Release Notes

for

OmniVista 2500 NMS
Version 4.8R1

August 2023

Revision B

Part Number 033724-00

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 20.04

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
4.8R1	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
4.4R1	C	09/09/19	Release Notes Update
4.4R1	B	07/24/19	Release Notes Update
4.4R1	A	07/15/19	GA Release
4.3R3	A	03/15/19	GA Release
4.3R2	B	01/21/19	Release Notes Update
4.3R2	A	11/27/18	GA Release
4.3R1	B	07/12/18	Release Notes Update
4.3R1	A	06/06/18	GA Release
4.2.2.R01	C	01/26/18	Maintenance Release 2
4.2.2.R01	B	12/11/17	Maintenance Release 1
4.2.2.R01	A	08/24/17	GA Release
4.2.1.R01	E	06/16/17	MR 2 Release Notes Update
4.2.1.R01	D	05/30/17	Maintenance Release 2
4.2.1.R01	C	02/02/17	Maintenance Release 1
4.2.1.R01	B	09/30/16	Release Notes Update
4.2.1.R01	A	09/22/16	GA Release
4.1.2.R03	A	01/29/16	GA Release

4.1.2.R02	A	05/22/15	GA Release
4.1.2.R01	B	12/19/14	Maintenance Release
4.1.2.R01	A	10/24/14	GA Release

1.0 Introduction

This document details known problems and limitations in OmniVista 2500 NMS 4.8R1 (OV 2500 NMS 4.8R1), 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 4.8R1 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 20.04.

Note: This release requires an upgrade to the 4.7R1 Patch 2 release before you upgrade to the 4.8R1 release. See OmniVista 4.8R1 Upgrade Paths for more information.

1.1 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

Email:ale.welcomecenter@al-enterprise.com

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.

1.2 Documentation

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

1.3 New in this Release

Hardware/Release Support

AOS Switches

The following new switch models are now supported:

- OS6570M-12
- OS6570M-12D
- OS6570M-U28
- OS6570M-U28D
- OS2360-P24M

Stellar APs

The following OmniAccess Stellar APs (Enterprise Mode) are now supported:

- OAW-AP1431
- OAW-AP1411

Software

- **AOS 5.2R3 -** OmniVista 2500 NMS now supports AOS 5.2R3 for the OS2260 and OS2360 Series Switches.
- **AOS 8.9R2** – OmniVista 2500 NMS now supports AOS 8.9R2 on all previously supported AOS Switches.
- **AWOS 4.0.7 -** OmniVista 2500 NMS now supports AWOS 4.0.7 on Stellar AP OAW-AP1431 and OAW-AP1411.

New Features and Functions

This section details new features introduced in this release.

OAW-AP1411 Dual Radio, Tri-Band Options

The OAW-AP1411 is a dual-radio, tri-band (2.4G, 5G, 6G) Access Point with configurable radio options. A “Radio Setting” attribute in the RF Profile allows you to select one of the following radio band options for the AP:

- 2.4G, 5G Full (default)
- 2.4G, 6G
- 5G Full, 6G

AP RadSec Client with Local RADIUS Server

An AP can now communicate as a RadSec client with a local RADIUS Server that uses RadSec (RADIUS-over-TLS). To establish a secure connection between an AP RadSec client and the local RADIUS Server:

- Upload a RadSec Certificate to the AP (refer to Appendix D - Local RadSec Certificate)
- Enable TLS on the local RADIUS Server.

Note:

- AP RadSec Client is not supported on AP1101, AP1201H, AP1201L, AP1201HL, and AP1261-RW-B models.
- AP supports one, and only one, TLS-enabled RADIUS server. As a consequence, you cannot have one TLS-enabled RADIUS server as Primary and another TLS-enabled RADIUS server as Secondary.
- RadSec communication is not supported for wired clients of the AP.

Stellar AP Syslog Over TLS

An option to enable the use of the TLS encryption method for logging of AP events to a remote Syslog server is now available. When this option is enabled, a Syslog Over TLS Certificate is selected to upload to the AP. Configuring up to four remote Syslog Servers is supported.

Stellar BLE (Asset Tracking) Data Sharing with Third-Party Applications

The Stellar BLE data reporting channel to any Asset Tracking application uses Kafka. However, the built-in common device certificate on the AP allows communication only with Stellar AP Asset Tracking solutions. You can now upload a custom device certificate to the AP that will support sending BLE data to third-party Asset Tracking applications.

Note: Refer to Appendix B - Stellar BLE Data Format for information about the data format used to send RTLS messages to third-party RTLS applications.

Stellar WiFi RTLS Data Sharing with Third-Party Applications

The Stellar WiFi RTLS data reporting channel uses Kafka. However, the built-in common device certificate on the AP allows communication only with the OmniVista Cirrus 10 Stellar WiFi engine. You can now upload a custom device certificate to the AP that will support sending WiFi RTLS data to third-party RTLS applications.

Note: Refer to Appendix C - Stellar WiFi RTLS Data Format for information about the data format used to send RTLS messages to third-party RTLS applications.

Private Group PSK

When a PSK-enabled SSID network is created, you can either create a static PSK or enforce Device Specific PSK. This provides a common Passphrase key, which is suitable for networks requiring network wide common PSK. Enabling the Private Group PSK (PPSK) allows you to create private groups of client devices on the same SSID network based on a PPSK Entry. Each client device specifies a Passphrase when connecting to an SSID. If the passphrase matches any of the PPSK Entry, the client is placed in the specified Access Role Profile.

Configuring the Private Group PSK option for an SSID network is only available when the Device Specific PSK option is disabled or set to “Prefer Device Specific PSK”. However, if the Device Specific PSK option is set to “Force Device Specific PSK”, OmniVista will not display the Private Group PSK option because the Passphrase specified in Company Property is used instead.

A Private Group PSK Entry that is used to define a group of devices, consists of the following configurable parameters:

- **Name** - Enter a unique name to identify the PPSK Entry. No two Entries can have the same Name.
- **Passphrase** - Enter a unique PSK Passphrase for authentication. No two Entries can have the same Passphrase.
- **Access Role Profile** - Select the name of an Access Role Profile.

Note: Each SSID can have up to 16 PPSK Entries. The total number of entries across all SSIDs that exist on an AP cannot exceed 64 on any AP.

UPAM

- **Company Property Check** – An add-on Network Enforcement Policy is now a configurable Authentication Strategy option. When enabled, OmniVista will check to see if the device MAC address is listed in the Company Property database. You can also specify an Access Role Profile, Policy List, or other attributes to apply to the device if the MAC address check is successful (found in Company Property) or unsuccessful (not found in Company Property).
- **Create Guest Device in Remembered Device List** – A new Guest Account function allows you to manually add a Guest device to the Remembered Device List. This is particularly useful for Guest devices that are not able to manage portal redirection. The Guest Account Administrator can manually add up to five devices (or whatever the configured limit is) to the Remembered Device List.

Application Updates/Enhancements

This section details updates and enhancements to existing OmniVista applications.

AP Mesh Configuration Enhancements

- 6G Band option is now available on OAW-AP1451, OAW-AP1431, and OAW-AP1411 in a specific number of countries.
- Configurable Multicast rate control option (default is 24 Mbit/s). The Multicast rate is applied to "Multicast Video Stream" to help reduce jitters in a Mesh environment.

RF Profile Updates

- **DRM Scheduling -** The DRM auto-channel selection algorithm defaults to an interval of every six hours starting when the device boots up. The following DRM scheduling options are now configurable to allow changing the time interval and/or start time of channel selection:
  - **DRM Time Control** – When enabled, allows you to specify a DRM start time.
  - **DRM Start Time** – Applies when DRM Time Control is enabled. You can specify any hour of the day between 0 and 23 hours.
  - **DRM Interval** – When DRM Time Control is disabled, you can adjust the time interval up or down (0.5 hour to 12 hours). By default, the interval time is set to every six hours.
- **Channel Switch Announcement (CSA)** – 6G Band now supported.

GRE Tunnel Profile TCP Maximum Segment Size (TCP MSS) Setting

Configuring a TCP MSS value for a GRE tunnel is now available. The value used can vary across different network segments, which helps to simplify tunnel provisioning.

The MTU tunnel setting is applicable to both UDP and TCP packets. The TCP MSS setting applies only to TCP packets and defaults to a 1250 value. The MTU value should be greater than the TCP MSS value, considering the difference of the IP header length as well as TCP header length.

Certificates

The following additional Certificates are now available to upload to APs:

- **Local RadSec Certificate** – Used for AP RadSec client communication.
- **Syslog Over TLS Certificate** – Used for AP remote logging over TLS.
- **Stellar BLE Certificate** – Custom device certificate used for sending BLE data to third-party Asset Tracking applications.
- **Stellar WiFi RTLS Certificate** – Custom device certificate used for sending WiFi RTLS data to third-party RTLS applications.

Access Role Profile VLAN-Mapping Enhancement

We have expanded the ability to bind up to 256 VLANs to a WLAN/SSID on the AP13xx/AP14xx models. However, not every AP model can accommodate 256 VLANs for all the configured SSIDs. The limitations are outlined below:

- AP1301H can support 256 VLANs on a maximum of 2 SSIDs, with a total of 512.
- AP1311/AP1301/AP1431/AP1411 can support 256 VLANs on a maximum of 4 WLANs/SSIDs, with a total of 1024.
- AP1320/AP1331/AP1351/AP1451 can accommodate 256 VLANs on a maximum of 7 WLANs/SSIDs, with a total of 1792.

SSID Enhancements

- **Extended SSID Scale** - The number of SSIDs that can be assigned to the AP Group has been extended to 14. A new option “Extended SSID Scale” is now available when configuring an SSID. Note that when this attribute is enabled, only AP models that support up to 14 SSIDs can join the AP Group. When this attribute is disabled, any AP model can join the group, but the limit is 7 SSIDs per AP Group.
- **Automatic WPA/WPA2 Encryption** - The Automatic WPA/WPA2, or mixed mode Encryption with dynamic keys support, option is now available while creating a new SSID for the following user networks:
    - Enterprise Network Employees using the 802.1X Authentication method,
    - Protected Network for Guest Users using pre-shared key and an optional Captive Portal Authentication method.
    - Protected Network for Enterprise Employees using pre-shared key and the BYOD Registration Portal Authentication method.

