Release Notes

for

OmniVista 2500 NMS Version 3.5.2

May 2012

Revision D

Part Number 032722-10

READ THIS DOCUMENT

Includes OmniVista for
Windows Server 2008/XP/Vista
Sun Solaris Systems
Red Hat Linux
Suse Linux

Alcatel-Lucent Corporation
26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500
(818) 880-3505 Fax

Table of Contents

Table of Contents (continued)

Revision History

Release	Revision	Date	Description of Changes
3.5.2	D	05/09/12	Maintenance Release
3.5.2	C	12/09/11	Maintenance Release
3.5.2	B	06/01/11	Release Notes Update
3.5.2	A	05/04/11	GA Release
3.5.1	B	10/12/10	Maintenance Release
3.5.1	A	08/04/10	GA Release
3.5	A	10/09/09	GA Release
3.4.2	A	11/13/08	GA Release
3.4.1	A	08/01/08	GA Release
3.4	B	02/19/08	Release Notes Update
3.4	A	11/30/07	GA Release
3.3	A	02/08/07	GA Release
3.1	B	08/15/06	GA Release
3.1	A	07/14/06	Pre-GA Release
3.0.1	BF	06/15/06	GA Release
3.0	BE	04/12/06	Release Notes Update
3.0	BD	03/31/06	Release Notes Update
3.0	BC	03/08/06	Release Notes Update
3.0	BB	02/09/06	GA Release
2.4.1	AA	11/17/05	Release Notes Update
2.4.2	Z	09/15/05	Maintenance Release for Quarantine Manager
2.4.1	Y	07/22/05	Release Notes update in Support Build
2.4.1	X	05/26/05	GA Release (Quarantine Manager)
2.4.0	W	01/14/05	GA Release
2.3.0	V	11/02/04	Post GA
2.3.0	U	10/27/04	GA Release
2.3.0	T	09/03/04	Beta Release
2.2.6	S	08/24/04	Internal Development Release Only
2.2.5	R	08/03/04	Maintenance Release
2.2.4	Q	07/13/04	Maintenance Release
2.2.3	P	04/22/04	Maintenance Release
2.2.2	O	02/26/04	Maintenance Release
2.2.1	N	10/16/03	Maintenance Release
2.2.0	M	08/29/03	GA Release

Release	Revision	Date	Description of Changes
2.2.0	L	07/11/03	Beta Release
2.1.0	K	01/10/03	GA Release
2.1.0	J	11/22/02	Beta Release
2.1.0	H	11/08/02	Alpha Release for OmniSwitch 6648, 6624, and 8800
2.0.1	F	08/27/02	GA Release
2.0	E	07/12/02	GA Release
1.1	B	10/11/01	GA Release
1.0	A	06/01/01	GA Release

1.0 Introduction

These Release Notes cover the basic feature set supported by OmniVista 3.5.2 for the following supported platforms:

- Windows
  - Windows 7 Professional (32/64-bit)
  - Windows Server 2008 Release 1/Release 2 (32/64-bit)
  - Windows XP
  - Windows Vista - Business (Client Only)
- Linux
  - Redhat Linux ES Version 5.4 (32/64-bit)
  - Suse Professional v10 (32/64-bit).
- Sun Solaris v10 (32/64 bit)

Note: Users can expect better performance on Windows Server 2008 than on Windows XP.

Known problems, limitations, and workarounds are included. Please read the applicable sections in their entirety as they contain important operational information that may impact successful use of the application.

1.1 Technical Support Contacts

For technical support, contact your sales representative or refer to one of the support resources below. Alcatel-Lucent Service and Support can be reached as follows:

- North America, Latin America, Other International
  - Phone
    - North America: 1-800-995-2696
    - Latin America: 1877-919-9526
    - Other International: 1-818-878-4507
  - World Wide Web: https://service.esd.alcatel-lucent.com
  - E-Mail for Non-Critical Technical Questions: esd.support@ind.alcatel.com
- Europe
  - Phone: +33 3 88 55 69 04
  - World Wide Web: https://businessportal.alcatel-lucent.com
  - E-Mail for Non-Critical Technical Questions: ebg_global_supportcenter@alcatel-lucent.com
- Asia Pacific
  - Phone: +65-6240-8484
  - World Wide Web: www.businesspartner.alcatel-lucent.com
  - E-Mail for Non-Critical Technical Questions: support.center@alcatel-lucent.fr

Note: For the most recent version of OmniVista Release Notes go to Alcatel Service and Support page at https://service.esd.alcatel-lucent.com. Under **Alcatel Support**, click on **Software Downloads**. Under **Public Access Software**, click on **Release Notes**, then locate the latest version under OmniVista.

1.2 Documentation

The user documentation is contained in the on-line Help installed with this product.

1.3 What's New in Release 3.5.2

Support for Windows 7 Professional 32/64-bit

OmniVista now supports Windows 7 Professional (32 and 64 bit). It is important to note that when running the webservices client in a web browser on Windows 7 Professional, the URL for the OmniVista Tomcat server must use the loopback address 127.0.0.1 (http://127.0.0.1:8080) instead of hostname “localhost”, or it will resolve to IP address 0.0.0.0 and give a "host-not-found" error.

Support for Windows Server 2008 Release 2 64-bit Support

- OmniVista now supports Windows Server 2008 R2 - 64-bit.

  Note: If you are running OmniVista on 64-bit Windows Server 2008, you must use the 64-bit version of OmniVista and Webservices.

Support for OA Wireless Release OAW 5.0

OmniVista 3.5.2 supports OmniAccess Wireless Devices, Release 5.0.

Support for OS6850E/AOS 6.4.4

OmniVista 3.5.2 supports OS6850E Devices. OmniVista will support features as supported in prior OS6850 releases. These devices support the Multiple VRF feature like the current OS6855-U24X Device. OS6850E devices also support daughter card modules that can be added but hot swap is not allowed.

Notes: Resource Manager does not support FPGA upgrade for any OS68xx Devices (OS6800/OS6850/OS6850E/OS6400/OS6250).

For an OS6850E mixed stack, Resource Manager will only allow install upgrade/restore when the mixed devices are OS6850 and OS6850E. The operation will be skipped for any other device mix (a message will be displayed and logged). Also, in a mixed stack of OS6850 and OS6850E, if the primary is a OS6850 and the software to install/restore is older than 6.4.4.R01, the operation is not allowed and a message will be displayed and logged. However, Resource Manager will allow restore of configuration only backup.

For OS6850E, firmware upgrade is not allowed if the software version is older than 6.4.4.R01. OS6850E devices are automatically filtered out from the device list when doing the upgrade if the upgrade software is not 6.4.4.R01 or newer.

Support for OS10K /AOS7.1.1

OmniVista 3.5.2 supports Alcatel-Lucent's new OS10K Device (AOS Release 7.1.1). OmniVista will provide the same level of support that currently exists for AOS devices, with the following exceptions:

Access Guardian

- Access Guardian is not supported on OS10K Devices.

Discovery

- OmniVista will support discovery of OS 10K devices out of the box. However, AMAP is not supported by OS10K Devices. OmniVista will skip AMAP discovery and use LLDP discovery for adjacency detection.

Health

- The OS10K does not have hourly or by-minute averages, so visual elements for these values are not in OmniVista.
- At the device-level, only "Temperature" is available in the ‘Current Average’ view. There are no minute or hourly averages for this variable.
- At the module-level, CPU max, Memory, Rx, TxRx, or Latest Averages values are not available.

Locator

- "Source Switch IP Address" and "Device Name" columns were added to the "Initial Lookup Table"

Notifications

- OmniVista will provide management for OS10K device Notifications very similar to AOS Devices. A new radio button was added to the “Configure traps” Wizard for OS10K devices. And a new screen with OS10K-specific traps was added for OS10K switches.

Quarantine Manager

- Quarantine Manager is not supported for OS10K devices.

Resource Manager

- OmniVista will provide support for Software Backup, Restore Backup, and Image Import/Upgrade for OS10K devices. However, OS10K devices do not support FPGA upgrade using SNMP, so FPGA upgrade will not be available for OS10K devices in this release of OmniVista.
- There is a new feature in the OS10K Device that enables the user to create multiple working directories with different file names to save different configurations that can then be loaded into the device. However, as in prior releases, OmniVista 3.5.2 only supports a single working directory and will only support backup and restore of the "flash/working" directory.
- In Service Support Upgrade (ISSU) is not supported on OS10K, 7.1.1.

Telnet/SSH

- OS10K Devices allow the user to define custom prompts. However, OmniVista will continue to use “->” as the prompt for telnet/SSH and Telnet Scripts.
- CLI Scripting now supports the following built-in variables:
    - $SYS_NAME – Name of the device as defined in sysName MIB-II variable
    - $SYS_LOCATION – Location of the device as defined in sysLoction MIB-II variable
    - $SYS_VERSION – MPM Version of the device as displayed in OmniVista
    - Cli.forgetPrompt() – This CLI script directive allows the reverse of cli.expectPrompt(), providing a way to ignore prompts that get in the way of script execution.
    - The user can enter Device Version in the Discovery Item along with sysLocation.

Topology

- OmniVista treats OS10K devices as a new type of device, with a new icon specific to OS 10K Devices.
- A new tab has been added for the Multi-Chassis Link/Virtual Fabric Link (MCLAG/VFL) feature that was added for the OS10. The user can view MCLAG/VFL information will have limited configuration options from within OmniVista.
- The OS10K multiple working directory feature is not supported in OmniVista. Note that "Reload From Working" will reload the switch from the *flash/working* directory. "Copy Working To Certified” means copy the current RUNNING DIRECTORY to the Certified Directory. "Copy Certified to Working” means copying the contents of the Certified Directory to */flash/working*. And “Save to Working” means saving the current RUNNING configuration.

  Note: If you receive SNMP Timeout errors from an OS10K Device, make sure the build on the device is 7.1.1.1668.R01 or later. And make sure the SNMP Timeout is set to 10 seconds (10000 milliseconds), with a Retry Count of 1. (Can be set in the Topology Application).

VLANs

- Some VLAN features that are supported in other AOS devices are not supported in OS10K Devices. These include IPX Routing, Port Mobility and Authentication, and Mobile Rules. In the VLAN Wizard, the IPX and Rules options will not be available for OS10K Devices.

Support for AOS 7.1.1 MCLAG and VFL

OS10K Devices have a new feature called Multi Chassis Link Aggregation (MCLAG). OmniVista discovers which devices support the VFL feature and displays the "Multi-Chassis Link Aggregation Tab for that device. This feature is supported by the use of a VFL (Virtual Fabric Link) between the two OS10K devices that support the Multi Chassis Link Aggregation. MCLAG and VFL links need to be visible through the LLDP protocol for OmniVista to display them in Topology. Therefore, you must enable LLDP on appropriate ports for OmniVista to discover links using LLDP.

State changes for Multi-Chassis VFL and MCLAG are communicated by the switch through Notifications. OmniVista cannot display the Link Inconsistency information for the VFL. Topology will display changes based on linkup/linkDown and multiChassisVFlinkDown notifications.

Topology

Contact Information Added to Topology Maps

The user can now specify contact information for all physical and logical maps. An Owner Contact Tab was added to the Map List window where the user can enter up to 255 characters of text detailing the contact information. The user can add/update information for a single map, or select multiple maps and configure and save the information for all selected maps. In addition, if contact information has been added for a map, a "Contact" icon appears at the bottom of the map in Map View. The user can hover the mouse over the icon to display the information.

Location Column Added to Topology Table

A Location column is now displayed in the List of All Discovered devices. This enables users to know about the location of the switch even when it is down. This field is filled with the setting saved on the switch once it is discovered, and updated as needed. The user can add/update the location information for one or more devices by selecting one or more devices in the List of All Discovered Devices, right-clicking, and selecting the “Change Attributes” menu item.. A window allows the user to enter/modify the Location information and save it to all selected devices.

Multi-Chassis Link Tab Added to Device View

A Multi-Chassis Link Tab was added to the Device View for OS 10K Devices (see "Support for AOS 7.1.1 MCLAG and VFL" below). The tab displays the current configuration and state of the Multi-Chassis Link/Virtual Fabric Link (VFL) and configuration. The user can perform certain configuration changes in this tab, but must use the CLI (Telnet/SSH from OmniVista) to configure a Multi-Chassis Link (VFL) and MCLAG. OmniVista will provide support to view the configuration, and make minor changes to VFL.

VFL Sub-Tab

This tab displays information about the configuration and state of the VFL and allows the user to make minor modifications to the VFL configuration. The user may also view/change loop detection settings for the VFL.

VFL Member Ports Sub-Tab

This tab displays information about the ports participating in the Multi-Chassis VFL link. No changes to configuration are allowed, however changes can be made using SSH.

Link Consistency Sub-Tab

This tab displays the information about the consistency of the VFL and the Multi-Chassis Link Aggregates connected to the device.

DHL/ERP Link Display Update in Map View

Previous releases of OmniVista displayed links that were "software down" in red (ERP-RPL or DHL links leaving LAG). OmniVista will now show all "software down" links using a dashed line. OmniVista will also display ERP-RPL and DHL links that are blocking to prevent loops using the same representation. The links will turn red if it is reported "Down" through a linkup/linkDown notification.

Link Aggregate Display Update in Map View

All Link Aggregates are now displayed on maps with an ellipse in the middle of the link to indicate it is a Link Aggregation.

Virtual Fabric Link (VFL) Display in Map View

OmniVista will display Virtual Fabric Links (VFLs) similarly to the display for Link Aggregates, with an ellipse in the middle of the link. However, a VFL will display with two black lines framing the link. The status display of the link will remain the same as other links (e.g., Green, Red).

Statistics

64-bit Counter Support in OmniVista Statistics Application

OmniVista Statistics now supports "Counter 64" values and displays them in chart and table views. Existing Statistics profiles will not be updated for 64 bit counters. The following SNMP variables were also added:

- New HC values for AOS in “Physical Port”
    - ifInOctets-> ifHCInOctets
    - ifOutOctets -> ifHCOutOctets
    - ifInUcastPkts -> ifHCInUcastPkts
    - ifOutUcastPkts -> ifHCOutUcastPkts
- New HC values for AOS 6.4.2 in “UDP”
    - udpInDatagrams -> udpHCInDatagrams
    - udpOutDatagrams -> udpHCOutDatagrams
    - tcpInSegs -> tcpHCInSegs
    - tcpOutSegs -> tcpHCOutSegs

  Note: Some "Counter 64" values such as "udpHCInDatagrams" are only available in certain versions of AOS. If a switch does not support a variable, the Statistics profile stops collecting data and an error is reported to user.

Support for In/Out Octets for Third Party and 7750-SR Devices

OmniVista now supports display of InOctets and OutOctets in the Statistics application for third party and 7750-SR devices. OmniVista, also supports all other counters supported in standard ifTable (IF MIB) for IPD 7750-SR and third party devices.

New Selection Tree

OmniVista now provides XOS-specific variables separately from Third Party and generic variables. All third party devices will now use a newly created Generic XML file based on the old XOS file with the addition of MIB-2 variables. These new specifications enable user to specify a full set of IF-MIB variables using Tree selection in the Statistics application. OmniVista also provides "canned" variables from which user can select multiple variables with one click.

Notification of Unsupported MIB Variables

Generic devices may not support all IF-MIB variables. If OmniVista detects unsupported MIB variables in a profile, the OmniVista Server will stop running the profile and notify all clients having access to that profile. At least one poll is required for an error to come back. OmniVista server will notify all clients having access to that profile.

Telnet

CLI Scripting - Syntax Extensions

The Telnet CLI Scripting feature has been modified to allow the user to write more flexible scripts. Support was added for extra build-in variables:

- $SYS_NAME – Name of the device as defined in sysName MIB-II variable
- $SYS_LOCATION – Location of the device as defined in sysLoction MIB-II variable
- $SYS_VERSION – MPM Version of the device as displayed in OmniVista
- Cli.forgetPrompt() – This CLI script directive will allow the reverse of cli.expectPrompt(), providing a way to ignore prompts that get in the way of script execution.

Notes:

- $SYS_VERSION is not a standard MIB variable and can only be used when OmniVista knows how to discover the version. For all other devices, user must look up sysDescription or other interfaces and parse it to get the MPM version value in the CLI Script, or use alternate means based on device type. Or the user can enter the version for the device.
- If the user has not set SYS_NAME and SYS_LOCATION for the device, the script will not be very effective! The user must set SYS_NAME and SYS_LOCATION and poll the information for affected switches before launching the script.

Groups

The OmniVista Groups application now contains a new tab, L2 VLAN Groups, that allows the user to create Layer 2 VLAN groups for the Policy View QoS and Secure View ACL applications.

PolicyView QoS

Additional Policy Conditions and Actions can now be configured in OmniVista. The new conditions/actions are accessed on the following tabs in the PolicyView QoS Expert Wizard:

Conditions

Interfaces Tab

- Ethernet Type - Restricts the policy to a specific type of ethernet traffic.

VLANs Tab

- Inner Source VLAN - An Inner Source VLAN condition is applied to double-tagged VLAN Stacking traffic and is used to classify the traffic based on the inner VLAN ID tag, also known as the customer VLAN ID.
- VRF Name - Restricts the policy rule to traffic flowing in the specified VRF.

802.1p Tab

- Inner 802.1 Priority - Restricts the policy to incoming traffic that has the configured Inner 802.1 Priority value in the frame header.

TCP Flags Tab (New Tab)

- The TCP Flags Tab, is used to create a condition based on TCP values. Typically, the TCP Flags policy condition is used in combination with Source IP, Destination IP, Source Port, Destination Port, Source TCP

Port, or Destination TCP Port conditions. Note that even though a TCP Flag condition can be used with most action parameters, it is mainly intended for ACL use.

Actions

TCM Tab (New Tab)

- The TCM Policy Action tab enables you to specify Tri-Color Marking (TCM) actions action to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface.

Ports Tab (New Tab)

- The Ports Policy Action tab enables you to specify QoS actions to impose on ports carrying traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.

SecureView ACL

Additional Policy Conditions and Actions can now be configured in OmniVista. The new conditions/actions are accessed on the following tabs in the SecureView ACL Expert Wizard:

Conditions

Interfaces Tab

- Ethernet Type - Restricts the policy to a specific type of ethernet traffic.

VLANs Tab

- Inner Source VLAN - An Inner Source VLAN condition is applied to double-tagged VLAN Stacking traffic and is used to classify the traffic based on the inner VLAN ID tag, also known as the customer VLAN ID.
- VRF Name - Restricts the policy rule to traffic flowing in the specified VRF.

802.1p Tab

- Inner 802.1 Priority - Restricts the policy to incoming traffic that has the configured Inner 802.1 Priority value in the frame header.

TCP Flags Tab (New Tab)

- The TCP Flags Tab, is used to create a condition based on TCP values. Typically, the TCP Flags policy condition is used in combination with Source IP, Destination IP, Source Port, Destination Port, Source TCP Port, or Destination TCP Port conditions. Note that even though a TCP Flag condition can be used with most action parameters, it is mainly intended for ACL use.

Actions

TCM Tab (New Tab)

- The TCM Policy Action tab enables you to specify Tri-Color Marking (TCM) actions action to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface.

Ports Tab (New Tab)

- The Ports Policy Action tab enables you to specify QoS actions to impose on ports carrying traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.

Access Guardian

UNP Dynamic Rule Configuration

OmniVista now supports UNP Dynamic Rules, a feature that was added in switch release 6.4.3 Post GA. This feature enables you to configure a dynamic map that automatically maps a user to a backup UNP (presumably with lower access levels) if a Host Integrity Check (HIC) Server goes down. The UNP Assignment Wizard was changed to allow you to assign Dynamic UNP mapping. If a UNP is selected assigned to a switch, its backup UNP is also automatically assigned to the switch.

> **Note:** OmniVista 3.5.2 does not support configuration of the Backup HIC Server. Also, OmniVista does no checking to see if the Backup UNP provides a lower level of access.

Access Guardian Application Displays Policy Names in 802.1x Queries

The Access Guardian application View Tab shows Access Guardian Policies on each port of selected device. OmniVista displays the name of the Access Guardian Policy that matches the policy on the port. This helps user instantly recognize the policy for that port.

Web Services

Web Services API Extension for Professional Services

This feature allows Professional Services access to OmniVista server Locator information to enable them to build their own IP/MAC Management solution. The OmniVista Locator database now includes UNP name, where possible, in addition to the information collected by Locator.

Framework Enhancements

MIB Support for the following devices has been discontinued; and the applicable mibsets and their MIBs have been removed from OmniVista. The mibsets.txt and trapd.conf files have also been updated to remove their references. These devices have been out of the Alcatel-Lucent product portfolio for more than 5 years.

- Tasman
- OmniCore-5010
- OmniCore-5022
- OmniCore-5052
- Airespace

> **Note:** Out of box installation of OmniVista will not support these devices by default. The mibsets are not included in the 3.5.2 Release and are removed in an upgrade to 3.5.2. However, the user can use the procedures in place for Third party device MIB import to enable support for these devices.

1.4 Feature Set Support

1.4.1 Element Manager Integration

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

Supported Element Managers

Element Manager	Supported Devices	Description
SwitchManager Client	XOS-based devices: OmniSwitch, Omni Switch/Router	SwitchManager provides a GUI interface in the form of a bitmap of the switch that enables you to configure and gather statistics from an XOS-based switch. The OV SwitchManager Client is not included with OmniVista. If installed, SwitchManager can be invoked in the OmniVista **Topology** application's All Discovered Devices table using the **SwitchManager** right click menu item.
WebView	OmniSwitch 6212, 6212P, 6224, 6224P, 6248, 6248P, 6224U OmniSwitch 6250 -8M, 6250-24M, 6250-24M Rev. B, 6250-24MD, 6250-24MDRev. B OmniSwitch 6400-24, 6400-P24, 6400-U24, 6400-DU24, 6400-48, 6400-P48, 6400-BPS-PS OmniSwitch 6624, 6648, 6600-U24, 6600-P24 OmniSwitch 6602-24, 6602-48 OmniSwitch 6800-24, 6800-48, 6800-U24, 6800-24L, 6800-48 OmniSwitch 6850, 6850-24, 6850-48, 6850-24X, 6850-48X, 6850-P24, 6850-P48, 6850-P24X, 6850-P48X, 6850 Lite Series OmniSwitch 6850E-C24, 6850E-P24, 6850E-C24X, 6850E-P24X, 6850E-C48, 6850E-P48, 6850E-C48X, 6850E-P48X, 6850E-U24X OmniSwitch 6855-14, 6855-U10, 6855-24, 6855-U24, 6855-U24X OmniSwitch 7700, 7800 OmniSwitch 8800 OmniSwitch 9600, 9700, 9800 OmniSwitch 9700E, 9800E OmniSwitch OS10K	WebView is platform independent and interfaces through a web browser. It can also be invoked in the OmniVista **Topology** application's All Discovered Devices table using the **WebPage** right click menu item.
Web-Based Manager	OmniAccess 5510, 5740 OmniStack 6124, 6148 OmniStack 6224, 6224P, 6248, 6248P OmniStack 6300-24 2nd Generation WLAN (OmniAccess 43xx, 6xxx, AP6x, AP70)	The Web-Based Manager is platform independent and interfaces through a web browser. It can also be invoked in the OmniVista **Topology** application's All Discovered Devices table using the **WebPage** right click menu item

1.4.2 Device Feature Support

The following table details OmniVista feature support by device.

OmniVista Device Feature Support

OmniVista Feature	OS10K (1)	AOS	XOS	61xx	62xx	OA WLAN	3rd Party Switches
Discovery	X	X	X	X	X	X	X (2)
Basic MIB-2 Polling and Status Display	X	X	X	X	X	X	X (2)
Trap Display/Trap Responder	X	X	X	X	X	X	X
VLAN Configuration	X	X	X	X			
Resource Manager BU/Restore/Upgrade	X	X	X	X	X		
Telnet	X	X	X	X	X	X	X
Statistics	X	X	X	Port Utilization Only	Port Utilization Only	Port Utilization Only	Port Utilization Only
MIB Browsing (see note)	X	X	X	X	X	X	X (3)
Quarantine Manager		X	X	Port Shutdown Only	X	X	
Topology Links (AMAP)		X	X	X	X		
Topology Links (LLDP)	X	X			X		
PolicyView-QoS	X	X	X				
SecureView-SA	X	X					
SecureView-ACL	X	X					
Health Monitoring	X	X	X		X		
CLI Scripting	X	X			X	X	X
Trap Replay	X	X					
Trap Absorption	X	X (4)	X	X	X	X	X
Locator	X	X	X	X	X	X	X (5)
Access Guardian		X					

1. OS10K Devices provide limited support for some features. See "Support for OS10K / AOS 7.1.1"for more details.
2. Cisco, Extreme, and 3Com supported by default. Other devices can be added manually by providing OIDs.
3. Basic MIB-2 browsing supported for 3rd-party devices. Custom MIBs may be imported and associated with 3rd party devices.
4. Trap absorption feature is already built into AOS devices.
5. Requires MIB-2 support for 3rd-party devices.

NOTE: MIB browser support is for monitoring purposes only, NOT for configuration.

1.4.3 SSH/Telnet Element Management

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

To access the telnet feature, select the device in the **Topology** application's **All Discovered Devices** table, right click and select the **Telnet** menu item. Refer to the switch's manual for information on how to use the CLI.

2.0 System Requirements

The following builds are certified to run OmniVista 3.5.2:

- AOS
  - OS6250 - 6.6.1.R01
  - OS6400 - 6.3.3.R01, 6.4.2.R01, 6.4.3.R01, 6.4.4.R01
  - OS6800 - 6.1.5.R01, 6.3.1.R01
  - OS6850 - 6.1.5.R01, 6.3.1.R01, 6.3.4.R01, 6.4.2.R01, 6.4.3.R01, 6.4.4.R01
  - OS6850E - 6.4.4.R01
  - OS6855 - 6.3.2.R01, 6.3.4.R01, 6.4.2.R01, 6.4.3.R01, 6.4.4.R01
  - OS7000, 8800, 6000 - 5.4.1.R01
  - OS9600 - 6.1.5.R01, 6.3.1.R01, 6.3.4.R01, 6.4.2.R01, 6.4.3.R01
  - OS9700 - 6.1.5.R01, 6.3.1.R01, 6.3.4.R01, 6.4.2.R01, 6.4.3.R01
  - OS9800 - 6.1.5.R01, 6.3.1.R01, 6.3.4.R01, 6.4.2.R01, 6.4.3.R01
  - OS9700E - 6.4.1.R01, 6.4.2.R01, 6.4.3.R01, 6.4.4.R01
  - OS9800E - 6.4.1.R01, 6.4.2.R01, 6.4.3.R01, 6.4.4.R01
  - OS10K - 7.1.1.R01
- XOS
  - OmniSwitch, OmniSwitch Router - 4.4.4.B
  - 4024 - 4.3.3.B
- OmniStack Series
  - 6200 - 1.0.2.41 and 1.5.0.93 (AMAP is supported). Note that when configuring traps, the whole list of traps recognized by 1.5.x will be displayed, but only traps recognized by 1.0.x will be configured on 1.0.x boxes.
- OmniAccess WLAN
  - 3.3.2.X
- OmniAccess WAN
  - 5510, 5740 - 3.0.0
  - 7X.X - 2.3.2
- OmniVista 3.5.2 upgrade paths certified
    - 3.5.1 to 3.5.2
    - 3.5.0 to 3.5.2
    - 3.4.2 to 3.5.2

2.1 Requirements for All Platforms

The following sections detail requirements for all supported platforms. **Please note that OmniVista 2500 NMS does not support, nor is it certified for, International Versions of OS and non-English locale**.

