM will then drop any response packets that do not contain the attribute but will continue to send RADIUS request packets to the external RADIUS Server for the specified number of Retries.
  - When the Require Message Authenticator flag is disabled for the external RADIUS server, UPAM does not check for the Message-Authenticator attribute in RADIUS response packets.

- **SMS Gateway Services**
  - Aliyun (China - https://dysmsapi.aliyuncs.com) – A “Messages Language” option to translate UPAM SMS messages into Chinese is now available. Templates that are used to access the Aliyun SMS function with OmniVista are generated based on the language selected.

OmniVista Framework Updates

Linux Distribution Update

- **OmniVista VA and RAP VPN VA** – Oracle Linux upgrade from version 8.7 to version 8.10.

Framework Updates

- **OmniVista 2500 NMS** – The following CVEs were fixed in this release:

CVE-2024-52046	CVE-2017-18342
CVE-2025-24813	CVE-2020-14343
CVE-2024-52316	CVE-2022-30123
CVE-2018-1270	CVE-2024-41110
CVE-2018-1275	CVE-2025-30215

- **New upgrade workflow** – This release introduces a new upgrade procedure that you must follow when upgrading from the 4.9R1 release to the 4.9R2 release. This facilitates the automatic inclusion of a required 4.9R1 patch. See OmniVista 2500 NMS 4.9R2 Upgrade Paths Certified for more important information.

1.5 Feature Set Support

1.5.1 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://ovc4x.ovcirrus.com/

1.5.2 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	1. All supported AOS OmniSwitch Devices, including OS2260 and OS2360	WebView
Web UI	• OS2200	Web UI Device Management
Web UI	• All supported Stellar APs	Web UI Device Management
Wireless Controller	• OAW-4030, OAW-4604, OAW-4704, IAP-105, IAP-205, IAP-225	OAW EMS
Third-Party	• Any network equipment with a built-in Web browser element for management.	Respective EMS

1.5.3 Device Feature Support

The following table details OmniVista 2500 NMS 4.9R2 feature support by device:

Feature	OS6900	OS6860/ OS6865*	OS9900	Other AOS**	OS2260 OS2360	Stellar APs	Legacy WLAN	3rd Party Devices
Discovery	X	X	X	X	X	X	X	X (10)
Locator	X	X	X	X	X	X	X	X (11)
Trap Absorption	X	X	X	X	X	X	X	X
Trap Display/Trap Responder	X	X	X	X	X	X	X	X
Basic MIB-2 Polling and Status Display	X	X	X	X	X		X	X (10)
CLI Scripting	X	X	X	X	X	X (12)	X	X (12)
PolicyView-QoS	X	X	X	X	X	X	X	
Topology Links (LLDP) (1)	X	X	X	X	X	X		
UNP	X	X	X	X	X	X		X (13)
Analytics	X	X	X	X	X (14)	X (14)		
Resource Manager BU/Restore/Upgrade	X	X	X	X	X	X		
Trap Replay	X	X	X	X	X	X		
Virtual Chassis	X	X	X	X	X			
VLAN Configuration	X	X	X	X	X (15)		X	
ClearPass (BYOD)	X	X	X	X		X		

Feature	OS6900	OS6860/ OS6865*	OS9900	Other AOS**	OS2260 OS2360	Stellar APs	Legacy WLAN	3rd Party Devices
Cloud Agent	X	X	X	X	X			
mDNS Gateway (2)	X	X	X	X		X		
mDNS Responder (3)	X	X	X	X		X		
Provisioning	X	X	X	X	X			
UPAM (Guest User, BYOD) (4)	X	X	X	X		X		
Unified Policies	X	X	X	X	X			
VM Manager (5)	X	X	X	X	X (16)			
Quarantine Manager (17)		X					X	
SPB/ERPv2 (6) (7)	X	X	X	X				
Unified Policy List	X	X	X	X				
VRF	X	X	X	X				
IoT (8)	X	X		X		X		
mDNS		X	X	X (18)				
Premium Service (BYOD)		X	X	X				
SIP		X	X	X				
Application Visibility		X (19)				X (19)		
VM Snooping	X (20)							
VXLANs	X (21)							
Web Content Filtering (9)						X		
WLAN (SSID)						X		

***OS6860/6865 (6860, 6860E, 6860N, 6865)
**Other AOS (6350, 6360, 6450, 6465, 6560, 6570)

Note: Earlier software versions may be referenced in the following notes. Please refer to System Requirements section for versions officially supported by this OmniVista release.

1. 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”.

2. mDNS Gateway is only supported on OS6450, OS6860E, OS6865, OS6900, and OS6860N.

3. The following devices can be configured as Responder Devices: OS6570, OS6860/E, OS6865, OS6900, OS9900. The following devices can be configured as Edge Devices:

OS6465, OS6560, OS6860/E, OS6865, OS6900, OS9900, and Stellar APs (except for OAW-AP1101).

4. LDAP Role Mapping is supported with 802.1x Authentication only. UPAM MAC and 802.1X authentication supported for wired clients. UPAM Authenticated Switch Access supports switch user authentication for basic read/write permissions on all features; does not support users with detailed access rights for different features or partition management.

5 The VM Manager (VMM) application is supported on Hyper-V 2012, 2012 R2, and 2016. VMM is not supported on Hyper-V 2019 or higher. In addition, only the English version of third-party software (VMware's vSphere or Microsoft Hyper-V) that VM Manager interfaces with is tested and certified; other languages may work, but they are not certified. VM Manager does not support Windows server 2022.

6. You can view SPB configurations in the Topology application. SPB Services can be configured in the Services application (Configuration – Services)

7. ERP v2 is supported on all AOS 8.x switch models that support ERP v2. You can view ERP configurations in the Topology application.

8. IoT Enforcement is only supported on OS6560-P48Z16 models with part number 904044-90. Models with part number 903954-90 are not supported.

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

10. 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.

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

12. CLI Scripting is not supported on Stellar APs or third-party devices; however, you can connect (SSH) to a Stellar AP or a third-party device using the CLI Scripting application.

13. The UNP feature within Unified Access is only supported for OAW Controller and OAW IAP.

14. 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

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

16. VMM VLAN configuration is not supported.

17. Quarantine Manager is supported on switches 6400, 6800, 6850, 6855, 6860, and 6865.

18. AOS 6.4.6.R01 and later switches only.

19. The Application Visibility feature is supported on OS6860E/OS6860N switches. The Application Visibility feature is not supported on OS6860, but it is 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, AP1201H, AP1201L, AP1201HL, and AP15XX. (AP132x and AP136x models require minimum Signature Kit version of 3.6.11. AP1301, AP1301H, and AP1311 require minimum Signature Kit version 3.8.3.)

20. 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.

21. VXLANs are supported on all AOS 8.x switch models that support VXLANs.

1.5.4 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 4.9R2:

AOS

- OS2260 – 5.2R5, 5.2R6, 5.2R7
- OS2360 – 5.2R5, 5.2R6, 5.2R7
- OS6350 – 6.7.2.R06, 6.7.2.R07, 6.7.2.R08
- OS6360 – 8.9R4, 8.10R2, 8.10R3
- OS6450 – 6.7.2.R06, 6.7.2.R07, 6.7.2.R08
- OS6465 – 8.9R4, 8.10R2, 8.10R3
- OS6560 – 8.9R4, 8.10R2, 8.10R3
- OS6570M – 8.9R4, 8.10R2, 8.10R3
- OS6860/E – 8.9R4, 8.10R2, 8.10R3
- OS6860N – 8.9R4, 8.10R2, 8.10R3
- OS6865 – 8.9R4, 8.10R2, 8.10R3
- OS6870 – 8.10R2, 8.10R3
- OS6900-X20, X40, T20, T40, Q32, X72 – 8.9R4
- OS6900-V72, C32, C32E, X48C6, T48C6, X48C4E, V48C8, X24C2, T24C2 – 8.9R4, 8.10R2, 8.10R3

- OS9907 – 8.9R4, 8.10R2, 8.10R3
- OS9912 – 8.9R4, 8.10R2, 8.10R3

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

Stellar AP Series Wireless Devices

The following AP models are supported. The recommended AWOS version is 5.0.2.

- 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-AP1261-RW-B
- OAW-AP1301
- OAW-AP1301H
- OAW-AP1311
- OAW-AP1321, OAW-AP1322
- OAW-AP1331
- OAW-AP1351
- OAW-AP1361, OAW-AP1361D, OAW-AP1362
- OAW-AP1451
- OAW-AP1431
- OAW-AP1411
- OAW-AP1511
- OAW-AP 1521

Note: If you are upgrading to OV 4.9R2 OmniVista from a previous release, it is recommended that you upgrade AWOS devices to AWOS 5.0.2 after the OmniVista upgrade.

Note: See the *AWOS 5.0.2 Release Notes* for more information on Stellar APs and details on any known issues.

OmniVista 2500 NMS 4.9R2 Upgrade Paths Certified

Detailed upgrade instructions are available in the *OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide*.

Important Note: The 4.9R2 release introduces specific changes to the Standalone and High-Availability upgrade procedure that you must follow to upgrade from 4.9R1 to 4.9R2. The upgrade workflow automatically includes a required upgrade to a 4.9R1 Patch 1 and ensures that the upgrade to the patch occurs first before the upgrade to 4.9R2. It is important that you follow this new upgrade workflow as documented in the "Upgrading from 4.9R1 to 4.9R2" section of the *OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide.*

Note:

- **Standalone Upgrade**
  - 4.9R2 Standalone Installation to 4.9R2 Standalone Installation.
  - To upgrade from older releases to 4.9R2, you must first upgrade to 4.9R1.
  - Upgrading an OV 2500 NMS from 4.9R1 to 4.9R2 automatically includes a required upgrade to a 4.9R1 Patch 1. As a result, there is a change to the upgrade workflow to ensure that the 4.9R1 upgrade to 4.9R1 Patch 1 occurs first, before the upgrade to 4.9R2. The new upgrade workflow is documented in "Upgrading from 4.9R1 Standalone to 4.9R2 Standalone" of the *OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide*.
- **High-Availability (HA) Upgrade**
  - The HA upgrade procedure requires first updating the Standby node then updating the Active node. For detailed steps on how to perform the upgrade procedure, refer to the following sections in the *OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide*:
    - "L2 High-Availability Upgrade Workflow" to upgrade an L2 HA installation.
    - "L3 High-Availability Upgrade Workflow" to upgrade an L3 HA installation.
  - Upgrading an OV 2500 NMS from 4.9R1 to 4.9R2 automatically includes a required upgrade to a 4.9R1 Patch 1. As a result, there is a change to the upgrade workflow to ensure that the 4.9R1 upgrade to 4.9R1 Patch 1 occurs first, before the upgrade to 4.9R2. The new upgrade workflow is documented in "Upgrading from 4.9R1 HA to 4.9R2 HA" of the *OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide*.
  - 4.9R1 HA Installation to 4.9R2 HA Installation.
  - To upgrade from older releases to 4.9R2, you must first upgrade to 4.9R1 HA.
  - An L3 HA cluster is supported only with a fresh HA installation; you cannot convert an L2 HA cluster to an L3 HA cluster.
  - Refer to High-Availability Installation Limitations for more information.
- **Standalone to High-Availability (HA) Conversion**

  You can convert a 4.9R2 Standalone Installation to a 4.9R2 HA Installation if the 4.9R2 Standalone installation was upgraded from a 4.3R2 or newer Standalone Installation.

Note: If you are using release 4.7R1:

1. Upgrade to the 4.7R1 Patch 2 release.

2. Upgrade to 4.8R1. Refer to the *OmniVista 2500 NMS 4.8R1 Installation and Upgrade Guide* for more information.
3. Upgrade to 4.8R2. Refer to the *OmniVista 2500 NMS 4.8R2 Installation and Upgrade Guide* for more information.
4. Upgrade to 4.9R1. Refer to the *OmniVista 2500 NMS 4.9R1 Installation and Upgrade Guide* for more information.
5. Upgrade to 4.9R2 (includes 4.9R1 patch). Refer to the *OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide* for more information.

2.1 Proxy Requirements

OV 2500 NMS 4.9R2 uses external repositories for Application Visibility Signature File updates, Fleet Supervision, 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 4.9R2 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, Fleet Supervision, and the Cloud-Based Device Fingerprinting Service:

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

Service	Port	Source/Destination
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 Authentication Forwarding	1814	External RADIUS/Net Device
RADIUS Accounting Forwarding	1815	External RADIUS/Net Device
RADIUS CoA – UDP Port	3799	UPAM/Net Device
VMM	135	OV Server/Hyper-V Server
	49152-65535 (RPC Dynamic Port)	Hyper-V Server/OV Server
High-Availability	TCP: 8000, 7801, 2224 UDP: 5405	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 4.9R2 (500, 2,000, 5,000, and 10,000 devices). These configurations should be used as a guide. Specific configurations may vary depending on the network, the number of wired/wireless clients, the number of VLANs, applications open, etc. For more information, contact Customer Support.

	Network Size*			
Configuration	**Low**	**Medium**	**High**	**Very High**
Total Number of Managed Devices (AOS, Third-Party, and Stellar APs)	500	2,000	5,000**	10,000**
Stellar AP Devices	500	2,000	4,000	4,000
Stellar AP Client Association	50,000	200,000	200,000	200,000

	Network Size*			
Configuration	**Low**	**Medium**	**High**	**Very High**
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 for Standalone	20GB	36GB	64GB	64GB
Minimum Reserved OmniVista VA RAM for HA	N/A***	40GB	64GB	64GB
HDD Provisioning	HDD1:50GB HDD2:512GB	HDD1:50GB HDD2:1024GB	HDD1:50GB HDD2:2048GB	HDD1:50GB HDD2:2048GB
Minimum Storage Read/Write Speed	100 MB/s	150 MB/s	200 MB/s	200 MB/s

*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 1000 AOS switches can be supported. If there are 4,000 Stellar APs in an HA “Very High” network size, up to 1500 AOS switches can be supported.