Password Security

- **Password Strength Enforcement** - The System Settings screen provides a new Enforce Strong Password option that is enabled/disabled at the Administrator level to enforce password rules. When Enforce Strong Password is enabled (the default), the following guidelines apply when configuring or editing the password for an OmniVista user profile:
  - Password length: 12 – 30 characters
  - Min number of upper-case letters: 1
  - Min number of lower-case letters: 1
  - Min number of digits: 1
  - Min number of special characters: 1 in the list of ~ ! @ # $ % ^ & * ( ) _ . +
  - Password should not contain username
  - Password is treated as case-sensitive

    In addition, a visual evaluation of password strength and a random password generator is provided for the “Password” field on the Create User screen.

    Note that strong password restrictions are not applied to existing users unless they attempt to change their user profile when password enforcement is enabled.
- **Two-Factor Authentication**

  Two-Factor Authentication can now be enabled/disabled for a user login based on the User Role. When enabled, a user is required to enter an authentication code after entering their login/password to access OmniVista 2500 NMS. The authentication code is a time-based, 6-digit code that is generated using the Google Authenticator App.

  The Two-Factor Authentication setting (enabled or disabled) for a User Role is applied to all users assigned to that Role through their User Group. You cannot have different login settings for different users in the same User Group. If a User Group has two User Roles and one is enabled for Two-Factor Authentication while the other is not, the user will still be required to use Two-Factor Authentication to log in.

G Suite Rebranded to Google Workspace

Google Workspace is an evolved version of G Suite designed for seamless integration between Google applications for productivity, team collaboration, and communication. The OmniVista IoT Inventory screen (Network - IoT) under the Chrome Devices option provides integration with Google Workspace. The OmniVista UI and error messages now reflect “Google Workspace”.

APAC Cluster Removed from IoT/Location/Advanced Analytics Server Options

The Asia Pacific (APAC) cluster option is no longer offered on the “Server IP/Host” drop-down menu when configuring an OmniVista Cirrus Advances Analytics engine type. Note that you can delete old engine profiles containing the APAC cluster only if the profile was not configured for an AP Group. If the profile is configured for an AP Group, edit the AP Group configuration to select a different engine profile.

OmniVista Framework Updates

OmniVista Service Availability During High-Availability Upgrade

During the upgrade time for an OmniVista 2500 NMS High-Availability cluster, OmniVista management functions, including UPAM authentication, remain available except for approximately 5 to 10 minutes.

Note:

- The improved OmniVista service availability is achieved only when upgrading from the 4.7R1 Patch 2 release and when you follow the new HA upgrade process in this release. Refer to the *OmniVista 2500 NMS 4.8R1 Installation and Upgrade Guide* for more information.
- During the Standby Node upgrade process, user-configured changes, and network updates (such as Authentication Records, SNMP Traps, Device up/down status) made in the database are lost.

Linux Distribution Update

The Oracle Linux update includes many security updates.

- **OmniVista 2500 NMS VA** – Oracle Linux version updated from 7 to 8.7.
- **RAP VPN VA** - Oracle Linux version updated from 7 to 8.7.

Remote Access Point (RAP) Enhancements

- RAP VPN VA updated to 4.8.1 running Oracle Linux 8.7.
- The default Hard Disk size is now 8GB for RAP VPN VA 4.8.1.

OmniVista 2500 NMS Virtual Machine Manager (VMM)

- Citrix XenServer no longer supported in this release (as previously announced).

Framework Enhancements

- Third-party packages updated to fix CVEs.
- OpenSSL updated to 3.1.0

1.4 Feature Set Support

1.4.1 OmniVista REST API Management

You can use REST APIs for scripting or integration with any third-party systems in your management network. Available OmniVista REST APIs can be found here: https://ovc4x.ovcirrus.com/

1.4.2 Element Manager Integration

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

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

Element Manager	Supported Devices	Description
WebView	• 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

1.4.3 Device Feature Support

The following table details OmniVista 2500 NMS 4.8R1 feature support by device:

Feature	OS6900	OS6860/ OS6865	Other AOS	OS2220	OS2260 OS2360	Stellar APs	Legacy WLAN	3rd Party Switches
Application Visibility (1)		X				X		
Analytics (2)	X	X	X		X	X		
Basic MIB-2 Polling and Status Display	X	X	X	X	X		X	X (3)
ClearPass (BYOD) (4)	X	X	X			X		
CLI Scripting	X	X	X		X	X (5)	X	X(5)
Cloud Agent	X	X	X		X			
Discovery	X	X	X	X	X	X	X	X (3)
IoT (6)	X	X				X		
Locator	X	X	X	X	X	X	X	X (7)
mDNS		X	X (8)					
mDNS Gateway (9)	X	X	X			X		
mDNS Responder (10)	X	X	X			X		
Provisioning (11)	X	X	X		X			
PolicyView-QoS	X	X	X		X	X	X	
Premium Service (BYOD)		X	X					
ProActive Lifecycle Mgmt (PALM)	X	X	X	X	X	X	X	

Feature	OS6900	OS6860/ OS6865	Other AOS	OS2220	OS2260 OS2360	Stellar APs	Legacy WLAN	3rd Party Switches
Quarantine Manager (12)		X	X				X	
Resource Manager BU/Restore/Upgrade	X	X	X		X	X		
SIP (13)		X	X					
SPB/ERPv2 (14) (15)	X	X	X					
Topology Links (LLDP) (16)	X	X	X	X	X	X		
Trap Absorption	X	X	X	X	X	X	X	X
Trap Display/Trap Responder	X	X	X	X (17)	X	X	X	X
Trap Replay	X	X	X		X	X		
UPAM (Guest User, BYOD) (18)	X	X	X			X		
Unified Policies	X	X	X		X			
Unified Policy List	X	X	X					
UNP (19)	X	X	X		X	X		
Virtual Chassis	X	X	X	X	X			
VLAN Configuration	X	X	X		X (20)		X	
VM Manager (21)	X	X	X		X (22)			
VM Snooping	X (23)							
VRF	X	X	X					
VXLANs	X (24)							
Web Content Filtering (25)						X		
WLAN (SSID)						X		

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. The Application Visibility feature is supported on OS6860E switches (AOS 8.2.1.R01 and later). It is also supported in a virtual chassis of OS6860/OS6860E switches where at least one OS6860E is present. It is also supported on all Stellar APs models, except AP1101, AP1201H, AP1201L, and AP1201HL. (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.) Application Visibility is supported on OS6860N Switches (8.7R2 and later).

2. The Analytics feature is supported on 6450 devices (6.7.1.R01 and later), OS6860/6860E and OS6865 (8.3.1.R01 and later), OS6860N (8.7R1 and later), OS6900 (8.3.1.R01 and later), and OS9900 (8.3.1.R02 and later). It is also supported on Stellar APs (except for Top N Ports, Top N Application and Clients – sFlow, and performance monitoring). Top N Clients are not supported on OS2260 and OS2360.

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

4. ClearPass (BYOD) is supported on OS6860N (8.7R1 and later), OS6450 (6.7.1.R02 and later), and OS6860 (8.3.1.R01 and later), and Stellar APs.

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

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

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

8. AOS 6.4.6.R01 and later switches only.

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

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

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

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

13. The SIP feature is only supported on the following devices running 6.4.6.R01 and later: 9700E (C-24/48, P24, U2/6/12/24), 9800E (C24/48, P24, U2/6/12/24).

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

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

16. OmniVista 2500 NMS does not display LLDP links reported by a single device. For a link to be displayed, both devices must be supported devices and LLDP MIB interface from each must have the Link.

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

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

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

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

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

21. The VM Manager application is not supported if OmniVista is deployed on Hyper-V 2019, 2022. 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. Support for Citrix XenServer was removed in this release.

22. VMM VLAN configuration is not supported.

23. VM Snooping is supported on OS6900 switches (7.3.4.R02 and later). VM Snooping is supported on a port/linkagg, fixed bridge port, UNP bridge port, service access port, and UNP Service Access Point. VM Snooping is not supported on eVB, SDP, or VXLAN service ports.

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

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

1.4.4 SSHv2/Telnet Element Management

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

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

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

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

2.0 System Requirements

The following builds are certified for OV 2500 NMS 4.8R1:

AOS

- OS2260 – 5.2R1, 5.2R2, 5.2R3
- OS2360 – 5.2R1, 5.2R2, 5.2R3
- OS6350 – 6.7.2.R06, 6.7.2.R07, 6.7.2.R08
- OS6360 – 8.8R2, 8.9R1, 8.9R2
- OS6360-P10A – 8.8R3, 8.9R1, 8.9R2
- OS6450 – 6.7.2.R06, 6.7.2.R07, 6.7.2.R08
- OS6465 – 8.8R2, 8.9R1, 8.9R2
- OS6560 – 8.8R2, 8.9R1, 8.9R2
- OS6570M – 8.9.107.R02
- OS6860/E – 8.8R2, 8.9R1, 8.9R2
- OS6860N – 8.8R2, 8.9R1, 8.9R2
- OS6865 – 8.8R2, 8.9R1, 8.9R2
- OS6900 – 8.8R2, 8.9R1, 8.9R2
- OS9900 – 8.8R2, 8.9R1, 8.9R2
- OS6900-T24 – 8.9R1, 8.9R2
- OS6900-X24 – 8.9R1, 8.9R2

WebSmart

- OS2220 – 8.3.1.2, 8.3.1.3

OmniAccess WLAN

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

OmniAccess WLAN IAP

- IAP-105 – OAW 6.5.4, 8.3.0
- IAP-205 – OAW 6.5.4, 8.3.0
- IAP-225 – OAW 6.5.4, 8.3.0
- IAP-325 – OAW 6.5.4, 8.3.0
- IAP-335 – OAW 6.5.4, 8.3.0

Stellar AP Series Wireless Devices

The following AP models are supported. The recommended AWOS version is 4.0.7.

- OAW-AP1101
- OAW-AP1201

- OAW-AP1201L (available for China/Brazil only)
- OAW-AP1201HL (available for China only)
- OAW-AP1201H
- OAW-AP1201BG
- OAW-AP1221, OAW-AP1222
- OAW-AP1231, OAW-AP1232
- OAW-AP1251
- OAW-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

Note: If you are upgrading to OV 4.8R1 OmniVista from a previous release, it is recommended that you upgrade AWOS devices to AWOS 4.0.7 after the OmniVista upgrade.

Note: See the *AWOS 4.0.7 Release Notes* for more information on Stellar APs and details on any known issues.

OmniVista 2500 NMS 4.8R1 Upgrade Paths Certified

This release requires an upgrade to the 4.7R1 Patch 2 release before you upgrade to 4.8R1. If you are already running the 4.7R1 Patch 2 release, you can directly upgrade to 4.8R1. Detailed upgrade instructions are available in the *OmniVista 2500 NMS 4.8R1 Installation and Upgrade Guide*.