2.1.1 Java Requirements

OmniVista includes the Java 2 Runtime Environment (JRE) Version 1.6.0_18-b07 for each of the following supported platforms: Windows Server 2008, Windows 7 Professional, Windows XP, Windows Vista (Business), Solaris v10, and Linux. The correct version of JRE is bundled with the installers for all supported platforms, and is automatically installed with OmniVista. Because the bundled JRE is installed in the OmniVista installation directory, it should NOT affect or conflict with any other JRE or Java Virtual Machine previously installed on your machine.

The Element Managers must be installed on the clients that will use them. Because of the different Element Manager implementations, hardware and software installation requirements vary. Refer to the release notes for the desired element manager for system and installation requirements for each Element Manager. Note that with the exception of the Web-Based Managers, the Element Managers are not included with OmniVista.

2.1.2 Server Platform Requirements

The OmniVista Server should be installed on a machine with a static IP address.

2.2 Recommended System Configurations

The tables below provide recommended system configurations based on the number of devices being managed by OmniVista 2500 NMS 3.5.2 (500, 1,000 and 3,000 devices). **These configurations should be used as a guide. Specific configurations may vary depending on the network, the number of clients, applications open, etc.** For more information, contact Customer Support.

> **Note:** Whether or not you purchase and activate the new Virtual Machine Manager application, the application has increased recommended system requirements, as shown in the following tables. Specific Virtual Machine Manager configuration recommendations, based on the VMM License purchased, are included at the bottom of each table.

Recommended System Configurations 500 Devices				
Operating System	**OV Server Processor**	**OV Client Processor**	**OV Server RAM**	**OV Client RAM**
Windows Server 2008 R1 (32 Bit)	3.0 GHz Dual Core	3.0 GHz	2 GB Allocated 1.0 GB	2 GB Allocated 800 MB
Windows Server 2008 R1/R2 (64 Bit)	3.0 GHz Dual Core	3.0 GHz	4 GB Allocated 1.5 GB	2 GB Allocated 1.0 GB
Windows XP (32 Bit)	2.4 GHz Dual Core	2.4 GHz	2 GB Allocated 1.0 GB	2 GB Allocated 800 MB
Windows 7 Professional (32 Bit)	2.4 GHz Dual Core	2.4 GHz	2 GB Allocated 1.0 GB	2 GB Allocated 800 MB
Windows 7 Professional (64 Bit)	3.0 GHz Dual Core	3.0 GHz	4 GB Allocated 1.5 GB	2 GB Allocated 1.0 GB
Windows Vista Business (32 Bit)	Not Recommended	3.4 GHz	Not Recommended	2 GB Allocated 800 MB

Recommended System Configurations 500 Devices				
Operating System	**OV Server Processor**	**OV Client Processor**	**OV Server RAM**	**OV Client RAM**
Sun Solaris (32 Bit)	Sun V210 2 Processors	2.0 GHz	2 GB Allocated 1.0 GB	2 GB Allocated 800 MB
Sun Solaris (64 Bit)	Sun V210 2 Processors	2.0 GHz	4 GB Allocated 1.5 GB	2 GB Allocated 1.0 GB
Linux Red Hat (32 Bit)	3.0 GHz Dual Core	2.4 GHz	2 GB Allocated 1.0 GB	2 GB Allocated 800 MB
Linux Red Hat (64 Bit)	2.6 GHz 2 Processors	2.4 GHz	4 GB Allocated 1.5 GB	2 GB Allocated 1.0 GB
Linux - Suse (32 Bit)	3.0 GHz Dual Core	2.4 GHz	2 GB Allocated 1.0 GB	2 GB Allocated 800 MB
Linux - Suse (64 Bit)	2.6 GHz 2 Processors	2.4 GHz	4 GB Allocated 1.5 GB	2 GB Allocated 1.0 GB
VmWare ESXi 4.1/5.0 (64 Bit)	VMware ESXi requires the same system configuration as the OS on which it is running. However, you will need to increase the recommended configuration to achieve the same performance.			
Disk Space Requirements	**Client -** 2 GB of free disk space on the drive on which you install OmniVista Client. **Server -** 5 GB of free disk space on the drive on which you install OmniVista Server. **Web Services -** 50 MB of free disk space on the drive on which you install OmniVista 2500 NMS (also requires 1 GB of additional dedicated memory).			

The configurations above supported the following:

No. of Traps on Server 60K

No. of Traps on Client 30K

No. of Traps per Second 10

No. of Concurrent Clients 2

Recommended System Configurations 1,000 Devices				
Operating System	**OV Server Processor**	**OV Client Processor**	**OV Server RAM**	**OV Client RAM**
Windows Server 2008 R1 (32 Bit)	Not Recommended	3.0 GHz	Not Recommended	4 GB Allocated 1.2 GB
Windows Server 2008 R1/R2 (64 Bit)	3.0 GHz Quad Core	3.0 GHz	6 GB Allocated 3.0 GB	4 GB Allocated 2.0 GB
Windows XP (32 Bit)	Not Recommended	2.4 GHz	Not Recommended	4 GB Allocated 1.2 GB
Windows 7 Professional (32 Bit)	Not Recommended	2.4 GHz	Not Recommended	4 GB Allocated 1.2 GB
Windows 7 Professional (64 Bit)	3.0 GHz Quad Core	3.0 GHz	6 GB Allocated 3.0 GB	4 GB Allocated 2.0 GB
Windows Vista Business (32 Bit)	Not Recommended	3.4 GHz	Not Recommended	4 GB Allocated 1.2 GB
Sun Solaris (32 Bit)	Sun V210 2 Processors	2.0 GHz	4 GB Allocated 1.8 GB	4 GB Allocated 1.6 GB
Sun Solaris (64 Bit)	Sun V210 2 Processors	2.0 GHz	8 GB Allocated 3.0 GB	4 GB Allocated 2.0 GB
Linux Red Hat (32 Bit)	3.0 GHz Quad Core	2.4 GHz	4 GB Allocated 1.8 GB	4 GB Allocated 1.6 GB
Linux Red Hat (64 Bit)	2.6 GHz 2 Processors	2.4 GHz	8 GB Allocated 3.0 GB	4 GB Allocated 2.0 GB
Linux - Suse (32 Bit)	3.0 GHz Quad Core	2.4 GHz	4 GB Allocated 1.8 GB	4 GB Allocated 1.6 GB
Linux - Suse (64 Bit)	2.6 GHz 2 Processors	2.4 GHz	8 GB Allocated 3.0 GB	4 GB Allocated 2.0 GB
VmWare ESXi 4.1/5.0 (64 Bit)	VMware ESXi requires the same system configuration as the OS on which it is running. However, you will need to increase the recommended configuration to achieve the same performance.			

Recommended System Configurations 1,000 Devices				
Operating System	**OV Server Processor**	**OV Client Processor**	**OV Server RAM**	**OV Client RAM**
Disk Space Requirements	**Client -** 2 GB of free disk space on the drive on which you install OmniVista Client. **Server -** 20 GB of free disk space on the drive on which you install OmniVista Server. **Web Services -** 50 MB of free disk space on the drive on which you install OmniVista 2500 NMS (also requires 1 GB of additional dedicated memory).			

The configurations above supported the following:

No. of Traps on Server 60K

No. of Traps on Client 30K

No. of Traps per Second 10

No. of Concurrent Clients 2

Recommended System Configurations 3,000 Devices				
Operating System	**OV Server Processor**	**OV Client Processor**	**OV Server RAM**	**OV Client RAM**
Windows Server 2008 R1 (32 Bit)*	Not Recommended	Not Recommended	Not Recommended	Not Recommended
Windows Server 2008 R1/R2 (64 Bit)	3.0 GHz Quad Core	3.0 GHz	12 GB Allocated 8.0 GB	12 GB Allocated 6.0 GB
Windows 7 Professional (32 Bit)*	Not Recommended	Not Recommended	Not Recommended	Not Recommended
Windows 7 Professional (64 Bit)	3.0 GHz Quad Core	3.0 GHz	12 GB Allocated 8.0 GB	12 GB Allocated 6.0 GB
Sun Solaris (32 Bit)	Not Recommended	2.6 GHz	Not Recommended	4 GB Allocated 2.4 GB
Sun Solaris (64 Bit)	Sun V210 2 Processors	2.0 GHz	12 GB Allocated 8.0 GB	12 GB Allocated 6.0 GB
Linux Red Hat (32 Bit)	Not Recommended	Not Recommended	Not Recommended	Not Recommended
Linux Red Hat (64 Bit)	2.6 GHz 4 Processors	2.6 GHz	12 GB Allocated 8.0 GB	12 GB Allocated 6.0 GB

Recommended System Configurations 3,000 Devices				
Operating System	**OV Server Processor**	**OV Client Processor**	**OV Server RAM**	**OV Client RAM**
Linux - Suse (32 Bit)	Not Recommended	Not Recommended	Not Recommended	Not Recommended
Linux - Suse (64 Bit)	2.6 GHz 4 Processors	2.6 GHz	12 GB Allocated 8.0 GB	12 GB Allocated 6.0 GB
VmWare ESXi 4.1/5.0 (64 Bit)	VMware ESXi requires the same system configuration as the OS on which it is running. However, you will need to increase the recommended configuration to achieve the same performance.			
Disk Space Requirements	**Client -** 2 GB of free disk space on the drive on which you install OmniVista Client. **Server -** 20 GB of free disk space on the drive on which you install OmniVista Server. **Web Services -** 50 MB of free disk space on the drive on which you install OmniVista 2500 NMS (also requires 1 GB of additional dedicated memory).			

*****There is insufficient memory available for a 3,000-device configuration.

The configurations above supported the following:

No. of Traps on Server 200K

No. of Traps on Client 99,999

No. of Traps per Second 20

No. of Concurrent Clients 10

> **IMPORTANT NOTE:** Large Enterprises with **complex configuration require increased server speed** (e.g., multi-core with a minimum speed of 2.4 GHz) **and increased memory allocation** on both client and server (increase allocations shown in table above from 8 GB to 12 GB on the Server; and from 6 GB to 8 GB on the client).

3.0 Installation

Previous OmniVista installations offered the core package (OmniVista 2520/2540) and separate optional packages (e.g., PolicyView, SecureView SA). Beginning with Release 3.5, OmniVista packaging combines all of these packages in one base package. The package has a single installer, single license, with a tier-based licensing process where the user's License determines the maximum number of devices that can be managed by OmniVista.

Previous versions of OmniVista had a mechanism in place to burn into the license key the maximum number of devices to be managed by OmniVista (e.g., only 15 devices per license for a Single User licenses). Licenses are now generated with different maximum numbers, depending on the user's purchase.

The maximum number of devices allowed is displayed in the License dialog within the OmniVista GUI. This dialog also displays the current number of devices and the percentage of the total allowed number that is currently being managed. 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**: The optional OmniVista Web Services application is included at no charge with all licenses and is included on the same DVD as the core package. However, it is installed after installing the core package. To install this application requires an additional 1 GB of RAM on your OmniVista Server machine.

Note: Note that you can only upgrade to OmniVista 3.5.2 from versions 3.4.0, 3.4.1, 3.4.2, 3.5.0, or 3.5.1.

3.1 Installing OmniVista on Windows Systems

To install OmniVista you must log on to Windows with a User Profile that has administrative rights.

1. Insert the **OmniVista 2500 NMS** DVD into the DVD-ROM drive.
2. Change to the **OmniVista2500** directory.
3. Double-click the **Disk1** folder.
4. Double-click the **InstData** folder.
5. Double-click the **Windows** folder.
6. Double-click the **install_win.exe** icon.
7. Follow the instructions in the installer to completion.

Note: The OmniVista installation software does NOT verify that the platform on which you are installing is supported or properly configured.

3.1.1 Element Manager Integration with OmniVista

The OV SwitchManager Client element manager can be installed before or after OmniVista. After installation, the element manager is integrated the first time it is invoked in OmniVista. It is invoked in the OmniVista Topology application's All Discovered Devices table using the SwitchManager right-click menu item.

3.2 Installing OmniVista on Sun Solaris Systems

Follow the instructions below to install OmniVista on the Sun Solaris platform.

1. Download and apply any patches to Solaris v10 required for the Java 2 SDK, Standard Edition, Version 1.6.
2. Go to http://java.sun.com/javase/6/webnotes/install/jre/install-solaris.html and follow the instructions for determining which patches are already installed on your system, which patches are required for Solaris v10, and how to obtain and install the required patches.
3. Insert the **OmniVista 2500 NMS** DVD into the DVD-ROM drive.
4. At the command prompt, change to the **OmniVista2500** directory.
5. Change to the **Disk1** directory, then to the **InstData** directory, and finally to the **Solaris** directory on the DVD. Now enter: **./install_sol.bin**.
6. Follow the instructions in the installer to completion.

Note: The OmniVista installation software does NOT verify that the platform on which you are installing is supported or properly configured.

3.3 Installing OmniVista on Linux Systems

Follow the instructions below to install OmniVista on the Red Hat or Suse Linux platform. Reverse DNS must be configured correctly for Linux OmniVista clients to work properly if they are using DHCP.

1. Insert the **OmniVista 2500 NMS** DVD into the DVD-ROM drive.
2. At the command prompt, change to the **OmniVista2500** directory.
3. Change to the **Disk1** directory, then to the **InstData** directory, and finally to the **Linux** directory on the DVD. Now enter: **./install_lin.bin**.
4. Follow the instructions in the installer to completion.

Note: The OmniVista installation software does NOT verify that the platform on which you are installing is supported or properly configured.

3.4 Installing Web-Services

3.4.1 Installing Web Services

Follow the steps in the applicable section(s) below to install OmniVista Web Services and Web Browser. After installation is complete, open a web browser and enter **http://*OmniVista Server IP Address*:8080** in the address line, then press **ENTER**. (If the client and server are installed on the same machine, you can enter **http://localhost:8080**.) Login with your administrative OmniVista Login/Password. The following browsers are supported in OmniVista 3.5.2:

- Windows - Internet Explorer Versions 6.0, 7.0, and 8.0
- Linux - Firefox Versions 1.5, 2.0, and 3.0.
- Sun Solaris - Firefox Versions 1.5 and 2.0.

3.4.1.1 Installing Web Services on Windows

To install Web Services on Windows, you must log on with a User Profile that has administrative rights.

1. Insert the **OmniVista 2500 NMS** DVD into the DVD-ROM drive.
2. Change to the **Webservices** directory (for 64 bit, change to the **Webservices_Win64bit** directory).
3. Double-click the **Disk1** folder.
4. Double-click the **InstData** folder.
5. Double-click the **Windows** folder.
6. Double-click the **install_win.exe** icon.
7. Follow the instructions in the installer to completion.

3.4.1.2 Installing Web Services on Sun Solaris

To install Web Services on Sun Solaris, you must log on with a User Profile that has administrative rights.

1. Insert the **OmniVista 2500 NMS** DVD into the DVD-ROM drive.
2. Change to the **Webservices** directory.
3. In the DVD-ROM drive window, open the **Disk1** folder.
4. In the Disk1 window, open the **InstData** folder.
5. In the InstData window, open the **Solaris** folder.
6. Enter **./install_sol.bin**.
7. Follow the instructions in the installer to completion.

3.4.1.3 Installing Web Services on Linux

To install Web Services on Red Hat or Suse Linux, you must log on with a User Profile that has administrative rights.

1. Insert the **OmniVista 2500 NMS** DVD into the DVD-ROM drive.
2. Change to the **Webservices** directory.
3. In the DVD-ROM drive window, open the **Disk1** folder.
4. In the Disk1 window, open the **InstData** folder.
5. In the InstData window, open the **Linux** folder.
6. Enter **./install_lin.bin**.
7. Follow the instructions in the installer to completion.

3.5 Upgrade Procedures

You do not have to uninstall the old installation prior to installing the new package. Keeping the old OmniVista version will preserve user-specific data and configuration. In this way, you get the benefits of the new release and continue to use your existing data as before. For Windows and UNIX, the installation program will detect the old installation and will offer to install it in your old installation directory. If you accept it, you will be able to use the data from your old system.

> **Note:** It is recommended that before the upgrade, you stop the OmniVista server and back-up the data (e.g., "C:\Program Files\AlcatelOmniVista 2500\data"). Use the Server Backup application to perform the backup.

3.5.2 Third-Party MIB Sets

When you upgrade OmniVista, any previous mibsets defined for Third-Party Device support will be lost. Follow the steps below to add the old third-party devices after an upgrade.

1. Check if <OV_InstallDir>/data/mibs/mibsets.txt file exists, if so rename it to mibsets.txt.bak2 (do not overwrite the mibsets.txt.bak if it exists under this directory).
2. Restart the OmniVista server and client. Open the Preferences application and select the Third-Party Device Support, and add a new OID (can be a fake one) and apply the changes.
3. Close the client and shutdown the server.
4. Open the newly created mibsets.txt file under <OV_InstallDir>/data/mibs with a text editor. Using separate text editors, open mibsets.txt.bak and/or mibsets.txt.bak2 files, and copy the lines that contain your old third-party devices, and paste them at the end of mibsets.txt file.
5. Save mibsets.txt file, and restart OmniVista server and client. You should see your old third-party devices in the Preferences application. You may delete the fake OID that you added earlier.

Note: When you upgrade, user authentication configuration in the LDAP database is preserved. No reconfiguration is required.

3.6 Upgrading an Evaluation OmniVista License to a Permanent License

A Demo Version of the OmniVista 2500 NMS Application is included on the OmniVista DVD that allows the user to install the application and configure up to five (5) switches without a license. However, any information stored on the server is lost at shutdown. To gain permanent use of the OmniVista software, the user must order a license card for the application. The following procedure describes how to obtain an OmniVista license key.

1. Purchase a permanent OmniVista license. You will receive a License Card that contains a serial number.
2. Once you receive your License Card, log onto the Customer Support website at http://service.esd.alcatel-lucent.com/portal/page/portal/EService/LicenseGeneration and select **OmniVista 2500 NMS**.
3. Enter your Site Name, Company Name, Phone, E-Mail, and Activation Code in the required fields. The e-mail address will be used to send a valid permanent license key to you. You can find the serial number on the License Card you received as part of your order. This serial number is used to verify that you have purchased a licensed copy of OmniVista.
4. Select the product from the drop-down menu for which you want a key.
5. Click **Submit**. An e-mail will be sent to you with a valid license key. The following is an example of such an e-mail:

   Company: ACME
   Name: John Smith
   Product: OV2500 - OmniVista 2500 NMS - Release 3.5
   Registration Number: SU340N1000-0000
   Date: MARCH 31, 2011 11:19:36 PST
   License Contact: License@ind.alcatel-lucent.com
   License Key: dhG$JDBG-BBVAEgi2-f8ohhr3r-$FGUMG18

6. Make a note of the License Key.

7. Under the OmniVista main **Help** menu, select **Licenses**.
8. Select **OV2500-CORE** and click **Relicense**.
9. Enter the license key and click **OK**. The new license will take effect immediately.

If you have questions or encounter problems upgrading your OmniVista license, please contact Alcatel Customer Support.

4.0 Launching OmniVista

When launching OmniVista, the server must be running before starting any clients. OmniVista is installed with a default Administrator login of **admin** with a default password of **switch**.

> **Note:** If the port used by the OmniVista server to receive traps is in use when the server is launched, the server will run (with an error message) but traps will not be received by the server. This applies to third party NMS applications like **HP OpenView**. If they are installed on the same machine as the OmniVista server, listening for traps on the same port, and are launched before the OmniVista server, they could prevent OmniVista from receiving traps.

4.1 Launching OmniVista on Windows

If you selected **Full Install** on the **Choose Install Set** window during the **OmniVista** installation procedure, the installer runs the server upon completion of the installation. In addition, the OmniVista server is installed as a Windows Service. Therefore, the server launches automatically when you turn on or restart the computer. You can also run the OmniVista server from the DOS Command Prompt. Just change to the directory in which you installed OmniVista, then enter: **wrapper**. There are two ways to launch a Client on Windows:

Double-click the **OmniVista** icon on your desktop or:

> Select **Start** > **Programs** > **Alcatel OmniVista 2500** > **OmniVista**.

4.2 Launching OmniVista on Sun Solaris

OmniVista is launched the same way on all supported UNIX platforms. The default port number used by the OmniVista server to receive traps is 162. The default can be changed using the **Preferences** application. To receive traps on the default trap port on UNIX, the OmniVista server must run as the UNIX root user. This is because UNIX only allows root users to access ports below 1024 and the default trap port number for OmniVista and most switches is 162. An alternative to running the server as root is to configure all switches to forward traps on a number greater than 1023 and use the **Preferences** application to change the OmniVista server **Port** to that same number. Note that after a standard installation on a UNIX platform, the LDAP server starts automatically. However, it must be launched manually after a system restart.

> **Note:** The default port for syslog messages is Port 514. The default port for TFTP is 69.

You can make the OmniVista server a UNIX daemon that runs at boot time (you should also make the LDAP Server run as a daemon). Create a file in the appropriate directory for boot startup scripts for your type of unix. The file must be a symbolic link to the **OVServer** script contained in the OmniVista installation directory. For example, on Solaris 2.9 the boot directory is /etc/rc3.d. You may have to consult the /etc/inid.d/README to determine the appropriate naming convention to use. If in doubt, consult your system administrator.

To launch the LDAP server:

> At the command prompt, change to the directory in which you installed OmniVista, then enter: **./OVLdap**.

To launch the server:

> At the command prompt, change to the directory in which you installed OmniVista, then enter: **./OVServer**.

To launch a client:

> At the command prompt, change to the directory in which you installed OmniVista, then enter: **./OmniVista**.

4.3 Launching OmniVista on Linux

The default port number used by the OmniVista server to receive traps is 162. The default can be changed using the **Preferences** application. To receive traps on the default trap port on Linux, the OmniVista server must run as the Linux root user. This is because Linux only allows root users to access ports below 1024 and the default trap port number for OmniVista and most switches is 162. An alternative to running the server as root is to configure all switches to forward traps on a number greater than 1023 and use the **Preferences** application to change the OmniVista server **Port** to that same number. The server must be launched manually after a system restart.

Note: The default port for syslog messages is Port 514. The default port for TFTP is 69.

You can make the OmniVista server a Linux daemon that runs at boot time (you should also make the LDAP Server run as a daemon). Create a file in the appropriate directory for boot startup scripts for your type of Linux. The file must be a symbolic link to the **OVServer** script contained in the OmniVista installation directory. If in doubt, consult your system administrator.

To launch the LDAP server:

At the command prompt, change to the directory in which you installed OmniVista, then enter: **./OVLdap**.

To launch the server:

At the command prompt, change to the directory in which you installed OmniVista, then enter: **./OVServer**.

To launch a client:

At the command prompt, change to the directory in which you installed OmniVista, then enter: **./OmniVista**.

5.0 Uninstalling OmniVista

5.1 General Concepts for Uninstalling on Any Platform

When you uninstall OmniVista and/or Add-on Applications, the directory where you installed OmniVista is not removed. For example, on Windows the default installation directory is: C:\Program Files\Alcatel OmniVista 2500. Preserved in this directory are two subdirectories:

- clientdata - contains client preference data on the client
- data - contains persistent storage on the server.

If you wish to completely uninstall OmniVista, delete the installation directory manually. Note that the data and clientdata directories contained in the installation directory can contain user-defined data that will be used if OmniVista is reinstalled to the same directory.

5.2 Uninstalling on Windows

To uninstall OmniVista on a Windows platform.

Select **Start** > **Programs** > **Alcatel OmniVista 2500** > **Uninstall OmniVista**.

5.3 Uninstalling on Sun Solaris

At the command prompt, change to the installation directory, then enter: **./Uninstall_OmniVista**.

5.4 Uninstalling on Linux

At the command prompt, change to the installation directory, then enter: **./Uninstall_OmniVista**.

6.0 Server

6.1 Maintenance

The OmniVista Server should be installed on a machine with a static IP address. (You can re-install; however, it is easier to edit the "properties.conf" file as described in Section 6.2.3.)

> **Note:** If you change the address for the OmniVista Server, you must also change the address for the LDAP Server. See section 7.1.12 for more information.

6.1.1 Trap Logging

The OmniVista Server maintains a log of traps received from network devices. This log is stored on the server machine hard drive and can be displayed and cleared in the **Notifications** application. The maximum number of traps logged by the server is 300,000. After this maximum is reached, the oldest trap in the log is cleared to make room for each new trap received.

> **Note:** The maximum number of traps (300,000) is only supported in Solaris 64-bit mode with at least 5 GB of RAM allocated to the server.

The **Notifications** application displays the log of traps detected by the OmniVista server. To display all traps logged by the server, select the **All** tree node. The **Notifications** table displays traps for all discovered devices. Select the tree node for an individual switch to display traps for that switch. Click on the **Switches** tab to view a trap count for each discovered device. To limit the maximum number of events displayed by the Notifications application, enter the desired maximum number in the field to the left of the **Change Max** button and click **Change Max**:

If the default of 30,000 traps logged by the server proves inadequate, it can be changed in the Notifications screen in the **Preferences** application.

6.1.2 Password File Security

Passwords are stored within the OmniVista installation directory on the server machine at \data\tables\security. You need to keep this directory appropriately secure.

6.1.3 Audit Log

The Audit application displays and maintains log files that record the activity of various applications and users in the system. Logs are automatically archived. When a Current Log File reaches its maximum number of entries (configured in the Preferences application), the current log is copied, indicative data is added to the end of the file name (like the date and time when the file was copied), and the file is archived. The contents of the original file are then cleared, making it ready to accept new entries. With the exception of the server.txt file, log files can also be manually archived. The files can also be exported as a .csv file.

6.1.3.1 server.txt File

The maximum server.txt file size (configured in the Preferences application) is 30 MB.

6.1.4 Server Shutdown Procedure

The recommended shutdown procedure for the OmniVista server is to use the Shutdown button in the OmniVista Control Panel application (in the OmniVista client, under "Administration").