***An HA installation should be done on a “Medium” or higher size VA.

Notes:

1. When deploying the OmniVista VA for the first time, do not add the new disks in the hypervisor until after OmniVista is configured and rebooted.
2. 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.
3. 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.
4. Set CPU Shares to “High”.
5. 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.
6. By default, OV 2500 NMS 4.9R2 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 the increase the HDD2 provision.

See the *OmniVista 2500 NMS 4.9R2 Installation and Upgrade Guide* for instructions on extending the partition.

7. 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.
8. 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 4.9R2, Stellar APs in your network should be running AWOS version of 5.0.2. **First** upgrade to OV 2500 NMS 4.9R2; then upgrade your Stellar APs to 5.0.2. Please refer to the *OmniVista 2500 NMS 4.9R2 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 Web GUI for the upgrades.

See the *AWOS 5.0.2 Release Notes* for more information on Stellar APs and details on any known issues.

2.4 High-Availability Installation Limitations

The following functionality is not supported in a High-Availability (HA) Installation:

- Cluster IP configuration in L3 Cluster
- Converting 4.9R2 Standalone to 4.9R2 HA if the 4.9R2 Standalone was upgraded from 4.3R1 Standalone. (You can convert 4.9R2 Standalone to 4.9R2 HA if the 4.9R2 Standalone was upgraded from 4.7R1 Patch 2 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.
- Converting an L2 HA installation to an L3 HA installation is ***not*** supported. Only a fresh L3 HA installation is supported. However:
    - You can add a second node to a fresh 4.9R2 standalone installation to convert the cluster to an L3 HA installation.

- You can also upgrade a 4.9R1 standalone installation to 4.9R2 and then convert it to an L3 HA installation.

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 4.9R2 from OV 2500 NMS OV 2500 NMS 4.9R1. See the *OmniVista 2500 NMS 4.9R2 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 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 4.9R2, 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 4.9R2 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 4.9R2 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 From and click **Submit**. A download prompt will appear.

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

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

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

4.0 Launching OmniVista 2500 NMS

OV 2500 NMS 4.9R2 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 4.9R2 Services must be started to launch OV 2500 NMS 4.9R2. By default, Watchdog should start automatically when OV 2500 NMS 4.9R2 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 4.9R2

After launching OV 2500 NMS 4.9R2 for the first time, log in using the Default Username and Password:

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

When you first log in to OmniVista using the “admin” username and “switch” password, OmniVista will prompt you to change the default password.

5.0 Known Problems

5.1 Known AP Registration Problems

5.1.1 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

5.1.2 Cannot Re-Upload a New Upload Key File When Creating an 802.1X Certificate

When you re-load an “Upload Key File” with the same name as the existing key file, the “Import” button is disabled. Files with the same name cannot be uploaded again.

Workaround: Upload a file with a different name.

PR# OVE-12732

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# OVE-2131

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# OVE-2264

5.2.3 OmniVista does not Indicate Failure Reason when NaaS Device is in Degraded Mode

OmniVista does not indicate the reason for a failure when a configuration or software upgrade through Managed Devices fails because the NaaS license has expired on the device.

Workaround: No workaround at this time.

PR# OVE-11354

5.3 Known Locator Problems

5.3.1 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

5.4 Known mDNS Problems

5.4.1 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

5.4.2 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 is sequence is not followed, users must share services again after the Responder and Edge Devices are configured for mDNS Services.

PR# OVE-9848

5.4.3 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

5.4.4 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, **u**se either the Eth0 port only or link aggregation (Eth0 and Eth1) on AP1351/AP1301 to connect to the switch.

PR# OVE-11033

5.5 Known PolicyView Problems

5.5.1 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

5.5.2 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

5.6 Known Resource Manager Problems

5.6.1 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

5.6.2 Cannot upgrade U-Boot with File Name "u-boot.5.2R03.3.tar.gz"

If the U-Boot file name is “u-boot.5.2R03.3.tar.gz”, the upgrade will fail.

Workaround: Rename the U-Boot file to “u-boot.5.2.R03.3.tar.gz”.

PR# OVE-13346

5.6.3 OmniSwitch 9912 and 9907 U-Boot Upgrade Fails

Upgrading the OmniSwitch 9912 and OmniSwitch 9907 U-Boot from OmniVista does not work.

Workaround: Informational. When performing a U-Boot upgrade on OS9907 and OS9912 switches, there are two U-Boot files involved: one regular and one Denverton. If the switch contains different types of NI modules, you need to perform the U-Boot upgrade twice with each of the applicable U-Boot files:

- The CMM2 and CNI-U20 modules have Denverton CPUs, so the Denverton coreboot Zip file is used (coreboot-uboot.denverton).
- The CMM1 and all the rest of the NI models have Rangeley CPUs, so the non-Denverton coreboot Zip file is used (coreboot-uboot).

The upgrade is successful on the NI modules for which the U-Boot Zip file is applicable.

PR# OVE-13040, OVE-13032

5.7 Known Topology Problems

5.7.1 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

5.7.2 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

5.7.3 The OmniVista Topology Map does not Display the LLDP Link Between an AOS 8.8R1 OmniSwitch and an AWOS 4.0.4 AP

If an AP is connected to an OmniSwitch running AOS 8.8R1, the LLDP link between the OmniSwitch and the AP does not always display on the OmniVista Topology Map. In addition, if an alias was configured for the OmniSwitch port to which the AP is connected, the port alias is not advertised to the AP; therefore, not reported by OmniVista. This problem does not occur if the OmniSwitch is running the previous AOS release; only when running 8.8R1.

Workaround: No workaround at this time. Problem will be fixed in the AOS 8.8R2 release.

PR# CRAOS8X-31942

5.8 Known Unified Access Problems

5.8.1 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

5.8.2 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

5.8.3 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

5.8.4 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

5.8.5 Switch Client Passes MAC Authentication Then Fails, but the Client is Assigned to the ARP from the Successful Authentication

If a client connected to a switch successfully authenticates but later fails authentication, the switch retains the Access Role Profile (ARP) from the successful authentication and continues to assign that ARP to the client. Note that switch clients that have never successfully authenticated receive the correct ARP after failed MAC authentication.

This issue is resolved in AWOS 5.0.1 and later, so clients connected to APs running AWOS 5.0.1 or above are not affected.

Workaround: No workaround for switches. For APs, upgrade AWOS to 5.0.1.

PR# OVE-13317

5.8.6 Unified Policy Switch Picker Does Not Display All VC Devices

If you remove a switch from a Virtual Chassis (VC) configuration to operate as a standalone unit, the switch still maintains the same VC ID. The Unified Policy Switch Picker then sees more than one switch with the same ID and will not display all the switches with duplicate IDs for selection.

- When a VC is created, the vcpolicy.cfg file is duplicated across all the members of the VC. This file contains the LDAP ID, which is used to identify the VC switches as a single system. When you add a switch to the VC, the vcpolicy.cfg ID on the new switch is overwritten to match the vcpolicy.cfg ID of the VC.
- If you remove a switch from the VC, it still has the same vcpolicy.cfg file containing the VC LDAP ID. As a result, the switch continues to operate in VC mode.
- QoS has no way of knowing if removing a switch from the VC was user-intended or if it was just a temporary issue with the VC. The ID is not regenerated because if it was a temporary VC split, there's no way to know which ID is the original VC LDAP ID.
- Removing a switch from a VC configuration results in switches with the same VC LDAP ID that do not belong to the same VC configuration. This causes confusion when determining which switches to include in the Unified Policy Switch Picker, thus not all the switches are displayed.

Workaround: Delete the "/flash/network/vcpolicy.cfg" file from the standalone switch and reboot the switch to generate a new switch ID.

PR# OVC-9896

5.9 Known UPAM Problems

5.9.1 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

5.9.2 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

5.9.3 Cannot Fully Customize UPAM Captive Portal Page

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

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

PR# OVE-834

5.9.4 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

5.9.5 802.1X 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

5.9.6 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

5.9.7 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

5.9.8 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: Change the validity period to 24 hours.

PR# OVE-11164

5.9.9 The UI Does Not Offer a TLS Port Field When TLS is Enabled for RADIUS Server

When creating a TLS-enabled Radius server, the Create RADIUS Server screen (Security – Authentication Servers – Radius) does not offer a field to specify the TLS Port value.

Workaround: Specify the TLS Port value in the “Authentication Port” field, which is 2083 by default.

PR# OVE-12747

5.10 Known Users and User Groups Problems

5.10.1 When You Configure the Analytics Application for a Role, the Performance Monitoring Application is Also Configured

In OV 4.3R1, Performance Monitoring is a new feature, and you can configure permissions of Analytics and Performance Monitoring application separately. However, if you upgrade to OV 4.3R1 from OV 422 MR2, the default permissions for the Performance Monitoring application are automatically derived from Analytics application permissions because the Performance Monitoring application is a sub-application of the Analytics application. This is expected behavior.
Workaround: NA
PR# OVE-1847

5.11 Known VM Manager Problems

5.11.1 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

5.11.2 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

5.11.3 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

5.12 Known Web Content Filtering Problems

5.12.1 If an AP Client is using a Mobile Application, WCF does not Work.

When client access uses a mobile application (e.g., Facebook, Twitter, YouTube, etc.), there are no restrictions; the application is not blocked and will load properly, as if WCF is disabled on the AP.

Workaround: No workaround at this time.

PR# OVE-10205

5.12.2 WCF Limitation when a Client Accesses the Internet through an HTTP/HTTPS Proxy

When a client is behind a proxy, the client doesn’t request the AP to resolve the DNS query but directly requests the proxy server. As a result, the AP does not get the opportunity to perform the WCF function, so the accept/reject of a website does not work as configured/expected by the user on OmniVista.

Workaround: No workaround at this time.

PR# OVE-11466

5.12.3 Web Content Filtering (WCF) on HA Node After Upgrade

After you upgrade an HA installation from 4.8R1 to 4.8R2, as described below, WCF is no longer enabled and the WCF licensing information is incorrect on the 4.8R2 Active node.

1. Two 4.8R1 HA nodes (Active OV1 and Standby OV2) with WCF enabled in AP Registration.
2. Upgrade nodes to 4.8R2 (upgrade OV2 first, then upgrade OV1).
3. The upgrade process is completed and OV1 is now the Standby node and OV2 is now the Active node.
4. Perform a failover operation, which changes OV1 back to the Active node and OV2 back to the Standby node.

5. After the failover, WCF is no longer enabled and the WCF licensing information is incorrect on the Active node (OV1).

Workaround: Manually restart the WMA service.

PR# OVE-13159

5.13 Known WLAN Problems

5.13.1 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.

5.13.2 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

5.13.3 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

5.13.4 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

5.13.5 Wireless Client Device Summary Does Not Display Complete Information

The wireless client device summary in OmniVista is not displaying the complete information when querying the data.

Workaround: Set the timezone of the browser to the same as that of the server.

PR# OVC-9976

5.14 Known Other Problems

5.14.1 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

5.14.2 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

5.14.3 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

5.14.4 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

5.14.5 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

5.14.6 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

5.14.7 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

5.14.8 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

5.14.9 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

5.14.10 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. 14.11 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. 14.12 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. 14.13 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. 14.14 Ignore Message on VA Console Login Screen

The message “Activate the web console with: systemctl enable –now cockpit.socket” appears on the login screen.

Workaround: Ignore this message; it is normal.

PR# OVE-12730

5. 14.15 VMWare Upgrade with Flexible NIC Fails

When using VMWare hypervisor to upgrade from a previous release to 4.8R1, the upgrade will fail if a Flexible NIC was used.

Workaround: Re-configure the IP with a different NIC type.

PR# OVE-12783

5.14.16 OmniVista on KVM Does Not Detect a New Hard Disk

OmniVista on KVM does not detect the first two disks but does detect the third disk onward. For example:

- OmniVista 4.8R2 on KVM is deployed with "VirtIO disk1" and "VirtIO disk2" as the default.
- Three more SATA disks: “SATA disk1", "SATA disk2" and "SATA disk3" are added.
- When navigating the VA menu to extend the disk space, OmniVista only detects “SATA disk3”.

Workaround: To extend the disk space for OmniVista on KVM:

1. Add "SATA disk1" with 1KB capacity because OmniVista will not detect it.
2. Add “SATA disk2” with 1KB capacity because OV will not detect it.
3. Add "SATA disk3" with the desired capacity (20GB, 50GB...).
4. Go to the VA menu and use the "SATA disk3" to extend the disk space.
5. Do not remove "SATA disk1" and "SATA disk2".

PR# OVE-13167

5. 14.17 Top N Application/Top N Clients Do Not Collect Data after Standby Node Takeover in an L3 HA Configuration

In an L3 High Availability configuration, when the standby node takes over from the primary node, the Top N Application and Top N Clients stop collecting data.

Workaround: No workaround at this time.

PR# OVE-13474

5. 14.18 The AOS 8.9R4 U-Boot Accepts Signed Images Only for OS6750M

If the U-Boot and AOS version is 8.9R4 or above and you downgrade the AOS version to 8.9R3 and reboot the switch, the switch cannot reboot. The 8.9R4 U-Boot only accepts signed images.

- OS6570M has a signed image; there is no unsigned image. All other switches have unsigned images.
- If the OS6570M running with the 8.9R4 U-Boot version is upgraded to AOS 8.9R4 or 8.10R1 (these versions offer signed images only for the OS6570M), then you cannot downgrade the switch to AOS 8.9R3 or below.
- If the OS6570M runs with an older U-Boot (that does not enforce signature validation), then you can upgrade the AOS version to 8.9R4 or 8.10R1 and downgrade to 8.9R3 or below without any limitations.

Workaround: Informational.

PR# OVE-13356

15.14.19 The OAW-AP1511 and OAW-1521 Do Not Support Application Visibility

The Application Visibility (DPI) feature is not supported on the AP1511 and AP1521 in this release.

Workaround: Informational.