Note:

- **Standalone Upgrade**
  - 4.7R1 Standalone Installation to 4.7R1 Patch2 Standalone Installation, to 4.8R1 Standalone Installation.
  - To upgrade from older releases to 4.8R1, you must first upgrade to 4.7R1, then 4.7R1 Patch 2.
- **High-Availability (HA) Upgrade** – Note that you must follow the new HA upgrade process in this release. Refer to the *OmniVista 2500 NMS 4.8R1 Installation and Upgrade Guide* for more information.
  - 4.7R1 HA Installation to 4.7R1 Patch 2 HA Installation to 4.8R1 HA Installation.
  - To upgrade from older releases to 4.8R1, you must first upgrade to 4.7R1 HA, then to 4.7R1 Patch 2 HA.
- **Standalone to High-Availability (HA) Conversion**

  You can convert a 4.8R1 Standalone Installation to a 4.8R1 HA Installation if the 4.8R1 Standalone installation was upgraded from a 4.3R2 or newer Standalone Installation.

2.1 Proxy Requirements

OV 2500 NMS 4.8R1 uses external repositories for Application Visibility Signature File updates, ProActive Lifecycle Management (PALM), and the OmniVista 2500 NMS Software Repository, which is used for software updates/upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS 4.8R1 to connect to the OmniVista 2500 NMS External Repository.

2.2 Firewall Requirements

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

- **ALE Central Repository -** ovrepo.fluentnetworking.com
- **AV Repository -** ep1.fluentnetworking.com
- **PALM -** palm.al-enterprise.com
  (Note that the PALM URL was changed from the previous release.)
- **Call Home Backend -** us.fluentnetworking.com
- **Device Fingerprinting Service -** api.fingerbank.org
- **Web Content Filtering –** api.bcti.brightcloud.com.

2.2.1 OmniVista 2500 NMS Ports

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

Service	Port	Source/Destination
SFTP/SSHv2	22	OV Server/Net Device
SFTP	22	SFTP Client/OV Server (via "cliadmin" user)
SSHv2	2222	SSH Client/OV Server (via "cliadmin" user)
Telnet	23	OV Server/Net Device
SNMP Request	161	OV Server/Net Device
SNMP Trap	162	Net Device/OV Server
FTP	21	OV Server/Net Device
TFTP	69	Net Device/OV Server
Policy (QoS) LDAP Server	5389	OV Server/Net Device
sFlow	6343	Net Device/OV Server
Web Server (HTTP)	80	OV Client/OV Server
Web Server (HTTPS)	443	OV Client/OV Server OV Server/Net Device (REST API Polling)
Secure MQTT	1883	Net Device/OV Server

Service	Port	Source/Destination
SMTP	TLS: 25 SSL: 465	OV Server/Third-Party Party SMTP Server
Log-MySQL	3306	UPAM/Log Server
Log-MSSQL	1433	UPAM/Log Server
LDAP	389	UPAM/LDAP Server or AD Server
LDAPS	636	UPAM/LDAP Server or AD Server
Active Directory (AD)	389	UPAM/AD Server
Syslog Listener	514	Net Device/OV Server, UPAM/Syslog Server
RADIUS Authentication	1812	Net Device/UPAM, UPAM/External RADIUS
RADIUS Accounting	1813	Net Device/UPAM, UPAM/External RADIUS
RADIUS CoA – UDP Port	3799	UPAM/Net Device
VMM	135	OV Server/Hyper-V Server
	49152-65535 (RPC Dynamic Port)	Hyper-V Server/OV Server
High-Availability	8000, 5405, 7801	Node 1/Node 2 Node 2/Node 1

2.3 Required Minimum System Configurations

The table below provides required minimum Hypervisor configurations based on the number of devices being managed by OV 2500 NMS 4.8R1 (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
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

	Network Size*			
Configuration	**Low**	**Medium**	**High**	**Very High**
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

*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:

- When provisioning RAM for a new VM for OmniVista, never allocate more memory than is available on the Host Server. For example, if you are running a Host Server with 128GB of memory and have already allocated 96GB of memory to your existing VMs, accounting for the Host Server’s own memory use, you are not left with enough memory to run OmniVista without incident. VM RAM is configured from the Hypervisor.
- Allocate the recommended amount of RAM for the OmniVista VM based on your network size as shown in the above table. In addition, it is recommended that you **reserve** that RAM for the OmniVista VM to prevent performance issues. VM RAM, including reserving VM RAM, is configured on the Hypervisor.
- Set CPU Shares to “High”.
- Do not exceed the number of Logical Processors recommended for your network size as shown in the above table. Hypervisor Processors are configured from the Hypervisor.
- By default, OV 2500 NMS 4.8R1 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 4.8R1 Installation and Upgrade Guide* for instructions on extending the partition.
- OmniVista can be configured to use SNMPv3 to communicate with devices. When editing this configuration, you can specify which algorithms should be used. A recommended algorithm is AES ("Advanced Encryption Standard"). To get the best performance from your hypervisor, we recommend that you use Intel processors with the AES-NI instruction set enabled.
- AES-NI was introduced by Intel in 2010 in its Westmere family of processors and allows your hypervisor and its VMs to manage AES-related workloads natively. To realize the full benefits of AES-NI, you need to ensure that it is made available to the VM running OmniVista. To do this:
  - Your hypervisor's CPUs must be newer CPUs (> 2010)

  - AES-NI must be enabled in your hypervisor's BIOS
  - The AES-NI feature must not be "masked" by your hypervisor.
- By default, VMWare and Hyper-V are "pass-through" meaning that OmniVista's VM will be able to use AES acceleration. When using VirtualBox, please verify that "Nested paging" is enabled.
- The High-Availability Feature supports up to 4,000 devices.

Important Note: For OV 2500 NMS 4.8R1, Stellar APs in your network should be running a minimum AWOS version of 4.0.1 (AWOS 4.0.7 is recommended). **First** upgrade to OV 2500 NMS 4.8R1; then upgrade your Stellar APs. Please refer to the *OmniVista 2500 NMS 4.8R1 Installation Guide* for details.

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

See the *AWOS 4.0.7 Release Notes* for more information on Stellar APs and details on any known issues.

2.4 High-Availability Installation Limitations

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

- Cluster IP configuration in L3 Cluster
- Converting 4.8R1 Standalone to 4.8R1 HA if the 4.8R1 Standalone was upgraded from 4.3R1 Standalone. (You can convert 4.8R1 Standalone to 487R1 HA if the 4.8R1 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.

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 4.8R1 from OV 2500 NMS OV 2500 NMS 4.7R1 Patch 2. See the *OmniVista 2500 NMS 4.8R1 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 4.8R1, 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 4.8R1 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 4.8R1 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 4.8R1 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 4.8R1 Services must be started to launch OV 2500 NMS 4.8R1. By default, Watchdog should start automatically when OV 2500 NMS 4.8R1 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 4.8R1

After launching OV 2500 NMS 4.8R1 for the first time, log in using the Default Username and Password:

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

Note: If you are launching OV 2500 NMS 4.8R1 for the first time after upgrading from a previous version, do a hard refresh (Shift+F5) of your browser window to ensure the display of the latest UI.

5.0 Known Problems

5.1 Known AP Registration Problems

5.1.1 Some Charts in the Statistics Application Do Not Support Chinese

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

Workaround: No workaround at this time.

PR# OVE-7596

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

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

Workaround: Set another web browser as your default browser.

PR# OVE-2096

5.1.3 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

5.1.4 SNMPv3 Username/Password Must Not Contain Certain Special Characters

If the SNMPv3 username/password contains the following special characters, communication with the SNMPv3 agent will fail:

- Password includes a dollar sign (for example, 123$).
- Password includes quotation marks (for example, "123").
- Password includes () (for example, (123)).
- Username starts with a dollar sign (for example, $123)

Workaround: Do not include any of the above special characters in the SNMPv3 Username/Password.

PR# OVE-12152

5.1.5 Syslog Over TLS Certificate Name Must Not Contain a Space

When creating a Syslog Over TLS Certificate, make sure there are no spaces in the certificate name. For example, "SyslogTLS" is correct, but "Syslog TLS" is not correct and will not be accepted.

Workaround: Specify a certificate name that does not contain any spaces.

PR# OVE-12702

5.3 Known Discovery Problems

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

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

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

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

Workaround: No workaround at this time.

PR# OVE-2264

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

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

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

PR# OVE-2198

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

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

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

PR# OVE-11112

5.3.5 Can't Display Running Directory Information for NaaS Device in Degraded Mode

When you launch an SSH session to a NaaS device in the Degraded License Mode and send the **show running-directory** command, an error message is displayed. For example:

```
-> show running-directory
ERROR: CLI commands are blocked in NaaS license degraded mode.
```

Workaround: No workaround at this time.

PR# OVE-11416

5.3.6 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-11475

5.4 Known Locator Problems

5.4.1 Cannot Locate End Stations Connected to OS2220

Unable to locate end stations connected to OS2200 Switch.

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

PR# OVE-1226

5.5 Known mDNS Problems

5.5.1 Video Source Unable to Discover Chromecast on Different VLAN

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

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

PR# OVE-8941

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

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

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

PR# OVE-9848

5.5.3 Video Source Able to Cast Video After mDNS Responder Disabled

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

Workaround: Informational.

PR# OVE-9112

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

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

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

PR# OVE-11033

5.5.5 Deleting a Responder Device Fails

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

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

Workaround: Restart the mDNS service to bypass this issue.

PR# OVC-8876

5.6 Known Notifications Problems

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

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

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

PR# OVE-3759

5.6.2 The alaNaasLicenseInstalledAlert Trap Shows the Wrong Value

When a Naas license (Management, Upgrade, Essential, Advanced) is installed on a switch, the alaNaasLicenseInstalledAlert trap is sent. However, when the trap is viewed on the Notifications Home Screen (Network – Notifications) the trap displays incorrect values.

Workaround: No workaround at this time.

PR# OVE-11374

5.6.3 The NaaS VC Device Sends the alaNaasInconsistentModeAlert Trap Multiple Times

When a device in a VC configuration changes mode (for example, CAPEX to NaaS), the alaNaasInconsistentModeAlert trap is sent multiple times and absorbed into the trapAbsorptionTrap. The alaNaasInconsistenModeAlert Trap should only be sent once when an inconsistent mode is detected.

Workaround: No workaround at this time.

PR# OVE-11414

5.6.4 The NaaS License Expiry Time is Reported in the Number of Whole Days Remaining until the License Expires

On a NaaS device, the **show naas license** CLI command displays the Expiry Time. This reflects the number of whole days (24 hours/day) until the license expires. For example, If the time remaining until expiration is 30 days and 21 hours, the Expiry Time is reported as 30 days not 31 days.