6.2 Troubleshooting the Server

6.2.1 Client Cannot Connect with Server

When you attempt to login as an OmniVista client and the client cannot contact the server in any way, you get the following message on the client:

> **Login Failed on Server** <*server IP address*> **port** <*port number*>**. Can't connect to server at** <*server IP address*>**. Connection refused to host:** <*server IP address*> **. Connection refused: no further information.**

This message may be issued due to the following possible error conditions:

- Network is down
- Server machine is down
- OmniVista server is listening on a different port
- Client and server are not running the same version of OmniVista.

6.2.2 OmniVista Server Fails to Run

When the OmniVista Server fails to load, the server.txt file looks something like this:

15 Mar 2011 10:58:01 INFO : ----------
15 Mar 2011 10:58:01 INFO : Starting OmniVista Server 1.0GA (Build 122, 3/12/2001)
15 Mar 2011 10:58:01 INFO : Server Location: 10.255.12.163
15 Mar 2011 10:58:01 INFO : Server Port : 1127
15 Mar 2011 10:58:01 INFO : Starting Security Services...
15 Mar 2011 11:15:37 ERROR : Exiting after fatal error. Security Service Error. Could not create Security Server. Could not bind SecurityServer
rmi://10.255.12.163:1127/SECURITY_SERVER to RMI registry. Couldn't rebind name 'rmi://10.255.12.163:1127/SECURITY_SERVER'. Exception creating connection to: 10.255.12.163. Operation timed out: no further information.

6.2.3 Possible Causes of a Server Run Failure

Following are some of the possible causes of an OmniVista Server launch failure.

Server Machine IP Address Incorrectly Set in OmniVista

The IP address of the server machine may not match the IP address specified in the properties.conf file. This plain ASCII text file is located in the OmniVista installation directory on the server machine. For example, on Windows, assuming the default installation location was used, this file is located at:

C:\Program Files\Alcatel OmniVista 2500\properties.conf

Solution: Make sure the IP address specified for the xyserver.location parameter in the properties.conf file matches the actual IP address of the server machine.

Inadequate Disk Space

OmniVista Server will not start if there is inadequate disk space ('no disk space' error).

Solution: Free up disk space.

6.2.4 Server Message Log File

The OmniVista Server writes informational and error messages to the plain ASCII text file, server.txt. This file can be viewed in the Audit application. This file is located in the OmniVista installation directory on the server machine at data\logs\server.txt.

7.0 Known Problems

7.1 Known General Problems

7.1.1 OmniVista Server Must Be Run As "ROOT" on UNIX

On Unix platforms, the OmniVista server must be run as "root". To receive traps on the default port of 162 on Unix, the receiving process must be running as the super user (root). The OmniVista server must be run on UNIX as root for traps, TFTP, and syslog.

Workaround: On Unix, become the super user before starting up the "OVServer" script, or start it up from the Unix boot process.

PR# 38215

7.1.2 Configuring Traps on AOS Switches With OmniVista Does Not Work Properly if Configured With SNMP Community Map Mode Enable

Configuring traps on an AOS switch with OmniVista will not work properly if the switch has been configured with "snmp community map mode enable". The entries created by OmniVista in the switch station table will use the community string that the switch was discovered by, for the "user name" that table requires. If community map mode is enabled, the community string will likely not be the name of an snmp-enable user, so the traps will not be sent. No error messages will appear in OmniVista trap configuration.

Workaround: The user name to be used must be specified to OmniVista in the "Trap Station User name" field of the switch "edit" dialog.

PR# 73566

7.1.3 Cannot Specify the Order In Which Ping Sweep Ranges Will Be Searched

Although OmniVista allows the user to enter more than one Ping Sweep range in the AutoDiscovery Wizard, there is no way to specify the order in which these ranges will be searched. A switch which appears in multiple subnets may be discovered by any of the addresses that it responds to, and will thereafter be known to OmniVista by that IP address, even though the user may have preferred it to be known by one of its other addresses.

Workaround: If a switch is automatically discovered by one address, but you would prefer it to be known to OmniVista by a different address, simply edit the device in OmniVista and select the desired alternate address manually. Thereafter, OmniVista will remember to use that address for that switch. (Bring up the Topology application, click on the Switches node, then right-click on the appropriate switch and select "Edit" from the pop-up menu. Then pick the desired alternate address from the "IP Address" drop-down menu).

PR# 74278

7.1.4 Installer Prompts For Maximum Memory Size For the Client and Server, But There is No User Interface for Changing Them

The installer prompts for a maximum memory size for the OmniVista client and the OmniVista server, but there is no user interface for changing these values once the product has been installed.

Workaround:

Server: If you want to change the servers maximum memory on **Windows**, you must modify the ***wrapper.conf*** file and restart the service. To change the servers maximum memory on **other platforms**, you must modify the ***RunOVServer.lax*** file and restart the server.

Client: To change the maximum memory for OmniVista client (**on any platform**), edit the ***OmniVista.lax*** file.

Edit the applicable file using a text editor such as vi or notepad and search for "-Xmx". You will find something like "-Xmx384m". Change the number in this argument to the desired limit in megabytes, e.g., "-Xmx512m". Do not forget the 'm' at the end.

PR# 75063, 116798

7.1.5 Previously Existing Filters For VLAN Tables and Security's "Users and Groups" are No Longer Available After Upgrading From Earlier Versions

When upgrading from earlier versions of OmniVista to OmniVista 2.3, the previously existing filters for VLAN tables and Security's "Users and Groups" are no longer available.

Workaround: The filters can be reentered, if desired.

PR# 76251

7.1.6 OmniVista Server Fails to Restart If Running in a Command Line Window on Windows

The server will fail to restart when using the Control Panel's "Restart" function or the Server Backup's "Backup" or "Restore" functions.

Workaround: Run the OmniVista Server as a Windows Service when on the Windows platform (this is the normal way that OmniVista is installed).

PR# 90820

7.1.7 Out of Memory and JVM Crash on Server if -Xmx Setting Too High

If the -Xmx setting is too high, the server will crash.

Workaround: If running the OmniVista server on a PC it is recommended that you do not run with an -Xmx setting of higher than 1280m. The maximum memory allocation for a windows platform should be 1.2 GB, or "-Xmx1280m" when editing the command line.

> **Note:** For Windows installations, you cannot set the server memory higher than 1216 during an install. If the server has already been installed with the memory set to a higher number, it can be changed using the procedure in Section 7.1.4.

PR# 91414

7.1.8 Firmware Cannot Be Backed Up When Backing Up OS6100 Series Switches

When backing up OmniStack Series switches, there is no way to backup the firmware: only the configuration files can be backed up.

Workaround: There is no known workaround at this time.

PR# 74855

7.1.9 OS6024 Devices With 16 MB CMM Return Invalid OID Errors During Discovery

OS6024 devices with (16 MB CMM) return invalid OID errors during discovery. This prevents the Software Version for the device in the Devices Table to be empty and failure to display Spanning Tree status in the VLAN application.

Workaround: Please install Software for OmniStack OS6024 - 16 MB CMM - version "V2.6.202" or better.

PR# 75055

7.1.10 Alcatel Router 7750 and Fortigate Do Not Show OEM Links in Topology Maps

Alcatel Router 7750 and Fortigate do not show OEM links in Topology maps.

Workaround: Use manual link.

PR# 92346

7.1.11 Unknown or Invalid 'Mailhost' Error Should Display in the Client's Status Window

When a responder attempts to send an e-mail to an unknown or invalid SMTP, an exception is written to the server.txt.

Workaround: After configuring an SMTP server, got to the E-Mail Preferences screen in the Preferences application to send a "Test" e-mail. Make sure that the e-mail was delivered, and check for error messages in the server.txt log using the Audit application.

PR# 92158

7.1.12 Failures If Server IP Changed After Installation

If the IP address of the PC is changed after the installation, the LDAP server and the OV server will not start.

Workaround:

1. Bring down the OmniVista server, if it is not already down.
2. Modify the properties.conf file, and change the "xyserver.location" line to have the desired IP address and port. For example, for IP address 1.2.3.4 and port 1127, enter "xyserver.location=1.2.3.4:1127"
3. Modify the script that launches the slapd LDAP server.

Modifying the slapd configuration on UNIX/Linux

This script 'privaterun.sh' is found in the 'openldap' directory beneath the OmniVista install directory. Its contents will be something like this:

#!/bin/shtouch slap.log

mv -f slap.log slap.log_old

/export/ov30/openldap/slapd -h "ldap://10.255.11.216:5389 ldaps://10.255.11.216:5636/" -f "/export/home/ov30/openldap/alcatel.conf" -n "OmniVista Ldap Server" 2>&1 | tee -a slap.log.

Change any instances of the computer's old IP address to be the desired new IP address.

Modifying the slapd configuration on Windows

This is more complicated than for the UNIX configuration, since Windows uses a special service called SCM (Service Control Manager) to control the startup, shutdown, and some runtime parameters for services.

The simplest thing to do is modify the Registry field that contains the TCP port URL. Using 'regedt32', find the key "HKEY_LOCAL_MACHINE\SOFTWARE\ldapsvr". It contains a field called "Urls". The URL will look something like this:

"ldap://10.255.11.216:5389 ldaps://10.255.11.216:5636/"

Change any instances of the computer's old IP address in the URL to be the desired new IP address.

4. Restart the OpenLDAP server and the OmniVista Server.

PR# 92921

7.1.13 LDAP Server Starts Automatically After Install, But Not After System Restart (UNIX/Linux)

On UNIX/Linux installations, the LDAP Server starts automatically and the last installation screen tells the user to run OV Server. If at some point after that, the server machine is rebooted, the LDAP Server does not automatically restart and the OV Server complains that it cannot connect to the LDAP Server.

Workaround: After a UNIX/Linux machine is rebooted, manually restart both the LDAP Server and the OmniVista Server.

PR# 98003

7.1.14 On Windows Installations, OmniVista Logs the User Out After Disabling/Enabling the PC NIC

When an OmniVista server is running on a windows platform, if the windows PC loses total connectivity to the network (by unplugging the network cable or disabling re-enabling the network interface) any OmniVista clients will be logged out, even if they are running on the same machine. This is due to a windows behavior of shutting down all local network connections when remote connectivity is lost.

Workaround: When the network access is restored, log into the server again.

PR# 80952

7.1.15 "Failed to Get Certified List for Device" Error During Backup from OmniVista

When a switch is rebooting, if a user tries to initiate a backup using OmniVista, an error may be displayed and the backup may fail. This error may be a complaint about being unable to retrieve a list of files. This is due to the switch not being completely up and some of its subsystems still being in a transitional state.

Workaround: Wait for the switch boot process to be completed before attempting to perform a backup.

PR# 99861

7.1.16 OmniVista Uninstall Fails on Solaris When a Non-Owner Performs the Uninstall

OmniVista uninstall fails when a non owner performs the uninstall on a Solaris box. If you are not logged in as the root or the owner, you can perform the uninstall, but it will not completely uninstall the application.

Workaround: Log in as root to Uninstall OmniVista.

PR# 101193

7.1.17 SNMP Retries Can Cause "No such variable name in this MIB. OID:.." Error

When making configuration changes to a switch using SNMP, the following message may occasionally be seen: "There is no such variable name in this MIB. OID: (some oid)". This can happen if the configuration change included a delete of an SNMP object, and the operation succeed but the switch did not reply to the request until the timeout value expired. When this happens, OmniVista will retry the request, so it will be asking to delete an object that has already been deleted.

Workaround: No action is required, since this is an error from an unnecessary retry, and no harm is done. However, the SNMP timeout value for the switch could be increased to minimize the likelihood of this happening.

PR# 66874

7.1.18 In the Web Client, Tables Can Take a Long Time to Display with Large Networks (3000 devices)

I/E is slow when rendering JavaScript (tables are generated using java script).

Workaround: Some browsers may be slow rendering large tables. A maximum row size of 500 is recommended.

PR# 108580

7.1.19 Extended Daylight Savings Time (DST)

Beginning in March 2007 DST will be extended four weeks, beginning in March and ending in November. Support for the new DST standards exists in the Java Virtual Machine software bundled with OmniVista Versions 3.0 and later. The JVM in OmniVista 2.4.1 does not support for the new DST. See Sun webpage: http://java.sun.com/developer/technicalArticles/Intl/USDST/.Also, it is not supported in some OS Platforms (see below).

All Windows Platforms: Updates to support new DST **not** yet available yet. Latest Microsoft bulletin: http://www.microsoft.com/windows/timezone/dst2007.mspx

Suse Linux: Support for new DST available with OS version 10.1:

See: http://www.novell.com/linux/download/updates/index.html

Red Hat Linux Enterprise 4: Support for new DST available in RHEA-2005:656-6:

See: http://rhn.redhat.com/errata/RHEA-2005-656.html

Solaris: Support for the new DST in Solaris releases as follows:

* Solaris 8 with patches 109809-02 or later and 108993-52 or later
* Solaris 9 with patches 113225-03 or later and 112874-33 or later
* Solaris 10 with patches 122032-01 or later and 119689-07 or later

  See: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102178-1

PR# N/A

7.1.20 Server Slow in Communicating with the Client When a Regular Poll is in Progress

When one of the regular poll cycles is being executed on the server, the responsiveness will be much slower, for example as much as 4x slower for performing a locator browse, slower for retrieving traps.

Workaround: No workaround at this time.

PR# 104829

7.1.21 Known Up At" Updates With the Switch's First Response During a Poll, Not Its Last

The "Last Known Up At" timestamp is not continuously updated on every successful I/O to the switch. It is updated whenever OmniVista notices a down-to-up transition, and at the start of a successful period or manual ping or poll

from OmniVista. It is also updated upon receipt of a trap from the switch if the current known 'lastKnownUpTime' is more than 10 minutes older than when the trap was received.

Workaround: N/A

PR# 104627

7.1.22 Server Takes 22 Minutes to Shutdown If a Large Number of Statistics Profiles Exist and the Server Has Just Started Up

The server may take a long time to shutdown if a shutdown is initiated immediately after startup, and a large number of statistics profiles exist. This can increase the installation time of optional packages when upgrading from an earlier OmniVista package, since each optional package installation forces a server restart.

Workaround: There is no workaround at this time.

PR# 108318

7.1.23 AMAP Links Not Supported for OmniVista 3600 Air Manager Before 3.1.0.13

AMAP links are not supported for OmniVista 3600 Air Manager prior to build 3.1.0.13.

Workaround: AMAP is not supported on OmniVista 3600 Air Manager devices before build 3.1.0.13. OmniVista 3600 Air Manager devices running prior versions cannot show AMAP links.

PR# 117244

7.1.24 McAfee 8.0.0 Blocks Access to Mail Server for OV Responders on Windows Systems

On a Windows computer with McAfee 8.0 or later installed, OmniVista Server and Client may fail to send notification e-mails because the system cannot access a mail server.

Workaround: Disable 'Prevent mass mailing worms from sending mail" function from Access Protection in McAfee 8.0 or later.

PR# 118240

7.1.25 Newly Added Printer Is Not Recognized by OV Client Until Client is Restarted

When adding a new printer to the machine running OmniVista Client, the client will not "see" this new printer until it is restarted.

Workaround: Restart OmniVista Client.

PR# 109463

7.1.26 Unable to Choose Installation Directory When Installing Optional Packages

OmniVista will not allow the user to choose the installation directory when installing Optional Packages (e.g. Policy View).

Workaround: OmniVista always displays the most recent installation path for adding optional packages. Install additional packages to an existing installation before you install a new version of OmniVista.

PR# 123909

7.1.27 OmniVista 3.4 b34 Server Will Not Start Because a Java VM Cannot Be Created

OmniVista 3.4 b34 server will not start because a Java VM cannot be created.

Workaround: Maximum size of JVM in windows is 1280MB. Java VM needs contiguous memory and in some configurations based on applications this memory size may have to be reduced. OmniVista server max memory on Windows has been reduced to 1216MB to help with this problem.

PR# 123195

7.1.28 OmniVista Server Will Not Start - 'java.net.UnknownHostException' Error Due to Missing /etc/hosts Entry

OmniVista server will not start and server.txt shows the following error: RMIBase constructor. The IP Address 'NMS-LINUX-148.alcatel-lucent.com: NMS-LINUX-148.alcatel-lucent.com' is unknown or invalid.

Workaround: For some machines, the hostname is configured along with IP address using DHCP. This is not a recommended setup. If there is no automatic resolution scheme available to translate the assigned hostname, a static name resolution is required. Enter 'uname -n' to determine the hostname and add an entry in /etc/hosts to resolve that hostname to the IP address of OmniVista server.

7.1.29 OmniVista Client in Redhat Linux Cannot Connect to Remote OV Server - '..Invalid argument or cannot assign requested address' Error Due to Improper Hostname

OmniVista requires a valid IP address for OV Server to call back to OV client. Hostname configured as localhost will resolve to a loopback address, which does not allow OV Server to do a call back.

Workaround: Change hostname using hostname <assigned-hostname> command and persist the host name by modifying /etc/sysconfig/network. Also, make sure to have an entry in /etc/hosts that resolves the <assigned hostname> to the address of OmniVista server.

7.1.30 OV Client Port Always Changing the Destination Port When Connecting Server After Service Down

OmniVista uses port 1127 (specified by user at installation time) but more ports are opened between client and server. Why are these random ports opened? Is there any way to know and fix the ports opened to specific port.

Workaround: The OmniVista Client and OmniVista Server cannot be separated by a firewall. The 1127 port is only used for part of the communication (primarily for login and then to initiate other communications based on client/server agreement). The other ports opened are random, as needed. The OmniVista Client should have full access to the OmniVista Server.

PR# 157088

7.1.31 OV PermGen Out of Memory Error

User receives a “java.lang.OutOfMemoryError: PermGen space” error message.

Workaround: Increase the PermGen size using the following VM options (for example doubling the existing numbers): -XX:PermSize=100m -XX:MaxPermSize=200m.

Server: To change the PermGen size on Windows, modify the wrapper.conf file and restart the service. To change the PermGen size on other platforms, modify the RunOVServer.lax file and restart the server.

Client: To change the PermGen size for OmniVista client (on any platform), edit the OmniVista.lax file.

Edit the applicable file using a text editor such as vi or notepad and search for "PermSize". Change the PermGen sizes to the desired values in megabytes (e.g., "-XX:PermSize=200m -XX:MaxPermSize=400m"). Do not forget the 'm' at the end.

PR# NA

7.1.32 OV 2500 Client Unable to Log into the Server After Upgrade from 3.4.2 to 3.5.2

Server.txt contains error: "Unexpected serious error: java.lang.OutOfMemoryError: Java heap space". OV 2500 client is unable to log into the server after upgrading from 3.4.2 to 3.5.2

Workaround: Allocate more memory in –Xmx parameter (see procedure in Section 7.1.4). It is also recommended to upgrade the JVM to Build 30 or 31. Also, make sure there is adequate memory/processor speed for your configuration. Refer to Section 2.2 – “Recommended System Configurations”, for recommended memory/processor requirements. Note that these requirements represent minimum requirement for common configurations. You may need more memory.

PR# 167228

7.1.33 "socket operation on non-socket: connect" Error After a Few Minutes of Inactivity When Logging In

"Socket operation on non-socket: connect" error, "OutOfMemoryError: Java heap space" error after a few minutes of inactivity when logging in.

Workaround: If you are upgrading from an older version of OmniVista (e.g., 3.4.x to 3.5.2) you must increase system memory to support new features included in the newer releases. Refer to Section 2.2 – "Recommended System Configurations", for recommended memory/processor requirements. Note that these requirements represent minimum requirement for common configurations. You may need more memory.

PR# 168302

7.1.34 "outOfMemory:PermGen" Error During Class A Network Discovery

Customer gets "outOfMemory:PermGen" Error During Class A Network Discovery.

Workaround: Install OV 3.5.2 Post GA Maintenance Build (3.5.2 Post GA Maintenance Build 16). Also, make sure there is adequate memory/processor speed for your configuration. Refer to Section 2.2 – "Recommended System Configurations", for recommended memory/processor requirements. Note that these requirements represent minimum requirement for common configurations. You may need more memory.

PR# N/A

7.2 Known Statistics Problems

7.2.1 Existing Profiles in the Statistics Application, Based on the Original IP Address, Do Not Get Updated to the Alternate IP Address

In Topology, it is possible to modify the discovery list by changing an IP address to an alternate IP address using the "Edit Discovery Manager Entry" dialog. However, existing profiles in the Statistics application, based on the original IP address, do not get updated to the alternate IP address and result in no new data being collected.

Workaround: If an IP address is changed to an alternate IP address, existing profiles based on the original IP address will need to be updated manually if the collection of new data is required. This can be done by removing the performance variable in the Legend Table containing the original IP address and replacing it with the same performance variable using the alternate IP address.

PR# 74463

7.2.2 The Statistics Application in OmniVista Does Not Support any ATM Performance Monitoring

The Statistics Application in OmniVista does not support any ATM performance monitoring.

Workaround: There is no known workaround.

PR# 75659

7.2.3 Client OutOfMemory When Opening Large Statistics Profile

When the user tries to open a statistics profile, if the product of the number of variables monitored by the number of days the user is trying to view is too high, the client runs out of memory.

Workaround: A good rule of thumb is that the number of variables monitored by the number of days open in the client must be less than 1,000 when running on Windows. Typically, these memory requirements match closely the ones of OmniVista client. That is, we assume here that Statistics is the only application open on this client. For example, if your polling frequency is 20 seconds and you apply this formula and find 1,000, this much data will use approximately 1.3 GB of memory.

Here are a few examples of client memory consumption:

- 1 variable * 1 day = 2 MB
- 1 variable * 10 days = 17 MB

- 1 variable * 30 days = 50 MB
- 10 variables * 1 day = 17 MB
- 10 variables * 10 days = 167 MB
- 10 variables * 30 days = 500 MB
- 100 variables * 1 day = 150 MB
- 100 variables * 10 days = 1.7 GB
- 100 variables * 30 days = 5.1 GB

Note: Discovery List items also use memory. Here is a quick breakdown of how much extra memory is required to open a statistics profile, depending on the number of devices in the Discovery List:

- 100 switches = 7.41 MB
- 1,000 switches = 74.08 MB
- 2,000 switches = 148.16 MB
- 3,000 devices = 222.24 MB

PR# 100011

7.2.4 6200 Port Utilization Spikes to 100% Approximately 3x Per Minute

On OS6200, port utilization spikes may be observed in statistics if the user sets the poll frequency to aberrant values, such as 1 second.

Workaround: Set polling frequency to more standard values. Greater than 20 seconds is recommended.

PR# 108629

7.2.5 If a Statistics Profile Includes a Switch that Is Down That is Not Known to Be Down All Statistics Polls Are Slow

If an active Statistics Profile includes a switch that is down or no longer reachable, and if that switch is not known to be down by OmniVista (i.e. is not marked with a red icon), then all Statistics polls to all switches will occur less often.

Workaround: There are two workarounds:

In Topology, make sure that the File menu's "Polling" option is checked, or alternatively that the red/green Stop/Start Polling control in the button bar is in the green "active" state. This will cause OmniVista to check for down switches every few minutes.

OR

If you don't want to leave routine polling enabled, and you notice that statistics are polling less often than normal, go to the Switches table in Topology, select all switches, right-click, and select "Ping Switch" or "Poll Switch" from the pop-up menu.

PR# 109353

7.2.6 Renaming a Profile Causes the New Profile Name to Display in the OmniVista Title Bar

In Statistics, if the user renames a profile, OmniVista's title bar is updated to reflect the new name. This can cause confusion when a different profile is already loaded, as the name displayed in the title bar will not match the loaded profile's name anymore.

Workaround: There is not loss of functionality; loading a new profile or restarting the Statistics client will update the title bar properly.

PR# 119353

7.3 Known Topology Problems

7.3.1 AMAP Links for OS6148/6124 Stack to 6300-24 Do Not Show Up in Topology Map

AMAP links for OS6148/6124 stack to 6300-24 do not show up in Topology Map.

Workaround: The AMAP entry is OK when the connection is between the 6148M (master) and the 6300-24.

PR# 86423

7.3.2 Topology:Devices:Link Agg Ports Table Filter Dialog: Column Slot/Port doesn't allow the "/".

Topology:Devices:Link Agg Ports Table Filter Dialog: Column Slot/Port doesn't allow the "/", so you can't input something like "1/2".

Workaround: Behind the scenes, the slot/port is really an IfIndex. The formula for creating the IfIndex for AOS switches is (port + slot * 1000) so 9/15 = 9015 and 10/10 = 10010. Using the results of this formula in the slot/port textbox and filtering will work just fine.

PR# 100046

7.3.3 Topology Popup Menu Help Description for "Show STP Ports" Needs to be Updated

"Designated Root Bridge" description should read: "Designated Root Bridge ID - The IP or MAC address of the Designated Root Bridge for the port. If the port is an Edge Port, the field will display ffff-ffffff.ffffff."

Workaround: N/A.

PR# 102830

7.4 Known Resource Manager Problems

7.4.1 Resource Manager (Version 2.3 and Up) Only Supports Upgrades from 2.x.x.x and Up on the OS6300-24

OmniVista Resource Manager (Version 2.3 and up) only supports upgrades from software version 2.x.x.x and later on OS6300-24 switches. Do not attempt to upgrade from 1.x.x.x with Resource Manager.

Workaround: Upgrade OS6300-24 switches with 1.x.x.x manually to 2.x.x.x. Once you do this, you will be able to use Resource Manager to perform the upgrade.

PR# N/A

7.4.2 Long Delays Occur When Polling and Pinging About 40 Switches, Then Starting a BMF Upgrade

Resource Manager Backup Files may fail to appear in the Backup Files table after reloading Resource Manager Application on UNIX platforms.

Workaround: Disable polling prior to performing a BMF upgrade.

PR# 86393

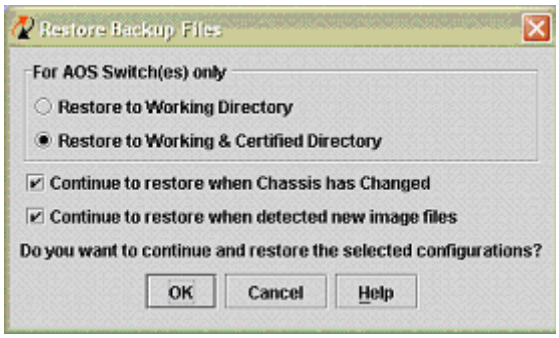
7.4.3 Resource Manager BMF Upgrade Will Fail on 32 MB Flash with 5.1.6.R01 Firmware Loaded

Resource Manager Backup Files may fail to appear in the Backup Files table after reloading Resource Manager application on Unix platforms.