15.14.20 HA Node Reboots After Failover Caused by Disconnecting Network Cables

When the network cables for the active node (OV1) are disconnected, the standby node (OV2) becomes the active node. When the OV1 node is then reconnected to the network, OV1 (now the standby node) automatically reboots. However, both nodes continue to function normally despite the reboot of OV1.

Workaround: This is a known issue that will be fixed in a future release.

PR # OVE-13650

15.14.21 High-Availability (HA) Warning Message During VA Upgrade

When upgrading from OmniVista HA 4.9R1 to HA 4.9R2, you may encounter the following warning message:

Please make sure data is fully synchronized between 2 nodes before continue. You can check it in “Show cluster status” menu.

Workaround: Wait enough time to allow all services to come up after upgrading the Standby Node to upgrade the Active Node. This issue is fixed in the next release.

PR# OVE-13842

15.14.22 Enforce Strong Password Enabled After Upgrade

If you disable the Enforce Strong Password setting in OmniVista 4.9R1, then upgrade to release 4.9R2, the following occurs when you access the Enforce Strong Password screen (Home > Administration > Preferences > System Settings > Enforce Strong Password):

- The Enforce Strong Password setting is automatically enabled.
- OmniVista logs you out and requires you to change your password.

Workaround: Change the password and log in again with the new password.

PR# OVE-13859

15.14.23 Cannot Apply Signature Profile for AOS 8.10R3 on OS6860/6860E (CRAOS8X-53944)

When applying an Application Visibility (DPI) signature profile to an OmniSwitch 6860/6860E running AOS 8.10R3, an error occurs. However, signature profiles applied to an OmniSwitch 6860/6860E running an earlier AOS release, continue to function after an upgrade to AOS 8.10R3.

Workaround: There is no workaround at this time.

6.0 Release Notes PRs Fixed

6.1 PRs Fixed Since 4.9R1 GA

6.1.1 Customer PRs

CR/PR Number	Description
Case: **00805332** *CRNOV-7112*	**Summary:** CVE-2025-24813 Apache Tomcat vulnerability is affecting OV NMS 2500 platform. **Explanation**: Tomcat version has been upgraded to 9.0.102 🔒 🔒 Click for Additional Information
Case: **00799993** *ALEISSUE-2101*	**Summary:** Special character "|" in captive portal credential **Explanation**: When the special character **"|"** is entered in the captive portal credentials, the error **"Non-ASCII code characters are not allowed"** is displayed. 🔒 🔒 Click for Additional Information
Case: **00785873** **00802950** *CRNOV-6813*	**Summary:** Unable to configure the email as Username in SMTP server config **Explanation**: A fix has been applied so that the username can be entered in the standard format while configuring the email in OV2500 NMS 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **00803065** *OVE-13722, CRNOV-7095*	**Summary:** The Link status is displayed as down in OV, and No traps were received during the link up. **Explanation**: OV did not compare the status of the link between the two devices. As a result, when a link_down occurs, it cannot update the status to UP 🔒 🔒 Click for Additional Information
Case: **730176, 797482** *CRNOV-5821*	**Summary:** OV2500 System Health - Memory utilization incorrect **Explanation**: OV2500 System Health Memory usage should be total memory usage from physical and swap memory, but is incorrectly including the buff/cache memory usage when that should be considered a part of available memory 🔒 🔒 Click for Additional Information
Case: **000078938** *CRNOV-6923*	**Summary:** Switch links in topology are showing inconsistent state. **Explanation**: Topology links appears to be down and marked in red, even though the connections are operational. 🔒 🔒 Click for Additional Information
Case: **00794656** *OVE-13686*	**Summary:** Introducing Transition mode in OVE for Guest SSID **Explanation**: Legacy devices which do not support enhanced open encryption will not see/unable to connect to the Guest SSID after enabling 6 Ghz band. 🔒 🔒 Click for Additional Information
Case: **00797471** *ALEISSUE-2091*	**Summary:** Unable to create a heat map when cloning a floor plan. **Explanation**: Null pointer found during reload. 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **797482** *ALEISSUE-2080*	**Summary:** Client auth issue with "Enable Device Specific PSK" **Explanation**: Device details imported via the file with the "Enable Device Specific PSK" option, devices are not authenticating with the SSID. 🔒 🔒 Click for Additional Information
Case: **00790388** *OVE-13693*	**Summary:** AOS 8.X switches (thin client mode) not rebooting after scheduled upgrade **Explanation**: AOS 8.X switches (thin client mode) not rebooting after scheduled upgrade from OV2500 if it is running in certified directory. 🔒 🔒 Click for Additional Information
Case: **00782476** *CRNOV-6772*	**Summary:** OV2500 chart statistics view does not show any data. **Explanation**: Reduce smnpbulkwalk max_repetitions from 50 to 20. No more telegraf timeouts seen 🔒 🔒 Click for Additional Information
Case: **00754514** *CRNOV-6287 OVE-10363*	**Summary:** Negative spike appears in the OV2500 graph **Explanation**: Negative spike appears in the OV2500 graph when the counters of an interface are reset from AOS 8.X switch CLI command. 🔒 🔒 Click for Additional Information
Case: **00777627** *CRNOV-6688*	**Summary:** SPB SPT highlighted path is not working **Explanation**: Selecting 2x SPB nodes, clicking on SPB network, picking a BVLAN, no SPB SPT gets highlighted as it should. 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **00731360** *CRNOV-5847*	**Summary:** Background images are not displaying in the topology maps **Explanation**: Patch to synchronize the background image. 🔒 🔒 Click for Additional Information
CR/PR Number	**Description**
Case: **739764** *OVE-13689* *CRNOV-5973*	**Summary:** 30 days analytics graph takes longer time to generate **Explanation**: Optimization has been done to refresh interval for all duration 🔒 🔒 Click for Additional Information
Case: **00788490** *CRNOV-6946*	**Summary:** Certificate for 802.1X doesn't work after HA failover **Explanation**: EAP TLS authentication with own custom certificate is not working when HA failover happens. 🔒 🔒 Click for Additional Information
Case: **00781567** *ALEISSUE-2002*	**Summary:** Android device not able to login using auto pop login **Explanation**: After Captive portal customization Android device not able to login using auto pop login. Issue noticed only with Android devices with the automatic pop-up windows. If we use web browser no problem noticed 🔒 🔒 Click for Additional Information

6.1.2 Release Notes PRs Fixed

- AP-Clients-disconnected-when-upgrading-the-system-from-48R2-to-49R1 (OVE-13448)
- Provisioning Fails for 8.10R1 Default Factory Switch (OVC-9884)

6.2 PRs Fixed Since 4.8R2 GA

6.2.1 Customer PRs

CR/PR Number	Description
Case: **00766266, 00745743, 00760164, 00768930, 00760350, 00757827, 00751419** *OVE-13333, CRAOS8X-45065*	**Summary:** Unable to create Access Role Profile in OV2500 with the following error after upgrade to 8.9R04. “Device error - some attribute values are not valid” AOS 8X switch had error in SNMP debug: swlogd SNMP aluSubagent_main DBG3: getTblNObjNums | mip_from_oid failed mip-table-id 0 mip-object-id 0 ERROR: -1 **Explanation**: AOS 8.9.R04 no longer supports the 4 attributes MaxIngressBandwidth, MaxEgressBandwidth, MaxIngressDepth, and MaxEgressDepth for AOS 6360, 6465, 6560, 6570M, 6860N, 6900-V72/C32, 6900-X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2, 9900. Until OVE 4.8R02, these 4 attributes are sent as SNMPSET requests with all default values along with Access-Role-Profile name to these unsupported switch modes as given above and it was rejected from 8.9R04. Fix is given to ignore these 4 attributes when applying the Access Role Profile. 🔒 🔒 Click for Additional Information
Case: **00753064, 00749321, 00754608, 00772406** *OVE-13264, CRNOV-6132, CRNOV-6226, CRNOV-5736*	**Summary:** OVE/OVC CLI scripting and logs page keep loading for long time. **Explanation**: Cli-scripting listens for events/messages from ActiveMQ's multipart_OVTelnetServiceQueue. The message sequences (end-flag) are not sequential, resulting in OV persistently listening to that queue. The "nothing to display" message occurs because the UI request exceeded its timeout period without receiving a response. This issue is fixed in OVE 4.9R01/OVC 4.9.1 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **00761049, 00763006, 00743519, 00764172, 00751534** *CRNOV-6023, OVE-13279*	**Summary:** Unable to acknowledge the traps in OVE. The error message noticed is “ERROR.ALARMS.ACKNOWLEDGGE.FAIL” **Explanation**: When huge number of traps are acknowledged in a single shot, the login session gets removed when reaching the given timeout value, therefore the exception is thrown leading to unable to acknowledge the Traps in "Notification" of OV2500. This issue is fixed in OVE 4.9R01. 🔒 🔒 Click for Additional Information
Case: **00728062** *CRNOV-5810*	**Summary:** OV2500 is sending AP IP as NAS IP address instead of the UPAM IP when UPAM proxy is enabled. **Explanation**: The NAS IP field in RADIUS CoA was having Stellar AP IP which was sent by OVE. External RADIUS server is sending RADIUS CoA request to Stellar AP instead of UPAM IP though UPAM proxy is enabled. This caused Stellar AP to ignore the RADIUS This issue is fixed in OVE 4.9R01. Fix is done to have NAS IP as UPAM IP for RADIUS CoA packets sent to external RADIUS server. 🔒 🔒 Click for Additional Information
Case: **00738138** *OVE-13288*	**Summary:** When writing the API script for the OV-managed switches, the API application frequently encounters a '401 Unauthorized' error, despite using the correct API key generated from the OV2500. **Explanation**: A new condition has been implemented to prevent the deletion of the access token, and this issue has been fixed in OV2500 version 4.9 R1. 🔒 🔒 Click for Additional Information
Case: **00755787** *CRNOV-6240, OVE-13375*	**Summary:** SNMP Trap ID 264- 277 is not available in OV2500. **Explanation**: OVE 4.9R01 has the fix to include the SNMP trap IDs 264 to 277 in trap definition and trap notification. 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **00764591** *CRNOV-6439, CRNOV-6274*	**Summary:** Inventory list of devices' modules in OVE does not show the friendly name/IP correctly if the IP is changes after the first discovery. **Explanation**: Workaround is to delete the device and rea-add the device, friendly name will show the correct IP address. Fix is given from OVE 4.9R01. 🔒 🔒 Click for Additional Information
Case: **00768910, 00740357, 00733669, 00741023, 00758393** *CRNOV-5876, CRNOV-5977, OVE-13271*	**Summary:** UNP IoT inventory device list is not displayed in OV2500 and the IoT menu displayed "Failed to load data from the server" error. **Explanation**: When there is device with empty MAC-address such as from 3rd party device, the IoT inventory data is displayed as blank. This issue is fixed from OVE 4.9R01. 🔒 🔒 Click for Additional Information
Case: **00723407** *CRNOV-5722, OVC-9614*	**Summary:** OV2500 receives an error message "Failed to load data from the server" while trying to access the topology tab. **Explanation**: It was determined that a child map shared the same OID as the parent map, resulting in a loop request from the UI. The workaround is deleting the child map resolved the issue, allowing the OV to load the topology maps normally. This issue is fixed from OVE 4.9R01. 🔒 🔒 Click for Additional Information
Case: **00750441, 00731996** *OVE-13376*	**Summary:** The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode but have the potential to leak information if used improperly. **Explanation**: The CBC ciphers are removed from the OV2500 from 4.9R01. . 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **00754147** *OVE-13500*	**Summary:** "Thin Client" Status as "Enabled" takes about 30 minutes to be reflected in "show cloud-agent status" in the Supplicant switch. **Explanation**: Provisioning rule configured to register the Supplicant device with MAC-address was not working after first call home. Workaround is to use Serial number in the provisioning rule of OVE instead of MAC-address of the supplicant. The fix is provided in 4.9R01. . 🔒 🔒 Click for Additional Information
Case: **00757212** *CRNOV-6275*	**Summary:** DRM interval is changed from 6 hours (Default) to 21600 hours if copied from existing RF profile to new RF profile. Expected interval in new RF profile is default value (6 hours) from the existing RF profile. **Explanation**: Fix is given to retain the same DRM interval when copying from one RF profile to another RF profile. The fix is provided in 4.9R01. . 🔒 🔒 Click for Additional Information
Case: **00744369** *CRNOV-6083, OVC-9697*	**Summary:** The remote HTTP web server / application (OV2500) is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie. **Explanation**: The HTTP cookies are secured in OVE 4.9R01. 🔒 🔒 Click for Additional Information
Case: **00721179** *CRNOV-5780*	**Summary:** Unable to login to OV2500 with passwords over 16 characters when authenticated with External RADIUS server. **Explanation**: There is an ASA authentication attempted for OV2500 log in with external RADIUS server. Encountered login issues on OVE when the password exceeds 16 characters, and only a shorter password is accepted while using an External Radius Server for authenticating. Fix is provided to allow password more than 16 characters. 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **00737450** *CRNOV-5976*	**Summary:** The VLAN changes made from OVE for one Access Switch affect the configuration for the same VLAN in the other managed switch(es) in OVE. **Explanation**: OVE does not check which devices need to be deleted. Fix is given to add the list of devices to be deleted and only remove devices in the list. 🔒 🔒 Click for Additional Information
Case: **00753077** *CRNOV-6257*	**Summary:** The MAP remains grey in the GEO MAP and only becomes visible when it is zoomed out once. If the globe is moved and returned to Europe, the switch disappears. Additionally, there is a partially incorrect display of uplinks and an incorrect interpretation of link type, showing copper instead of fiber. **Explanation**: Fix is provided in OVE to not set cluster coordinates for the marker when zooming in on the map. 🔒 🔒 Click for Additional Information
Case: **00723405** *CRNOV-5723*	**Summary:** Missing 802.1x-username, client IPv4 address in the Wireless client session tab in OVE for Stellar connected clients under non-roaming conditions. **Explanation:** Inconsistency in pulling wireless client session report is fixed in OVE 4.9R01. 🔒 🔒 Click for Additional Information
Case: **00746624** *CRNOV-6095*	**Summary:** Customizing the country flag in the captive portal page is not working in OmniVista 2500/OVE. **Explanation:** Fix is given to reflect the correct country flag in the captive portal customization configuration in OVE for the Stellar AP clients. 🔒 🔒 Click for Additional Information