A NaaS device sends the alaNaasExpirtyDayAlert trap at 30 days, 7 days, and 0 days. If the remaining time before the license expires is 10 hours, this trap is not sent until those 10 hours have elapsed. However, the Expiry Time will show “0 days”.

Workaround: No workaround at this time.

PR# OVE-11415

5.6.5 The Days Left for Expiry is Incorrect for an AP NaaS License

The “Days Left for Expiry” field on the NaaS License Information on Device screen does not display the correct number of days until the license expires for an AP device.

Workaround: Refer to the “Expiry Date” field instead.

PR# OVC-9151

5.7 Known PolicyView Problems

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

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

Workaround: No workaround at this time.

PR# 201688

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

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

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

PR# OVE-653

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

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

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

PR# OVE-678

5.8 Known Resource Manager Problems

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

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

Workaround: No workaround at this time.

PR# 219688

5.9 Known Topology Problems

5.9.1 AMAP Entries for ERP-RPL Links Are Not Always Displayed

AMAP is a proprietary protocol and has been deprecated, so AMAP Entries for ERP-RPL Links are not always displayed.

Workaround: AMAP Adjacency Protocol functionality on the switch does not work properly with ERPv2 in case of ERP-RPL link, which may affect ERPv2 functionality. Use LLDP as the adjacency protocol when working with ERPv2.

PR# 177202

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

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

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

PR# OVE-1491

5.9.3 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

5.10 Known Unified Access Problems

5.10.1 Device Config - Port and Dynamic Service Access Auth Profile Displayed Incorrectly for OS6900-Q32/X72

Device Config - Port and Dynamic Service Access Auth Profile Displayed Incorrectly for OS6900-Q32/X72 switches.

Workaround: Switch issue. No workaround at this time.

PR# 219133

5.10.2 Device Config - Cannot View Access Role Profile of AOS 8.2.1 Devices

Cannot view Access Role Profiles on Device Config Screen.

Workaround: No workaround at this time.

PR# 220259

5.10.3 Unified Policy Sometimes Works Abnormally

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

Workaround: Do not turn on the Reflexive option.

PR# OVE-10083

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

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

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

PR# OVE-10696

5.11 Known UPAM Problems

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

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

Workaround: There is no workaround at this time.

PR# OVE-779

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

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

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

PR# OVE-818

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

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

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

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

PR# OVE-833

5.11.4 Cannot Fully Customize UPAM Captive Portal Page

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

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

PR# OVE-834

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

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

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

PR# OVE-1693

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

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

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

PR# OVE-2025

5.11.7 802.1X Authentication with External Windows LDAP Failed When Logging in with User Credential

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

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

PR# OVE-3000

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

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

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

PR# OVE-4999

5.11.9 No IPv4 or IPv6 Value Displayed in UPAM Authentication Record

Client IP address is not displayed in UPAM Authentication Record.

Workaround: No workaround at this time.

PR# OVC-6061

5.11.10 Radius Service Cannot Start After Secure LDAP Server is Stopped

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

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

PR# OVE-8986

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

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

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

PR# OVE-9528

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

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

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

PR# OVE-10128

5.11.13 WiFi4EU not Connected to Captive Portal

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

Workaround: Change the validity period to 24 hours.

PR# OVE-11164

5.11.14 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

5.11.15 OmniVista ClearPass Integration Fails When Adding APs to AP Group

When a new AP is added to an AP Group, the configuration is not automatically added to the ClearPass Device List or the AP. Automatic synchronization with ClearPass when a new AP device is added to an AP Group is not supported.

Workaround: Use the “override” function to re-apply the ClearPass configuration to the new AP devices.

PR# OVE-12378

5.12 Known Users and User Groups Problems

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

In OV 4.3R1, Performance Monitoring is a new feature and you can configure permissions of Analytics and Performance Monitoring application separately. However, if you upgrade to OV 4.3R1 from OV 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

5.13 Known VM Manager Problems

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

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

Workaround: N/A

PR# 163314

5.13.2 VMM Locator VM Count Can Be Greater Than VMM License VM Count or Reported by vCenter

If VMs are using multiple Physical NIC Interfaces, the same VM will be bound to different MAC Addresses and OmniVista 2500 NMS will display multiple rows for the VM in VMM Locator search and browse applications. However, this will not affect VM Manager Licensing. The VMM License Manager will count multiple references as single Virtual Machine its UUID and the count will match the number of Virtual Machines reflected in vCenter.

Workaround: N/A

PR# 163885

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

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

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

PR# 174181

5.14 Known Web Content Filtering Problems

5.14.1 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

5.14.2 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

5.15 Known WLAN Problems

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

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

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

1. GRE Tunnel from AP to AOS Switch - This is the typical Guest Tunnel uses case where AOS acts as the Guest Tunnel Termination Switch. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".

2. GRE Tunnel from AP to Non-AOS Switch/Server (e.g., Nokia 7750 SR/Standard Linux Tunnel Server) - This is the Guest Tunnel use case with a non-AOS switch. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by the Switch/Server.

3. GRE Tunnel Between AP and OV VPN Server Appliance - This is the regular Data VPN tunnel use case between Remote APs and OV VPN Server acting as the Data VPN Server. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by OV VPN Server.

4. GRE Tunnel from AP to AOS Switch, Over the Data VPN tunnel Between AP and OV VPN Server Appliance - This is a rare use case of using the Data VPN tunnel to reach from a Remote site where the AP is located, to the Central Site where the AOS Switch is located. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".

The following combinations of values are not supported:

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

5.15.2 AP1321 Advertises Incorrect SSID Name in Some Cases

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

Workaround: No workaround at this time.

PR# OVE-9545

5.15.3 Client Name Field Blank for Clients Running iOS 14

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

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

PR# OVC-8287

5.15.4 Intrusive AP Page and Widget Time Out When Loading Data

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

Workaround: No workaround at this time.

PR# OVE-9693

5.15.5 RF Profile Not Supported on AP1201BG

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

Workaround: No workaround at this time.

PR# OVE-10781

5.15.6 WMA in a Not Responding State on the Standby Node

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

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

PR# OVE-10513

5.15.7 Social Login Fail with Google Account

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

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

PR# OVC-8901

5.15.8 Stellar AP Connectivity to OS22x60 does not Work

The trust VLAN tag option on OS22x60 ports connected to a Stellar AP does not work. As a result, the wireless client VLAN-tagged traffic forwarded by the AP to the switch is blocked.

Workaround: No workaround at this time.

PR# OVE-11467

5.15.9 The 6GHz SSID Interface Will Not Function if PMF State Is Not Set to “Required”

When 6GHz is part of the selected band for an SSID, the correct Protected Management Frame (PMF) setting is “Required”. If you change the PMF state to “Optional”, the 6GHz SSID interface will not function.

Workaround: Do not change the PMF state to “Optional” when configuring 6GHz SSID.

PR# OVE-12727

5.16 Known Other Problems

5.16.1 U-Boot Version for OS6450 Devices Shows as "NA" in Inventory Report

U-Boot Version for OS6450 Devices Shows as "NA" in OmniVista 2500 NMS Inventory Report.

Workaround: This is a hardware issue with the OS6450. No workaround at this time.

PR# 181085

5.16.2 Unable to Access Web UI Using IP Address on I/E

Unable to access Web UI using IP address on Internet Explorer browser, locally on a Windows 2012 R2 system.

Workaround: Have the correct mapping for 'localhost' in the hosts file and use 'localhost' instead of IP address to access the Web UI locally.

PR# 194913

5.16.3 Apostrophe Is an Invalid Character in SNMP Community String

Apostrophe Is an Invalid Character in SNMP Community String.

Workaround: Remove Apostrophe from the SNMP community string.

PR# 195715

5.16.4 OV Hostname Cannot Be More than 15 Characters

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

Workaround: Informational.

PR# CRNOV-793

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

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

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

PR# OVE-1568

5.16.6 Failover During VM Sync in HA Installation

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

Workaround: If it was a temporary problem with the Active Node that caused the failover, the Active Node may come up again and complete the sync. If the Active Node is permanently down, SSH to the Standby Node. On the HA Virtual Appliance Menu select **3 – Configure Cluster**, then select **14 – Cluster Error Check**. When the error check is complete, the Standby Node will come up as the Active Node. Note that it may not have the most recent data since the sync was interrupted.

PR# OVE-1629

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

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

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

PR# OVE-1776

5.16.8 WMA/UPAM Memory Not Updated After Upgrade

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

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

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

PR# OVE-1993/2048

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

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

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

PR# OVE-2127

5.16.10 OmniVista Cannot be Accessed by Web Client

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

Workaround: Restart ovclient or tomcat service.

PR# OVE-2220

5.16.11 Unsupported Features in High-Availability (HA) Installation

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

- Cluster IP configuration in L3 Cluster
- You cannot convert a 4.5R2 Standalone installation to an HA installation if the 4.5R2 Standalone installation was upgraded from a 4.3R1 Standalone installation.
- Changing the OmniVista IP address and Hostname after creating the Cluster.
- Memory synchronization. When the active service is not available and failover happens, the data in memory of that service will be lost.
- Failover while re-syncing between nodes.

Workaround: NA

PR# OVE-2327

5.16.12 Failover Banner Directs User to Inoperable HA Standby Node

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

Workaround: Informational.

PR# OVE-3113

5.16.13 Offline Upgrade from 4.3R3 to 4.4R1 Failed

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

Workaround: Contact Customer Support for Offline Upgrades

PR# OVE-5006

5.16.14 Cannot Push Policy with IPv6 Conditions to AOS 6.4.6

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

Workaround: Upgrade to a supported build.

PR# OVE-5793

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

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

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

PR# OVC-7240

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

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

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

PR# OVE-8050

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

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

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

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

PR# OVE-8019

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

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

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

PR# OVE-8874

5.16.19 OV Restore Fails with Error “Failed to Start ovldap Service

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

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

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

PR# OVE-9782

5.16.20 VA Console Displays Error Message when Joining Cluster

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

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

PR# OVE-10576

5.16.21 OmniVista Does Not Detect When a New NIC is Added

When you add or remove a NIC for OmniVista, the change is not detected in the Hypervisor console. For example, if a new NIC is added, it doesn’t show up in the console (menu option 2, menu option 17).

Workaround: Reboot OmniVista to detect NICs added or removed in the Hypervisor

PR# OVE-12647

5.16.22 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

5.16.23 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

6.0 Release Notes PRs Fixed

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

6.1.1 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"

CR/PR Number	Description
	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. **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

CR/PR Number	Description
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 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.