Workaround: These upgrade steps are performed on the 8800 switch. Please use the "shadmin_Fwebimageclean.script" for the 7000 switch.

1. Open the Resource Manager application and perform a full backup on the switch you will be upgrading.
2. Open the Telnet application and run the canned script called "shadmin_Ewebimageclean.script".

3. Open the Preferences application and set the system-wide preferences/Resource Manager minimum upgrade space to 4000 (Kbytes) and apply all.
4. Open the Resource Manager application and perform an FPGA upgrade.
5. After the switch has been reloaded, open the Resource Manager application and perform a restore on the switch. Please use the following settings when restoring.



6. Open the Topology application, right-click on the switch, and perform a "Copy working to certified." This will certify and synchronize the switch.

You have now completed the FPGA upgrade and all image files will have been restored on the switch.

PR# 91502

7.4.4 OmniVista Resource Manager Firmware Upgrade "install" Command May Fail

When performing a major AOS switch firmware upgrade using Resource Manager, for instance upgrading from 5.3.1.R02 to 6.1.2.R03, the install command which gets run at the end of the upgrade may fail due to firmware incompatibility. In these cases the install command must be run after Resource Manager reboots the switch.

Workaround: After rebooting the switches for which a major upgrade has been performed, select the desired switches in the OmniVista Telnet/SSH application and run the canned script - "shadmin_install_images.script".

PR# 102188

7.4.5 Some Button Icons in OmniVista Are Missing in Solaris Native Look and Feel Mode

Running OmniVista in Solaris Native Look & Feel mode causes some buttons in OmniVista applications to shrink, which will make the icons for the buttons to be hidden.

Workaround: Always use Java Look & Feel mode when running OmniVista on Solaris.

PR# 84998

7.4.6 Resource Manager Schedule Time Not In Sync with Server

If the client and server are not synchronized to the same time, use of general scheduling functions using the client GUI may result in inconsistent results. All scheduled operations are executed on the server, so all times are set relative to the server time.

Workaround: Synchronize the client and server machines, possibly using NTP services.

PR# 79977

7.4.7 Cannot View a Captive Portal File in Switch File Set Tab with Windows Vista

When running Windows Vista, user is unable to view Captive Portal files in the Switch File Set Tab in Resource Manager.

Workaround: There are two options for a workaround.

1. Right click the OmniVista launch icon and select "Run as Administrator". or

2. Go to Windows Vista Control Panel/User Accounts, and turn off User Account Control.

PR# 137826

7.4.8 OV Backup Fails with Error "Unable to Create Repository" in the Backup Logs

When attempting to perform a backup in OmniVista, the backup fails with the following message in the Backup Logs: "Unable to Create Repository".

Workaround:

This indicates that you have too much data backed up. While you can increase the memory as described below, you may also want to delete unnecessary logs/backups (specially if they include images). You may also want to delete Telnet script logs to free up memory. To increase the memory allocation, follow the instructions below.

Server: If you want to change the servers maximum memory on **Windows**, you must modify the ***wrapper.conf*** file and restart the service. To change the servers maximum memory on **other platforms**, you must modify the ***RunOVServer.lax*** file and restart the server.

Client: To change the maximum memory for OmniVista client (**on any platform**), edit the ***OmniVista.lax*** file.

Edit the applicable file using a text editor such as vi or notepad and search for "-Xmx". You will find something like "-Xmx384m". Change the number in this argument to the desired limit in megabytes, e.g., "-Xmx512m". Do not forget the 'm' at the end.

PR# 156354

7.5 Known Locator Problems

7.5.1 Locator Does Not Show VLAN of Host for L2 Linkagg 802.1q Port, AOS/XOS Only

VLAN data may not appear in AOS switches with older builds. Locator VLAN reporting will operate properly under the following releases of AOS software and above:

- 5.1.5.193.R04
- 5.1.6.434.R01
- 5.1.6.103.R02
- 5.3.1.175.R02
- 6.1.1.340.R01.

Workaround: Upgrade problem-AOSs to their respective 'working' software.

PR# 95451

7.5.2 Locator Fails to Find IP Address in Live Search Unless User Pings Host First

Locator can only find an IP address if the address is in ARP cache.

Workaround: Ping the host from a switch that supports that subnet. This will add the IP address to the ARP cache and Locator will be able to discover the device as expected.

PR# 123745

7.6 Known Telnet Problems

7.6.1 OmniVista Telnet Menu Bar Edit Drop-Down Menu Is Never Enabled

The Edit drop-down menu in the OmniVista window frame does not enable the editing or deletion of scripts.

Workaround: Use the Edit or Delete buttons in the Create Scripts tab.

PR# 91909

7.6.2 Telnet CLI Scripting Guidelines

The following guidelines should be kept in mind when creating scripts for the Telnet application:

You must always use semicolons to mark the end of a line/statement.

- You must always use semicolons to mark the end of a line/statement.
- Multi-line comments are supported. Single-line comments ('//') are not.
- The dollar sign being used to identify user-defined variables, if you need to use it in another context, you need to go through a variable. For instance, to use it in a JavaScript variable called 'dollar': *var dollar = String.fromCharCode(36)*
- The <tapps>...</tapps> tags are not meant to be used for proper scripting; they are only commodity methods, allowing you to execute one command at a time. In other words, each tapps command must to have its own <tapps> tags.

  For example:

  <tapps>import file1</tapps>

  <tapps>import file2</tapps>

  Rather than:

  <tapps>

  import file1

  import file2

  </tapps>

PR# N/A

7.6.3 Auto Scripting Telnet Sessions (not ssh) Lock Up on Switches with LDAP Auth

When running scripts from OV using telnet protocol, to switches that have been configured for LDAP authentication, sessions to some switches may hang.

Workaround: A simple workaround is to add a few blank lines at the beginning of each script, before the first command. The problem appears to be caused by longer delays introduced by the LDAP authentication, and also appears never to happen using SSH protocol.

PR# 119261

7.6.4 Confirm Response Javascript Fails in SSH, not Telnet

The 'Exit' confirmation response fails when using SSH in Telnet Scripting.

Workaround: Currently, the scripting application automatically confirms 'exit' for usr regardless of Telnet or SSH. For this reason, parsing after the 'exit' command is issued is unnecessary and should be advised against. Simply, that will contradict the default behavior of the application, which has mechanism in place to take care of nuances between SSH and Telnet packages.

PR# 140336

7.6.5 Problems Sending Scripts to OA5510

Impossible to send CLI scripts to OA5510 SR/Te.

Workaround: Make sure the device is discovered to use SSH. This is set by default during discover. But if a user changes SSH to Telnet the user will be unable to send CLI scripts to those devices. The setting can be viewed/edited by right-clicking on the device in the List of Discovered Devices (Topology) and selecting Edit. The Shell Window parameter should be set to "Prefer SSH".

PR# 148036

7.7 Known Other Problems

7.7.1 OmniVista Trap Configuration is Not Available for the OmniStack 5010, 5022, and 5052

OmniVista trap configuration is not available for the OmniStack 5010, 5022, and 5052.

Workaround: Use telnet and the switch's Command Line Interface or User Interface to configure the switch for traps. Refer to the switch's user manual.

PR# 69127

7.7.2 OmniVista Client/Linux/DHCP Cannot Log Into Remote OV Server. Works if Static IP

When a Linux OmniVista client runs on a box that gets its IP address from a DHCP server, this client may not be able to connect to OmniVista Server. This is because the client needs to know the hostname associated with that IP address.

Workaround: Setup a DNS Server that will provide reverse resolution for the pool of DHCP IP addresses by either configuring the client to use that DNS Server (preferred); or using a DHCP Server that is capable of automatically configuring the Linux client to use that DNS Server. Alternatively, the whole pool of IP addresses could be resolved using another method such as storing the information in the client's /etc/hosts system file; but this is much less convenient.

PR# 83449

7.7.3 The Server Process Should Disassociate With Its User Session on UNIX/Linux

When OmniVista is installed and/or the OmniVista server is started using X Window, the server gets terminated when the user logs out from the system.

Workaround: After completing the OmniVista installation either locally or remotely using X Window, log out of the system and use rlogin/rsh/ssh/telnet instead to start the OmniVista server.

PR# 85553

7.7.4 Exception Error When Changing Configuration of AMAP on 6300-24

Changing the AMAP state on OS6300-24 device running software version prior to v2.2.0.3 in the Topology application can return an exception or fails to change.

Workaround: This problem is fixed in OS6300-24 software version v2.2.0.3 or better. Most of the time this problem is benign, even though the exception is returned, the AMAP state is actually changed.

PR# 85553

7.7.5 Install Does Not Prompt User for Syslog Port As it Does for the Trap and LDAP Ports

There should be an Install screen that prompts the user for the Syslog port, and then checks to see if that port is available, like it does for the trap and LDAP ports.

Workaround: St/change the Syslog Port in the Preferences Application.

PR# 91804

7.7.6 Server on Linux Will Not Start with X-window Variable Set by Default in JVM 1.5

On UNIX platforms, the OmniVista 3.1 server may not start properly, or may shutdown prematurely, if the environment variable "DISPLAY" is set in the session used to start it.

Workaround: Explicitly "unset" the environment variable "DISPLAY" before starting the server. Using the c-shell, that would be "unsetenv DISPLAY".

Using BASH, that would be "unset DISPLAY".

PR# 99591

7.7.7 Cannot Stop or Delete a Scheduled Task That is Stuck in an Executing State

If a scheduled task fails to complete, it cannot be rescheduled or deleted from the Schedule application. Attempting to do this will invoke an error message "Task State is not Waiting! It cannot be rescheduled or deleted."

Workaround: The OmniVista Server must be restarted to clear this problem.

PR# 99259

7.7.8 OmniVista Server Goes into Pause Mode in DOS Window if Quick Edit Mode Enabled

OmniVista server goes into pause mode if you click anywhere on the DOS window while running server in the console mode with the Quick Edit Mode option enabled on the DOS window property.

Workaround: It is recommended that this option be disabled. To disable this setting, right click on the top blue bar of the DOS window, click on the properties, click on options, Unchecked the "Quick edit mode" and apply.

PR# N/A

7.7.9 Fortinet Devices Must Be Configured for Discovery

You must add Fortinet devices to Third Party Device Support and add the OmniVista Server IP address to the Fortinet device in order to communicate with it.

Workaround:

1. Use the Preferences application to add the Fortinet OID in 3rd-party preferences. Fortinet uses the OID prefix of 12356 , leaving mib-2 as the directory. Restart discovery if previously open.
2. Make sure the SNMP v1/v2c configuration is made on the Fortinet device. Create the SNMP community and add the OmniVista server IP address to the Host list in the SNMP Community page.
3. Configure Discovery with OEM links enabled, Telnet as default, select snmpv1/v2 and the switch IP address.
4. Go to the Topology application and verify that the switch was added.

PR# 91405

7.7.10 Error Dialog Pop Up on Fortigate Since "Getbulk" Default Max Reps Have Gone From 5 to 10

Some third party devices, including Fortigate, may return the following SNMP error message if OmniVista is configured to manage them with the snmpv2 defaults: "getbulk(10): error-status: 1: Response message would have been too large." This means that the device cannot process some getbulk requests with a maxreps value of 10.

Workaround: When configuring OmniVista to manage these devices, choose a "Maximum Repetitions" value less than the default of 10 (5 or less works with most devices). Or, disable the "getbulk" option altogether.

PR# 104229

7.7.11 Preferences Application Does Not Prompt User to Logout After Changing from Native back to Java 'Look and Feel' in Linux

In Linux, changing the current look and feel may not prompt the user to logout, then log back in again for this change to take effect.

Workaround: The user needs to re-login for this change to take effect.

PR# 109118

7.7.12 "Undo Failed" SNMP Error Messages

AOS switches running release 6.1.3.R01, and 6.1.1.R02 may get into a mode where errors of type "undo failed" are returned for every snmp set operation. When in this mode, the sets are actually succeeding, but an error message is returned for each. This is being worked as a switch problem (PR 108333).

Workaround: Using the switch CLI:

write memory

copy working certified

Poll the switches exhibiting the behavior.

PR# 100937

7.7.13 OmniVista Showing VRRP Address Instead of Physical Address in Topology Tabs

Switches configured for VRRP may respond to SNMP queries on their shared VRRP address, confounding OmniVista. If more than one switch is configured to use the same VRRP address (which normally is the case), then one or more of the switches may respond to general SNMP requests to that VRRP address. This can cause theses switches' main IP address in OmniVista to fluctuate whenever discovery or polling occurs.

Workaround: Create a file on the OmniVista server machine, in *{OmniVista Install Directory}/data/stopdiscover.txt*. Each line of the file should contain an IP address where OmniVista should not attempt to discover a switch. Include all of your switches' VRRP addresses in this file, one IP address to a line.

PR# 117161

7.7.14 OmniVista Access Guardian Returns a Status Note that Policies Have Been Assigned with Read-Only Privileges

If you login as a user with insufficient permission to set Access Guardian Policies and try to set a policy, Access Guardian will display an error message and not perform the action. However, it will erroneously display a message in the status area that the Access Guardian policies were set.

Workaround: Login with NetAdmin permissions.

PR# 119421

7.7.15 OmniVista Quarantine Manager Pull Feature Needs to Be Documented

The new Quarantine Manager Full feature is not documented sufficiently in the help system for Release 3.4.

Workaround:

Quarantine Manager can now use a new Fast Re-cache mechanism for switches that support this feature (6850 release 6.3.1). The previous re-cache mechanism flushed all policies and reloaded all policies from LDAP assigned to the switch. With the new mechanism, the switch will look through LDAP only for the existence of quarantine MAC groups.

To use the new 'Fast Re-cache' mechanism you must first create a MAC group on the LDAP server. The MAC group is created by using the OmniVista Groups Application and Selecting the L2 MAC Groups Tab. Click the New Button and create a MAC Group with the name 'Quarantined' and apply your change. See the Quarantine Manager Configuration on-line help for more information on creating a MAC Group.

The new 'Fast Re-cache' mechanism does not require an ACL to be associated with the MAC Group name. If you are upgrading an existing Quarantine Manager and have already created Quarantined ACL and this ACL has an Action other than "drop", the 'Fast Re-cache' mechanism will not be used and the ACL will continue to work as it did previously.

Note that the name of the MAC group that you created with the Groups application and the name of the 'MAC Group Name' in the QM Configuration Tab must match. Further, the name of the Quarantine MAC group on the switches that use the Fast Re-cache must match as well. By default this name is 'Quarantined'. If you are currently using Quarantine Manager and have modified the Quarantine Mac Group Name in the Configuration Tab to something other than 'Quarantined', you will need change the name of the Quarantined MAC group on the switch to match the name known by Quarantine Manager. To modify the Quarantine MAC group name on the switch use the CLI command:

qos quarantine **mac-group** *mac_group*

where *mac_group* is the name you of your Quarantined MAC group

In addition performing a 'Fast Re-cache' the switch can be set up to provide a remediation server for quarantined devices. The CLI command

qos quarantine *path_url*

*w*here *path_url* is the URL of your remediation server

Then add the IP address of the remediation server (required) and any exception subnets (optional) to the QoS alaExceptionSubnet network group:

policy network group *alaExceptionSubnet ip_addr*

where *ip_addr* is the IP address of the remediation server.

See Chapter 30 "Configuring QoS" the of the *Network Configuration Guide* for more information on how to set the MAC group name and configure a remediation server.

PR# 119415

7.7.16 OmniPCX Traps Sent as SNMPv2 Traps Do Not Show in OmniVista

OmniPCX traps sent as SNMPv2 traps do not show in OmniVista. Instead an error is seen in the audit log.

Workaround: OmniPCX traps do not follow SNMPv2 standards and OmniVista can not find the trap definition in the MIB when it comes as an SNMPv2 trap. OmniVista will display the OmniPCX traps that arrive using SNMPv2 as unknown traps. To handle these traps properly, OmniPCX traps must be sent only using SNMPv1.

PR# 126988

7.7.17 OmniVista Device Discovery on Broadcast IP Address

If a Broadcast address is specified in the PING Sweep Discovery, it can cause OmniVista to wrongly discover devices on the broadcast address in certain cases. For example: IP 172.15.16.42/255.255.255.252, where if Ping discovery is done on subnet 172.16.15.1/255.255.255.0, a device can be discovered on 172.16.15.43, the broadcast address for the given subnet

Workaround: To resolve this problem, the user can adopt one of the following solutions:

- Do not manually discover devices on their Broadcast address.
- Do not include such subnets in Ping Discovery.
- Provide an appropriate Subnet range. in discovery (e.g., 172.16.15.40/255.255.255.252) .
- Add the Broadcast address to the Stop List for OmniVista Discovery as described below.

  Edit the "stopdiscover.txt" file in the directory in which you installed OmniVista. If the file does not exist, create it. Add a line in the file with the IP Address that you do not want to discover (e.g., 172.16.15.43). For multiple devices, you can specify each single IP Address you do not want to discover in a **new line** in this file. When doing Ping discovery, all IP Addresses from this list will be ignored.

  So, if the IP address 172.16.15.43 is added to the "stopdiscover.txt" file, and a Ping Sweep range of 172.16.15.0 172.16.15.254 with mask: 255.255.255.0 is used; the device at IP address 172.16.15.43 will not be discovered because it is in the "stopdiscover.txt" file.

  Note that this Stop List does not apply to device IP addresses that are manually added by the user.

PR# 139245

7.8. Known PolicyView Problems

7.8.1 PolicyView Installer May Fail to Locate OmniVista Basic Installation on UNIX Platforms

If the disk space on "/var" directory is full, PolicyView installer may not be able to locate OmniVista Basic installation.

Workaround: Uninstall OmniVista Basic and free up some disk space on "/var". Re-install OmniVista Basic and then install PolicyView.

PR# 69094

7.8.2 One Touch Functionality in OmniVista PolicyView Shows a Time Lag Sensing State Has Changed

If the user has changed the state of the "qos classifyl3 bridged" flag via WebView, CLI or SNMP, the One Touch functionality in OmniVista PolicyView shows a time lag sensing the state has changed.

Workaround: The switches require polling from Topology before a change of status in this flag occurs. If you change the state of the L3 classification, you must poll the affected switches in order for OmniVista to be aware the state has changed.

PR# 72636

7.8.3 AOS 5.1.5 - PolicyView Possible Recache Failure - Ref 82571

In AOS 5.1.5, SNMP in support of the Policy Management MIB is broken in terms of the table directoryServerTable. This means that PolicyView cannot guarantee it will set the proper LDAP server entry in this table if this table is NOT empty.

Workaround: To ensure that PolicyView will correctly set this table, the user will use WebView and go to the Policy page, then choose Network Services, then LDAP servers. The table of LDAP servers will be shown and the user will then delete all entries. Once completing this, the user will re-apply/notify the switch to re-cache policies using PolicyView. This will ensure the correct LDAP server entry is written to the device so that it may re-cache its policies from LDAP as required. To ensure that PolicyView will manage the switch correctly, the user should use upgrade the switch to AOS 5.1.6.R01.

PR# 83276

7.8.4 OTV Policies Do Not Recache on WinXP Service Pack 2

On Windows XP with Service Pack 2, OmniVista server is unable to communicate with the rest of the world due to the firewall that is automatically installed with SP2.

Workaround: Two very easy fixes:

- Either run OmniVista client on the server computer; Windows will ask the user whether to grant access to javaw.exe; just select to allow it.
- Or disable the firewall

PR# 85026

7.8.5 Cannot Edit Network Groups in NAT Tab for Policies Involving NAT

There is no "Edit Groups" button on the NAT Action tab in PolicyView.

Workaround: You can edit a Network or MAC Group in PolicyView by going to the IP or MAC Condition tab - an "Edit Groups" button is available.

PR# 108438

7.8.6. PolicyView PBR Does Not Work on OS6800, 6850 or 9000 Series Switches

The following version 6.1.3 switches will not properly load PBR actions from policies created by PolicyView: OS6800, 6850 or 9000.

Workaround: For the above mentioned 6.1.3 switches, use OmniVista Telnet scripting to create a policy with PBR actions.

PR# 109233

7.9 Known SecureView-SA Problems

7.9.1 SecureView-SA Unable to Launch Due to Port Conflict

If another process opens the same port as the OmniVista LDAP server, SecureView will fail to initialize with the error message. "Problem running SecureView SA: Initialization failure".

Workaround: Use the netstat command to determine if there is a port conflict. If there is, stop the process that conflicts with the OmniVista LDAP server.

PR# 96800

7.10. Known Quarantine Manager Problems

7.10.1 Switches Added After 'Quarantined' VLAN Is Created Must Be Added Manually to the VLAN

If the user adds new switches, then there is no warning to the user they will have to add the VLANs manually. If you expect to protect your switches, then you 'must' add the Quarantined VLAN to them.

Workaround: This is as per design, since it is not necessarily true that all switches will be included in a Quarantine VLAN. That is a decision that is up to the network administrator. If it is desirable to always include all discovered switches in the Quarantine VLAN, a CLI script could be created to do that and run periodically. Also, In a subsequent release there will be a mechanism called "network segmentation" to specify a subset of the management network to be included in quarantines.

PR# 92018

7.10.2 Attack from Outside the Managed Network Cannot Be Quarantined

A quarantine cannot be applied without determining a local MAC address to be blocked, so an attack coming from outside the managed network can be detected but not quarantined. When this happens, an entry will be written to the Quarantine log stating that the MAC address could not be found for the source IP of the attack.

Workaround: Periodically check messages posted in the OmniVista Audit application quarantine.log to find any entries where QM was not able to determine the associated MAC address from the Locator database. If the switch the attack is coming through a device that is not managed by OmniVista, adding that switch to the OmniVista managed devices should allow Quarantine Manager to find the MAC address of the attacking IP.

PR# 92017

7.10.3 Quarantined MAC Group Address Cannot Be 00:00:00:00:00:00

The "Dummy" MAC address recommended for the Quarantined MAC group (written into the Telnet canned script) is invalid in Policy Manager on the switch. It rejects such a MAC group created in L2 Groups in OmniVista and send via SecureView; and the Policy Manager events log does not identify the problem.

Workaround: Do not use all zeros in the MAC group for SecureView ACLs.

PR# N/A

7.10.4 Port Disable Not Possible on Cisco Catalyst 3500xl (public/private on 10.255.11.99)

Attempts to use the Quarantine Port Disable Feature with the Cisco Catalyst 3500xl switches may disable the incorrect port. This is caused by a problem in the snmp mib-2 support available from that device.

Workaround: Do not use the port disable function with the Cisco Catalyst 3500xl.

PR# 99238

7.10.5 In OmniVista 3.1, OmniVista 3600 Air Manager Rule 3 Trigger Fails Due To syslog Message Changes in 2.5.3.0 From OAW4308 Controller

Due to a change in the format of OAW4308 Controller syslog message in release 2.5.3.0, one of Quarantine Manager's built-in rules no longer triggers a quarantine action in OV 3.1.

Workaround: In the Quarantine Manager application:

1. Click on the **Rules** tab.
2. Select the rule with the name "OA WLAN: Station w/ Rogue AP" and click the **Modify** button.
3. Modify the "Trigger Expression:" field from:

   "STA with MAC.*associating with Rogue AP BSSID" to

   "STA with MAC.*associating.*Rogue AP".
4. Click on the **OK** button.

The new trigger expression will work with both the old and new syslog message.

PR# 109372

7.11 Known VLAN Problems

7.11.1 Spanning Tree Status Changes Fail for OmniStack Series Devices

Trying to change Spanning Tree setting for OS6124 or OS6148 devices in OmniVista VLAN application does not work.

Workaround: OS6124 or OS6148 devices do not support per VLAN Spanning Tree. OmniVista reports current Spanning Tree status for these devices. Use Telnet or Web Browser to modify the Spanning Tree for these devices.

PR# 95561

7.11.2 Unable to Change the VLAN ID When Editing an IP Interface

When editing IP Interfaces for a device in VLAN application, the VLAN ID does not change when editing an IP Interface using switches with software level 5.1.6.

Workaround: Delete the IP Interface entry and recreate a new entry with proper values or use WebView to make this change. This problem is fixed in switch software 6.1.1 or better.

PR# 97789

7.11.3 Older Switch Software Causes Wrong STP Root Instances to be Displayed in "Show STP Ports" View

Some older switch software causes OmniVista to display incorrect STP root instances in "Show STP Ports" view.

Workaround: The following switch software versions fix this problem:

- OS68 5.3.1 R02 build 160
- OS7 5.1.6 R01 build 425
- OS7 5.1.6 R02 build 89
- OS9 6.1.1 R01 build 688
- OS97 6.1.1 R02 build 103
- OS6850 6.1.2 R03 build 117

PR# 102692

7.11.3 Unable to Create a VLAN on OS6200

Omnivista cannot assign tagged vlan to a 6200 interface if the target interface is "access mode".

Workaround: Use cli or webview to change the interface to "trunk mode".

PR# 139159

7.12 Known Server Backup Problems

7.12.1 Server Backup File Size Limited on 32-Bit Platform

A 32 bit platform is limited to Server Backup file size of 2GB.

Workaround: The maximum size of the backup file supported will depend on Operating System.

PR# N/A

7.12.2 Server Backup Can Fail if FTP Is Not Used for Backup or Restore

Schedule Backup or Restore can fail with "Can't update Scheduled Task Manager" error. This error only shows up in cases when FTP is not used for Server backup or restore.

Workaround: When defining the Backup or Restore task, make sure to create the definition with FTP enabled. Once the FTP Port number is set and saved, the FTP setting can be disabled and this error will not appear.

PR# 98432

7.12.3 Authentication Fails for Backup with 'Passwordless' RSA, SFTP to Remote Machine

SFTP allows connections either using passwords, or through the use of pre-installed public keys on both sides of the connection. OmniVista does not take advantage of any public keys that may have been installed to allow passwordless' connections via SFTP, so any use of SFTP in OmniVista must include the correct password.

Workaround: Supply both the correct username and the required password when configuring SFTP in OmniVista.

PR# 109679

7.12.4 Server Backup Generates Large File Sizes on Older Versions of OmniVista

OmniVista versions prior to 3.4.1 allow the user to erroneously choose a location under the OmniVista 'data' directory as the repository for backup files. If the user does this, when each backup is performed, the new backup file will be twice the size of the previous since the old backup files are also be backed up along with the rest of the OmniVista data.

Workaround: Manually move the backup files from the OmniVista installation 'data' directory (or any sub-directory in the data directory) to outside of the data directory. Using the Server Backup application, remove the configuration entry/entries that refer to the 'data' directory . Then, create a new valid repository configuration using the new Server Backup location.

OmniVista 3.4.1 does not allow User to specify the data directory for Server Backup. If using old versions that specify data directory, Server Backup will not be performed and error will be logged to inform the User.