CR/PR Number	Description
Case: **00769539, 00752335, 00754511, 00772196, 00753480** *CRNOV-6190, ALEISSUE: 1867*	**Summary:** Stellar Wireless clients receiving "upam.receiveTimeout"' when authenticating through the captive portal SSID managed in OVE/OVC. **Explanation:** When UPAM sends a COA-Request, it saves a record of the COA-Request. This record is used to retrieve the corresponding COA-Request when a COA-ACK or COA-NAK is received, allowing for subsequent operations. COA proxy feature in OVE 4.8R02 causes saved COA-Request record to potentially be deleted after sending the COA-Request. As a result, when a COA-ACK or COA-NAK is received, the corresponding COA-Request record cannot be found. The system will then consider the COA-ACK or COA-NAK as invalid data and will discard it without processing. Fix is given to not delete the saved CoA-Request record even when CoA proxy feature is used. 🔒 🔒 Click for Additional Information
Case Number: 00738959 PEROV-359, OVE-13295, CRNOV-5942	**Summary:** Unable to use Redhat IDM as authentication server for OV2500 users. Testing authentication fails with error in logs: "LDAP authentication failed." **Explanation**: Redhat IDM is not supported in 4.8R2 and earlier. Support is added in 4.9R1 Click for Additional Information
Case number: 00744956 *CRNOV-6086/ALEISSUE-1844*	**Summary:** No data in downloaded XLSX file of company property in UPAM. **Explanation:** The time type was not handled properly during export when the device specific PSK is enabled for the client while adding in the company property database. Click for Additional Information
Case number: 00739766 *CRNOV-6040/OVE13323*	**Summary:** Time from graphs and CSV export are not in the same time zone. **Explanation:** The time zone is not updated properly. The time zone set in UI is Madrid and the time zone in MongoDB is Africa/Windhoek. Click for Additional Information

CR/PR Number	Description
Case number: 00755619 *CRNOV-6310/OVE-13422*	**Summary:** Modifying the SNMP setting removes the GEO info in the managed devices. **Explanation:** OV updates geolocation to null when editing multiple devices. Click for Additional Information
Case Number: 00757467/ALEISSUE-1893	**Summary:** After updating to OV4.8R2, the following log has been generated in EXTERNAL RADIUS. "Thu Jun 6 19:06:40 2024 : Error: Received conflicting packet from client ov port 1814 - ID: 60 due to unfinished request in module sql. Giving up on old request." **Explanation**: When captured the packets, found that there was a conflict in the RADIUS packets. This issue is also occurring in both EXTERNAL RADIUS for MAC authentication and EXTERNAL RADIUS for web authentication. Click for Additional Information
Case Number: 00756661 CRNOV-6264	**Summary:** Unable to ACK/Clear notifications **Explanation**: ACK/Clearing a large number of notifications causes the OV session to timeout. Future attempts will result in errors. Fix: the session will not timeout. Click for Additional Information
Case Number: 00767075 CRNOV-6493	**Summary:** Support for upgrading switches in "aaa switch-access mode enhanced" **Explanation**: "Upgrade Image" feature will now check for files containing "sum" in the filename and upload them without needing them mentioned in the software.lsm file. Click for Additional Information

CR/PR Number	Description
Case Number: 00764008 CRNOV-6418	**Summary:** OV2500 report feature not sending automated email **Explanation**: The email report is not received because OV defaults to using SSL with Port 465. However, the configuration has SMTP Authentication disabled, requiring OV to use Port 25 instead. As a result, OV cannot connect to the mail server and send the report email. **Solution:** Implement a logic check for SMTP Authentication and set the appropriate port accordingly. Fix done in 4.9 R1 Click for Additional Information
Case Number: 00767851 CRNOV-6499	**Summary:** External Captive portal not working with newly added Stellar AP's. **Explanation**: External captive portal is displayed, once we click on "connect" , the captive portal is displayed again. This is happening only with newly added Stellar APs. Click for Additional Information
Case Number: 00745269 CRNOV-6141 / ALEISSUE-1861	**Summary:** EAP-TLS authentication fails if CN contains space. **Explanation:** If the certificate contains a space, UPAM radius reject the authentication, same authentication EAP-TLS works fine will all users that CN does not contain space. Click for Additional Information
Case Number: 00730352 CRNOV-5827	**Summary:** The discovery process stops working after some time. **Explanation:** The discovery process stops working after some time, rebooting OV2500 will fix the issue but after 1 or 2 days issue is back. Click for Additional Information

CR/PR Number	Description
Case Number: 00724486 CRNOV-5931	**Summary:** OV2500 failure of scheduled upgrades of multiple switches **Explanation:** Scheduled update task with only one switch in the task everything works fine. If you add more switch in the task some switches fail upgrade. Click for Additional Information
Case Number: 00745101 CRNOV-6079	**Summary:** Backup/restore compare page is kept loading. **Description:** The old snap that caused the issue was removed from the OV2500 as a workaround. The fix is included in the release 4.9.R01. Click for Additional Information
Case Number: 00764430 CRNOV-6483	**Summary:** Links between the OS6860E switches are disappearing randomly in OV2500 **Description:** The links were created after reviewing the "lldpStatsRemTablesLastChangeTime" collection in MongoDB; nevertheless, OV does not display the link. The fix is merged in 4.9.R01 release. Click for Additional Information

6.2.2 Release Notes PRs Fixed

- Statistics Collection May Stop if SNMP Credentials are Changed (OVE-13114)
- The Days Left for Expiry is Incorrect for an AP NaaS License (OVC-9151)
- Device Does Not Display When Editing a Scheduler Job (OVC-9798)

6.3 PRs Fixed Since 4.8R1 GA

6.3.1 Customer PRs

CR/PR Number	Description
Case Number: **661780** OVE-11876/CRNOV-4526	**Summary:** Unable to view the history of traps for more than an hour. **Description:** Cannot export more than 1000 lines of "Notification" to .csv file. Click for Additional Information
Case Number: **00693551** OVE-12811/CRNOV-5162	**Summary:** OV backup failure. **Description:** Generating an immediate backup was not possible when we have a scheduled backup enabled. Click for Additional Information
Case Number: **694690** OVE-12791/CRNOV-5206	**Summary:** License consumed wrongly in OV2500 **Description:** License of the UniFi switch is seen as an Alcatel device and not as a 3rd party device in OV2500. Click for Additional Information
Case Number: **697416** OVE-12770/CRNOV-5219	**Summary:** OV2500 displays different free space. **Description:** After extending the Hard disk space. OV not displaying the right amount of free space. Click for Additional Information
Case Number: **698846** OVE-12810/CRNOV-5253	**Summary:** Not able to set aaa server timeout value to 0 from OV2500 **Description:** Changes have been made to support this value. Click for Additional Information

CR/PR Number	Description
Case Number: **699809** OVE-12914/CRNOV-5264	**Summary:** UNP polices are showing not saved. **Description:** Unified Policies are always showing "Unsaved" no matter what user do on OV web. Click for Additional Information
Case Number: **704440/00703228/726522** OVE-12813/CRNOV-5322/CRNOV-5341	**Summary:** NTP service does not restart after reboot. **Description:** User set ntp server and enable ntp. ntpd service won't start automatically after reboot. Click for Additional Information
Case Number: **705945** OVE-12944/CRNOV-5364	**Summary:** Problem with Locator Feature. **Description:** The Client IP Address does not show when using the Browse function.
Case Number: **00705969/725422** CRNOV-5404/ALEISSUE-1675 CRNOV-5767/ALEISSUE-1675	**Summary:** Unable to load Captive portal certificate on OV2500. **Description:** Certificate import fails. Click for Additional Information
Case Number: **706043/00708301/00715507** ALEISSUE-1688/CRNOV-5442	**Summary:** Unknown Exception found in UPAM after OVE 4.8 R01 upgrade. **Description:** Auth request from any NAS client which does not contain the service type attribute on it face problem. Click for Additional Information

CR/PR Number	Description
Case Number: **706143** CRNOV-5376/ALEISSUE-1668	**Summary:** Captive portal authentication not happening randomly. **Description:** Users get following Error "The authentication failed. The related associate certification record couldn't be found" users got "The authentication failed. The related associate certification record couldn't be found." Click for Additional Information
Case Number: **706710** OVE-12848/CRNOV-5378	**Summary:** High memory traps received. **Description:** False High memory traps on OV 2500. Click for Additional Information
Case Number: **708572** CRNOV-5451/OVE-12878	**Summary:** Information in scheduled tasks table not displayed. **Description:** Information on the updated devices of the scheduled upgrades is not displayed. Click for Additional Information
Case Number: **708866** ALEISSUE-1698/CRNOV-5500	**Summary:** Self-registration request optimization. **Description:** Improvements has been made to check the post request contain right company domain in the approval request. Click for Additional Information
Case Number: **712671** **OVE-12923/CRNOV-5515**	**Summary:** Omni Vista 2500 Failover is not performed properly. **Description:** HA failover optimization has been done. Click for Additional Information

CR/PR Number	Description
Case Number: **00728847 /715974** CRNOV-5567 CRNOV-5813 OVE-13137/OVE-12975	**Summary:** LLDP links displays wrong bandwidth and link type. **Description:** LLDP Connections in the Topology section are not updated automatically. Click for Additional Information
Case Number: **00719011** CRNOV-5615/OVE-13128	**Summary:** OV2500 ISSU for the OS6865 switches. **Description:** Fix is enhanced in OVE 4.8R2. Click for Additional Information
Case Number: **00720367** CRNOV-5642/OVE-13020	**Summary:** OV Enterprise & OV Cirrus vulnerability to CVE-2023-4911 **Description:** Fix is present in this Release. Click for Additional Information
Case Number: **721511** **OVE-13109/CRNOV-5752**	**Summary:** Statistics Chart shows no data in Byte level for OS6860N/OS9912. **Description:** Fixed in this Release. Click for Additional Information
Case Number: **723273** **OVE-13104/CRNOV-5697**	**Summary:** Topology map do not show link details in OV 2500 **Description:** Fixed in this Release. Click for Additional Information

CR/PR Number	Description
Case Number: **723358** OVE-12439/CRNOV-5719	**Summary:** Unable to acknowledge traps. **Description:** Fixed in this Release. Click for Additional Information
Case Number: **725729/00721952** CRNOV-5500/ALEISSUE-1698	**Summary:** Last character in Email Suffix from Guest Access Strategy is missing. **Description:** Fixed in this Release. Click for Additional Information
Case Number: **725911** CRNOV-5774	**Summary:** AOS switches showing auth server down after upgrade to OV 4.8 R01 **Description:** Fixed in this Release. Click for Additional Information

6.3.2 Release Notes PRs Fixed

- Using SSH to connect to a device that has credentials already stored in MongoDB allows the user to see the credentials in plaintext. (OVC-9666)
- Roaming and RSSI history of the client device displayed for only 24 hours. (OVC-9754)
- SNMPv3 Username/Password Must Not Contain Certain Special Characters (OVE-12152)
- The 6GHz SSID Interface Will Not Function if PMF State Is Not Set to “Required” (OVE-12727)
- After Editing an SSID With PPSK Entries, Access Guardian Service Does Not Respond to Any Requests Until Restarted Manually (OVE-12818)
- Network Analytics Statistics Port-Based Statistics Counters are Fixed (OVE-13109).
- Lost static network route after rebooting RAP VPN VA 4.8.2. (OVE-13156)
- Syslog Over TLS Certificate Name Must Not Contain a Space (OVE-12702)
- OmniVista Does Not Detect When a New NIC is Added (OVE-12645)

6.4 PRs Fixed Since 4.7R1 GA (Patch 2, build 30)

6.4.1 Customer PRs

CR/PR Number	Description
Case Number: 00659698,00691695 OVE-12294 CRNOV-4554	**Summary:** OV2500 is experiencing a delay on the initializing stage **Description:** After upgrade to 4.7.R1, user in China experiencing delay on the OV2500 initializing stage. After the initializing stage, no delay was observed, and all modules were working normally. Click for Additional Information
Case Number: 00657427 OVE-12401 CRNOV-4498	**Summary:** LLDP links between Linkagg ports of AOS 8.X switches are incorrectly displayed in OV2500 Topology map **Description:** It was found that the OV parsed the wrong link port between Switch. Click for Additional Information
Case Number: 00668942,00685665,687100 ALEISSUE-1496 ALEISSUE-1592 CRNOV-5051 CRNOV-4640	**Summary:** Access policy config mapped to a specific SSID was lost randomly **Description:** Duplicate Entry was found in the Guest Access Strategy table. Fixed by manually removing the duplicate Entry. Optimization will be done in OVE 4.8 R01 to avoid the duplicate entry getting created. Click for Additional Information
Case Number: 00686006 OVE-12523	**Summary:** To update the installation guide of OV2500 regarding the information about "HDD3" **Description:** User guide will be updated accordingly. Click for Additional Information
Case Number: 00680328 OVE-12487 CRNOV-4873	**Summary:** Stellar AP in OVE mode connected to OS6465 VC.