CR/PR Number	Description
	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. **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

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

CR/PR Number	**Description**
CRNOV-4841 OVE-12474	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. **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

CR/PR Number	Description
	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:** 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

CR/PR Number	Description
	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
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

6.1.2 Release Notes PRs Fixed

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

6.2 PRs Fixed Since 4.7R1 GA

6.2.1 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.

6.3 PRs Fixed Since 4.6R2

6.3.1 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

6.3.2 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)

6.4 PRs Fixed Since 4.6R1

6.4.1 Customer PRs

CR/PR Number	Description
Case: **00591018** *OVE-11396*	**Summary:** 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:	**Summary:**

CR/PR Number	Description
00578171 *OVE-11252*	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

6.4.2 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)

6.5 PRs Fixed Since 4.5R3

6.5.1 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” Click for Additional Information

CR/PR Number	Description
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 Click for Additional Information

CR/PR Number	Description
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 Click for Additional Information

CR/PR Number	Description
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

6.5.2 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)

6.6 PRs Fixed Since 4.5R2

6.6.1 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
Case: **00508695** *OVE-9949*	**Summary**: OV 2500 Generating a report is blank in "Managed Devices". Click for Additional Information

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

CR/PR Number	Description
	Click for Additional Information

6.6.2 Release Note PRs Fixed

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

6.7 PRs Fixed Since 4.5R1

6.7.1 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: **00468024** *OVC-7743*	**Summary:** OV Cirrus - Tunnel Profile creation failed on OV Cirrus. Click for Additional Information
Case: **00440153** *OVE-8105*	**Summary:** OV 2500 - Quarantine Manager not blocking the intruder MAC Click for Additional Information
Case:	**Summary:** OV 2500 - Unable to install the VMware tools

CR/PR Number	Description
00467694 *OVE-8495*	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: **00461232** *OVE-8210*	**Summary:** OV 2500 - Firmware version cannot be set for AOS 8.x devices in the Auto Configuration's instruction file Click for Additional Information
Case: **00447382** *OVE-8888*	**Summary:** OV 2500 - External web session from OV Click for Additional Information
Case:	**Summary:** OV 2500/OV Cirrus - WiFi4EU Captive Portal does not display correctly.

CR/PR Number	Description
00462741 *CRNOV-1967*	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. 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

CR/PR Number	Description
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
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

CR/PR Number	Description
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
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

CR/PR Number	Description
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
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

CR/PR Number	Description
Case: **00503755** *OVE-9487*	**Summary:** OV 2500 – service ovclient stuck to “starting” Click for Additional Information

6.7.2 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)

6.8 PRs Fixed Since 4.4R2

6.8.1 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
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

CR/PR Number	Description
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
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

CR/PR Number	Description
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
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

CR/PR Number	Description
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
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

CR/PR Number	Description
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)

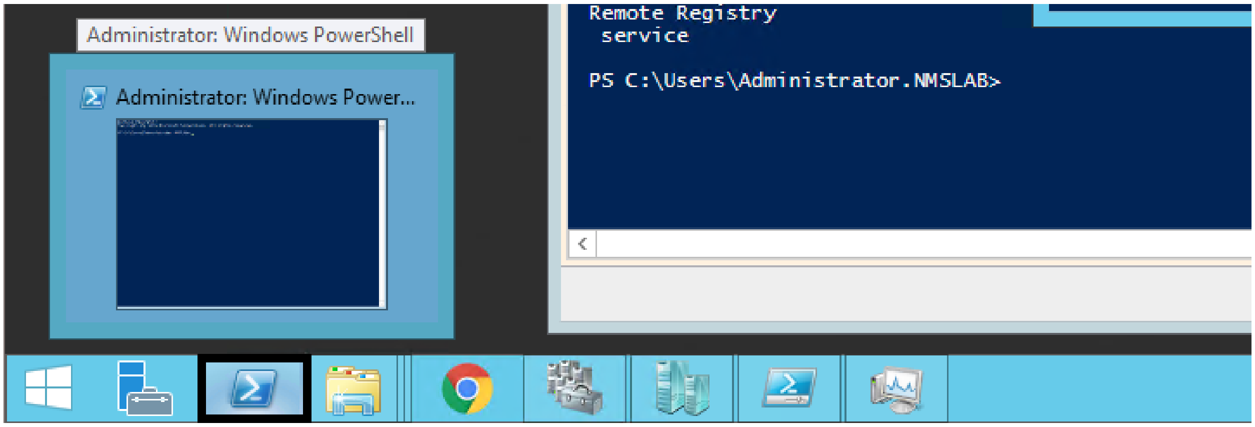
The following steps are specific to Windows 64 bit only.

1. Log in Hyper-V Server.

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

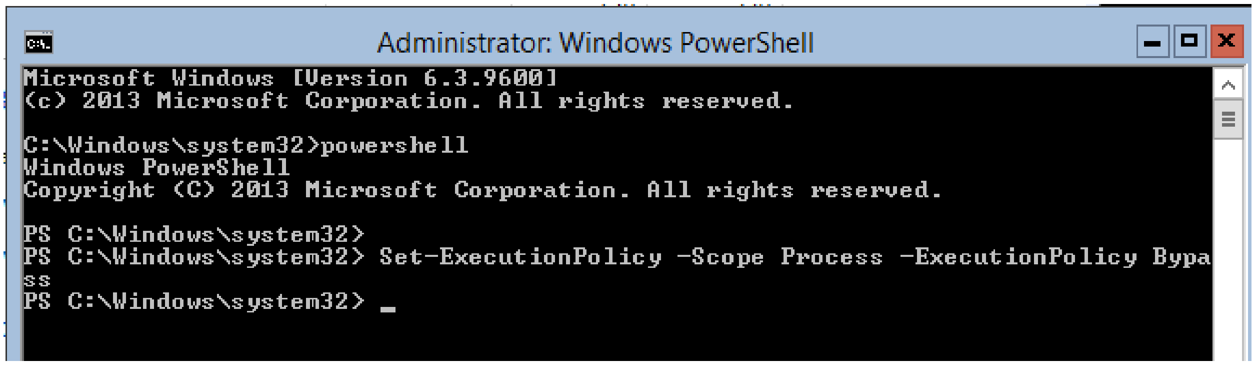
HyperV_Enable_DCOM_x64.ps1

3. Run Powershell.


Administrator: Windows PowerShell
Administrator: Windows Power...

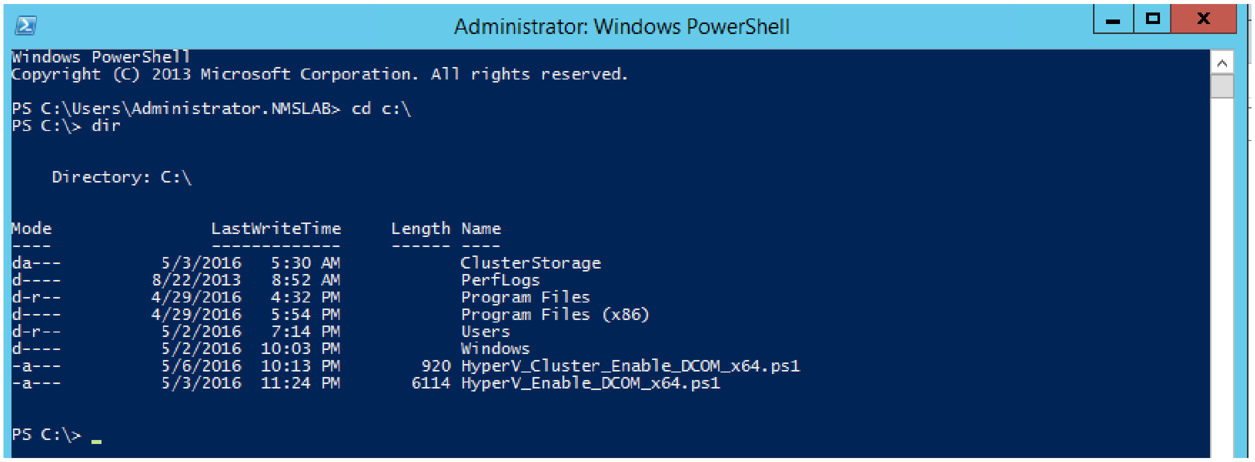
```
Remote Registry
 service

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

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



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

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

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

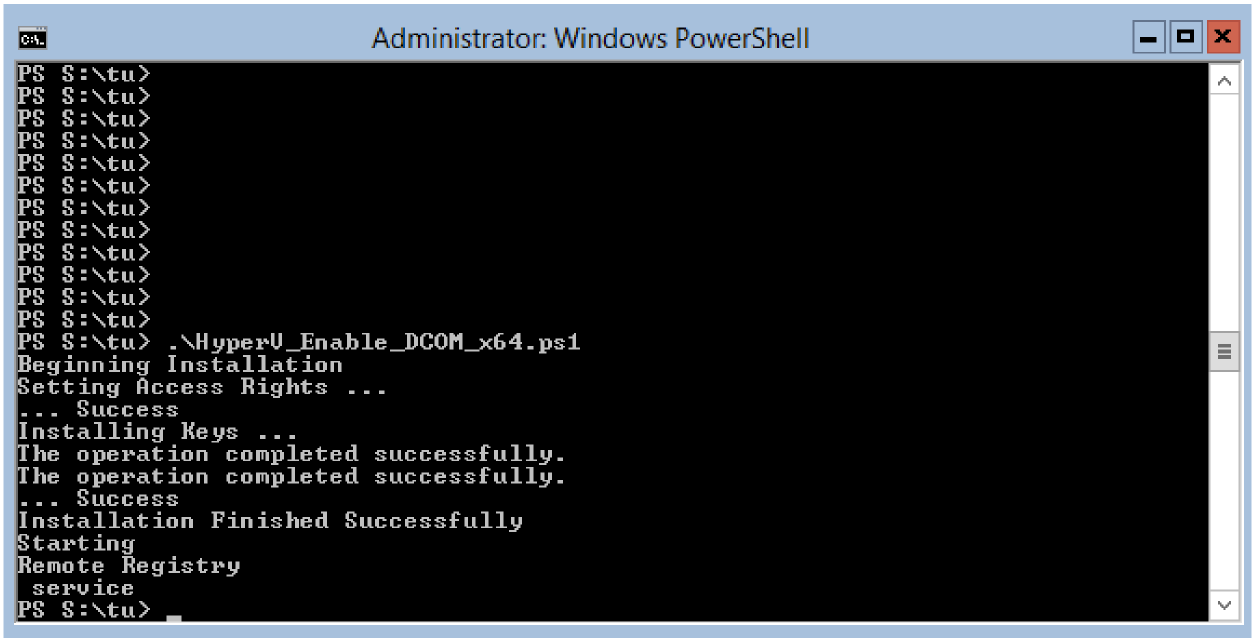
5. Change to the directory that contains the downloaded script from Step 2.



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

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


    Directory: C:\


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


PS C:\> _
```