PR# 120126

7.13 Known Web Services Problems

7.13.1 Topology Table Takes 14 Minutes to Display with 3,000 Devices

Some Browser may be slow in rendering tables with a large number of rows.

Workaround: Recommend a maximum row size of 100.

PR# 108580

17.13.2 Unable to Start the Webservices (Apache server) With OV 3.5.1, Build 10

User with OV 3.5.1, Build 10 - 32 bit in Windows 2008, with 64 bit server. The Webservices ran fine 3.5.0 GA. after upgrading to OV 3.5.1, Build 10, the user is unable to start the Webservice. The following error is seen when he is trying to start the web services.

Workaround: The JVM version used in OV 3.5.0GA is 1.6.0_16, which was compatible with the 32-bit Tomcat that was being used in Webservices, which is why it worked in OV 3.5.0. In OV 3.5.1GA, we added real support for 64-bit Windows 2008 Server, and updated our JVM version to 1.6.0_18. However this JVM version is no longer

compatible with 32-bit Tomcat, which is why we have added 64-bit version of Tomcat (Webservices) in OV 3.5.1GA in order to support the 64-bit Windows 2008 Server platform. So the recommended way to run OV on 64-bit Windows 2008 Server is to use the 64-bit version of OmniVista and Webservices.

PR# 156359

8.0 Problems Fixed

8.1 Problems Fixed Since Release 3.5.1

- Unable to assign UNP profiles via OV for OS9000 and OS9000E Devices (PR 151284)
    - OS 9000 and OS 9000E running 6.4.3.R01 and newer now support "VLAN-only" UNP. When applying a UNP to these switches, only the UNP name and associated VLAN ID are sent to the switch. Any HIC flag or policy list name specified in the UNP is ignored. This information is displayed in the message area and logged in Access Guardian Audit Log File.
- OV Policy List Name displays incorrectly in UNP (PR 151616)
    - OV now allows selection of empty policy list name to be associated with a UNP.
- Link not removed from Topology map after moving the node (PR 153548)
    - Link is now removed from the Topology map after moving the node. If the user wants to keep track of a link even if it goes down, configure that link as a "Manual Link".
- Unable to create IP Router interface in non-default VRF for OS10K (PR 154865)
    - Make sure the Rushmore Device is running Release 7.1.1.1668.R01 or later. Also, make sure the SNMP Timeout is set to 10 seconds (10000 milliseconds), with a Retry Count of 1. (Can be set in the Topology Application).
- 'Get Bulk' of some tables timed out in OS10K using SNMPv3 User. Tried to increase the Time out from 5 seconds to 50 seconds , but issue persists. (PR 154920)
    - Make sure the Rushmore Device is running Release 7.1.1.1668.R01 or later. Also, make sure the SNMP Timeout is set to 10 seconds (10000 milliseconds), with a Retry Count of 1. (Can be set in the Topology Application).
- If policy is assigned to switch with UNP, it cannot be removed from switch unless deleted in LDAP (PR 155041)
    - If a policy is part of a policy list that has been assigned to a switch via UNP, you cannot remove the switch using the UNP Wizard picker. A warning message will be displayed, instructing the user to either delete the associated policy list or remove the policy from the policy list, in which case the switch will be automatically removed from the policy. The policy/policy list can then be removed from the switch by doing a re-cache (NOTIFY) from the Expert tab.
    - Adding/Deleting a policy to/from a policy list will automatically update any switch roles that contain this policy list with the updated policies. When a UNP that contains this policy list is assigned to the switch, the content of the policy list will be updated and the associated policies will be added/deleted on the switch.
    - When a UNP is removed from the switch, all of its policy lists and associated policies are automatically removed from the switch if not shared by other UNPs on the switch.
    - Removing a policy list from a UNP and then assigning the UNP to a switch will not automatically remove the policy list and its associated policies from the switch. To remove the policy list on the switch, delete the policy list from the Policy List tab and then do a re-cache (NOTIFY) from the Expert tab.
    - Request for updating mibset for Fortinet devices (PR 156559)
        - Fortinet MIBs updated to OS4.0.

- "getbulk" Errors From 3rd Party Devices (PR 156643)
    - SNMPv1 is now obsolete. In release 3.5.2 of OmniVista, SNMPv2 is the default for all devices. A user may see this error occasionally because devices that previously used SNMPv1, will attempt to use SNMPv2 with "getBulk, which may generate this error. If using SNMPv2/v3, reduce the number of max repetitions. If the error persists, turn off the "getBulk" option as a workaround.

8.2 Problems Fixed Since Release 3.5.0

- Collisions counter does not update (PR 127366)
- Ethernet Interface Statistics table does not show Tx/Rx Counters correctly (PR 127906)
- OV scheduled backup based on MAPS is not backing up devices added after creating the scheduled backup (PR 14121)
- Status bar shows AMAP is inactive after polling cycle (PR 142553)
- RADIUS authentication does not use NAS Identifier in OV Release 3.4.2.13 (PR 142643)
- A license key with a device count that is a multiple of 31 is decoded by OV as invalid (PR 143288)
- Restoring a backup in RMan displays an error message even when "Continue Restore" option is selected (PR 143290)
- [NCV] native support of OA5510 R2.3.2 device for KPN - NCV project (PR 144103)
- [NCV] native support of OA5300 R3.3.1 device for KPN - NCV project (PR 144104)
- OmniVista fails to discover information over Multiple VPRNs fo SR7750 version 7.0 (PR 144877)
- On OA5300, CLI script does not end while doing restart in the script (PR 148278)

8.3 Problems Fixed Since Release 3.4.2

- SecureView ACL notify policy on wrong switches (PR 138875)
- Collisions counter does not update (PR 127366)
- Ethernet Interface Statistics table does not show the Tx/Rx Counters correctly (PR 127906)
- Service will not start after a server backup if there is no disk space (PR 129126)
- OV Locator displaying invalid port number on third party switch in Locator IP/MAC search results (PR 133081)

8.4 Problems Fixed Since Release 3.4.1

- Java Heap Space Error During Server Backup (PR 119431)
- OV3.4. client freezes while using Telnet/SSH in an interactive session (PR 121651)
- 'OutOfMemory' Message if a Large Number of Devices Are Selected in a Device Table (PR 123464)
- Omni Vista Fails to Report IP Address as Unreachable When Admin Downed (PR 122850)
- Limited Single User Install is Not Refused When Downgrading a License on Suse Linux (PR 123958)

8.5 Problems Fixed Since Release 3.3

- View Device in Current Window" Option Creates an Invalid Entry in Browse History (PR 71784)
- Exception in Thread "AWT-EventQueue-0" When Closing Help Window (PR 95953)

- Using Invalid Characters for a Switch Name Results in Failure to Access the Device with OmniVista (PR 101618)
- Policy Log I/O Exception Returned on Solaris/Linux Server (PR 108195)
- Topology Right-Click Reboot From Working "Reboot in 1 or 2 Minutes" Causes Device to Turn Red (PR 109117)
- A Switch-Picker Change From "All" to "None" Does Not Turn Off Validation in PolicyView (PR 109322)
- Login Fails When Using Web Server's DNS Name in the Login URL (PR 109604)
- Physical Port Performance Categories are Missing for Some Modules (PR 89397)
- Deleting Selected Traps Cancels Manual Pause in Notifications (PR 99551)
- Audit Server Log File Messages not Being Written After a Server Backup/Restore (PR 109403)
- ESC in Progress Dialogs Does Not Select Cancel Button in Progress Dialog (PR 66257)
- Audit Tables Only Autoscroll to Second to the Last Row (PR 72113)
- Statistics Properties Pop-Up Menu Item Disabled when Statistics Run from Other Application (PR 01824)
- Client/Server Out of Memory Rearranging a Large Number of Switch Icons on Topology Map (PRs 91020, 91837)
- Arranging a Hub of Switches as Networked Does Not Work The First Time (PR 86618)
- Cannot Edit Manual Links Slot/Port Fields (PR 91573)
- Topology Application Fails to Show Imported Backgrounds with a Different Data Directory (PR 102539)
- Locator Browse All Displays "Endstation Search Finished" Message Before All Results Are Displayed (PR 104441)
- The Trap Replay Feature Has the Wrong Default Setting in OmniVista 3.0 GA (PR 100228)
- OmniVista Discovery Ranges List Returns an Error After Editing and Saving Settings (PR 98684)
- Summary Table Profile View Accumulates Entries After a Filter is Turned On Then Off (PR 101746)
- Health Device Temperature CMM CPU Latest Not Supported on 9600/9800 Switches (PR 97281)

8.6 Problems Fixed Since Release 3.1

- SecureView-SA: User Should Not Be Allowed to Modify Bundled Open LDAP Credentials from SecureView (PR 86923)
- Resource Manager: Cannot View or Modify Scheduled Backup Settings (PR 75215)
- Resource Manager: Resource Manager Stops Listing Backup Files if You Select Another Tab (PR 102887)
- Resource Manager: Resource Manager Should Not Allow BootROM/Miniboot and FPGA Upgrade at the Same Time (PR 108717)
- Resource Manager: Resource Manager Fails to Upgrade the U-Boot on 6.1.3.R01 (6850) (PR 108533)
- Resource Manager: Resource Manager "Cancel Backup" Leaves Files with no Details (PR 102899)

8.7 Problems Fixed Since Release 3.0.1

- General: Traps Sent to Clients Fall Behind When the Server Rewrites the Trap Cache File (PR 99905)
- General: Client GUI Freezes for Long Periods When Deleting Many Devices (PR 90358)
- General: Server OutOfMemory Processing Many Traps for Never-Polled Unpollable Devices (PR 102849)
- General: Solaris OutOfMemory Processing Many Topology Changes in Large Network (PR 102697)

- General: Solaris Server Spends 27% of Its Time Garbage Collecting (PR 102525)
- General: Client OutOfMemory Copying a 30-Day Statistics Profile (PR 99907)
- Groups: User Must Double-Click on Help Buttons in Groups Application to Bri9g up Help Page (PR 98822)
- Locator: Locator is Slow in Conducting Live Searches in XOS-Heavy Networks (PR 98881)
- Locator: Live Search with Big Discovery List Can Fill up Polling.log and All 10 Copies with Meaningless Information (PR 91855)
- Notifications: Notifications Are Purged on "Oldest Received" but Displayed in "Adjusted Time" Order (PR 99204)
- Notifications: Client Performance is Slow with 99,999 Sorted Traps and One Row Selected (PR 99487)
- Notifications: Trap Table is Much Slower with Replayed Traps (PR 99731)
- Notifications: Notifications is Very Slow to Unfilter Due to Slow SysName Access (PR 101810)
- Notifications: Launch by Read-only or Write Users is an Order of Magnitude Slower than by Admin (PR 102215)
- Notifications: Acknowledging 99,999 Sorted Traps Takes Over 2 Minutes at 99% CPU vs. 10 Seconds Unsorted (PR 102621)
- Quarantine Manager: QM Does Not Allow Hex Extraction Expressions (e.g., ipaddr 0xaff0b07). This is the Format used in OmniAccess WLAN syslog Messages (PR 97581)
- Resource Manager: Resource Manager Cannot Distinguish Between Image and BMF Upgrade Failures (PR 101371)
- Resource Manager: Resource Manager FPGA upgrade needs to identify a TDO mismatch (PR 101382)
- Resource Manager: Sorting Backup Files Table by Name, Type or Backup Type is Slow (1 Min for 4800 Rows). (PR 99064)
- SecureView SA: SecureView Cannot Connect to LDAP Server (PR 102070)
- SecureView SA: SecureView SA Needs SSH and SCP/SFTP Added to the Family Privileges (PR 102277)
- Server Backup: Server Backup Throws Spurious Errors During Backup on Solaris Server (PR 97248)
- Statistics: Statistics Stops Exporting Data Without Warning When Profile is Unloaded (PR 99883)
- Statistics: It Takes About 20 Minutes at 99% CPU for the Client to Load a Maximum Size Profile (PR 102614)
- Topology: Client Unresponsive During Add/Delete Switches When Display Mode is Name or DNS (PR 99668)
- VLANs: VLAN Wizard Rules Config Select All Takes Several Minutes with 3000 Devices (PR 102612)
- Notifications: GUI Temporarily Freezes When Receiving Traps if Max Display is Larger Than Max Stored (PR 92310)

8.8 Problems Fixed Since Release 3.0

- Client Received OutOfMemory Error Messages (PR 99142)
- Toolbar in Topology Physical Map Refers to Mobility Drop-Down from VLANs (PR 98497)
- Cannot Restart Locator Browse After It's Been Canceled (PR 100093)
- Locator Browse Results Table Shows Previous Results Until New Search Is Complete (PR 99837)
- Source MAC Address Radio Option for MAC Groups May Not Show up Until Window is Expanded on Linux (PR 98755)

- "Out Of Memory" Problem After Stopping syslogd on Some UNIX Configurations (PR 97852)
- Wrong Slot/Port Datatype When Exporting Search Results for Locator Browser (PR 82735)
- aaas Retries Can Only Be Set from 0 - 5 Documentation says 0 - 32 (PR 88567)
- Unexpected Tags on Non-English (U.S.) Windows XP Clients (PR 100628)
- Two-Minute Delay After 'Save to Working' Before Any Configuration Operations Can Be Performed on the Switch (PR 100810)

8.9 Problems Fixed Since Release 2.4.2

- Combination of Spacebar and Enter Keys Automatically Logs Off AOS Telnet Sessions (PR 86252)
- SSH Scripting Hangs for Switches Discovered via EMP Port (PR 91315)
- No Canned Scripts for OV Admin Users Other Than Default (Admin, Switch) (PR 88887)
- "Show Traps State In Switch..." is a Per-User Preference, Not System-Wide (PR 80956)
- Loading from Certified Directory and Rebooting the Entire Switch Causes OmniSwitch 9000 to Fail (PR 96347)
- Discovery Loses its Progress Reporting After Being Canceled and Restarted (PR 91788)
- If Recurrence Time Equal or Exceeds 4 Weeks, Then Scheduled Profile Will Not Start Again (PR 85096)
- SwitchManager not Working with OmniStack 63xx (PR 78593)
- For Upgrade Installs, Fields Should be Pre-Filled with Existing Settings, Rather than Default Values (PR 91805)
- Cryptic Error Message Return When Trying to Set a Rule for 127.0.0.0/8 (PR 88831)
- Cryptic Error Message When Setting a Rule for Host 155.14.12.1/255.255.255.255 (PR 88832)
- QM Should Replace Existing MAC Rule So it Can Create a New MAC Rule in Quarantined VLAN (PR 93110)
- QM Should Replace Existing DHCP MAC Rule So it Can Create a New DHCP MAC Rule in Quarantined VLAN (PR 93111)
- After Notifying a AOS Switch to Load New Policy, the Status Panel Displays Inappropriate Error Message (PR 80468)
- For Invalid SMTP Server, the server.txt Error Should Name the Invalid Server Rather Than 'Mailhost' (PR 92156)
- OV Server Does Not Shutdown Gracefully When Solaris Box is Rebooted (PR 91710)
- Setting OV Server's -Xmx Setting to the Maximum When Installing in 32-bit Environments Can Cause "OutofMemory" Errors (PR 96104)
- Vertical Scrollbar Does Not Track for Extremely Large Data Values (PR 75433)
- Unsaved Changes to a Map Are Lost If Additional Changes Are Made By Another and Saved at the Same Time (PR 75257)
- OmniVista Topology Switch Connection is Lost When a Redundant Link Goes Down (PR 91182)
- Topology Links Do Not Show for the 6124 Release 3.40.31 (W 97464) (PR 97307)
- Locator Does Not Display the Correct VLAN ID for a Corresponding MAC Address (PR 94010)
- OmniVista Trap Configuration is Not Available for the OmniStack 6024, 6124, 6148, and 8008 (PR 69126)

- Exceeding Maximum LDAP Server Entries on Switch Produces "general failure" or "not writeable" SNMP Error (PR 61920)
- PolicyView Unable to Launch Due to Port Conflict (PR 96800)
- aaas Retries Can Only Be Set from 0 - 5 Documentation says 0 - 32 (PR 88567)

8.10 Problems Fixed Since Release 2.4.1

- Combination of Spacebar and Enter Keys Automatically Logs Off AOS Telnet Sessions (PR 86252)
- SSH Scripting Hangs for Switches Discovered via EMP Port (PR 91315)
- No Canned Scripts for OV Admin Users Other Than Default (Admin, Switch) (PR 88887)
- Telnet logs-Out User With Up-Arrow for AOS Switches (PR 92083)
- 'ls' <ent> Key Combination in Telnet AOS Sometimes Causes Session to Disconnect (PR 91473)

8.11 Problems Fixed Since Release 2.4.0

- Filtering Not Allowed On All Columns Displayed in the "All Discovered Devices" Table in Topology View (PR 70450)
- Background Image Listbox is not Updated when Image is Imported from Remote Client (PR 83828)
- All Discovered Devices Table Shows Microcode Loaded not Microcode Working (PR 845200)
- Resource Manager Backup File Disappears After Upgrading from OV2.2.5 to OV2.3 for Solaris 2.9 Only (PR 86452)
- Add Item Dialog Takes Almost 4 Minutes to Come Up with 2,000 Switches (PR 86573)
- Y-Axis Max is Miscalculated When Different Variables Have Different Scale Multipliers (PR 87201)
- OmniVista Creating a IP VLAN with Switch Running 5.1.6 Code Fails (PR 88364)
- OutOfMemory on Server Receiving and/or Replaying Traps (PR 88483)
- OV 2.3 Shows AOS Devices as Unsaved after Taking Backup (W88640) (PR 88589)
- After Switch Reboot, New Traps Get Inserted After Oldest Available Seq # Instead of Current Seq # (PR 88676)
- OV2.4 Client Times Out with an "Error processing Discovery Events" Message (PR 88761)
- SSH Gets Stuck in Double-Strike Mode Frequently (PR 88943)
- OmniVista Inventory Says Product Description Not Available for GSX-K-FM-2W/K3 Module (PR 89258)
- Discovery Wizard Menu Item is Disabled for Writer and Read-Only Users (PR 89287)
- Closing Statistics with Unsaved Profile gives NullPointer Exception (PR 89360)
- Launching MIB Browser Generates Error After Importing New MIBs (PR 89385)
- Inventory from OmniVista Changes the Switch Status to UNSAVED (W88649) (PR 89528)
- OmniVista Server 'outofmemory' with 2.4 Release During Discovery (PR 90228)
- OV Exported Statistics Data Not Having Slot and Port Information (PR 90278)
- Server Won't Run as a Service After regsync (PR 90844)

8.12 Problems Fixed Since Release 2.3.0

- When Subnets Overlap, Traps Display in Both Subnets (PR 81239)

- OmniSwitch 6800, 6600 Stack 2nd CMM Not Showing in Chassis Table on General Tab, Topology Applications (PR 86825)
- OmniVista SNMPv3 Setting Does Not Work After a Takeover on a Stack of Two 6600s (PR 87406)
- OpenLDAP Server as Installed Allows Anonymous Binds (PR 87649)
- SNMPv3 Discovery of Non-Existent Switches Breaks OV Polling of Existing SNMPv3 Switches (PR 87651)
- OV 2.3 Not Displaying SNMP v1 Traps (PR 88877)
- Source IP of One Switch is Being Replaced with Other Switch's IP During Trap Display on OmniVista (PR 89482)
- SNMPv3 Not Working for 6300-24 - Chassis Information Table SNMPv3 Get Request Timeout (PR 86489)

8.13 Problems Fixed Since Release 2.2.5

- CLI Warning Sent When the Number of Protocol Rules Exceeds Its Limits on OS7700/7800 and OS8800 (PR 68605)
- The "Context Name" and "Context ID" Fields in the SNMP Settings Dialog Cannot be Used for Alcatel AOS Switches (PR 70692)
- Displaying Large Data Values on Chart May Get Corrupted When Changing the Horizontal Scale Value From Minutes to Hours (PR 74389)
- "Delete Previous Links" Check Box in the Discovery Wizard Has No Effect on the Links Discovered (PR 74497)
- Right-Click Menu Stays On the Screen Until Save Process Has Completed (PR 74826)
- User Not Instructed to Manually Reboot AOS Switches After Restore/Install (PR 74891)
- Links Do Not Immediately Change to Green When the Switch Comes Online After Going Down (PR 75187)
- Configuring Traps Will Fail For AOS Devices If Telnet/FTP Username Specified in OmniVista Does Not Have SNMP Access (PR 75238)
- Using the "Profile Manager" Dialog When Renaming a Profile May Cause Some Profiles to Stop Collecting New Data (PR 75378)
- "Time Zone Not Found" Box Comes Up After Opening the Backup Window (PR 79757)
- OmniVista Does Not Discover OmniAccess 4012/4024/4102 Device Unless it is Enabled for SNMPv1 (PR 79764)
- Server Is Having 'Out of Memory' Problem (PR 82369)
- 'Out of Memory' Error in OmniVista Statistics Client (PR 83839)

8.14 Problems Fixed Since Release 2.2.4

- OmniVista Client Crash with Polling Service On (PR 84505)

8.15 Problems Fixed Since Release 2.2.3

- Client PC Locks Up During Importing Notifications, etc. (PR 82710)

8.16 Problems Fixed Since Release 2.2.2

- After Installing OmniVista 2.2, the Client PC Locks Up for Almost 5 Minutes During Polling (PR 77198)

- OmniVista 2.2 Cannot Discover More Than 600 Switches (PR 81220)
- Topology "Switches" Table Sorts "Type" Extremely Slowly, Especially Over Slow client-server link (PR 81854)
- OmniVista 2.2.3 Uses a New API. Show a Dialog at Login Time if the Client Ver <> Server Ver (PR 81855)
- Tried to Change Write Community on 1765 Switches and Got Errors. Server Finally Shutdown (PR 81963)
- The Upgrade Installer Doesn't Find Previous Copy of OmniVista 2.2 on a PC with a German Windows (PR 79913)

8.17 Problems Fixed Since Release 2.2.1

- Cannot Add 802.1Q Port Numbers >32 to VLANs on OmniSwitch 6600 Using OmniVista
- Physical Port Statistics of 66xx Switches Gives "Error decoding XML File for Category Tree: null"
- After Enabling the FTP Banner, the Backup Configuration Feature Doesn't Work from OmniVista
- Symbol Not Removed in OV Wizard Checkbox (PR 79667)
- Port Operational State for 6300-24 Shows as '7' Instead of LowerLayerDown for Interfaces Table (PR 79714)
- Select Backup Configuration and Click X From the Warning Window and the Backup Starts (PR 79728)
- Select X From the Main Backup Window and From the Exit Wizard Window Select No (PR 79729)
- Deleting Entries From the Backup. Select X From the Delete Backup Warning Window (PR 79728)
- Client Only Install: Installer Displays Warning Message on the Last Screen (PR 79788)
- After Deleting an Imported File it Leaves a File Detail in the Lower Upgrade Image Window (PR 79805)
- OmniVista Drop Down View, Task. Click on a Running Task and Click End Task (PR 79809)
- Missing 'Type' Information in All Discovered Devices Table for OmniAccess 4012/4024/4102 - sysDescr (PR 79833)
- MIB Browser Loads AOS MIBs When Pointed to a New MIB Directory (PR 79876)
- MIBs Imported Into a Standard Directory Do Not Show Up in MIB Browser (PR 79901)
- Install Images Upgrade Images Window. Click X and You Get an Install Image Message in the Lower Box (PR 79943)
- OmniVista Doesn't Realize that OmniStack 6xxx V3.30.05 Supports AMAP (PR 80099)

8.18 Problems Fixed Since Release 2.2.0

- Reverse DNS Lookup Causes Client Running Control Panel to Temporarily Freeze Up (PR 76231)
- Canceling a Multiple-Switch Restore Only Cancels One Switch (PR 76258)
- Resource Manager Slow, Issues Many Discovery Client Requests if Backup Row is Selected When Polling Occurs (PR 76239)
- "Completed Reading Backup Files" Message Displays Before Table Finishes Displaying (PR 76244)
- All Rows not Removed from Backup/Restore Table When Deleting Multiple Backups (PR 76269)
- Memory Leak Switching Tabs in Resource Manager (PR 76243)
- Resource Manager Unable to Backup an XOS Switch (PR 76556)
- Client is Not Notified if OmniStack Series Restore (or Install) Exceeds Retransmit Limit (PR 76314)

- Expert Mode: MAC Wildcards Not Written to LDAP as Colon Separated Value - Policy Manager Rejects (PR 76610)
- Server Can Run Out of Memory If It Can't Send Discovery Events to Logged-In Client (PR 76840)
- Reload from OmniVista 2.2 of a 6600 Does Not Work (PR 76811)
- Topology Takes a Long Time to Load When the Discovery List Contains Many Switches (PR 77241)
- Ports OmniStack Tab Calls Up the XOS Tab Help Instead of OmniStack Tab Help
- Click on OS Device to Display VLAN Definitions, then Help and Wrong Help File Displays
- OS Ports VLAN Table Help Displays Mobility Help File

8.19 Problems Fixed in PolicyView

- PolicyView OneTouch Voice Sets Both Layer2 and Layer3 Policies in the Switch(es) (PR 69198)
- PolicyView OneTouch Data Will Not Be Applied Unless Classify Layer3 Bridge is Enabled (PR 69199)
- Protocol TCP/UDP Ports Cannot be Modified or Deleted (PRs 57684, 61223)
- Intermittent LDAP Access (SNMP Timeout) Errors If You Install, Uninstall, and Then Reinstall (PR# 61141)
- One Touch Policy Actions for XOS 4.5 or Less Cannot Contain 802.1p Priority (PR# 61629)
- Environment Unstable After PolicyView Install is Updated (PR# 61918)
- LDAP Database May Be Left with Unused Roles (PR# 65052)
- In Expert Mode, A Canceled Policy Still Shows Up in the "Switches Pending Notification" Screen (PR# 75592)
- Additional LDAP Server Set-Up is Required When Upgrading to PolicyView or SecureView-SA 2.2 (PR# 76285)

9.0 Archived List of New Features

9.1 Release 3.5.1

Hardware/Software

OmniVista 3.5.1 supports the following hardware/software.

OmniAccess 5510 and 5740 Device Support

OmniVista now supports OA5510 and 5740 devices, which are an upgrade to the OA7XX line of products. OmniAccess 7XX were supported in OmniVista as Third Party devices. Now, OmniVista will be the primary Network Management tool for these devices and support for these devices will be extended to include:

- Advanced third party support (2.3.2 and 3.0):
  - Generic 3rd party level Support out of the box (Topology display , 2.3.2 MIB support, MIB browsing), Trap notification support, Telnet/CLI
  - Device MIB-II display/Topology/Interfaces Panel
  - MIB-II capabilities if applicable
  - CLI scripting engine support
  - Contextual launch for EMS Web Page
- Locator Support if 3.0 MIBs are available and can be validated (3.0 only)
- Statistics Support for Port Utilization (3.0 only)
- Backup/Restore using CLI Scripting (3.0 only)

Microsoft Windows 2008 Server 64-bit Support

OmniVista now supports Microsoft Windows 2008 Server 64 bit. This will enable OmniVista to support a larger number of devices because of access to more memory on Windows machines.