CR/PR Number	Description
	Description: In the topology link of the OVE/OVC, the link of chassis device OS6465 is the wrong slot/port. Cause in the code OV lack of conditions to OV parse slot/port correctly. Click for Additional Information
Case Number: **00676367** CRNOV-4797 OVE-12410	**Summary:** OV2500-Traffic does not pass-through proxy configured **Description:** From OV2500 4.8R01 onwards, the traffic meant to Brightcloud.com will be sent via the proxy server if configured. Click for Additional Information
Case Number: **00677215, 00669567, 00668290** CRNOV-4793 OVE-12454	**Summary:** Unable to configure additional NIC in OV Enterprise. **Description:** Server where there are 2 Ethernet NIC cards installed. The additional NIC cannot be configured with an IP address. This is fixed in 4.8 R01 Click for Additional Information
Case Number: **00678997** CRNOV-4850 OVE-12482	**Summary:** Details are missing in inventory while API request send for a single device. **Description:** When API request is sent for all devices a detailed data is received as expected from OV API when polling all devices from OV. However, when polling from a specific device by filter few data are missing. Click for Additional Information
Case Number: **00672824** OVE-12378 CRNOV-4703	**Summary:** OmniVista ClearPass integration fails. **Description:** OmniVista ClearPass integration fails to automate the NAS Device creation on CCPM when adding a new AP into the AP Group

CR/PR Number	Description
	Click for Additional Information
Case Number: 00672476 OVE-11143 CRNOV-4695	**Summary:** Trust Tag on Access auth profile is disabled by default from 4.7 R01. **Description:** Till OV 4.6 R02 when we create an Access auth profile in OV. Since 4.7 R01 Trust tag option is enabled by default. Click for Additional Information
Case Number: 00673054 OVE-12377 CRNOV-4704	**Summary:** OmniVista 2500 and Cirrus 4.7 - Issues with DSPSK/Captive Portal and external Radius. **Description:** When creating SSID with internal Captive Portal and MAC Authentication, we cannot select the external radius server. Click for Additional Information
Case Number: 00669351 CRNOV-4641, ALEISSUE-1500	**Summary:** Sorting with AP uptime is not working under Access Point page in OV. **Description:** The sorting is not happening correctly when filtered with AP up time in the AP registration page. Click for Additional Information
Case Number: 00670314 OVE-12420 CRNOV-4693	**Summary:** LLDP link in OV2500 is not correctly reported with OS2360-U48X, stack of 5. **Description:** OS6465 or OS2360 switch is connected to slot 5 of OS2360 stack, OV2500 shows incorrectly the LLDP link details. Click for Additional Information
Case Number: 00671334 OVE-12304 CRNOV-4473	**Summary:** OV services are Running Slow in the VA menu, and the Swap Memory usage is full when RAM is free.

CR/PR Number	Description
	Description: The Swap memory usage is displayed 3 Gig out of total 3 Gig, while still free memory exists. Click for Additional Information
Case Number: 00673692,00661634 OVE-12439 CRNOV-4733 CRNOV-4543	**Summary:** Error during trap configuration in OV2500 **Description:** Error during trap configuration in OV2500 “The requested login session cannot be found -- perhaps it has been closed" Click for Additional Information
Case Number: 00671501 OVE-11796 CRNOV-4552	**Summary:** OV2500-HA Setup: After upgrading to 4.7R1 the services not running in standby node. **Description:** After upgrading the OV2500 HA from 4.6.R2 to 4.7.R01 release, the services are not running in one of the nodes (Standby node). The CPU utilization on the standby node is 9,47GHz, however, the active node is working fine. Click for Additional Information
Case Number: 00642763 OVE-11530	**Summary:** OV Cirrus / OV 2500 - devices running in Opex mode **Description:** OV Cirrus / OV 2500 - devices running in Opex mode have reached the degraded mode and no alerts/status received from OVC Click for Additional Information
Case Number: 00652176 ALEISSUE-1437 CRNOV-4429	**Summary:** Unable to delete an AP from the AP list **Description:** AP had reported the online time of wired clients which had length larger than the DB filed length. Click for Additional Information
Case Number: 00645319 OVC-9303 CRNOV-4218	**Summary:** OS2260 models do not have possibility for downloading the tech support engineering complete. **Description:**

CR/PR Number	Description
	OVC 4.6.2 - In Administration -> Collect Support Info - > Select AOS 5.x switch like OS2260 models - we do not have possibility for downloading the tech support engineering complete Click for Additional Information
Case Number: **653470** OVE-12247 CRNOV-4379	**Summary:** OV2500 - Unable to schedule ISSU upgrade **Description:** There is no option to schedule an ISSU upgrade in OVE 4.6R02. Click for Additional Information
Case Number: **00685015** ALEISSUE-1584 CRNOV-5029	**Summary:** OmniVista Cirrus - in the Guest Access Strategy, the email suffix is not preserved. **Description:** In Guest Access Strategy, email suffix is not preserved. If we are only editing the email suffix, changing it from one value to another, the 'Apply' button is greyed out. Click for Additional Information
Case Number: **651995** ALEISSUE-1429 CRNOV-4413	**Summary:** Unable to download the pre provisioning Template for Access points **Description:** Unable to download the pre provisioning Template for Access points Click for Additional Information
Case Number: **00661837** CRNOV-4841 OVE-12474	**Summary:** The VRF name is not consistent with the assigned AAA Servers **Description:** In OV2500, while creating a new "Access Auth Profile" with VRF name that was already used for another Access Auth Profile with same VRF name is not getting accepted Click for Additional Information
Case Number: **00651129** CRNOV-4354 OVE-11654	**Summary:** OV2500: Scrambled synopsis order in the trap definition.

CR/PR Number	Description
	Description: The Mac information in the trap definition should be received in sequence number 4, however, it is displayed in sequence number 5. The trap's synopsis sequence is scrambled. Click for Additional Information
Case Number: **00651378** CRNOV-4355 CRNOV-4328 ALEISSUE-1412	**Summary:** OV2500: Exporting floorplan resulted in Tomcat service restart **Description:** Issue happens as there is no limit on the number of floorplans that can be exported to PDF Click for Additional Information
Case Number: **00655621** CRNOV-4434 ALEISSUE-1439	**Summary:** Experiencing an issue with the UPAM External Syslog Server in OV2500 **Description:** The UPAM External Log Server feature is sending the logs with the hostname OMNI Click for Additional Information
Case Number: **00660740** ALEISSUE-1453 CRNOV-4504	**Summary:** OVE Receiving Error message while generating a Client Session Report **Description:** An "Error" message is shown when trying to generate a report in the Client session with a filter applied, as well as when no data is found for the selected Date Click for Additional Information
Case Number: **00653277** ALEISSUE-1424	**Summary:** OV 2500 Radius CoA proxy is not working **Description:** The Radius disconnect ACK packet sent by the AP to OV is not forwarded to the Radius server (CPPM) Click for Additional Information
Case Number: **00631884** CRNOV-4048 OVE-12268	**Summary:** Services in OV 2500 is displaying slowly **Description:**

CR/PR Number	Description
	When try to select "Display status of all services", the output is taking hours to complete. Click for Additional Information
Case Number: 00652612 CRNOV-4383 OVE-12233	**Summary:** The OV2500 GUI displays incorrect IP in UPAMRadiusServer. **Description:** The OV2500 GUI displays the incorrect IP in UPAMRadiusServer, but the CLI "display configuration" shows the correct virtual IP. Click for Additional Information
Case Number: 00643209 CRNOV-4232 ALEISSUE-1379	**Summary:** Records having "Full name" with space are not getting imported. **Description:** When trying to import a lot of guest users using OVE guest account template, not able to use empty spaces between first and last names on field "Full Name". Click for Additional Information
Case Number: 00650577 ALEISSUE-1415	**Summary:** Support of Channels 36-52 on stellar APs and OV2500 for country code TW(Taiwan). **Description:** Support of Channels 36-52 on stellar APs and OV2500 for country code TW(Taiwan). Click for Additional Information
Case Number: 661634 OVE-12439 CRNOV-4543	**Summary:** Discovery stop working after some time **Description:** The discovery process stops working after some time, rebooting OV2500 will fixed the issue but after 1 or 2 days issue is back. Click for Additional Information

CR/PR Number	Description
Case Number: 703016 CRNOV-4858 CRNOV-5317	**Summary:** AOS OmniSwitch - "CallHome Request returned failure" due to "SSL certificate problem: certificate has expired" when onboarding switch on OV 2500 **Description:** SSL certificate from OV2500 has expired. New Certificate updated, Click for Additional Information
Case Number: 00684901 ALEISSUE-1590 CRNOV-5042	**Summary:** APs not using configured RF profile settings. **Description:** Channel 149-165 are supported in UK and it should be configurable both on AP and OV. Changes has been made. Click for Additional Information
Case Number: 00674412 **OVC-9367 CRNOV-4772**	**Summary:** Randomly cannot access the OV GUI and noticing high CPU status. **Description:** Number of events in the Topology limited and consistent with the network size of the OV will be used. Click for Additional Information
Case Number: 00677307 ALEISSUE-1530 CRNOV-5143	**Summary:** Wireless client roaming history wrong graphical view shows client often offline **Description:** WMA collects data needs to be optimized Click for Additional Information

CR/PR Number	Description
Case Number: 00640928 ALEISSUE-1399 CRNOV-4304	**Summary:** Client density graph is plotted incorrectly in OV2500/OV-Cirrus. **Description:** Difference in the timezone between the server & AP cause the problem. Click for Additional Information
Case Number: 00648344 OVE-12185 CRNOV-4281	**Summary:** Resource manager Max device Config Error. **Description:** Updated documentation to the right Value. Click for Additional Information
Case Number: 608290 OVE-12261 CRNOV-3750	**Summary:** New trap "healthMon..." push to OV doesn't update by Severity. **Description:** Fixed in this Release. Click for Additional Information
Case Number: 700562 OVE-12291 CRNOV-5273	**Summary:** Device which has no matching Provisioning rule are still onboarded. **Description:** AOS sent data with an empty getVcMacAddress. This is the root cause for device getting the wrong rule in the provisioning process. Click for Additional Information

6.4.2 Release Notes PRs Fixed

- CSA Limitation on 6GHz (OVC-9306)
- User should not set AP to RAP twice in GOV (OVC-9627)

6.5 PRs Fixed Since 4.7R1 GA

6.5.1 Customer PRs (Patch 2, build 30)

CR/PR Number	Description
Case Number: **00651930**	**Summary:** In UPAM authentication, any user can elevate his rights to the admin user. **Description:** When a user tries to login and fills-in the anonymous field with a non-existing user, the user receives the access with the rights of the username. If the user fills-in the username of the admin account under the "Anonymous" field, that user is given the admin user's rights without having the admin's credentials.
Case Number: **00666551**	**Summary:** UPAM LDAP/AD configuration: Unable to configure the LDAP server in the OV2500. **Description**: This issue concerns fresh installation of OV 2500 4.7R01. An incorrect files' rights does not allow to configure the LDAP/AD integration.
Case Number: **00653466**	**Summary:** The value is always displaying 0 for the first hour in WLAN client summary report, **Description:** WLAN client session records are found, however, the data is not found in the WLAN summary graph.
Case Number: **N/A.**	**Summary**: Cannot receive email from Report application: Cannot receive email from Report app when Encryption TLS is set. **Description**: In Email Settings when Encryption is set to TLS, emails generated by TRAP Responder fail.
Case Number: **00660891**	**Summary**: WiFi Clients connected to SSID with Map to Tunnel case lost IP address after upgrading OV to 4.7.1. **Description**: Access Role Profile mapping type move from "VLAN" to "Vlan and Tunnel" causing Client association issue.
Case Number: **00660698**	**Summary**: Dashboard does not load widgets and shows communication failure.

CR/PR Number	Description
	Description: Dashboard shows Communication Failure, widgets fail to load because of scheduler issue.
Case Number: **N/A**	**Summary**: Cannot change Mongo Database Password on VA menu: Cannot change Mongo Database Password on VA menu.
Case Number: **00643473** **00676222** **00643473**	**Summary**: UPAM fails 802.1x authentication with Windows 11 clients due to missing TLS 1.3 support. **Description**: Windows 11 WLAN Clients use by default EAP-TLS 1.3 which is not supported by OV/UPAM radius server
Case Number: **00540257** **00666871**	**Summary**: Cannot install VMware tool 4.7R1. **Description**: VMWare Tools installation fails because of incompatibility of a Linux package.
Case Number: **00680614**	**Summary**: Cannot upgrade 4.7R1 using ALE default repo: Please check the connectivity or your repository configuration. **Description**: SSL CA Certificate is not validated.