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

7. Run .\HyperV_Enable_DCOM_x64.ps1.



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

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

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

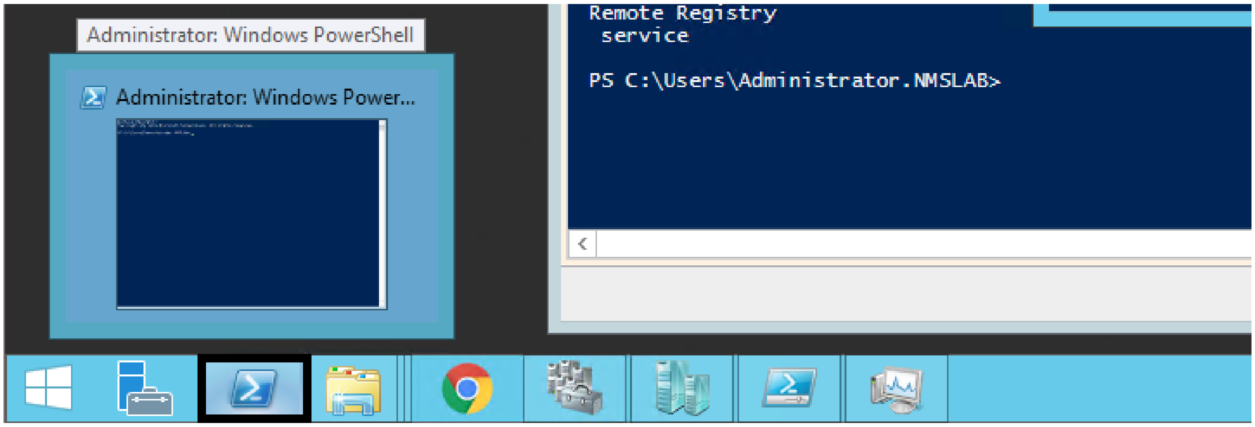
2. Download both files from the attachment and place them on the same directory:
HyperV_Cluster_Enable_DCOM_x64.ps1

HyperV_Cluster_Enable_DCOM_x64.ps1

HyperV_Enable_DCOM_x64.ps1

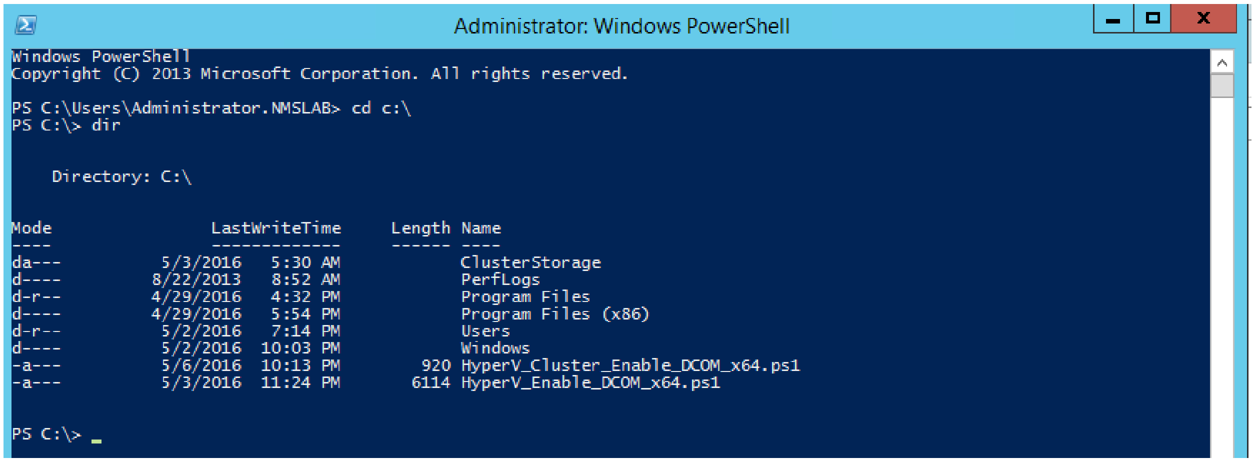
HyperV_Enable_DCOM_x64.ps1

3. Run Powershell.


Administrator: Windows PowerShell
Administrator: Windows Power...

```
Remote Registry
 service

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

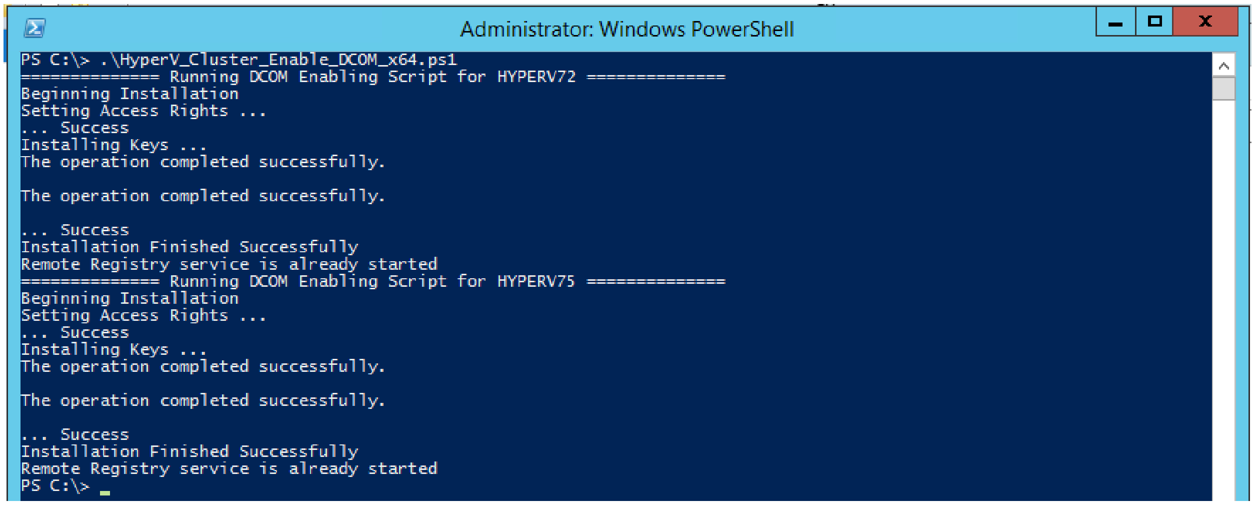
4. Change to the directory that contains the downloaded scripts from Step 2.



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

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


    Directory: C:\


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


PS C:\> _
```