Internet Explorer 8.0 Support

OmniVista now supports Internet Explorer 8.0 for the OmniVista Web Services application and element managers launched from OmniVista (e.g., WebView).

Support and Certification of VmWare ESXi 4.0

OmniVista is now certified to be deployed and certified with Virtualization and Hypervisor package VmWare ESXi 4.0 for server.

- VMware ESXi 4.0 requires 64 bit hardware for running any 64 bit OS like Windows 2008 64 bit or RedHat 5.4 64 bit.
- For 64 bit virtualization, the VT option must be enabled in BIOS.
- When installing an operating system using a DVD in the newly created virtual machine partition, you must assign the DVD to the associated virtual machine at boot up.
- When installing OmniVista inside a VM, you must assign the DVD-ROM to the VM before trying to install.
- Virtualization requires that OmniVista is installed on a machine that is more powerful than needed for similar OmniVista running in native OS. You must assign the appropriate number of CPUs, memory and disk space based on requirements.
- OmniVista is certified to run on a VM running Windows 2008 32/64 bit and RedHat Linux 5.4 32/64 VM over VmWare ESXi 4.0.
- Certification is for one instance of OmniVista on a VM under VmWare ESXi 4.0.

Redhat Linux ES Version 5.4 (32/64bits) Support

OmniVista now supports Redhat Linux 5.4 - both 32 and 64 bit.

AOS 6.4.3 Certification and MIB Support

AOS release 6.4.3.R01 provides support for new features such as Auto Configuration. OmniVista will add general support for this release. All MIBs in OmniVista will be updated to reflect the changes in 6.4.3 MIBs for AOS devices support.

> **Note:** OmniVista will support the banner.jpg file, which is now part of the Captive Portal Custom File Set. Captive Portal profiles created using prior versions will not allow addition of banner.jpg file since they are based on older template.

Framework

Unlimited License Support

A new "Unlimited" License is now available for OmniVista as part of the "Tiered" License Plan. The certified maximum number of devices OmniVista can manage is currently 3,000. OmniVista can support more than the certified number; however exceeding the maximum number may cause performance issues.

Topology

OmniVista 3600 Air Manager Launch

The pop-up menu in the List of Discovered Devices now includes an option to launch the OmniVista default browser with a URL pointing to the OmniVista 3600 Air Manager Network Management application for the selected wireless device. You can set the OmniVista 3600 Air Manager URL using the OmniVista 3600 Air Manager option in the Preferences application. However, if the URL is not defined in Preferences, then the user is

prompted for the URL the first time this option is selected. Once the user defines the URL, either in the Preferences application or at the prompt, OmniVista 3600 Air Manager will automatically launch when it is selected in the pop-up menu.

Dynamic Maps

You can now create Dynamic Maps based on certain device attributes (e.g., sysName, model). To create a Dynamic Map, you define a filter that dynamically adds/removes devices from the map based on the filter (e.g., sysName, model). OmniVista determines membership in the map by dynamically evaluating network devices for the user-configured filter associated with the map. All devices that match the assigned map filter are dynamically added to/deleted from the map. Dynamic Maps reduce the overhead of having to manually add devices to maps for subsequent use, speeding up time-consuming operations such as backing up a group of switches.

ERP and DHL Link Status

Topology maps now display link status for DHL and ERP Links. Note that secondary links associated with DHL or ERP configurations (Standby DHL Link and Ring Protection Link) will display as down if the are in standby mode (DHL Standby Link) or blocking mode (Ring Protection Link).

Telnet

CLI Scripting Secondary Password Variable Support

OmniVista CLI scripting now supports a Secondary Password built-in variable that uses the Secondary Password value defined in the Discovery List. It can also be used for CLI scripting for devices that require a secondary login.

Device Filtering For Sending Telnet Scripts

The Device Filtering Feature (already available in other areas of OmniVista) is now available to select the devices to which the user wants to send a Telnet Script. The user can use an existing filter, or create a new filter to display only those switches in the Discovered Devices List. When the user sends the script, it will only be sent to those devices.

New CLI Script Directive

A "Last Command" directive is now available for CLI scripting. On some devices (e.g., OA5510-TE), commands such as 'reload' will 'hang' the OmniVista Telnet session because the switch telnet session will end without closing the telnet session with OmniVista. The 'last command' directive, <tapps> lastcmd </tapps>, alerts OmniVista that the next command is the last command and a response may not be received after this command. OmniVista will gather whatever response is given after issuing the reload command and close the session.

Resource Manager

Automatic Remote Configuration Support

The Automatic Remote Configuration feature provides automatic configuration or upgrade of an OmniSwitch without user intervention. When a switch is initially deployed in a network, an Instruction File is sent to the switch to download the applicable files from remote servers to bring the switch online in the network. The feature can also be used to automatically upgrade existing network switches on boot up. OmniVista simplifies the process by enabling the user to easily configure the Instruction File, which contains all of the information required to automatically locate and download all of the necessary files to configure a new switch/upgrade an existing switch on the network. The user can create an Instruction File for each switch model on the network (e.g., 9000, 6850, 6855) . When a new switch comes online, the switch type is sent to the DHCP Server using Option 60 to select the Instruction File for that device type.

Backup/Restore of All Configuration Files

In previous releases, Resource Manager only backed up the boot.cfg file in a Configuration Backup and the boot,cfg file and the image files in a Full Backup. Resource Manager Configuration Backup now includes all configuration-related files in all directories (e.g., user credentials, time zone, banner). A Full Backup will still include all configuration-related files, plus the image files.

There are some Configuration files that may need to be excluded from a backup due to security considerations. The user has the option of including/excluding Security files. By default, Security files are included in the backup. Also, previous releases did not include diagnostic and dump files in a Full Backup due to user system disk space concern. Users now have the option of including/excluding diagnostic and dump files.

Note: These new features are only available on AOS devices.

boot.cfg File Comparison

A new "Diff" Utility is available to compare backup configuration files on a line for line basis. You can select devices/files from the Backup Files Table in the Backup/Restore Tab to compare files on different devices, or compare files on the same device. You can also use the utility to compare text files on the local file system. Although the "boot.cfg" file is the target of this utility, you can use it to compare any text-based files.

Modify/Restore boot.cfg

On AOS devices, you can edit the boot.cfg file in an existing "Configuration-Only" backup and save the changes as a new backup. This new "Configuration-Only" backup can then be used to restore the modified boot.cfg to the switch. This modified backup will appear in a different row in the Backup Files Table and will be displayed in blue to indicate that it is a user-modified configuration-only backup. The name, IP address, switch type, backup type, and the version will be the same as the original backup. The description will be changed to reflect the fact that this is a user modified backup.

This new backup can be further modified using the **View/Edit boot.cfg** right-click option if needed. The new boot.cfg file can then be uploaded to the /flash/working/directory on the switch. However, further modifying a user-modified backup will not create another new backup file. You can only continue to modify the same user-modified backup.

Software Image Optimization

A Software Image Optimization feature has been added to the Resource Manager that enables the user to delete redundant image file backups to save disk space on the OmniVista Server. When OmniVista is upgraded, redundant image files are added to the existing backup snapshots stored on the OmniVista Server. Software Image Optimization deletes redundant image files from the server and uses the applicable image file in the Upgrade Image Repository for a restore operation. Deleting the redundant local image files saves disk space on the server, by utilizing the single copy of the image files stored in the Upgrade Image Repository.

This feature is only supported on AOS devices and only pertains to image files. For AOS Devices, beginning with OmniVista 3.5.1, a single set of image files will be stored in the OmniVista Upgrade Image Repository for Backup/Restore purposes. The Software Image Optimization Feature can be used to optimize snapshots created in previous versions of OmniVista by deleting redundant image files from the OmniVista Server. Once all snapshots are optimized, it will no longer be necessary to use the feature. All subsequent snapshots will utilize the single set of image files stored in the OmniVista Image Repository

Web Services

Locator User Search in Web Services

The Locator application within Web Services now provides an "Authenticated User" search option (in addition to the current options of IP Address and MAC Address). Results from a user search will be augmented with the bridging (net forwarding) information. Similarly, bridging results from an IP or MAC search will also be augmented with user information.

Web Services API for CLI Scripting

OmniVista's Web Services application now include functionality for accessing CLI Scripts with Create, Read, Update, and Delete (CRUD) capabilities. This also enables the user to send scripts to the switches and poll the status of the sending process. After sending is complete, the user can view the captured results in the Script Logs Area. A sample Telnet Script Program is provided in Appendix A.

Note: Supported software versions: SOAP 1.1, JAX-RPC 1.1.

Access Guardian

User Network Profile Support for OS9000 and 9000E Devices (Maintenance Release - October 2010)

The User Network Profile (UNP) feature within Access Guardian is now supported on OS 9000 and OS 9000E devices running 6.4.3.R01 and later for "VLAN-Only" UNP. When a UNP is applied to these devices, only the UNP name and the associated VLAN ID is sent to the switch; any Host Integrity Check (HIC) flag or policy list name specified in the UNP are ignored. The information is displayed in the message area and logged in Access Guardian Audit Log File.

9.2 Release 3.5.0

Enhanced Packaging and Licensing Process for OmniVista 2500 NMS

Previous OmniVista installations offered the core package (OmniVista 2520/2540) and separate optional packages (PolicyView 2730, SecureView SA2750, SecureView ACL 2760, Quarantine Manager 2770, Web Services 2790). Beginning with this release, OmniVista 2500 NMS packaging combines all of these packages in one base package. The package has a single installer and a single license, which is based on maximum number of deployed devices that a user can manage with OmniVista 2500 NMS.

Access Guardian

The Access Guardian Application has been reorganized and enhanced to include the following features.

User Network Profile

OmniVista now supports the User Network Profile (UNP) feature as implemented in AOS 6.3.4.R01 and 6.4.2.R01. This AOS feature provides a way to bind a "profile name" returned from the authentication server to a list of policy QoS/ACL rules and assign them to the selected switches. The list of policies typically defines a common set of network resources that need to be accessed. UNP is supported in Release 6.3.4.R01 and later. It is not supported for OS6250 devices in Release 6.6.1.

Host Integrity Check

OmnVista now supports configuration of a Host Integrity Check (HIC) Server for the switch. HIC is a mechanism for verifying the compliance of an end user device when it connects to the switch. HIC policies are used to specify, evaluate, and enforce network access requirements for the host. (For example, is the host running a required version of a specific operating system or anti-virus software up to date.) The Access Guardian implementation of HIC is an integrated solution consisting of AOS switch-based functionality, the InfoExpress compliance agent for the host device (desktop or Web-based), and interaction with the InfoExpress CyberGatekeeper Server (the HIC Server) and its Policy Manager application. HIC interacts with the UNP feature. If a HIC-enabled UNP is triggered on a switch, Access Guardian will redirect traffic to the HIC Server for compliance before allowing the user access to the network.

DHCP Snooping

The Access Guardian application now supports DHCP Snooping. The user can configure DHCP Snooping on a per-switch or per-VLAN basis and "push" the configuration to the network. The user can also view and configure entries in the DHCP Snooping MAC Address Binding Table.

Access Guardian Policies

MAC Authentication of 802.1x and Non-802.1x Clients

The Access Guardian Application allows MAC authentication to be performed on 802.1x supplicants as well as non-supplicants that are attached to a mobile port. 802.1x supplicants non-supplicants that are attached to a mobile port can any 802.1x authentication and use the MAC authentication instead. A user can specify MAC Authentication when creating an Access Guardian policy profile.

Captive Portal

A Captive Portal option is available when configuring an Access Guardian Policy. Captive Portal allows web-based clients to authenticate through switch using HTTP authentication. When the Captive Portal option is invoked, a Login Web Page is presented to the user device. If authentication returns a VLAN ID, the device is assigned to that VLAN. If a VLAN ID is not returned or authentication fails, a separate Captive Portal policy then determines the network access control for the supplicant or non-supplicant. Captive Portal Web Pages are configured/customized using the Resource Manager application.

Captive Portal Web Page Design

A "Switch File Set" Tab was added to the Resource Manager application. This tab is used to "push" customized Captive Portal Web page files (e.g., Login Page, Background images) and Banner files to devices on the network in a single operation.

View Tab

The new View Tab within Access Guardian is used to view specific policies assigned to switch ports. The tab displays Access Guardian Policies, Supplicant/Non-Supplicant information, and the 802.1x Authentication Servers, the MAC Authentication Servers and the 802.1x Accounting Servers that have been assigned to the selected switch.

Diagnostics Tab

The new Diagnostics Tab can be used by a Network Administrator to diagnose end user problems by locating the user's end station and displaying any Access Guardian Policies for the End Station. If, for example, a user cannot access certain resources, the Network Administrator can enter the user's IP or MAC address to determine the switch and port of the End Station to which the user is attached. The Diagnostic Tab also displays the 802.1x Authentication server, MAC Authentication Server and 802.1x Accounting Server for the switch.

Quarantine Manager Enhancements

Etherbreaker Traffic Anomaly Detection

A new tab in the Quarantined Manager application OmniVista enables the user to create/modify/edit Etherbreaker (TAD) Group profiles with log/trap/quarantine actions and count/period/sensitivity thresholds. With support for TAD and Quarantine Manager in this release, OmniVista can automatically ban offender across the network rather than a single switch.

Quarantine Manager Incident Count Information

A new "Incident Count" column was added to the Quarantine Manager Candidates Tab to display the number of times a specific anomaly was seen for a candidate. This will help users make better decisions about banning a device.

Quarantine Remediation Server

Within the Configuration Tab, Quarantine Manager now supports configuration of a Quarantine Remediation Server (QMR) on the switch. A Remediation Server works with Quarantine Manager to notify the user when a device is placed into the Banned List, and can also be configured to utilize programs/patches to debug the device and restore network access.

Locator

A new "User ID"search criteria (in addition to the current MAC or IP Address) is available in the Locator application. The search result is listed in a new User ID column in the Search Results table on the initial locator screen. The new User ID criterion is the user id authenticated for bridging purpose on devices through the 802.1X tables.

Topology

Topology Support for 802.1ab LLDP Protocol

OmniVista now discovers and displays links in Topology that are available through support for 802.1ab LLDP Protocol on the switch. Links will show their status as "Blocked" if the link is down because of STP has blocked it. Links discovered through 802.1ab will co-exist with links like AMAP supported by previous version of OmniVista. Users can specify link type display priority using a new "Topology" Preference panel. This will help resolve duplicates where both LLDP and AMAP report the link over the same port for showing in Tooltip. Active Links panel will continue to show all links discovered by all protocols. This feature is supported on OS6200, OS625X, OS6400, OS68XX, and OS9XXX devices.

802.1ab MED Extension Information

A new MED Information Tab was added to the Device Information window in the Topology application. There are two sub-tabs within the MED Extension tab. The LLDP 802.1ab End Station Inventory, displays MED extension information for end stations. The LLDP 802.1ab End Station Inventory tab displays MED extension information for end station policies. These tabs are only displayed for devices supporting LLDP 802.1ab MED Extensions (currently AOS devices running 6.3.4, 6.4.2 and higher).

OmniVista 2500 NMS Framework Upgrades

The Locator application includes support for multiple Virtual Private Routing Networks (VPRNs) on SR 7750 devices. During a regular poll of 7750 devices, OmniVista 2500 NMS now checks for multiple VPRNs in the ARP Table. If present, the information is gathered using SNMPv2 and SNMPv3 and stored in the Locator Database.

Tootips in Table Cells

OmniVista 2500 NMS Table Tooltips now display whenever a user mouses over a table cell. This enables the user to view the contents of the cell even when the table column is not wide enough to view the data.

Drop-Down Menu Extension

A "New" option was added to certain drop-down menus that allows the user to create a new configuration option. In addition to selecting from one of the drop-down options, the user can select "New" and is presented with a window to create a new configuration option. For example, if a user wants to create a User Network Profile (UNP) and Policy Lists have been created, the user can click on New to Policy View QoS Policy List Creation panel and create a new Policy List for the UNP. The user can then press the Back button to return to UNP Profile panel and continue configuring the UNP.

Port Lists

To allow the user perform actions on a number of ports, OmniVista now discovers additional port attributes (e.g., type, speed, default VLAN) in addition to basic slot/port attributes. This provides the user with greater flexibility in specifying which ports should be included in a Port List. In this release, a Port will provide filtering on the following attributes: Slot, Port, Type, ifIndex, Speed, Default VLAN, and whether or not the port is Mobile, Authenticated, LLDP,AMAP, 8021.Q, or LAG.

Port Filters

A Port Filter selection panel has been added in any context where Port Filtering/selection is required. All new features where Port Filtering is needed will use this filter. For existing features, if this Port List is needed then changes may be made with SQA agreements. Three factory defined Port filters are provided in the Port Filter Drop Down list to the user:

- allPorts All ports in the device are selected.
- edgePorts Only the mobile or authenticated ports are selected.
- networkPorts Only the ports that are AMAP or LLDP or LAG or 802.1ab or have Port speed >= 2.4Gb/sec are selected.

The user can edit these definitions and can revert them back to the original factory defined filters. The user can also create and save custom port filters that will be available in the drop-down menu. In addition to the filter, a user can select an option to "Exclude" or "Pre-Select: Manual Link Ports.

Support for OmniSwitch 6250 Devices

OmniVista now supports OmniSwitch 6250 stackable devices. OmniSwitch 6250 devices, a low cost stackable chassis devices. These devices do not support Routing, Ethernet OAM, or VLAN Binding Rules. They do not support AVLAN (not supported by OmniVista), HIC, or TAD, and have limited support for UNP (can only specify VLAN associated with the UNP).

Support for OS 6855-U24X Devices

OmniVista supports OS6855 U24x stackable devices. These devices will have the same support as the OS6855 devices, which are already supported by OmniVista.

Support for Windows 2008

OmniVista now supports Microsoft Windows 2008 (32 bit).

Support for FireFox 3.0

OmniVista now supports Firefox, version 3.0 as detailed below.

- Microsoft Windows Version 3.5.2
- Linux Version 3.5.2

Note: Sun Solaris is only certified with Version 2.0.0.14.

9.3 Release 3.4.2

Locator Application

The Locator application includes support for multiple Virtual Private Routing Networks (VPRNs) on SR 7750 devices. During a regular poll of 7750 devices, OmniVista now checks for multiple VPRNs in the ARP Table. If present, the information is gathered using SNMPv2 and SNMPv3 and stored in the Locator Database.

Resource Manager

The Resource Manager application includes support for the In-Service Software Upgrade (ISSU) feature, which is available on 9700E/9800E Switches with dual CMMs installed. ISSU enables the user to upgrade application firmware running on a CMM without causing any loss or interruption of L2 data traffic and a minor loss of data loss of L3 base traffic.

Support for 128 Link Aggregates

OS9700E and 9800E switches provide support for up to 128 Link Aggregates to be defined over up to 256 ports. OmniVista does not provide support for creating Link Aggregates, but will now display up to 128 Link Aggregates within the Locator, Topology, and VLAN applications.

Multiple VRF Support

In Release 6.4.1, OmniVista supports display of multiple Virtual Routing and Forwarding (VRF) instances in routing table displays. Specifically, the VLAN application will discover IP routers for each VRF and allow the user to create or modify IP interfaces for specific VRFs. The Topology application will display each VRF and its IP interfaces in the tool tip, and the STP Information Tab for each device will also display VRF information.

> **Note:** The Multiple VRF feature is only available on 9700E/9800E Switches, Release AOS 6.4.1.R01. SNMPv3 is required to manage VRF instances.

Support for OS9700E and 9800E Series Switches

OmniVista supports OS9700E and 9800E Series Switches, Release 6.4.1, throughout the product wherever OS9700 and 9800 devices are already supported. The following sections detail some key feature areas.

Hardware and Modules

OmniVista 3.4.2 contains the knowledge of OIDs and new modules supported by OS9700E/9800E Switches.

Updated MIB Set

The OmniVista AOS 6.4.1.R01 MIB Set includes changes for OS9700E/9800E Switches.

Discovery

The Discovery application supports discovery of OS9700E/9800E Switches.

Topology

The Topology application supports OS9700E/9800E Switches. Topology mapping of device OIDs, model types and description were added to support the Chassis View General and Modules Tabs. The icon used by OS9700/9800 devices is used to display OS9700E/9800E Switches.

Inventory

OmniVista Inventory supports OS9700E/9800E Switches. OS9700E/9800E Switches support UBoot/Miniboot/FPGA information similar to OS9700/9800 Switches.

Policy View

The Policy View application supports OS9700E/9800E Switches. OS9700E/9800E Switches support the same policies as OS9700/9800 devices.

Quarantine Manager

OS9700E/9800E Switches are included in the list of devices for discovery of Quarantine MAC Group information.

VLAN

On 9700E/9800E Series Switches, Release AOS 6.4.1.R01 (running SNMPv3), the VLANs application allows the user to configure interfaces on non-default VLANs. The user can also view VRF configurations in Device and VLAN table views. OS9700E/9800E Switches do not support the ForceTAGInternal flag for 802.1q tagging, or VLAN Binding Rules. OS9700E/9800E Switches do not support IPX routing.

Resource Manager

OS9700E/9800E Switches support the new In Service Software Upgrade (ISSU) feature for dual-CMM devices. Backup/Restore is identical to OS9700/9800 devices.

9.4 Release 3.4.1

Support for OS6400 Switches

OmniVista supports the OS6400 Switch, Release 6.3.3.R01 throughout the product, wherever OS6850 devices are already supported. The following sections detail some key feature areas.

Hardware and Modules

OmniVista 3.4.1 contains the knowledge of OIDs and new Modules supported by OS6400 Switches. OS6400 devices are similar to OS6850 devices for most part and will be treated as such by OmniVista. However, there are some differences in the way these devices behave that will be accounted for by OmniVista.

Updated MIB Set

The OmniVista AOS MIB Set includes changes for OS6400 Switches.

Discovery

The Discovery application supports discovery of the MPM version for OS6400 Switches. These devices are classified as 6800/6850 devices while still having their own sub-family as OS6400.

Topology

The Topology application supports OS6400 Switches. Topology mapping of device OIDs, model types and description were added to support the Chassis View General and Modules Tabs. The icon used by OS6850 devices is used to display OS6400 Switches.

Inventory

OmniVista Inventory supports OS6400 Switches. OS6400 Switches support UBoot/Miniboot like OS6850 switches.

Policy View

The Policy View application supports OS6400 Switches. OS6400 Switches support the same policies as OS6850 devices. A Policy Validation Matrix for OS6400 devices was added.

Notifications

OS6400 Switches have support for four (4) new Traps.

- arpMaxLimitReached
- ndpMaxLimitReached
- ripngRouteMaxLimitReached
- ripRouteMaxLimitReached

Note: OmniVista provides a uniform interface by offering user the ability to select traps from a list that contains all BOP traps. OmniVista server handles configuring appropriate traps on the device.

Quarantine Manager

OS6400 Switches are included in the list of devices for discovery of Quarantine MAC Group information. OS6400 Switches have support for "Smart Recache" as supported in OS6850 devices in 6.3.1.R01. During discovery, OS6400 devices are treated as devices that support "Smart Recache".

VLAN

As is the case with OS 6850 Switches, OS6400 Switches do not support the ForceTAGInternal flag for 802.1q tagging. All VLAN Rules as supported by the OS6850 are supported for OS6400 Switches.

Resource Manager

OS6400 software file names have a G prefix. The main OS image is named Gos.img and rest of the files is similarly named. Resource Manager supports OS6400 devices, with processing similar to OS6850 devices

Support for OS6855 Devices

OmniVista supports OS6855 Switch, Release 6.3.2.R01. OmniVista supports the OS6855 Switch, Release 6.3.2.R0 throughout the product, wherever OS6850 devices are already supported. The following sections detail some key feature areas.

Hardware and Modules

OmniVista 3.4.1 contains the knowledge of OIDs and new Modules supported by OS6855 Switches. OS6855 devices are similar to OS6800 devices for most part and are be treated as such by OmniVista. However, there are some differences in the way these devices behave that are accounted for by OmniVista.

Updated MIB Set

The OmniVista AOS MIB Set includes changes for OS6855 Switches.

Discovery

The Discovery application supports discovery of the MPM version of OS6855 Switches. These devices are 6850 family devices while still having their own sub-family as OS6855; however. OS6855 is not a stackable device in Release 6.3.2.R01.

Topology

The Topology application supports OS6855 Switches. Topology mapping of device OIDs, model types, and description support the Chassis View General and Modules Tabs. The icon used by OS6850 devices is used to display OS6855 devices.

Same icon as used by OS9800, OS6850 etc will be used to display OS6855 Etna Switches.

Inventory

OmniVista Inventory supports OS6855 Switches. OS6855 devices support OS9000 Fuji like Miniboot and FPGA information.

Policy View

OmniVista Policy View supports OS6855 Switches. OS6855 Switches support the same policies as OS6850 devices. A Policy Validation Matrix for OS6855 devices was added.

Notification

There are no changes for OS6855 devices. They support the same traps that the S6850 supported in OmniVista 3.4.

Quarantine Manager

OS6855 Switches are included in the list of devices for discovery of Quarantine MAC Group information. OS6855 Switches have support for "Smart Recache" as supported in OS6850 devices in 6.3.1.R01. During discovery, OS6855 devices are treated as devices that support "Smart Recache".

VLAN

As is the case with OS 6850 Switches, OS6855 Switches do not support the ForceTAGInternal flag for 802.1q tagging. All VLAN Rules as supported by the OS6850 are supported for OS6855 Switches.

Resource Manager

OS6855 software file names have a K2I prefix. The main OS image is named K2Ios.img and rest of the files are similarly named. Resource Manager supports OS6400 devices, with processing similar to OS6850 devices. OS6855 devices behave much like OS9xxx Fuji devices as they support FPGA. The OS6855-U24 does not support FPGA and will be treated like 6850 device, with support for Uboot/MiniBoot.

9.5 Release 3.4

Alcatel-Lucent Rebranding for OmniVista 2500 and 2700

All text and graphics within OmniVista 2500 and 2700 have been updated with the new Alcatel-Lucent name and logo.

OmniStack LS 6200 Support

Inventory Support

Inventory Support for OmniStack LS 6200 Series switches is supported, including single and stacked modes. The user can generate inventory reports, including:

- System Information
- Flash File Information
- Chassis Overview

- Detailed Modules Information
- Chassis Information
- Average CPU Utilization.