6.6 PRs Fixed Since 4.6R2

6.6.1 Customer PRs

CR/PR Number	Description
Case: **00642763** *OVE-11530*	**Summary:** OV 2500/OV Cirrus – The devices running in NaaS mode have reached the degraded mode and no alerts/status is received on OVC Click for Additional Information
Case: **00638353** *OVE-11595*	**Summary:** OV 2500/OV Cirrus – Administrator cannot acknowledge or delete traps, ERROR.ALARMS.DELETE.FAIL is displayed Click for Additional Information
Case: **00625856** *OVE-11949*	**Summary:** OV 2500/OV Cirrus – Locator Live Search with first only Match option does not work. All matches are returned. Click for Additional Information
Case:	**Summary:**

CR/PR Number	Description
00627831 *OVE-11705*	OV 2500/OV Cirrus – Improve the provisioning (Network -> Provisioning) flow with IP static setting. Click for Additional Information
Case: **00627831** *OVE-11705*	**Summary:** OV 2500/OV Cirrus – WLAN PSK Passphrase does not allow special characters such ":" and "." but AP running in Cluster (Express) mode does Click for Additional Information
Case: **00628883, 00623225** *OVE-11275*	**Summary:** OV 2500/OV Cirrus – Date time for trap record is wrong Click for Additional Information
Case: **00629887** *OVE-12061*	**Summary:** OV 2500 in HA mode display alarm about disk HDD2 size Click for Additional Information
Case: **00622796, 00595697** *OVE-11875*	**Summary:** OV 2500 / OV Cirrus – No WLAN Client summary data displayed on charts (Client Density, Download Throughput, Upload Throughput) Click for Additional Information
Case: **00623623** *OVE-11947*	**Summary:** OV 2500 / OV Cirrus – The dynamic LLDP Link is not displayed between OS6560 and Stellar AP in the Topology MAP because the switch returns wrong slot/port. Click for Additional Information
Case: **00623623, 00621750** *OVE-11947*	**Summary:** OV 2500 / OV Cirrus – The dynamic LLDP Link is not displayed between OS6560 and Stellar AP in the Topology MAP because the switch returns wrong slot/port. Click for Additional Information
Case: **00624505, 00602485, 00599397, 00606897** *ALEISSUE-1326*	**Summary:** OV 2500 – WLAN Registration email for Guest Users is not generated when email SMTP server only supports TLS 1.2 Click for Additional Information
Case: **00618694** *OVE-11743*	**Summary:** OV 2500 – Captive Portal default certificate is expired after upgrade to 4.6R02 Click for Additional Information
Case: **00615057** *ALEISSUE-1276*	**Summary:** OV 2500 – BYOD self-service login not working against the AD credentials Click for Additional Information
Case:	**Summary:**

CR/PR Number	Description
00570881 *OVE-11528*	OV 2500 – Running in HA mode the OV Health chart is showing 99% of memory utilization Click for Additional Information
Case: **00604968** *OVE-11598*	**Summary:** OV 2500 – Authentication Policy and Authentication strategy are unexpectedly deleted Click for Additional Information
Case: **00608290** *N/A*	**Summary:** OV 2500 / OV Cirrus – Traps with severity Major are displayed with severity Minor on OV Notifications page
Case: **00500010** *OVE-11585*	**Summary:** OV 2500 / OV Cirrus – Unable to export/Print IoT Inventory of more than 1000 lines Click for Additional Information
Case: **00607413** *OVE-11615*	**Summary:** OV 2500 – OVF file has only 16Go of Memory but the release note recommends that 20Go as minimum Click for Additional Information
Case: **00600620** *OVE-11591*	**Summary:** OV 2500 – UPAM Guest security issue on GUEST Add Account API Click for Additional Information
Case: **00587838, 00595897, 00613501** *OVE-11275*	**Summary:** OV 2500 – SNMP Traps from AOS switch after Virtual Chassis unit takeover as new Master is not received in OV Notifications Click for Additional Information
Case: **00542676** *OVE-11164*	**Summary:** OV 2500 / OV Cirrus – Clients associated to Wifi4EU SSID are not redirected to Captive Portal after 24 hours Click for Additional Information
Case: **00564196** *OVE-11046*	**Summary:** OV 2500 / OV Cirrus – Cannot create a new Topology Map Click for Additional Information
Case: **00597637, 00597346** *OVE-11394*	**Summary:** OV 2500 / OV Cirrus – Vulnerability on the SSH Terminal – weak key exchange algorithms Click for Additional Information
Case: **00614001** *OVE-11641*	**Summary:** OV 2500 / OV Cirrus – OpenSSL Vulnerability CVE-2022-0778

CR/PR Number	Description
	Click for Additional Information
Case: **00594540, 00579140** *OVE-11275*	**Summary:** OV 2500 / OV Cirrus – APStation/Deassociation traps are displayed in wrong timestamp Click for Additional Information
Case: **00612328, 00586568** *OVE-11426*	**Summary:** OV 2500 / OV Cirrus – All the received notifications traps are not displayed on real time Click for Additional Information
Case: **00565988** *OVE-11601*	**Summary:** OV 2500 / OV Cirrus – QOS Policies pushed to switches status is reache-failure Click for Additional Information
Case: **00607371** *ALEISSUE-1240*	**Summary:** OV 2500 / OV Cirrus – BYOD online devices show accounts that no longer exist and cannot be kicked-off Click for Additional Information

6.6.2 Release Note PRs Fixed

- "Export VPN Settings" with Shorthand Mask Option does not Show the List Peer IP Address (OVE-11444).
- Editing an AP Group to Add a New Profile Resets the Timezone to the UTC-8 Default Value (OVE-11531)
- Cannot Work Simultaneously on Two SSH Tabs Opened Inside CLI Scripting (OVC-9022)
- Advertises Incorrect SSID Name in Some Cases (OVE-9545)
- The alaNaasLicenseInstalledAlert Trap Shows the Wrong Value (OVE-11374)
- The NaaS VC Device Sends the alaNaasInconsistentModeAlert Trap Multiple Times (OVE-11414)
- The NaaS License Expiry Time is Reported in the Number of Whole Days Remaining until the License Expires (OVE-11415)
- Can't Display Running Directory Information for NaaS Device in Degraded Mode (OVE-11416)
- Stellar AP Connectivity to OS22x60 does not Work (OVE-11467)

6.7 PRs Fixed Since 4.6R1

6.7.1 Customer PRs

CR/PR Number	Description
Case:	**Summary:**

CR/PR Number	Description
00591018 *OVE-11396*	OV 2500/OV Cirrus - The synopsis of the trap is different from the detailed information of the trap. Click for Additional Information
Case: **00587088** *N/A*	**Summary:** OV 2500/OV Cirrus - Pressing the 'Tab' key to complete the CLI command does not work as expected in OV Terminal Window Click for Additional Information
Case: **00578171** *OVE-11252*	**Summary:** OV 2500/OV Cirrus - The OV Dashboard widget does not link to the right window Click for Additional Information
Case: **00577642** *OVE-11252*	**Summary:** OV 2500 - incorrect SPB topology view displayed Click for Additional Information

CR/PR Number	Description
Case: **00576881** *OVE-11194*	**Summary:** OV2500_The AP devices belong to the same group are automatically selected when viewing the chart at App Bandwidth Usage https://myportal.al-enterprise.com/alebp/s/tkc-redirect?000064970
Case: **00571709** *CRNOV-3314*	**Summary:** OV 2500/OV Cirrus - Radius Shared Secret with special characters (Backslash, column) doesn't work after reboot Click for Additional Information
Case: **00571709** *OVE-11161*	**Summary:** OV 2500/OV Cirrus - Backslash is not allowed on SSID PSK/Passphrase Click for Additional Information
Case: **00567899** *OVE-11161*	**Summary:** OV 2500 / OV Cirrus - SMB1 vulnerabilities on OV Click for Additional Information
Case: **00542342** *OVE-11174*	**Summary:** OV 2500 / OV Cirrus – Locator shows a wrong endStation.name and for some devices only shows one record
Case: **00549404** *CRNOV-3054*	**Summary:** OV 2500 / OV Cirrus – “Select columns to show” option is not available on several pages after upgrading to 4.5 version Click for Additional Information
Case: **00559846** *CRNOV-3187*	**Summary:** OV 2500 / OV Cirrus – Incorrect sorting of data for the wireless client values Click for Additional Information
Case: **00549327** *OVE-10916*	**Summary:** OV 2500 / OV Cirrus – Notification synopsis scrambled in email and in web interface
Case: **00560615** *OVE-10977*	**Summary:** OV 2500 / OV Cirrus – IoT Category manufacturer and endpoint columns are not displayed when exceeding max retry counter
Case: **00561430** *OVE-11344*	**Summary:** OV 2500 / OV Cirrus – SSH Authentication trap is raised when we perform a manual audit from Network -> Provisioning result page Click for Additional Information

6.7.2 Release Note PRs Fixed

- Trap Configuration Fails when the Switch Name Contains a “#” Character (OVE-10558)
- Increase Buffer Size of Interactive SSH Terminal in Web UI (OVE-11170)
- HTTPS Captive Portal Redirection with Proxy Reduces Performance (OVE-11482)

- Backup/Restore on HA System Can't Restore on System Upgrade to OV46R1 Build 44 (OVE-11172)
- Deleting a Responder Device Fails (OVC-8876)
- Social Login Fail with Google Account (OVC-8901)

6.8 PRs Fixed Since 4.5R3

6.8.1 Customer PRs

CR/PR Number	Description
Case: **00559299** *OVE-10635*	**Summary:** OV 2500: Fresh installation in 4.5R03 - Installing VMWARE tools failed Click for Additional Information
Case: **00542487** *ALEISSUE-1009*	**Summary:** OmniAccess Stellar – Wi-Fi 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** *OVE-3051*	**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** *OVE-10933/ OVE-10061*	**Summary**: OV 2500: High resource usage while creating manual links on discovery tool Click for Additional Information
Case: **00558241** *OVE-10333*	**Summary**: OV 2500: Locator fails to load the Netforward table of few switches Click for Additional Information
Case: **00548874** *ALEISSUE-1066*	**Summary**: OV 2500: Email server settings set to TLS - exchange fails with error "TLS Alert: unknown certificate" Click for Additional Information
Case: **00548841** *OVE-10748*	**Summary**: OV 2500: "Scheduled devices backup using MAP" is not working Click for Additional Information
Case: **00549435** *OVE-10651*	**Summary**: OV 2500: Error "Failed to connect to the device. Please check the user name and password" Click for Additional Information
Case: **00550500** *OVE-10787*	**Summary**: OV 2500: User with “Network Admin” role does not have access to view “Schedulers”

CR/PR Number	Description
	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** *OVE-10760 and OVE-10762*	**Summary**: OV 2500: IP of devices/switches disappear in "Policy Roles" (Policy View-Expert Mode) Click for Additional Information
Case: **00545307** *OVE-10756*	**Summary**: OV 2500: HA cluster unstable after the active OV server reboot Click for Additional Information
Case: **00546230** *OVC-8492*	**Summary**: OV 2500 / OV Cirrus: IoT classification fails or is not displayed Click for Additional Information
Case: **00546094** *OVE-10707*	**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** *OVE-10690*	**Summary**: OV 2500: Trap-Filter with Mac-Address on the SnmpVariable returns Invalid Syntax Click for Additional Information
Case: **00541800** *OVE-10614*	**Summary**: OV 2500: After upgrade from 4.5R01 to 4.5R02 the services ovav and ovwma are not Running Click for Additional Information
Case: **00541177** *OVE-10385*	**Summary**: OV 2500: VLAN Type is displayed as “Standard” instead of “Dynamic” for a VLAN which has been learned through MVRP. Click for Additional Information
Case: **00541178** *OVE-10385*	**Summary**: OV 2500: The "Type" and "Device Type" are blank on the "Configuration -> VLAN Manager" Click for Additional Information
Case: **00543643** *OVE-10645*	**Summary**: OV Cirrus / OV 2500: Application Visibility - We cannot remove AP Group from Signature profiles

CR/PR Number	Description
	Click for Additional Information
Case: **00540266** *OVE-10639*	**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" Click for Additional Information
Case: **00538815** *OVE-10613*	**Summary**: OV Cirrus / OV 2500: Guest Operators are unable to generate Guest Accounts using option Batch Creation Click for Additional Information
Case: **00524131** *OVE-10577*	**Summary**: OV Cirrus / OV 2500: Not showing LLDP link on some switches
Case: **00524129** *OVE-10385*	**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. Click for Additional Information
Case: **00527168** *OVE-10614*	**Summary**: OV 2500: High memory issue
Case: **00529945** *ALEISSUE-971*	**Summary**: OV Cirrus / OV 2500: Portal users still have internet access after clicking on logout Click for Additional Information
Case: **00531174** *ALEISSUE-961*	**Summary**: OV Cirrus / OV 2500: Captive portal Logo does not maintain right aspect ratio Click for Additional Information
Case: **00531597** *OVE-10514*	**Summary**: OV Cirrus / OV 2500: Cannot create a new topology map when lot of child maps Click for Additional Information
Case: **00531221** *OVE-10481*	**Summary**: OV Cirrus / OV 2500: Stops receiving traps after user changes Trap Port from 162 to another value Click for Additional Information
Case: **00513237** *OVE-11112*	**Summary**: OV 2500: Link between 6450 & core OS10K switch are not shown in topology map Click for Additional Information
Case: **00531818** *OVE-10553*	**Summary**: OV 2500: High CPU and Web GUI not responding when using Top N PoE Analytics

CR/PR Number	Description
	Click for Additional Information
Case: **00556303** *ALEISSUE-741*	**Summary**: OV 2500/OV Cirrus: wifi4eu banner shall be displayed full size
Case: **00547689** *OVC-8746*	**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** *OVC-8703*	**Summary**: OV 2500/OV Cirrus: IoT device remains into Pending state after IoT enforcement Click for Additional Information
Case: **00538748** *OVC-8634 and OVE-10608*	**Summary**: OV 2500/OV Cirrus: It takes a long time to load “Geo Location View” on Topology app Click for Additional Information

6.8.2 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)
- 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)
- Client Name Field Blank for Clients Running iOS 14 (OVC-8287)
- OV Restore Fails with Error “Failed to Start ovldap Service (OVE-9782)

6.9 PRs Fixed Since 4.5R2

6.9.1 Customer PRs

CR/PR Number	Description
Case: **00526846** *OVE-10388*	**Summary:** OV 2500: No option to input VLAN information in "Filter Data". Click for Additional Information
Case: **00522580** *OVE-10299*	**Summary:** OV 2500 Enterprise: IOT problems on wired and wireless clients. Click for Additional Information
Case: **00479752** *OVE-9228*	**Summary**: OV 2500 Scheduled backups with dynamic maps. Click for Additional Information
Case: **00491445** *OVE-9581*	**Summary**: OV 2500 Stellar AP are unable to register or disappear from registration after a while. Click for Additional Information
Case: **00492353** *OVE-9497*	**Summary**: OV 2500 configuration save issue from Notifications tab. Click for Additional Information
Case: **00481162** *OVE-9483*	**Summary**: OV 2500 Login activity not displayed for guest operator. Click for Additional Information
Case: **00481748** *OVE-9053*	**Summary**: OV 2500 - failed to push the Policy List config to the OS6860 switch. Click for Additional Information
Case: **00494007** *OVE-9556*	**Summary**: OV 2500 APs upgrade status is not shown in managed tab. Click for Additional Information
Case: **00496811** *OVE-10200*	**Summary**: OV 2500 fails to configure policies with multiple conditions to AOS 6x and AOS 8x. Click for Additional Information

CR/PR Number	Description
Case: **00508695** *OVE-9949*	**Summary**: OV 2500 Generating a report is blank in "Managed Devices". Click for Additional Information
Case:**00501928** *ALEISSUE-853*	**Summary**: OV 2500 Spellcheck for Swedish translation of OmniVista UPAM Captive Portal. Click for Additional Information
Case: **00508643** *OVE-10155*	**Summary**: OV 2500 External Radius Server changes updated to switch automatically. Click for Additional Information
Case: **00511547** *OVE-10077*	**Summary**: OV 2500 Telnet connections are seen from OV2500 to switch. Click for Additional Information
Case: **00511432** *OVE-10025*	**Summary**: OV 2500: ovtomcat service consumes high CPU Utilization. Click for Additional Information
Case: **00512076** *OVE-9198*	**Summary**: OV 2500 - Application Visibility - Signature Profiles stuck to Loading. Click for Additional Information
Case: **00512305** *OVE-10039*	**Summary**: OV 2500 - Data sync error in HA - DRBD diskless status on standby after partition extended. Click for Additional Information
Case: **00512405** *OVE-10034*	Summary: OV 2500 while generating CSV for Home - WLAN - Client - Summary, nothing displayed for last 30 or 90 days. Click for Additional Information
Case: **00514612** *OVE-10159*	**Summary**: OV 2500 Wireless Clients fail to authenticate. Click for Additional Information
Case: **00517044** *OVE-10167*	**Summary**: OV 2500 Tomcat error in the GUI. Click for Additional Information
Case: **00517438** *OVE-10203*	**Summary**: OV 2500 / OV Cirrus - Policy list updating is failing after removed device from devices list. Click for Additional Information
Case: **00518955** *OVE-10255*	**Summary**: OV 2500 Unable to recreate the disk with new copied virtual disk file while upgrading the VPN VA server.