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

6. Execute HyperV_Cluster_Enable_DCOM_x64.ps1.

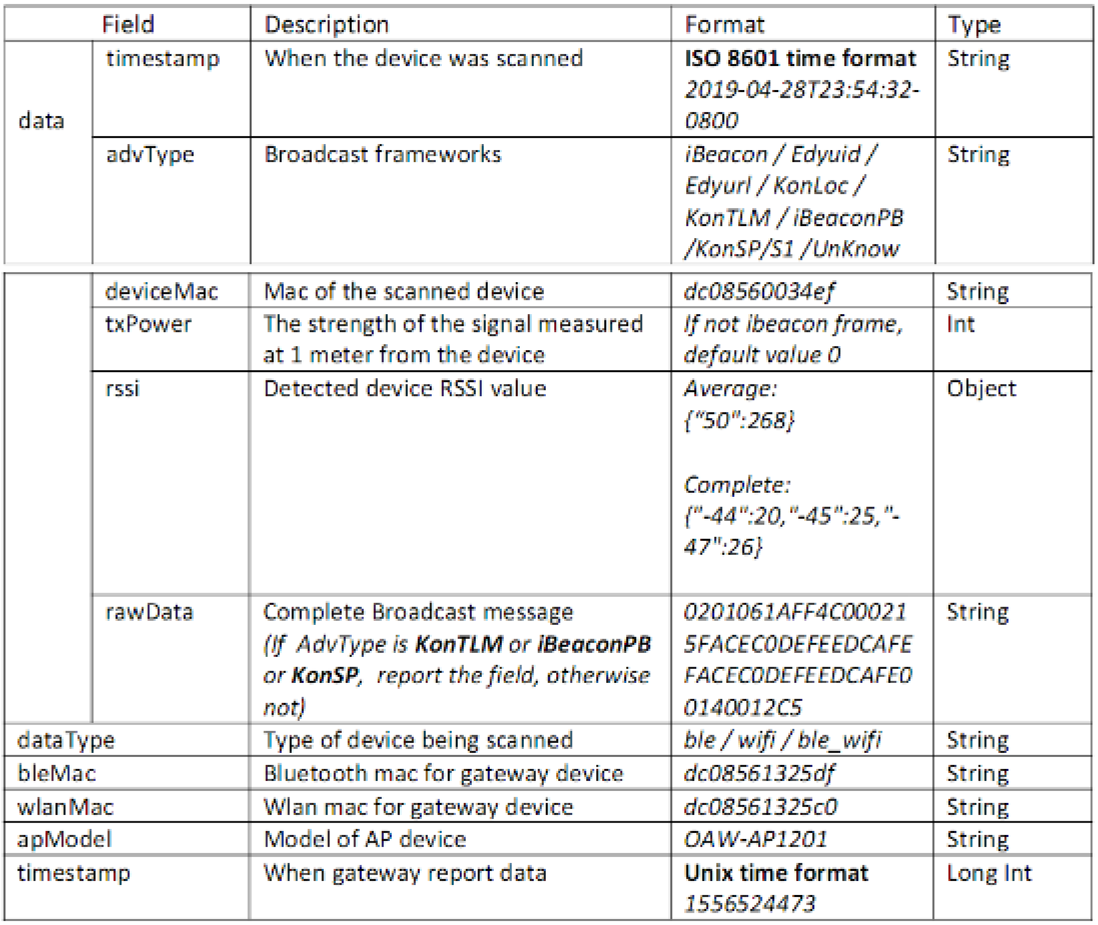


```
PS C:\> .\HyperV_Cluster_Enable_DCOM_x64.ps1
============== Running DCOM Enabling Script for HYPERV72 ==============
Beginning Installation
Setting Access Rights ...
... Success
Installing Keys ...
The operation completed successfully.

The operation completed successfully.

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

The operation completed successfully.

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

Appendix B – Stellar BLE Data Format

Consider the following information and data format that is used to send BLE messages to third-party Asset Tracking applications:

- The payload data format of the Bluetooth gateway report is an array of JSON, which contains one or more Bluetooth device information scanned in a reporting cycle.
- The reported information includes information about the scanned Bluetooth device and the Bluetooth gateway. Consider the following data format used to report the scanned information.



Field		Description	Format	Type
data	timestamp	When the device was scanned	**ISO 8601 time format** *2019-04-28T23:54:32-0800*	String
	advType	Broadcast frameworks	*iBeacon / Edyuid / Edyurl / KonLoc / KonTLM / iBeaconPB /KonSP/S1 /UnKnow*	String
	deviceMac	Mac of the scanned device	*dc08560034ef*	String
	txPower	The strength of the signal measured at 1 meter from the device	*If not ibeacon frame, default value 0*	Int

	rssi	Detected device RSSI value	*Average:*
			{"50":268}
			Complete:
			{"-44":20,"-45":25,"-47":26}
				Object

	rawData	Complete Broadcast message *(If AdvType is **KonTLM** or **iBeaconPB** or **KonSP**, report the field, otherwise not)*	*0201061AFF4C000215FACECODEFEEDCAFEFACECODEFEEDCAFE00140012C5*	String
dataType		Type of device being scanned	*ble / wifi / ble_wifi*	String
bleMac		Bluetooth mac for gateway device	*dc08561325df*	String
wlanMac		Wlan mac for gateway device	*dc08561325c0*	String
apModel		Model of AP device	*OAW-AP1201*	String
timestamp		When gateway report data	**Unix time format** *1556524473*	Long Int

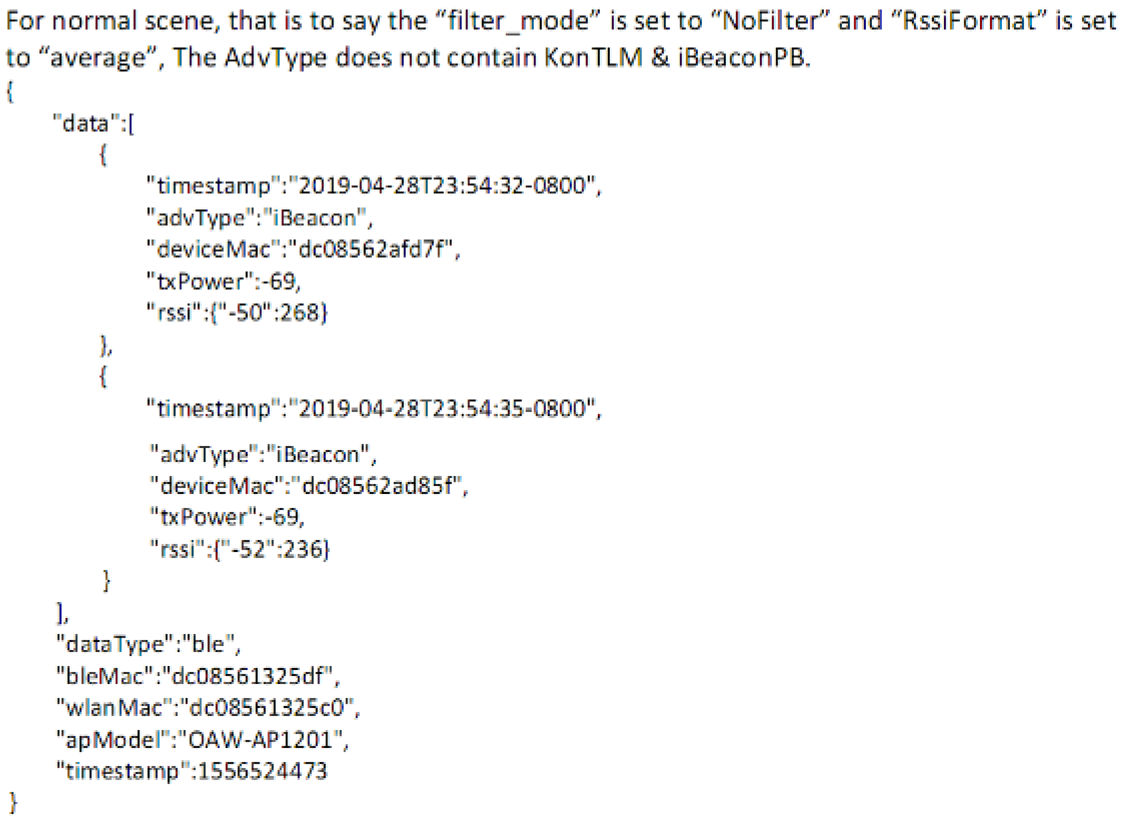
Notes:

1. To get smoothing BLE data, if the RssiFormat is “average” and the number of scans in a reporting cycle is greater than three, the highest and lowest values are removed and the average value is taken.
2. To include the channel of the BLE channel of collected RSSI:
    a. BLE has only three fixed broadcast channels, and in a broadcast event, a broadcast packet is transmitted on each channel. As a result, it is not possible for the scanning device to specify that the scanning should take place on a specific channel.

b. In a scanning event, the device will scan three channels in turn, and the scanned response data does not contain the channel.

c. If it is the scanning channel of the WiFi, that is supported.

The reporting JSON data format is similar to the following:



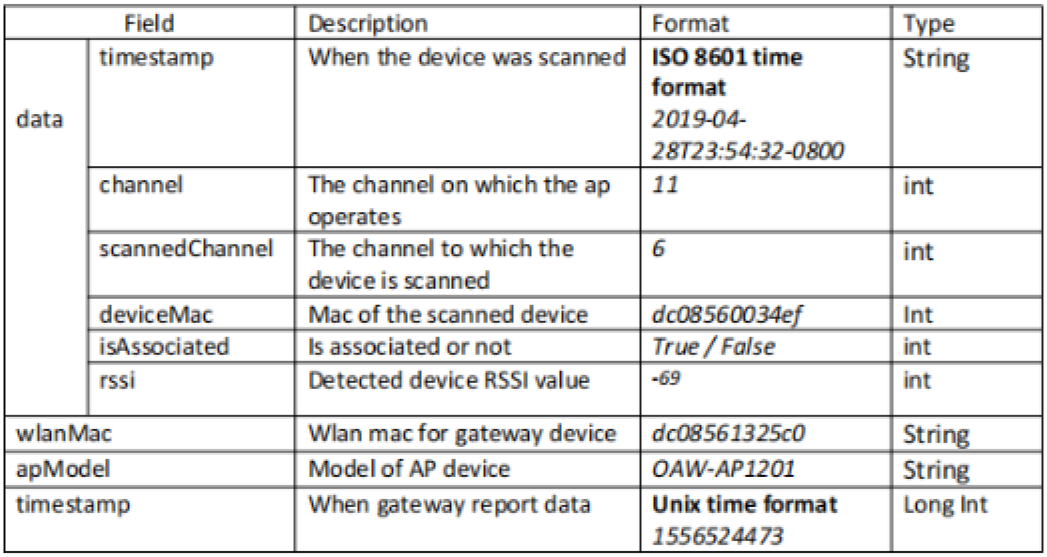
For normal scene, that is to say the “filter_mode” is set to “NoFilter” and “RssiFormat” is set to “average”, The AdvType does not contain KonTLM & iBeaconPB.

```
{
    "data":[
        {
            "timestamp":"2019-04-28T23:54:32-0800",
            "advType":"iBeacon",
            "deviceMac":"dc08562afd7f",
            "txPower":-69,
            "rssi":{"-50":268}
        },
        {
            "timestamp":"2019-04-28T23:54:35-0800",
            "advType":"iBeacon",
            "deviceMac":"dc08562ad85f",
            "txPower":-69,
            "rssi":{"-52":236}
        }
    ],
    "dataType":"ble",
    "bleMac":"dc08561325df",
    "wlanMac":"dc08561325c0",
    "apModel":"OAW-AP1201",
    "timestamp":1556524473
}
```

Appendix C - Stellar WiFi RTLS Data Format

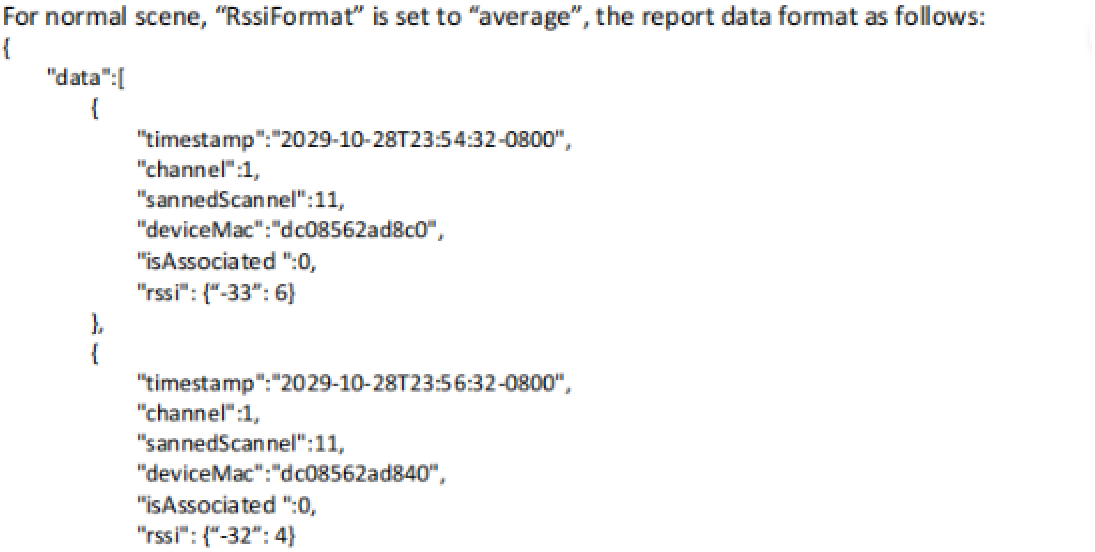
Consider the following information and data format that is used to send WiFi RTLS data to third-party RTLS applications:

- The payload data format of the gateway report is an array of JSON, which contains one or more WiFi device information scanned in a reporting cycle.
- The reported information includes information about the scanned WiFi device and the gateway. Consider the following data format used to report the scanned information.



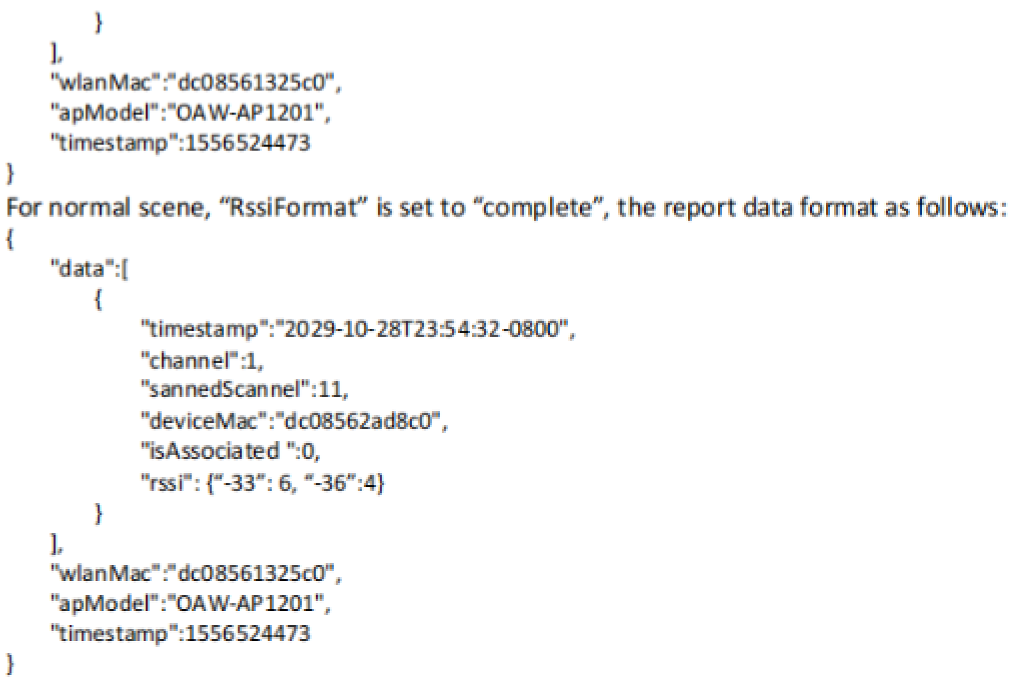
Field		Description	Format	Type
data	timestamp	When the device was scanned	**ISO 8601 time format** *2019-04-28T23:54:32-0800*	String
	channel	The channel on which the ap operates	*11*	int
	scannedChannel	The channel to which the device is scanned	*6*	int
	deviceMac	Mac of the scanned device	*dc08560034ef*	Int
	isAssociated	Is associated or not	*True / False*	int
	rssi	Detected device RSSI value	*-69*	int
wlanMac		Wlan mac for gateway device	*dc08561325c0*	String
apModel		Model of AP device	*OAW-AP1201*	String
timestamp		When gateway report data	**Unix time format** *1556524473*	Long Int

The reporting JSON data format is similar to the following:



For normal scene, “RssiFormat” is set to “average”, the report data format as follows:

```
{
    "data":[
        {
            "timestamp":"2029-10-28T23:54:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad8c0",
            "isAssociated ":0,
            "rssi": {“-33”: 6}
        },
        {
            "timestamp":"2029-10-28T23:56:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad840",
            "isAssociated ":0,
            "rssi": {“-32”: 4}
```



```
        }
    ],
    "wlanMac":"dc08561325c0",
    "apModel":"OAW-AP1201",
    "timestamp":1556524473
}
```

For normal scene, “RssiFormat” is set to “complete”, the report data format as follows:

```
{
    "data":[
        {
            "timestamp":"2029-10-28T23:54:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad8c0",
            "isAssociated ":0,
            "rssi": {“-33”: 6, “-36”:4}
        }
    ],
    "wlanMac":"dc08561325c0",
    "apModel":"OAW-AP1201",
    "timestamp":1556524473
}
```

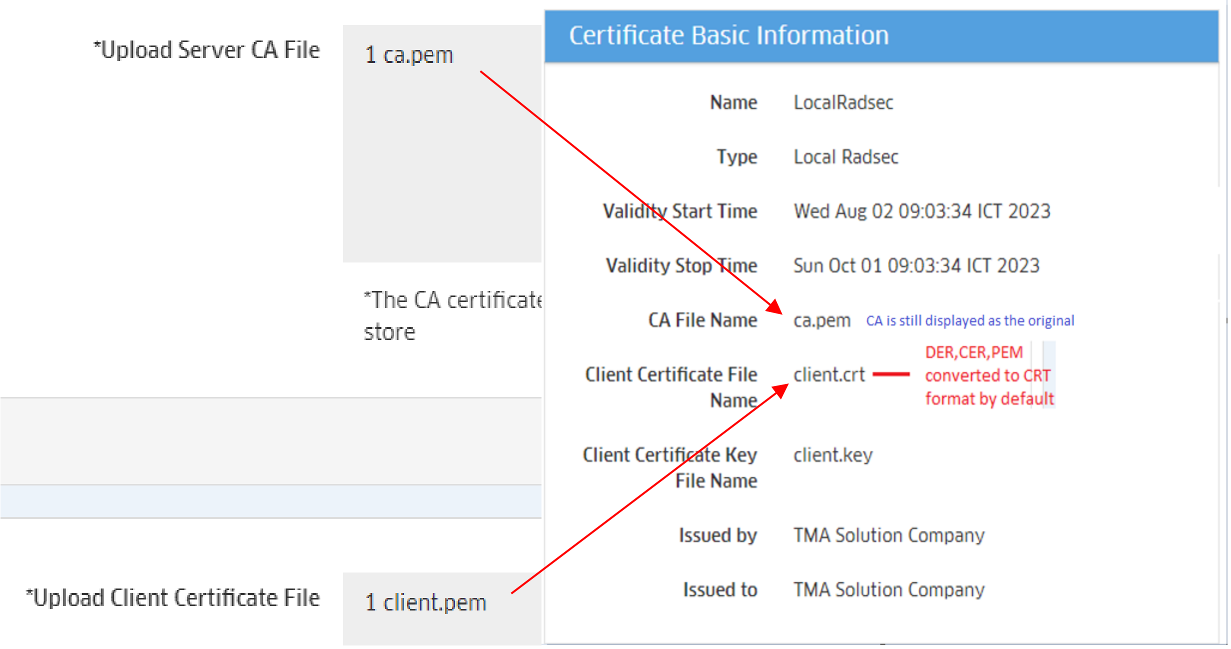
Appendix D – Local RadSec Certificate

Local RadSec Certificate in OmniVista is supported to provide a TLS-enabled connection between RadSec Client (Stellar AP) and RadSec Server (TLS-enabled RADIUS server). Creating a certificate consists of four ingredients: CA, Client Certificate, Client Key and Password for the Key. From OmniVista, an Admin user can push these certificates to the AP by selecting the Local RadSec option in the AP Group.

To create a Local RadSec Certificate in OmniVista, you must upload and import three ingredient files:

- **CA Certificate file:** Supports only PEM or DER encoded certificates (e.g. .pem .cer. der .crt) and multiple CAs with issuance order.
- **Client Certificate file:** Supports only PEM or DER encoded certificates. However, OV will translate all acceptable formats to **.crt** format due to AP's requirement.
- **Client Key file:** Supports only **.key** file.

And, Password for Client Key.



*Upload Server CA File: 1 ca.pem

*The CA certificate store

*Upload Client Certificate File: 1 client.pem

Certificate Basic Information

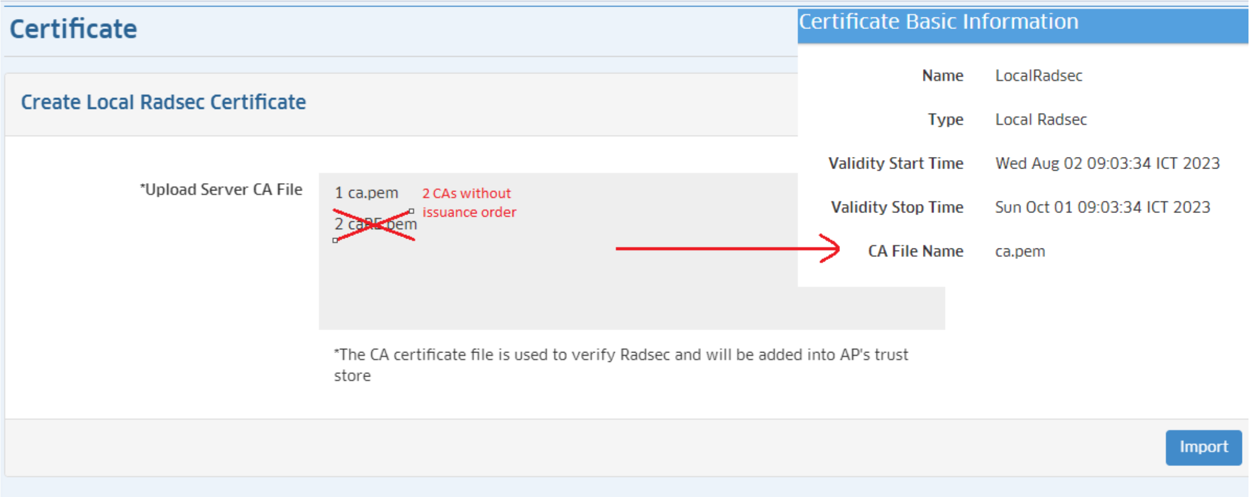
Name	LocalRadsec
Type	Local Radsec
Validity Start Time	Wed Aug 02 09:03:34 ICT 2023
Validity Stop Time	Sun Oct 01 09:03:34 ICT 2023
CA File Name	ca.pem
Client Certificate File Name	client.crt
Client Certificate Key File Name	client.key
Issued by	TMA Solution Company
Issued to	TMA Solution Company

CA is still displayed as the original

DER,CER,PEM converted to CRT format by default

Notes:

1. Do not import multiple CAs without an issuance order. If you import multiple CAs without an issuance order, OmniVista only parses and applies the first one to the AP.



Certificate

Create Local Radsec Certificate

*Upload Server CA File

1 ca.pem

~~2 caRE.pem~~

2 CAs without issuance order

*The CA certificate file is used to verify Radsec and will be added into AP's trust store

Certificate Basic Information

Name	LocalRadsec
Type	Local Radsec
Validity Start Time	Wed Aug 02 09:03:34 ICT 2023
Validity Stop Time	Sun Oct 01 09:03:34 ICT 2023
CA File Name	ca.pem

2. Make Client Certificate and Client Key in two files separately. Client Certificate file should not include Client Key because when OmniVista converts certificate to CRT format, only the certificate part is converted, and the private key part is ignored.
3. CA Certificate file will be converted to CRT format and applied to AP, but content of the Certificate part is not changed.