These reports will be similar in organization and appearance to AOS reports.

VLAN Management Support

VLANs are now supported for OmniStack LS 6200 Series switches. Support includes:

- Displaying VLAN information
- Adding, editing, removing VLANs
- Using the VLAN browse option
- Using the VLAN device list
- VLANs Ports Mode Change VLANs ports mode (equivalent to AOS port mobility) includes: General (802.1Q), Access, Trunk and Customer modes
- Device List View VLAN information on an individual device basis
- VLAN Wizard Create a new VLAN using the VLAN wizard
- Setup IP addresses (Static and DHCP) on the devices interfaces (VLANs, LAGs, and ports).

Health Support

Health monitoring for OmniStack LS 6200 Series switches is now supported on a limited basis. The items monitored are CPU utilization (system wide) and temperature (per unit).

Notifications Support

Trap configuration is supported on OmniStack LS 6200 Series switches, including:

- Enable/disable traps globally
- Enable/disable global Authentication Notifications
- Define trap recipients
- Filter traps, internally based on OIDs.

Access Guardian Application

The Access Guardian application enables the user to apply 802.1x functionality across a set of ports on one or more switches in a single operation. Moreover, this functionality is supported for both 802.1x clients (Supplicants) and non-802.1x clients (Non-Supplicants) through configurable 802.1x device classification policies to handle both Supplicant and Non-Supplicant access to 802.1x ports. This application is only available on OmniSwitch 6800, 6850, and 9000 Series devices using AOS 6.1.3 or later; and is only accessible to a user with Network Administrator privileges.

AMAP Support for OAWLAN Wireless Access Switch

OmniVista supports discovery of Mapping Adjacency Protocol (AMAP) links from OAWLAN devices. This support includes:

- Discovery of AMAP links for OAWLAN OmniAccess switches
- Display of AMAP Links
- AMAP and linkup/Down Traps for OAWLAN OmniAccess switches.
- Port Discovery Updates as needed.

Authentication Servers: TACACS+ Configuration Support

Users can configure a TACACS+ Authentication Server in the Authentication Servers application. Functionality is similar to existing LDAP, RADIUS, and ACE Authentication Servers.

Brick Manageability Support by OmniVista 2500 and 2700

Brick is an Alcatel-Lucent VPN Firewall. Brick support in this release includes support for discovering LSMS devices only. Discovery is not automatic; the user must manually add LSMS devices. Once discovered, LSMS information is available in the Topology application. In addition, Quarantine Manager includes a rule to detect alarms generated by the group "LSMS Devices".

MSTP Support

OmniVista supports discovering and displaying Spanning Tree instances and Multiple Spanning Tree Protocol (MSTP) configurations on AOS devices. AOS devices with support for MSTP include OS7xxx, OS8xxx, OS62xx, OS66xx, OS68xx and OS9xxx devices.

Windows Vista and Internet Explorer 7.0 Support

OmniVista supports Microsoft's Windows Vista (Business) operating system and Internet Explorer 7 on OmniVista Clients.

Notifications: SNMP Trap Forwarding Based on Subnet, Region or Device Range

The Notifications application Responders tree node has been enhanced with new functionality that permits selecting traps by logical regions, physical subnets, and IP address range.

OmniAccess 700 WAN Series Support

OmniVista now supports OmniAccess 700 WAN Series devices. Support includes:

- Discovery and MIB Browser support
- New Icons will be used for OmniAccess 700 Series devices
- Ability to receive Traps and display them in the Notifications Application
    - MIB-2 Traps - linkUp, linkDown
    - Private Traps - dsx1LineStatusChange, frDLCIStatusChange
- Chassis Panel display.

OmniAccess SafeGuard Support

OmniVista supports OmniAccess SafeGuard devices. This eliminates the need to manually add the OID and mibs using the 3rd party support. These devices, if present in the network, will be automatically discovered.

OmniVista 2520 Limited Single User

A new limited single user license is available. This version can discover and manage up to fifteen (15) devices. Optional OmniVista 2700 applications (e.g., PolicyView, SecureView) are not available with this version.

Quarantine Manger: QM-Pull

Quarantine Manager uses a new Fast Re-cache mechanism. The previous re-cache mechanism, flushed all policies and reloaded all policies from LDAP assigned to the switch. With the new mechanism, the switch will look through LDAP only for the existence of quarantine MAC groups. The contents of the MAC group are added to the quarantine settings without flushing any other policies. This feature is only available on the 6850 Series Switches running 6.3.1.R01 or later.

Resource Manager: Retention Policy Upgrade

The user can now configure a retention policy for backups specifying a maximum number of days and a minimum number of backups to keep per switch. If a backup for a switch is older than the maximum number of days and the

total number of backups is at least the minimum number specified, the backup is deleted when a new backup is created for the switch..

SecureView ACL: Multicast ACL Rules Support

OmniVista supports creation IP Multicast ACL/QoS rules. OmniVista needs to support creating ACLs that prevent users from receiving specific IP Multicast flows. This is done using rules that are enforced when the switch receives an IGMP Report requesting a new IP multicast flow (also known as an IGMP join message). The ACL denies the IP multicast flow on the switch or on the port of the switch and does not process the IGMP join request.

SecureView SA: Require Administrative Level Permission to Configure Switch Access Rights

Only Administrators with full administrative rights can now set up authentication servers on a switch and to add, modify or delete users in the LDAP database.

Telnet: Language-Based CLI Scripting

Allows the user to use a standard scripting language for CLI scripting, providing for if/then modal situations. It offers more capabilities than existing CLI scripting by allowing the user to develop more complex automation. Specifically, the scripting part of the Telnet application now allows users to type in JavaScript (and other scripting languages supported in the future) within a script. A script can contain both CLI commands and sections of JavaScript.

Topology: Topology Map Enhancements

Topology's map engine has been enhanced to provide a better user experience and performance level. Enhancements include:

- No height and width limitations. The new map engine provides a canvas of a virtually infinite size. If a map was created prior to this release, its width and height values shall be discarded. No adverse effect to previously created maps is expected.
- To navigate through this virtual space the user can click on the maps background and drag the mouse around.
- A Filter field is available, allowing the user to quickly simplify the current view by only displaying a subset of the devices currently visible.
- The user can zoom in and out very quickly using the mouse wheel or, if using a wheel-less mouse, by right-clicking then dragging the mouse up and down.
- Multiple device selection is more accurate and entails the use of the Shift key along with a mouse action: clicking on devices and/or dragging around devices.
- An Overview Panel is located in the applications tree. This overview is updated in real-time as the user navigates around the map and zooms in/out. The user can also move the Topology display by clicking in the Overview Panel.

Trap Filtering: Trap Filtering Based on SNMP Variables

OmniVista Client's "Filter" dialog has been enhanced so that when a Trap filter is created, the user can designate a filter for the value of an SNMP Variable in a Trap notification.

Users and User Groups: OmniVista Visibility Management

A higher security level is now required to see a whole network. Network Administrators are not able to view all networks. Instead they are only be able to view and manage networks that the groups they belong to can see. Only Security Administrators are able to see and interact with the whole network as discovered by OmniVista.

VLANs: Filtering by Subnet/Map

OmniVista supports filtering of VLAN displays using subnets/maps. This allows the user to view the VLANs defined in the selected subnet. It could be used to find the VLANs that despite having the same VLAN ID do not communicate across subnets.

9.6 Release 3.3

OmniStack LS 6200 Switch Series Support

Topology Support

The user can now configure OS6200 devices in Topology.

Resource Manager Support

Backup/Restore/Upgrade Images/Configuration files, Image install, and Switch reboot for OS6200 devices are now supported.

Statistics Display Enhancement

Statistics displays for OS6200 devices now filter out non-connected ports that do not exist in the stack. The tree for Ports contains the physical ports from the device.

Quarantine Manager Support

MAC based VLAN quarantine actions are now support for OS6200 devices.

Web Services API/Web Browser

A new optional Web Application enables the user to use a Web Browser to access the OmniVista Server and basic versions of the following OmniVista applications: Locator, Notifications, and Topology. The application includes:

- Web Services - Northbound API for accessing OmniVista data through industry-standard web service scripting tools, such as Java, PHP, Perl.
- Web GUI - Support for a web browser-based GUI. The following platform/browser has been certified:
    - Windows - Internet Explorer, Versions 6.0 and 7.0
    - Solaris - Firefox, Versions 1.5 and 2.0.

OmniSwitch 6850 Lite Series Switch Support

OmniVista 2500 and 2700 now support the OS6850 Lite throughout the product wherever the OS6850 Series Switch is already supported.

OmniSwitch 9800 Series Switch Support

OmniVista 2500 and 2700 now support the OS9800 Series Switch throughout the product, wherever the OS9700 Series Switch is already supported.

Discovery: Support for Fortigate

OmniVista 2500 now automatically discovers Fortigate Series devices and provides a set of MIBs. The user no longer has to manually add the OID and MIBs using 3rd party support.

Global QoS: Global QoS Configuration

A new feature, "Global QoS", enables the user to configure the overall QoS configuration for all AOS switches.

Locator: Control Added to Enable/Disable Port

A sub-menu was added to the Locator device pop-up menu to enable/disable a port. If any Locator client is currently displaying the port for that switch in any end-station tables, the displays will change and the notices display will post a message of the port state change and who invoked it.

Notifications: "Switch Down/Switch Up" Traps

A new Switch Down trap is generated when a switch status is changed to down because the switch stops responding to SNMP polling (alaOvSwitchDown). A Switch Up trap is generated when a switch resumes responding to OmniVista (alaOvSwitchUp).

PolicyView: Support for Policy Based Routing

The PolicyView QoS Expert Wizard contains a new Tab for Policy Based Routing. The PBR tab allows configuration capability for PBR attributes - default gateway and alternate gateway.

Preferences

Filtered OmniVista Locator

A new preference was added to the Preferences application that allows a user to optionally exclude 802.1q tagged ports from polling results and live searches in Locator in the event AMAP / XMAP is not operating or a link is not present on the tagged port.

Locator Data Retention Setting

A new Preferences screen gives the user the ability to set limits on Locator data retention.

Resource Manager

Incremental Backups

An Enable Incremental Backup checkbox was added to the Scheduling section of the Backup Configuration wizard. This checkbox is enabled only when Configuration only backup type is selected. If this option is selected for a scheduled backup, Resource Manager will initiate the backup only when there are changes in switch configuration files since the last configuration only backup, i.e. when any of the files has a newer timestamp than the previous backup. If no files have been updated,, no backup will be created.

Modifying Scheduled Tasks

Resource Manager provides a mechanism to dynamically update the scope of existing scheduled backup tasks by linking a scheduled task with Topology map regions.

Simplified Backup Scheduling

The user can now modify the schedule for an already-scheduled backup in one step. Previous versions of Resource Manager required scheduled backups to be removed and re-added to change the scheduled time.

U-Boot Upgrade Support

Support was added to Resource Manager to allow upgrade of the U-Boot file.

Statistics: Selective Export of Chart Data

Certain fields in the Performance Summary Table can be edited and the columns can be re-arranged. A right-click menu item (Export Data) was added the existing pop-up menu to allow the selected subset of the variables to be exported. Current data export (within the chart) will remain unchanged (with exception that modified variable names will be used).

Sun Solaris v10 Support

OmniVista will support Solaris v10.

Telnet

Schedule CLI Scripting

A "Schedule Script" option was added to Send Script Tab that allows the user to schedule a script to run at a specific time. The script can be scheduled to run once or to recur at a specific time.

CLI Scripting - Parameter Passing

A user can create a "template" script in the Telnet application contains special NON-CLI syntax and keywords that represent OmniVista built-in variables or user defined variables. This allows a single CLI script to be reused without making a separate script.

Topology

Access Controls for Topology Map Viewing

An extra Security tab was added to the Map edit panel that will open up access for a map to others. The viewing permissions available are:

- **None** Map visible to only the owner and Network Admin
- **Owners Group** Map visible to the owner, all users of the groups he belongs to, and Network Admin
- **All** Map visible to all.

OmniVista Launch Option for Mobility Manager for OmniAccess WLAN Series Devices

The Mobility Management System is accessed from a web browser. A "Mobility Manager" menu item was added to the Topology Devices pop-up menu for wireless devices. When selected, OmniVista launches the client default web browser with the configured URL to access Mobility Manager. The URL is configured in the Preferences application using the "Mobility Manager" preference page.

9.7 Release 3.1

Audit: Trap Archiving

When traps are received, OmniVista logs the information about a trap to a trap archive log file (traps.txt) located in the installation directory/data/logs folder. The traps.txt file will not be listed under Current Log Files in the Audit application like other log files. When the traps.txt file reaches the configured maximum file size, OmniVista will automatically archive a copy of the file under Archived Log Files of the Audit Application. The number of trap archived files cannot exceed the maximum number of audit file copies configured in the Preferences application.

Discovery: Discovery Timestamp

A new "Discovered" column was added to all standard "Switches" tables displayed throughout OmniVista (e.g., Topology application's "Switches" node, VLANs "Devices" node). The column displays the date and time that OmniVista first successfully pinged or polled the switch. Once OmniVista has successfully pinged a switch and set the "Discovered" date/time, the value remains unchanged until the switch is deleted.

Notifications: Sort Devices by Traps View

A new "Switches" Tab was added to the Notifications Application. The tab displays a list of all discovered switches with an additional "Trap Count" column that displays the total number of traps received on each switch. The "Trap Count" column initially sorts the list of discovered switches in descending order. In addition to the standard switch table filter functions, you can use the "Notifications" Tab and the new "Switches" Tab to filter by trap type and switch. When you create a trap filter using the "Notifications" Tab, the "Switches" Tab is automatically filtered to display the switches generating the filtered trap. After applying the filter in the Notifications Tab, click on the Switches Tab. The switches generating that trap will be displayed at the top of the list. If you have previously applied a filter to the Switches Tab, the list will also be filtered by that Switch Filter; or you can apply a different/new filter.

Preferences Application: Absorption of Duplicate Traps from Non-AOS Devices

The new Trap Absorption option in the Preferences Application extends trap absorption to non-AOS devices. When this feature is enabled, similar traps received from non-AOS devices during the trap absorption period are 'absorbed,' and a 'trapAbsorbtionTrap' trap is generated similar to existing AOS traps. This trap contains details, such as the total number of 'sufficiently-similar' traps received since the original trap.

Support for BootROM and Miniboot Upgrade on OS6800 and OS6850 Switches

The Resource Manager Application now supports BootROM/Miniboot upgrades on OS6800 and OS6850 Series Switches.

Support for OS9600 Switches

In addition to the previously supported OS9700 switch, OmniVista now supports OS9600 switches. This includes full native support for OS9600 series switches from all OmniVista applications, including optional packages.

Topology: Create Maps From Subnets and Filter by VLAN

Also added to the Topology application is a new feature that allows the user to create maps from subnets using a Wizard, and filter those maps by VLAN. On the second screen of the wizard, you have the option of creating the map to include all devices in the map or filtering the map by VLAN.

Topology: Spanning Tree View

A new STP "Tooltip" feature was added to Topology maps. When the user places the cursor over a device in the map, basic STP link information is displayed. In addition, a new popup menu item was added - "Show STP Ports." When the user right-clicks on a device in the Topology map, and selects "Show STP Ports" from the popup menu, a window opens showing STP port information collected for the selected switch. In addition, on AOS devices, STP information for LAG ports is displayed. If the switch is configured for MST, only non-MST information is displayed. You must have "Write" permission to perform this function. This feature is only available on AOS and XOS devices.

VLANs: VLAN Information Browser

A "Browse" node was added to the VLANs Application tree. When the user clicks on the "Browse" node, the VLAN Information Browser wizard is displayed. The wizard allows the user to sort and display a list of devices based on rules configured on the devices (e.g., MAC Rules, Port Rules). The results are displayed in a "Devices" Table that can then be sorted and filtered.

9.8 Release 3.0.1

Alcatel-Lucent Service Router(SR) 77xx Series and Ethernet Services Switch (ESS) 74xx Support

Includes discovery, MIB browsing, monitoring, trap display, statistics, and a right-click menu to launch the 5620 SAM client. The specific SNMP MIBs for the devices are included and automatically associated. The 5620 server is expected to be installed on a separate machine.

64-bit Linux Support

Includes 64-bit java support for 64-bit Suse Linux OS running on 64-bit AMD processors.

6850 Series Switch Support

Includes full native support for OS6850 series switches from all OmniVista applications, including optional packages.

9000 Series FPGA Upgrade

Includes support in Resource Manager for future FPGA upgrades on the OS9700.

Resource Manager: Fail-Safe Mechanism for Switch Software Upgrade

Any failures of Resource Manager switch upgrades are shown and sortable in Topology; and the "reload from working" operation is disable for those switches until the problem is resolved by a successful upgrade.

Topology: Converting Topology Map into Drawing File

Includes an export option in the Topology application to create a bitmap image.

9.9 Release 3.0

Installation Support

Licensing Enhancements

All OmniVista components are included in the same packaging. There are two CDs: one contains the Main Application (OV2500) and, if applicable, a second CD that contains the optional applications (OV2730/50/60/70). License and serial numbers are not attached to the OmniVista NMS CD. Applications are activated by ordering a license card. The card includes a serial number and SKU description, and is issued after customer registration and activation.

Basic Demo Version Available

A Demo Version of the OmniVista Basic Application is included on the Basic CD that allows the user to install the application and configure up to five (5) switches without a license. However, any information stored on the server is lost at shutdown.

Managed Device Support

OS9700 Support

OS9700 Series switches (Release 6.1.1.R01) are supported.

Security Enhancements

Authentication via External RADIUS Server

The System Administrator has the option to select Radius authentication of all OmniVista login users. In this mode, all OmniVista user accounts and passwords are created and maintained external to OmniVista. User authentication is performed using the remote Radius server, but the authorization is still controlled within OmniVista.

SecureView-SA: Configuration of RADIUS Accounting Server

The System Administrator can choose different IP addresses for the authentication and accounting servers. This is a capability that the AOS switches have had, but it was not supported in previous versions of SecureView-SA.

GUI Usability Enhancements

Selection by Device Group

All applications screens that allow selection of multiple devices, currently by selection of multiple rows in a device table (e.g., Discovery, Topology, VLAN), offer an additional control to select one or more network regions. A new "Select Switch Group" Dialog allows the user select groups of devices using one or more Physical or Logical (user-defined) maps.

DNS Name Support for IP Displays

IP addresses for discovered devices can be extended to include the DNS name for the device. When names are not available for IP addresses, they will continue to be displayed as IP addresses.

Subnet Names

Two new attributes were added to manual subnets: "name" and "description". The names should be short, preferably one word descriptions such as "Backbone", "Development", "WebView". The description attributes should be one line descriptions such as "Backbone Switches", "Switches for Development". Under "Physical Network", an option was added to allow the user to display "name" field instead of "Subnet", for the "Subnet (IP address)" in tree node. When the "View Devices By" mode is set to "Name" or "DNS," the Manual Subnet Name field is displayed in the Physical Network tree.

Print Titles with Tables

OmniVista prints table titles, as displayed in OmniVista, on each page of a printout. The user can shrink a table to fit the width of a page or print across as many pages as it takes to print all columns. Each page will show the table headers of the columns being printed; and a page number is printed at the bottom of each page.

Contextual Help Button on the Topology Toolbar

A contextual help button, labeled '?', appears on the Topology toolbar that goes directly to the "Viewing the Network" section of OmniVista help. This restores the 2.2 functionality that was inadvertently removed in the 2.3 GUI redesign.

Update OmniStack Series Link Status by Link Down Trap

When a link is down it is displayed in red, and when the link up trap is received, or the switch goes green (if the linkup trap was missed) the state will be changed back to Unknown (blue).

Global Device List Filters

There are multiple places throughout the OmniVista where the managed device list (Discovery List Table) is displayed (Topology VLANs Resource Manager). If a table filter is created for one OmniVista Application, it is available for all of them. It does not have to be recreated multiple times by the user.

Messages Added to the Status Panel for Topology "Import Devices"

When using the Topology "Import Devices" option, the following progress messages were added:

- When starting the import: Importing devices from {filename}
- When the import has been completed: Device import completed.

Add "NOT" Operator for Table Filters

The Table Filter Dialog offers a "Not Op" attribute in the Condition panel. The Default value for this attribute is empty. If the "Not" operator is selected, the effect is to negate the result of the condition being defined. Having this feature eliminates the need to have a "Not Equal" Operator in the Condition panel. Any existing condition using the "Not Equal" operator will be converted to set "Not Op" and Operator set to "Equal" for the Condition before the condition is displayed in the GUI.

Extended Support for Multiple Device Addresses

OmniVista Failover to Alternate Switch IP Addresses

If a switch fails to respond to SNMP requests, an attempt is made to reach the switch using the known alternate IP addresses as displayed in the switch "edit" panel. If the attempt is successful on any of them, all subsequent management traffic is diverted to that new address.

Device Visibility in Multiple Subnets

In the Topology application, the user has the option to display switches in all of the maps in which the switch has an address. That is, if a switch has any IP address that is appropriate to the selected subnet, the switch will be displayed in the map.

Locator Enhancements

VLAN Information Added to Locator Search Results

A column was added to the Locator search results that shows the VLAN number associated with each end-station IP/MAC. This column appears in both the Browse and the Search tab results panels.

DNS Name Resolution Included in Locator Results

The Locator search results display the DNS name for the IP address of the end station(s) found. The DNS lookup is performed in background threads and uses server events to post data. The result is that the DNS columns in Locator are initially blank. Over time, the DNS names are filled in.

Right-Click Actions for Browse Feature Results

Right-click actions are available in Locator tables. Consistent pop-up functionality is included across the Locator application.

Action to View/Modify VLAN Information

The user can right-click in the Locator search results table to launch the VLAN application with the device's associated VLAN if a VLAN ID was found for the search MAC.

Action to Create Quarantine

The user can right-click in the Locater search results to launch the Quarantine Manager application (if installed), and hand off the MAC address of the end-station.

Automatic DNS/IP Address Conversion

If a user enters a name in the IP address field, it is automatically converted to an IP address using DNS, if possible.

VLAN Enhancements

Add a Switch to an Existing VLAN

A user can apply the existing configuration of a VLAN to a set of additional switches by copying the definition of an existing VLAN from an AOS device and adding more devices to this VLAN.

Apply Rules to a User-Defined Group of Switches

A user can copy existing VLAN Rules from an AOS device and add selected rules to other AOS devices in the same VLAN.

Resource Manager Enhancements

Full Backup/Additional Restore Options

The user can perform a "full backup" that will save all files in all directories (Certified, Working, Switch, Network). This option is available in the Configuration Parameter wizard panel in the Backup Configuration window.

Cancel Button Added to Backup Dialog

When devices are selected for backup, and some are not on-line, a warning dialog box appears. A "Cancel" button is included to allow the user to cancel the backup.

Default Descriptions Added for Standard Extensions

The "Description" includes a standard description based to the filename extension instead of displaying "Unknown".

- .log -> Log file
- .img -> Software file
- .cmd -> Command file

New 'Uboot' System File Found on OmniSwitch 9000 Devices

OmniSwitch 9000 will support uploading of the "Uboot" System file to the switch (after which it must be manually installed using the CLI).

Notifications Enhancements

Trap Definition Display Updates

The "View Trap Definition" panel now includes the list of variables for the selected trap, including the description fields from the MIB for each variable.

Preferences Enhancements

"Move Up/Down" Controls for Custom Menu Panel

"Move Up" and "Move Down" controls were added next to the Customized Menu Commands Panel too allow the user to organize the order in which the commands will appear on the right-click menu.

Trap Replay Polling Preference

In the Notifications panel, an option was added to enable/disable "trap replay polling". This option to automatically poll AOS devices for missing traps is now changed to default ON for this release, but can be disabled with this preference control.

Telnet and CLI Scripting Enhancements

"Delete" and "Export" Buttons Added to View Log Panel

"Delete" and "Export" buttons were added to the View Log panel of the Telnet application. "Delete" allows the user to delete the selected log files; and "Export" brings up a dialog box allowing the user to export the selected log files to a directory of choice.

"Name" Column Added to View Log Panel

A "Name" column was added to the View Log panel of the Telnet application. The column displays the name of the switch, defined either as the SNMP "sysName" value or the DNS name, according to the Preference setting.

Password Pop-Up Dialog Added for "Send Script" Function

If there are switches without a Telnet username/password, a dialog box pops us allowing the user to add the username/password to multiple or single switch(es) as in Resource Manager.

Quarantine Manager Enhancements

New Quarantine Manager "Canned" CLI Scripts

There are two new "canned" CLI scripts available in the Telnet application in support of Quarantine Manager. One is used to create a MAC group called "Quarantine" and the other to delete it. Quarantine Manager, based on its internal set of rules, will add a MAC address to this MAC group when present on a device.

External Notification

A user can specify external e-mail addresses or scripts to be run when quarantine actions are taken. This provides a way to integrate with trouble-ticket systems. Like the Notifications application, this application depends on the user setting the SMTP Server from the Preferences applications (in the Sending E-mail section). Also included is the definition of a trap or syslog event that will cause Quarantine Manager to release a quarantine for a MAC address to allow an external trouble-ticket system to release the quarantine.

Network Segmentation

The user can limit the deployment of a quarantine to a subset of managed switches, rather than applying it to all switches as in release 2.4. This can improve the quarantine deployment performance, and minimize the usage of finite switch resources like MAC rule tables.

Action to Disable/Enable Port

The user can create a quarantine action to disable a port rather than creating a VLAN or ACL rule. The Configuration tab of Quarantine Manager contains a checkbox for disabling a port, I addition to the Quarantine VLAN name and the MAC Group Name. If the checkbox is checked the port is disabled when a Quarantine Rule is matched. To further control the use of port enable/disable, the user can right-click a switch, select the Edit menu item, and bring up a dialog box that indicate whether ports on the switch can be enabled or disabled.

Quarantine Manager/SecureView-ACL Interaction

The SecureView Access Control List (ACL) Wizard allows the user to create an ACL that can be used by the Quarantine Manager application. The user creates a MAC Group that includes any devices he wants in the ACL, then configures that MAC Group in the Quarantine Manager application (9000 series switches only).

Automatic DNS/IP Address Conversion

If a user enters a name in the IP address field, it is automatically converted to an IP address using DNS, if possible

Topology Enhancements

AMAP Links VLAN ID Display

The Topology application displays the remote VLAN ID associated with an AOS device AMAP Link. This includes AOS devices that run AOS AMAP software. Many OmniStack Series devices like 6xxx and OS6300-24 also support AMAP and can provide the VLAN ID associated with a link. Links for these devices will also show their VLAN information. XOS Adjacency Tables do not keep VLAN information and OmniVista will not display VLAN information for XOS devices.