CR/PR Number	Description
	Click for Additional Information
Case: **00521123** *OVE-10281*	**Summary**: OV 2500 UPAM services is in out of memory. Click for Additional Information

6.9.2 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)
- Database Connection Stuck at “Connecting/Standalone" Status on HA System (OVE-8874)
- Client Disconnects on First Authentication if UPAM Fails Over to Backup External Radius Server (OVE-9528)
- Guest User Account Names Are Not Case-Sensitive in OVE 4.4R1 (OVE-4999)

6.10 PRs Fixed Since 4.5R1

6.10.1 Customer PRs

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

CR/PR Number	Description
00468024 *OVC-7743*	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
Case: **00418540** *OVE-8279*	**Summary:** OV 2500 -Fails to provide Captive portal page every week Click for Additional Information
Case: **00461255** *OVE-8459*	**Summary:** OV 2500 - Report only shows the parent pie-chart statistics not the sub-tree statistics Click for Additional Information
Case: **00460570** *CRNOV-1925*	**Summary:** OV Cirrus - Issues adding the OV Cirrus Captive portal URL on the WiFi4EU Portal. Click for Additional Information
Case:	**Summary:**

CR/PR Number	Description
00461232 *OVE-8210*	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** *OVE-8888*	**Summary:** OV 2500 - External web session from OV Click for Additional Information
Case: **00462741** *CRNOV-1967*	**Summary:** OV 2500/OV Cirrus - WiFi4EU Captive Portal does not display correctly. Click for Additional Information
Case: **00426224** *OVE-8279*	**Summary:** OV 2500 - UPAM crash and no more 802.1x Authentication processed Click for Additional Information
Case: **00478884** *CRNOV-2143*	**Summary:** OV 2500 - Bulk Notification AP Stopped/Resumed Responding to OV Click for Additional Information
Case: **00480606** *OVE-8171*	**Summary:** OV 2500 - 100% Disk space. Click for Additional Information
Case: **00434325** *OVE-8382*	**Summary:** OV 2500 - Report failures. Click for Additional Information
Case: **00465897** *OVE-8316*	**Summary:** OV 2500 - ASA requests are not proxied by OV to external RADIUS Server Click for Additional Information
Case: **00466510** *CRNOV-2063*	**Summary:** OV 2500 - High CPU and synchronization issue with HA peer node Click for Additional Information
Case: **00454490** *OVE-8848*	**Summary:** OV 2500 - Opening Notifications results in error message “Communication failure” Click for Additional Information
Case: **00457434** *OVE-7937*	**Summary:** OV 2500 - Screen object changes when doing Logout and login. Click for Additional Information
Case: **00471352** *OVE-8407*	**Summary:** OV 2500 - OV GUI and CLI slowness issue.

CR/PR Number	Description
	Click for Additional Information
Case: **00457582** *OVE-8043*	**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** *OVE-8279*	**Summary:** OV 2500 - ovupam service down. Click for Additional Information
Case: **00431484** *OVE-7454*	**Summary:** OV 2500 - netadmin user not able to create AP Groups and manage AP association. Click for Additional Information
Case: **00423181** *OVE-7007*	**Summary:** OV 2500 - Policies ACL/QOS "notified all" and "notified selected" does not work all the time. Click for Additional Information
Case: **00450497** *OVE-8204*	**Summary:** OV 2500 - experiencing slowness while accessing GUI. Click for Additional Information
Case: **00470058** *OVC-7688*	**Summary:** OV 2500 - Duplicate IP leasing issue in RAP Data VPN configuration. Click for Additional Information
Case: **00475712** *OVE-8671*	**Summary:** OV 2500 - Wired users MAC authentication failing after upgrade to 4.5 R01. Click for Additional Information
Case: **00477543** *OVE-8860*	**Summary:** OV 2500 - Time Period in Wireless Client List is always 24h Click for Additional Information
Case: **00478110** *OVE-8675*	**Summary:** OV 2500 - Backup is not working after upgrade to 4.5R1. Click for Additional Information
Case: **00463967** *OVE-8269* *OVE-8105*	**Summary:** OV 2500 - Quarantine Manager Rule - Add restriction for OS6560 and OS6465 Click for Additional Information
Case: **00470560** *OVE-8171*	**Summary:** OV 2500 - Unable to upgrade to 4.5R01 due to space issue. Click for Additional Information

CR/PR Number	Description
Case: **00483504** *OVC-8056*	**Summary:** OV 2500 / OV Cirrus – Wifi4EU language flag overlaps logo. Click for Additional Information
Case: **00484663** *OVE-8627*	**Summary:** OV 2500 - High disc utilization when using Top N Applications analytics Click for Additional Information
Case: **00485017** *CRNOV-2262*	**Summary:** OV 2500 - Most of the services in OV were continuously restarting and the HA sync was stuck. Click for Additional Information
Case: **00486274** *OVE-8279* *OVE-8407* *OVE-8627*	**Summary:** OV 2500 - High Availability failed to work. Click for Additional Information
Case: **00489662** *CRNOV-2292*	**Summary:** OV 2500 - Channel 144 is missing in OV with Singapore country code. Click for Additional Information
Case: **00465552** *OVE-8309*	**Summary:** OV 2500 - Mismatched AP license count. Click for Additional Information
Case: **00481748** *OVE-8627*	**Summary:** OV 2500 - Failed to push the Policy List configuration to OS6860 switch.
Case: **00482002** *OVE-8406*	**Summary:** OV 2500 - "ovldap" service failed to start. Click for Additional Information
Case: **00470905** *ALEISSUE-692*	**Summary:** OV 2500 – Captive Portal customization issue. Click for Additional Information
Case: **00453284** *OVE-7902*	**Summary:** OV 2500 - Unable to execute Action (Copy Certified to working/ Running) on 8x switches.
Case: **00451799** *OVE-7873*	**Summary:** OV 2500 – Not possible to create an Unified Policy with condition source IP and Tricolor marking on OS6450 Click for Additional Information

CR/PR Number	Description
Case: **00490777** *OVE-9294*	**Summary:** OV 2500 – There was a JMS Request timeout error noticed when we enable IoT on Stellar AP Click for Additional Information
Case: **00494012** *OVE-9490*	**Summary:** OV 2500 – AP Group is not visible for 40 minutes after creating it Click for Additional Information
Case: **00497999** *OVE-8475*	**Summary:** OV 2500 – Top N PoE Switches Utilization Summary widget/report stuck to “Loading” Click for Additional Information
Case: **00475299** *OVE-8407*	**Summary:** OV 2500 – Not possible perform a OmniVista backup after upgrade to 4.5R01 Click for Additional Information
Case: **00474701** *OVE-8658*	**Summary:** OV 2500 – After power on/off the VPN-VA all Stellar RAPs are down Click for Additional Information
Case: **00461567** *OVE-9586*	**Summary:** OV 2500 – Down devices are listed as “unsaved” devices on Notifications bell icon Click for Additional Information
Case: **00467006** *OVE-7405*	**Summary:** OV 2500 – Dummy stellar AP called "no-name" in OV2500 Managed devices cannot be deleted Click for Additional Information
Case: **00496113** *CRNOV-2387*	**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** *OVE-9622*	**Summary:** OV 2500 /OV Cirrus – “Condition mismatch…” displayed when user is creating policy with multiple conditions Click for Additional Information

CR/PR Number	Description
Case: **00499118** *OVE-9581*	**Summary:** OV 2500 - AP not able to register on OV, maximum MQTT connections were reached Click for Additional Information
Case: **00499753** *OVE-8702*	**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** *OVE-9487*	**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** *OVE-9487*	**Summary:** OV 2500 – service ovclient stuck to “starting” Click for Additional Information

6.10.2 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)
- 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)
- Problem Connecting to Switch with OV Assistant When Multiple Bluetooth Dongles Present (OVC-7240)

6.11 PRs Fixed Since 4.4R2

6.11.1 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
Case: **00434606** *OVC-5400*	**Summary:** OV Cirrus Guest access portal is not working. Click for Additional Information
Case: **00434966** *OVC-7167*	**Summary:** OV Cirrus If the admin password is different than the default one, the provisioning fails. Click for Additional Information
Case: **00452519** *CRNOV-1790*	**Summary:** OVC - Provisioning Failed state. Click for Additional Information

CR/PR Number	Description
Case: **00447389** *OVE-7712*	**Summary:** OV 2500 4.4R2 / OV Cirrus 3.1.0 Duplicate SSID on WLAN -> SSIDs page. Click for Additional Information
Case: **00443735** *OVE-6775*	**Summary:** OV Cirrus Managed Inventory Ports, Wrong PoE Status and Wattage for OS6860E-P24. Click for Additional Information
Case: **00436366** *OVC-6861*	**Summary:** Wrong expiration date for Guest Accounts in UPAM. Click for Additional Information
Case: **00430474** *OD-894*	**Summary:** OVC - AP and switch are down. Click for Additional Information
Case: **00437271** *OVC-7154*	**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** *OVC-7364*	**Summary:** OV Cirrus LDAP server management not taken into account when "Admin name" changed. Click for Additional Information
Case: **00419713** *OVE-6470*	**Summary:** OV 2500 4.4R2 GA (Build 37) issue when we select Unified Profile -> Workflow -> MAC Authentication. Click for Additional Information
Case: **00405472** *CRNOV-1251*	**Summary:** OV2500 NGINX service Stopped and do not restart. Click for Additional Information
Case: **00411920** *CRNOV-1425*	**Summary:** OV2500 VLAN Manager misbehavior. Click for Additional Information
Case: **00423209** *CRNOV-1555*	**Summary:** Guest Access Service Level is ignored when using Access Code. Click for Additional Information
Case: **00423292** *CRNOV-1508*	**Summary:** OV2500 objects are flickering when we are zooming. Click for Additional Information

CR/PR Number	Description
Case: **00423298** *CRNOV-1506*	**Summary:** Editing existing AAA Server Profile in Simplified SSID App fails. Click for Additional Information
Case: **00423036** *ALEISSUE-515*	**Summary:** If account name is empty chosen Service Level does not affect settings. Click for Additional Information
Case: **00423038** *ALEISSUE-514*	**Summary:** UPAM Guest - Service Level - Level 4 - *Device Validity Period cannot not be changed! Click for Additional Information
Case: **00427821** *OVC-7003*	**Summary:** Unable to add the captive portal server in the ARP profile. Click for Additional Information
Case: **00429261** *ALEISSUE-534*	**Summary:** UPAM Guest: Verification Code not working on IOS devices. Click for Additional Information
Case: **00432688** *OVE-7084*	**Summary:** OV 2500 Add the command lsblk on the CLIADMIN Advanced Menu for HA troubleshooting. Click for Additional Information
Case: **00432778** *OVE-7089*	**Summary:** OV 2500 Enhance logs for OV HA Troubleshooting (during upgrade and normal operation). Click for Additional Information
Case: **00431484** *OVE-7217* *OVE-7454*	**Summary:** OmniVista user Access rights. Click for Additional Information
Case: **00439743** *OVE-7210*	**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** *CRNOV-1779*	**Summary:** Captive portal IP config issue - OV2500. Click for Additional Information

CR/PR Number	Description
Case: **00448845**	**Summary:** OV2500 Version 4.4R2: Scheduled Backup Not Working. Click for Additional Information
Case: **00431586** *OVE-7927*	**Summary:** The application bandwidth usage and application flow count widget not showing correct data. Click for Additional Information
Case: **00455156** *CRNOV-1779*	**Summary:** CRNOV-1894: OV2500 Error: IP Unavailable. Click for Additional Information
Case: **00451633** *CRNOV-1779*	**Summary:** OV2500 IP-Add Configuration Keeps On Appearing. Click for Additional Information
Case: **00454512** *CRNOV-1877*	**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** *OVE-6983*	**Summary:** Error message while changing SSID password on stellar WIFI managed by OV-Cirrus. Click for Additional Information
Case: **00419855** *CRNOV-1467*	**Summary:** Unable to delete whole employee account at once. Click for Additional Information
Case: **00441376** *CRNOV-1725*	**Summary:** OV2500: Scheduler job task concurrently failed. Click for Additional Information
Case: **00435316** *CRNOV-1662*	**Summary:** OV2500: Unable to Apply the Signature Profile. Click for Additional Information
Case: **00444773** *ALEISSUE-625*	**Summary:** Machine auth issue - OV2500. Click for Additional Information
Case: **00444226** *OVE-7906*	**Summary:** OV2500_Managed Devices Menu Options Not Working. Click for Additional Information