Multiple Switch Pop-Up in Topology Maps

A user can select multiple devices and right-click to display a pop-up menu that will apply to all selected devices. The pop-up menu for switches in Topology Map support for the following three actions:

- Find in Tree - This option is available only when a single device is selected. It is not available when multiple switches are selected.
- Poll Links - This option is available for all maps. Links for the selected switches are polled.
- Remove from the Map - This option is available to authorized users on all logical maps.

New Applications Added

Groups

The Groups application enables you to create groups, which can be used in various policy conditions of PolicyView QoS and SecureView ACL applications.

Authentication Servers

The Authentication Servers application enables you to create, modify, and delete authentication servers in OmniVista.

SecureView ACL

The SecureView ACL application, available as an add-on package, is used to create and manage Access Control Lists (ACLs).

New Platforms Supported

Suse Linux Platform

Novell's Linux Suse Professional 9.3 is supported as an alternate Linux platform. It is expected that other Suse Linux will also work correctly.

9.10 Quarantine Manager

ACL Support

Quarantine Manager now supports Access Control Lists (ACL).

DHCP MAC Rule

DHCP requests from a banned device are now sent to the Quarantine VLAN. The Network Administrator can direct banned traffic from the Quarantined VLAN to a Remediation Server that will provide the user with information explaining why their device was banned and what steps to take to connect to the network.

Fortinet Event Descriptions

The user can automatically access the Fortinet web site for a detailed description of any Fortinet event by clicking on the event in the Candidate or Banned Tables.

Wireless Device Rules

Quarantine Manager now includes Built-In Rules for wireless devices.

9.11 Release 2.4.1

6800L Series Switch Support

OmniVista now supports the OmniSwitch 6800-24L and 6800-48L.

Notifications: Trap Responder Includes Agent Name

Trap Responder Tables now supports a new Agent Name variable.

Preferences: New Audit Log Size Preference Element

The Audit Log Size Preference now allows you to set the maximum audit file copies.

Quarantine Manager

The Quarantine Manager Application enables the Network Administrator to quarantine devices to protect the network from attacks. The application works with an external third-party Intrusion Prevention System (IPS), such as Fortinet, or a network device, such as an Alcatel-Lucent AOS switch, which sends either a Syslog message or SNMP trap to Quarantine Manager when it blocks any network traffic.

Second Generation OmniAccess Wireless and Access Point Support

Second generation OmniAccess WLAN devices (OmniAccess 43xx, 6xxx, AP6x, and AP 70) are supported as third party devices.

Solaris 64-bit Mode

A new release of JRE1.4.2 is installed with OmniVista 2.4.1. On Solaris, this JRE is 64 bit-capable. On installation, only the 32 bit mode is enabled. However, it is possible to enable 64 bit mode by editing the corresponding ".LAX" files and editing the line that contains the '-d32' flag to contain '-d64' instead.

Topology: Port Alias Names Displayed in the Device Status Screen

Port Alias names are displayed in the Physical Port Tab of the Device Status Screen in the Topology application.

Topology: MiniBoot and BootROM Information Added to Device Inventory

Device inventory information includes BootROM, MiniBoot, and FPGA information.

VLANs: Multinetting on 7700 and 8800 Switches (Release 5.1.6)

AOS Release 5.1.6 supports multiple IP router interfaces per VLAN. The VLAN application enables the user to create up to eight (8) IP interfaces per VLAN, per switch.

VLANs: New Implementation of STP

STP protocol options within the VLANs application have been updated in Release 5.1.6.

XOS 4.4.5 MIBs

OmniVista 2.4.1 is shipped with version 4.4.5 of the XOS MIBs.

9.12 Release 2.4.0

6800 Series Switch Support

The new OmniSwitch OS6800 family of switches (OS6800-24 and OS6800-48) is now supported.

Notifications

Trap Display

When viewing traps for a specific switch in the Notifications application, all traps received from any valid IP address associated with the switch are now displayed. In previous releases, only traps with a source IP address matching the management address used by OmniVista were displayed.

Trap Forwarding Feature

Traps can be forwarded to a specific IP address.

New Column Added to Notifications Table

A new column was added to the Notifications Table in the Notifications application. The "Agent Name" column displays the value of the "sysName" variable from the switch.

Custom Menu "Scope" Option in the Preferences Application

A "scope" option was added to the "Customized Menu Commands" option in the Preferences application. This enables users to configure custom pop-up menus for different devices. The customized pop-up menu can be configured with the following parameters:

- **All** - Matching the behavior of 2.3. Custom menu commands appear for all applicable devices. This is the DEFAULT value.
- **Mibset** - Specifies one or more mibsets names. All devices that use these mib sets will include the custom menu item.
- **OID** - Specifies an explicit OID string. All devices whose "sysObjectID" value starts with the values specified will include the custom menu item.

Polling for Missing Traps

AOS switches already send traps labeled with a sequence number, which can be used to detect missing traps. The switch can be asked to replay traps for a given listener, starting with a given sequence number. Upon detecting a gap in the sequence numbers of received traps from a switch, OmniVista will immediately request that the switch send the missing traps, starting from the beginning of the oldest known gap which has data available on the switch.

9.13 Release 2.3.0

Support for AOS 5.1.5

Basic discovery and monitoring support has been added for all AOS 5.1.5 devices. This includes chassis/module display, statistics support, and updated MIBs.

Support for OS6600-U24, 6600-P24, 6602-24, and 6602-48 Switches

The new OmniSwitch 6600 family of switches (OS6600-U24, OS6600-P24, OS6602-24, and OS6602-48) are now supported..

Support for OS6300-24 Switches

The OS6300-24 switches are now supported.

OmniVista Data Backup/Restore

A new application called "Server Backup" has been added that provides live backups of discovery, security, MIB caching, and all application-specific data. In addition, the contents of its data store and the LDAP server component are also backed up at the same time.

Coexistence with 4760 Server on Same PC

Both OmniVista 4760 and 2500 can now exist on the same workstation. If both the OmniVista 2500 and 4760 are installed on the same server, they will each include their own private LDAP server.

Subnet Mask Control

OmniVista 2.3 offers controls to define subnets of arbitrary granularity, and define arbitrary names for the subnets.

Polling Enhancements

In 2.2, there was no indication in the GUI when regular polling cycles are invoked. With 2.3, a set of 5 indicator lights in a horizontal row has been added for this purpose. The display is at the lower right-hand corner, to the left of "Status Indicator Light".

AMAP Support for OS6300-24 Switches

The OS6300-24 switches now support AMAP adjacency protocol, and with this release of OmniVista we use that capability to place these switches on the topology maps automatically.

AMAP Support for 6600-U24, 6600-P24, 6602-24, and 6602-48 Switches

The OS6600-U24, OS6600-P24, OS6602-24, and OS6602-48 switches now support AMAP adjacency protocol, and with this release of OmniVista we use that capability to place these switches on the topology maps automatically.

Integrated SSH2

In release 2.3 both Telnet and SSH, including SSH version 2, are supported directly from the OmniVista GUI using a licensed third party product.

CLI Scripting

Both Telnet and SSH has built-in support for scripting, including auto-login. In 2.3 scripting is supported on AOS switches.

Resource Manager

The inventory feature now supports the OS6600-U24, OS6600-P24, OS6602-24, and OS6602-48 series of switches. In addition, XOS extended memory is now supported.

Trap Responder Extensions

In 2.3 you can generate responses based on individual traps. The selection mechanism is the same "filter" mechanism that can be used to customize the trap display (or any table display). Instead of selecting by severity, the selection will be by filter.

Trap Export

Support has been added for exporting traps in the .csv format. This format can be used by spreadsheets such as Microsoft Excel.

Client-Server SSL Option

In release 2.3 an option for encrypting client/server communications using the Secure Socket Layer (SSL) protocol is now supported.

Rescheduling Support for Backup

OmniVista backups can be done immediately or scheduled for a later time and date.

Ability to Schedule Switch Reboot

The "reboot" dialog displayed when you select the menu item labeled "Reboot [From Working|From Certified]" now lets you decide between an immediate reboot and a delayed one. In addition, a checkbox to that dialog labeled "Reboot All" will let you perform a complete reboot of the CMMs and the NIs.

> **Note:** The "Reboot Al" is only available in the "Reload from Certified" not the "Reload from Working" selection. This command performs a complete reboot of CMM-A, CMM-B, and all NIs.

Locator Application Enhancements

Locator now supports OmniSwitch 6600-U24, 6600-P24, 6602-24, and 6602-48 switches and OmniStack 6300-24 switches.

WLAN (OmniAccess 4012/4024 and 4102) Enhancements

An option to import icons associated with third party devices has been added. In addition, an associate element manager launch with specific third party OID has been implemented.

Windows 2003 Sever Support for All OmniVista Applications

Microsoft Windows 2003 Server is now supported for all OmniVista applications.

BootROM, MiniBoot, and FPGA (BMF) Upgrades Supported on OmniSwitch 7700/7800/8800

The Resource Manager application now supports BootROM, MiniBoot, and FPGA (BMF) upgrades on OmniSwitch 7700/7800/8800 switches only. (This feature is not supported on OS6600 switches.)

> **Note:** This new feature requires that the switch(es) you upgrade must be running with 5.1.5.R03 (or later) image files before you start the upgrade.

Appendix A - Sample Telnet Scripting Program

```
package com.alcatel.ov1.ws1.client;
import java.net.InetAddress;
import java.net.UnknownHostException;
import java.rmi.RemoteException;
import java.text.SimpleDateFormat;
import java.util.StringTokenizer;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLSession;
import javax.xml.rpc.ServiceException;
import javax.xml.rpc.Stub;
/**
 * Sample Standalone client for testing Telnet Scripting Web Services
 *
 * @version 1.0
 */
public class TelnetScriptingClient
{
```

```
public static final String FILENAME   = "TelnetScriptingData.fileName";
public static final String TIMESTAMP = "TelnetScriptingData.timeStamp";
public static final String LOG_FILENAME = "TelnetScriptingLogData.fileName";
public static final String LOG_DATE  = "TelnetScriptingLogData.date";

/*
 * Copied from TelnetScriptingSendResultData server object
 */
public static int NO_ERROR = 0;
public static int PARAMETER_ERROR_MISSING_VARIABLES = 1;
public static int PARAMETER_ERROR_MISSING_LOGINS = 2;
public static int RUN_ERROR = 4;

public static final int EQUALS             = 0;
public static final int NOT_EQUALS         = 1;
public static final int LESS_THAN          = 2;
public static final int LESS_THAN_EQUAL    = 3;
public static final int GREATER_THAN       = 4;
public static final int GREATER_THAN_EQUAL  = 5;
public static final int STARTS_WITH        = 6;
public static final int ENDS_WITH          = 7;
public static final int CONTAINS           = 8;
public static final int OPS_SIZE           = 9;    // Number of operations

private boolean _ssl = false;
public TelnetScriptingClient(String[] args)
{

String testScriptName = "MyScript";

   WebService1 ovWeb = null;

   try {
   String newScriptContent = "no more\n" +
     "show system\n" +
     "show chassis\n" +
     "show hardware info\n";
```

```
String endPoint = "http://yourOmniVistaServerIP:8080/axis/services/OVWeb1";
String deleteScript = "Y";
String deleteLogs = "N";
String switchIp = "10.255.11.161";
String username = "admin";
String password = "yourPassword";
String secondaryPw = "yourSecondPassword";

  if (_ssl == true)
  {
     //
     // Bypass security check for self-signed peer certificate
     //
     HostnameVerifier hv = new HostnameVerifier() {
        public boolean verify(String urlHostName, SSLSession session) {
           System.out.println("Warning: URL Host: "+urlHostName+" vs. "+session.getPeerHost());
           return true;
        }
     };
     HttpsURLConnection.setDefaultHostnameVerifier(hv);
  }

  int MAX_RESULTS = 500;
  WebService1ServiceLocator ovWebService = new WebService1ServiceLocator();
  if (endPoint != null)
  {
  System.out.println("Setting end point to: " + endPoint);
  ovWebService.setOVWeb1EndpointAddress(endPoint);
  }
  ovWeb = ovWebService.getOVWeb1();
  Stub stub = (Stub)ovWeb;
  stub._setProperty(Stub.SESSION_MAINTAIN_PROPERTY, Boolean.TRUE);
  System.out.println("Login");
  ovWeb.login(username.getBytes(), password.getBytes());
  System.out.println("Login succeeded");

  /* We can construct sorter or filter and pass it to querying method
  SortObj[] mySorters = new SortObj[1];
  mySorters[0] = new SortObj(false, FILENAME); // descending sort order
```

```
        FilterObj[] myFilters = new FilterObj[1];
        myFilters[0] = new FilterObj(FILENAME, STARTS_WITH, "test".getBytes(), true);
        */
        TelnetScriptingResultSet results = ovWeb.queryScriptFiles(null, null, /*myFilters, mySorters,*/
MAX_RESULTS);
        long cnt = results.getNumResults();
        System.out.println("Result contains " + cnt + " rows.\n\n");

        System.out.println("Query available scripts on the system\n");
        TelnetScriptingData[] tnsData = ovWeb.getScriptFilesData(results.getUniqueId(), 0, MAX_RESULTS);
      System.out.printf("%-50s %-20s\n\n", "File Name", "Create Timestamp");



      SimpleDateFormat fmt = new SimpleDateFormat("MMM dd yyyy hh:mm a");
        for (int i = 0; i < tnsData.length; i++) {
        TelnetScriptingData tns = tnsData[i];
        long createTimeMillisec = tns.getTimeStamp();
        System.out.printf("%-50s %-20s\n", tns.getFilename(),   fmt.format(createTimeMillisec) );
        }

        SortObj[] sorters = new SortObj[1];
        sorters[0] = new SortObj(false /*descending*/, FILENAME);

        ResultSet sortedResults = ovWeb.sortScriptFilesResults(results.getUniqueId(), sorters);

        System.out.println("\n============================================================
============================================================\n\n");
        System.out.println("Sort objects on file names descending\n\n");
        System.out.printf("%-50s %-20s\n\n", "File Name", "Create Timestamp");
        tnsData = ovWeb.getScriptFilesData(sortedResults.getUniqueId(), 0, MAX_RESULTS);
        for (int i = 0; i < tnsData.length; i++) {
        TelnetScriptingData tns = tnsData[i];
        long createTimeMillisec = tns.getTimeStamp();
        System.out.printf("%-50s %-20s\n", tns.getFilename(),   fmt.format(createTimeMillisec) );
        }
        System.out.println("\n============================================================
============================================================\n\n");
        System.out.println("Filter objects on file names starting with 'sha' from previous sorted result\n\n");
        System.out.printf("%-50s %-20s\n\n", "File Name", "Create Timestamp");
        FilterObj[] addOnFilters = new FilterObj[1];
```

```
addOnFilters[0] = new FilterObj(FILENAME, STARTS_WITH, "sha".getBytes(), true);
ResultSet filteredResults = ovWeb.refineScriptFilesResults(sortedResults.getUniqueId(), addOnFilters);
tnsData = ovWeb.getScriptFilesData(filteredResults.getUniqueId(), 0, MAX_RESULTS);
for (int i = 0; i < tnsData.length; i++) {
TelnetScriptingData tns = tnsData[i];
long createTimeMillisec = tns.getTimeStamp();
System.out.printf("%-50s %-20s\n", tns.getFilename(),   fmt.format(createTimeMillisec) );
}


// Dispose of the result sets when we no longer need to fetch or do sorting/filtering from it.
ovWeb.disposeScriptFilesResults(results.getUniqueId());
ovWeb.disposeScriptFilesResults(sortedResults.getUniqueId());
ovWeb.disposeScriptFilesResults(filteredResults.getUniqueId());
System.out.println("\n============================================================
============================================================\n\n");

System.out.println("Create a script file " + testScriptName + "\n");

// Create a test file what requires 2 user-defined variables - $parm1 and $parm2 when it gets executed
ovWeb.createScriptFile(testScriptName, newScriptContent.getBytes());

results = ovWeb.queryScriptFiles(null, null, MAX_RESULTS);
cnt = results.getNumResults();

System.out.println("Query available scripts on the system\n");
System.out.println("Result contains " + cnt + " rows.\n\n");

tnsData = ovWeb.getScriptFilesData(results.getUniqueId(), 0, MAX_RESULTS);
System.out.printf("%-50s %-20s\n\n", "File Name", "Create Timestamp");

for (int i = 0; i < tnsData.length; i++) {
TelnetScriptingData tns = tnsData[i];
long createTimeMillisec = tns.getTimeStamp();
System.out.printf("%-50s %-20s\n", tns.getFilename(),   fmt.format(createTimeMillisec) );
}
ovWeb.disposeScriptFilesResults(results.getUniqueId());

System.out.println("\n============================================================
============================================================\n\n");
```

```
        System.out.println("Get file content of  " + testScriptName + "\n");

        byte[] contentBin = ovWeb.getScriptFileContent(testScriptName);
        String fileContent = new String(contentBin);
        System.out.println("\n++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++");
      StringTokenizer strTok = new StringTokenizer(fileContent, "\r\n");
        while (strTok.hasMoreTokens())
        {
        String line = strTok.nextToken();
        System.out.print("+");
        System.out.printf("%-100s", line);
        System.out.println("+");
        }
        System.out.println("++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++");

        System.out.println("\n============================================================
============================================================\n\n");



        TelnetSwitchInfo swInfo = new TelnetSwitchInfo();
        swInfo.setSwitchIp(switchIp);
        swInfo.setUsername(username);
        swInfo.setPassword(password);
        swInfo.setSecondaryPassword(secondaryPw);

        TelnetScriptingSendRequest tnRequest = new TelnetScriptingSendRequest();
        tnRequest.setSwitchInfos(new TelnetSwitchInfo[] {swInfo});

        String clientIp = "";
try {
clientIp = InetAddress.getLocalHost().getHostAddress();
} catch (UnknownHostException ex) {
ex.printStackTrace();
}

        tnRequest.setClientIp(clientIp);
        tnRequest.setParamNames(new String[]{"$showParm1", "$showParm2", "$tcpParm"});
        tnRequest.setParamValues(new String[] {"configuration", "snapshot", "ports"});
```

```
    System.out.println("Sending Script " + testScriptName);
    tnRequest.setScriptName(testScriptName);

    TelnetScriptingSendResultData result = ovWeb.sendScriptFile(tnRequest);

    try {
  if (result == null)
  {
  System.out.println("Result object is null.");

  }
  else if (result.getErrorCode() == PARAMETER_ERROR_MISSING_LOGINS)
  {
  String[] missingLogins = result.getMissingLoginSwitchIps();
    System.out.println("Missing Logins: ");
    for (int i = 0; missingLogins != null && i < missingLogins.length; i++)
    {
    System.out.println(missingLogins[i]);
    }

  }
  else if (result.getErrorCode() == PARAMETER_ERROR_MISSING_VARIABLES)
  {
  String[] missingParams = result.getMissingParamsNames();
    System.out.println("Missing Params: ");
    for (int i = 0; missingParams != null && i < missingParams.length; i++)
    {
    System.out.println(missingParams[i]);
    }
  }
  else
  {
  long startTime = System.currentTimeMillis();
  boolean isCancelled = false;

  while (result.getErrorCode() == NO_ERROR && result.getUniqueId() != null &&
result.getProgress().intValue() < 100)
        {
```

```
   // Conditional to abort abort the operation if it takes too long
   if (System.currentTimeMillis() - startTime > 120 * 1000 )
            {
   ovWeb.cancelSendScriptTask(result.getUniqueId());
   isCancelled = true;
            break;
            }

   result = ovWeb.getSendScriptProgress(result.getUniqueId());

            // In the mean time check for progress every second
                  System.out.println("Progress = " + result.getProgress() + "%");
                  try {
Thread.sleep(1000);
} catch (InterruptedException ex) {
ex.printStackTrace();
}
         }

   if (result.getErrorCode() != NO_ERROR) // This could be RUN_ERROR
   {
   System.out.println("Error encountered: " + result.getErrorMessage());
   }
   else {
   if (isCancelled)
   {
   System.out.println("Cancelled.\n\n");
   }
   else
   {
   System.out.println("Done.\n\n");
   }
   }



         System.out.println("Telnet Scripting Send messages:");

   String[] messages = ovWeb.getSendScriptEventMessages(result.getUniqueId());
```

```
            System.out.println("\n++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++");
      for (String aMesg : messages)
      {
      System.out.print("+");
      System.out.printf("%-100s", aMesg);
      System.out.println("+");

      }
            System.out.println("++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++\n\n");
      }



         }
   finally
   {
    if (result != null)
    ovWeb.disposeSendScriptResults(result.getUniqueId());
   }

         results = ovWeb.queryScriptFiles(null, null, MAX_RESULTS);
         cnt = results.getNumResults();

         System.out.println("Query available scripts on the system\n");
         System.out.println("Result contains " + cnt + " rows.\n\n");
         tnsData = ovWeb.getScriptFilesData(results.getUniqueId(), 0, MAX_RESULTS);
         System.out.printf("%-50s %-20s\n\n", "File Name", "Create Timestamp");

         for (int i = 0; i < tnsData.length; i++) {
         TelnetScriptingData tns = tnsData[i];
         long createTimeMillisec = tns.getTimeStamp();
         System.out.printf("%-50s %-20s\n", tns.getFilename(),   fmt.format(createTimeMillisec) );
         }
         ovWeb.disposeScriptFilesResults(results.getUniqueId());

         System.out.println("\n============================================================
============================================================\n\n");
```

```
        System.out.println("\n============================================================
============================================================\n\n");



        if ("Y".equals(deleteScript.toUpperCase())) {
            System.out.println("Delete " + testScriptName + "\n\n");
int numFilesDeleted = ovWeb.deleteScriptFiles(new String[] { testScriptName });
   }

        TelnetScriptingLogResultSet resSet = ovWeb.queryScriptLogFiles(null, null, MAX_RESULTS);
        cnt = resSet.getNumResults();

        System.out.println("Query available telnet scripting log files\n");
        System.out.println("Result contains " + cnt + " rows.\n\n");

        TelnetScriptingLogData[] logData = ovWeb.getScriptLogFilesData(resSet.getUniqueId(), 0,
MAX_RESULTS);
      System.out.printf("%-20s %-20s %-40s %-30s\n\n", "Ip Address", "Name", "Filename", "Date");

        for (int i = 0; i < logData.length; i++) {
        TelnetScriptingLogData tsl = logData[i];
        System.out.printf("%-20s %-20s %-40s %-30s\n", tsl.getIpAddress(),
        tsl.getSysName(), tsl.getFileName(), fmt.format(tsl.getDate()));
        }

        sorters = new SortObj[1];
        sorters[0] = new SortObj(true /*ascending*/, LOG_FILENAME);

        sortedResults = ovWeb.sortScriptLogFilesResults(resSet.getUniqueId(), sorters);
        logData = ovWeb.getScriptLogFilesData(sortedResults.getUniqueId(), 0, MAX_RESULTS);

        System.out.println("\n\nSort log files on file names ascending\n");
        System.out.println("Result contains " + cnt + " rows.\n\n");

        System.out.printf("%-20s %-20s %-40s %-30s\n\n", "Ip Address", "Name", "Filename", "Date");

        for (int i = 0; i < logData.length; i++) {
        TelnetScriptingLogData tsl = logData[i];
        System.out.printf("%-20s %-20s %-40s %-30s\n", tsl.getIpAddress(),
        tsl.getSysName(), tsl.getFileName(), fmt.format(tsl.getDate()));
```

```
        }

        String filterString = "MyScript";
        addOnFilters[0] = new FilterObj(LOG_FILENAME, STARTS_WITH, filterString.getBytes(), true);
        TelnetScriptingLogResultSet filteredRes = (TelnetScriptingLogResultSet)
ovWeb.refineScriptLogFilesResults(resSet.getUniqueId(), addOnFilters);
        cnt = filteredRes.getNumResults();
        logData = ovWeb.getScriptLogFilesData(filteredRes.getUniqueId(), 0, MAX_RESULTS);

        System.out.println("\n\nFilter log files on file names starting with '" + filterString + "' \n");
        System.out.println("Result contains " + cnt + " rows.\n\n");

        System.out.printf("%-20s %-20s %-40s %-30s\n\n", "Ip Address", "Name", "Filename", "Date");

        for (int i = 0; i < logData.length; i++) {
        TelnetScriptingLogData tsl = logData[i];
        System.out.printf("%-20s %-20s %-40s %-30s\n", tsl.getIpAddress(),
        tsl.getSysName(), tsl.getFileName(), fmt.format(tsl.getDate()));
        }



        ovWeb.disposeScriptLogFilesResults(resSet.getUniqueId());
        ovWeb.disposeScriptLogFilesResults(sortedResults.getUniqueId());
        ovWeb.disposeScriptLogFilesResults(filteredRes.getUniqueId());

        if (logData.length > 0)
        {
        String testLogFileName = logData[0].getFileName();

        System.out.println("\n============================================================
============================================================\n\n");
        System.out.println("Get log file content of  " + testLogFileName + "\n");

        String switchIP = logData[0].getIpAddress();
        String filename = logData[0].getFileName();
        contentBin = ovWeb.getScriptLogFileContent(switchIP, filename);
        String content = new String(contentBin);
        System.out.println("\n++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++");
        strTok = new StringTokenizer(content, "\r\n");
```

```
        while (strTok.hasMoreTokens())
        {
        String line = strTok.nextToken();
        System.out.print("+");
        System.out.printf("%-100s", line);
        System.out.println("+");
        }

        System.out.println("++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++\n\n");

        if (logData != null && logData.length > 0)
        {
        String[] switchIPs = new String[logData.length];
          String[] filenames = new String[logData.length];

          for (int i = 0; i < logData.length; i++)
          {
          switchIPs[i] = logData[i].getIpAddress();
          filenames[i] = logData[i].getFileName();
          }


   if ("Y".equals(deleteLogs.toUpperCase()))
                        {
System.out.println("Sending request to delete log files \n");
ovWeb.deleteScriptLogFiles(switchIPs, filenames);
System.out.println("Done deleting log files.");
   }
        }

       }

         System.out.println("DONE.");


      }
      catch (RemoteException ex) {
        System.out.println("RemoteException " + ex);
```

```
    }
    catch (ServiceException ex) {
        System.err.println("ServiceException " + ex);
    }
    catch (Exception ex) {
       System.out.println("Exception " + ex);
    }
    finally
    {
       try
       {
          if (ovWeb != null)
             ovWeb.logout();




       }catch(Exception ex1)
       {
          System.out.println("Error logging out of Web Services");
       }
    }
  }

  public static void main(String[] args)
  {
  if (args.length < 2)
  {
  System.out.println("usage: TelnetScriptingClient <configFile> <scriptFile>");
  return;
  }
     TelnetScriptingClient tnsc = new TelnetScriptingClient(args);
  }
}
```

TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS CODE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.