CR/PR Number	Description
Case: **00445322** *CRNOV-1737*	**Summary:** OV2500 as internal Radius server to authenticate switch login. Click for Additional Information
Case: **00445718** *OVE-6598*	**Summary:** OV2500: OV CPU utilization is high on VM-ESXI. Click for Additional Information
Case: **00437236** *CRNOV-1718*	**Summary:** Telegraf Logs in OV2500 with Error. Click for Additional Information
Case: **00444164** *CRNOV-1768*	**Summary:** Unable to take the Backup of the OV2500. Click for Additional Information
Case: **00446941** *ALEISSUE-584*	**Summary:** Stellar Enterprise with OV2500: device limitation fur Guest User with access-code not working. Click for Additional Information
Case: **00450766** *OVE-1817*	**Summary:** CLI script issue- OV2500 4.4R2. Click for Additional Information
Case: **00454040** *CRNOV-1834*	**Summary:** OmniVista services stopped after IP change. Click for Additional Information
Case: **00458796** *CRNOV-1913*	**Summary:** OV2500: SSL Error Message. Click for Additional Information
Case: **00459196** *OVE-6983*	**Summary:** Changes made on OV SSID template is not pushed to the AP group. Click for Additional Information
Case: **00442743** *CRNOV-1739*	**Summary:** OV2500 - OV is not accessible through GUI. Click for Additional Information

Appendix A – Enabling DCOM on Hyper-V

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

Enable DCOM on Hyper-V (Standalone Installation)

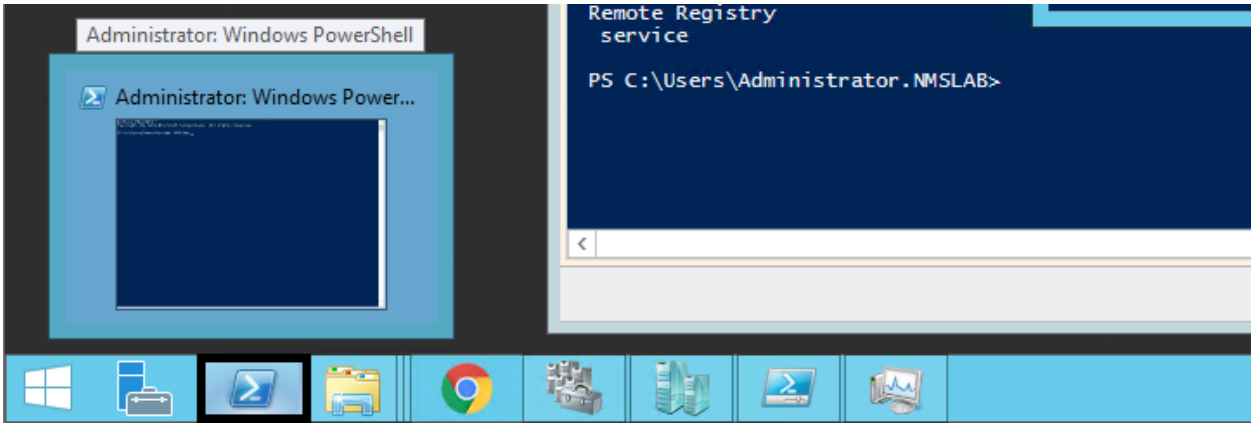
The following steps are specific to Windows 64 bit only.

1. Log in Hyper-V Server.

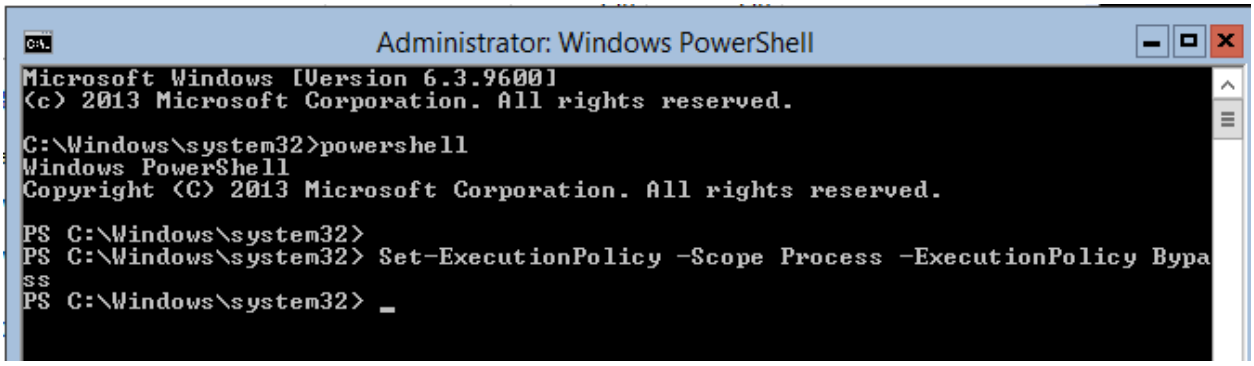
2. Get the Powershell script from attachment: HyperV_Enable_DCOM_x64.ps1.

HyperV_Enable_DCOM_x64.ps1

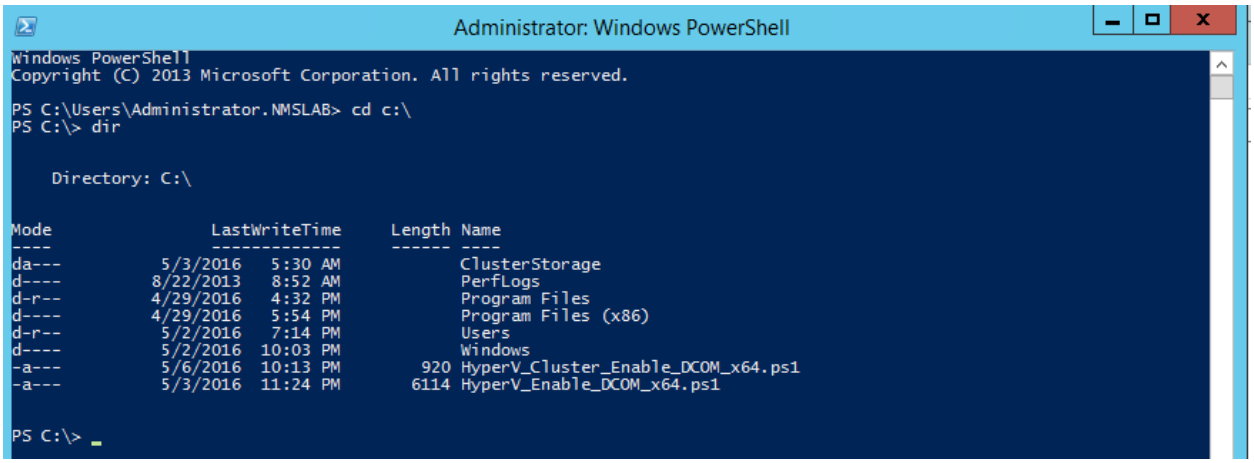
3. Run Powershell.



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

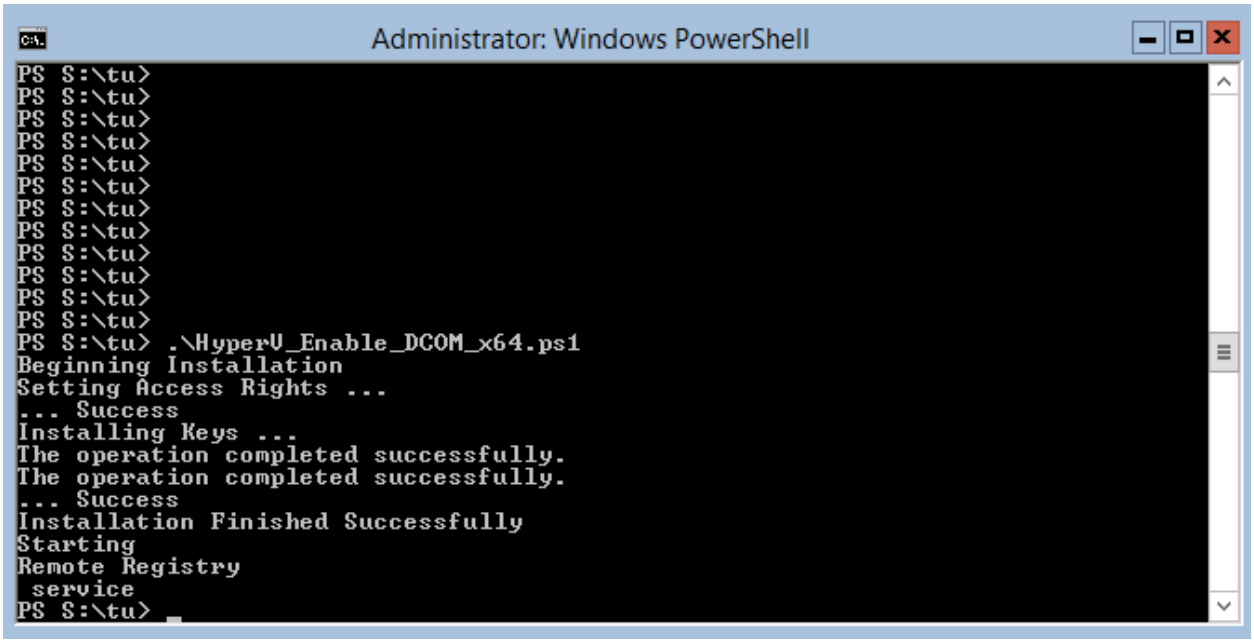


5. Change to the directory that contains the downloaded script from Step 2.



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

7. Run .\HyperV_Enable_DCOM_x64.ps1.



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

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

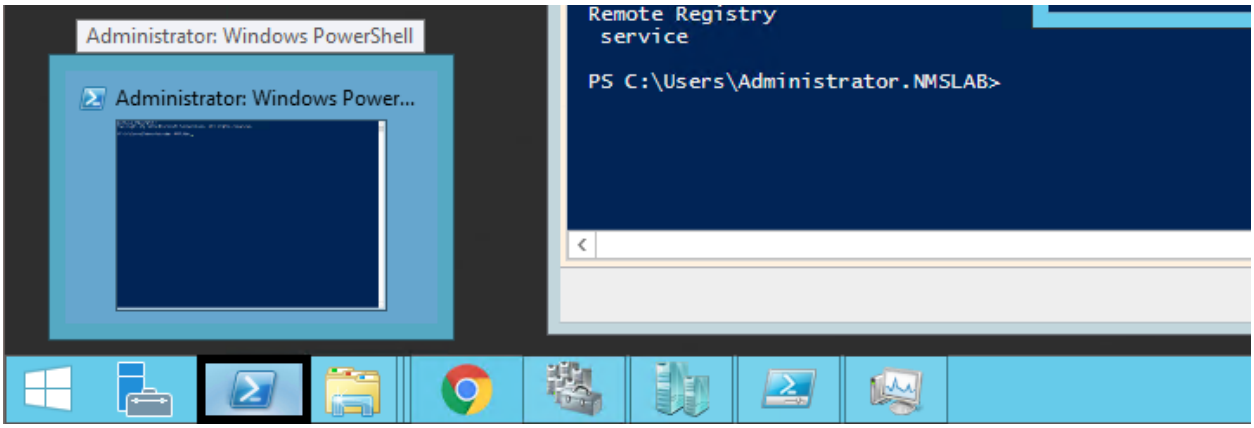
2. Download both files from the attachment and place them on the same directory:
HyperV_Cluster_Enable_DCOM_x64.ps1

HyperV_Cluster_Enable_DCOM_x64.ps1

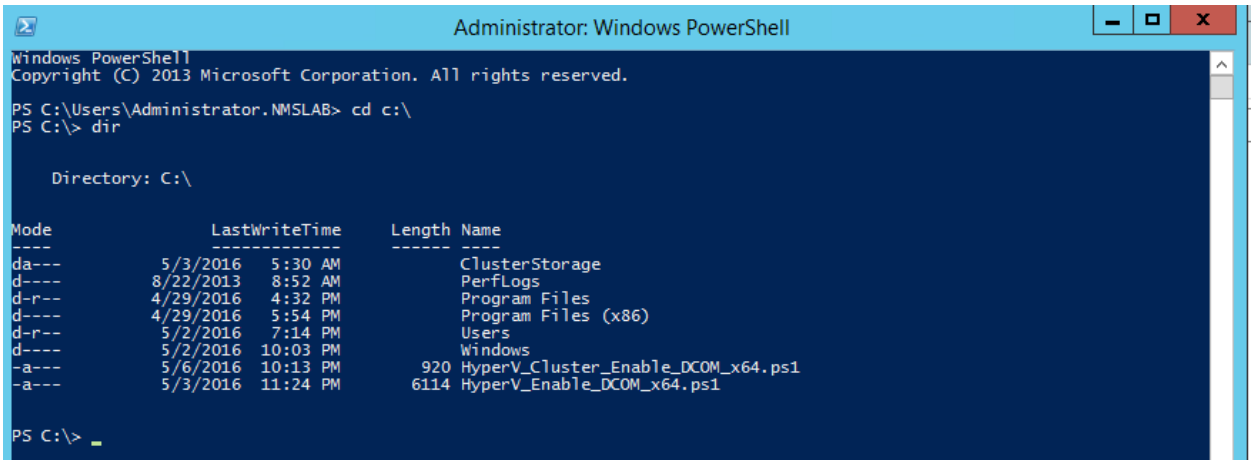
HyperV_Enable_DCOM_x64.ps1

HyperV_Enable_DCOM_x64.ps1

3. Run Powershell.



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



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

6. Execute HyperV_Cluster_Enable_DCOM_x64.ps1.