Release Notes

for

OmniVista 2500 Version 3.0

PolicyView 2730 Version 3.0

SecureView-SA 2750 Version 3.0

SecureView-ACL 2760 Version 3.0

Quarantine Manager 2770 Version 3.0

April 2006

Revision BE

Part Number 031858-10

READ THIS DOCUMENT

Includes OmniVista for
Windows Server 2003/Windows XP
Sun Solaris Systems
Red Hat Linux
Suse Linux

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

Table of Contents

Revision History

Release	Revision	Date	Description of Changes
1.0	A	06/01/01	General Availability Release
1.1	B	10/11/01	General Availability Release
2.0	E	07/12/02	General Availability Release
2.0.1	F	08/27/02	General Availability Release
2.1.0	H	11/08/02	Alpha Release for OmniSwitch 6648, 6624, and 8800
2.1.0	J	11/22/02	Beta Release
2.1.0	K	01/10/03	General Availability Release
2.2.0	L	07/11/03	Beta Release
2.2.0	M	08/29/03	General Availability Release
2.2.1	N	10/16/03	Maintenance Release
2.2.2	O	02/26/04	Maintenance Release
2.2.3	P	04/22/04	Maintenance Release
2.2.4	Q	07/13/04	Maintenance Release

2.2.5	R	08/03/04	Maintenance Release
2.2.6	S	08/24/04	Internal development release only
2.3.0	T	09/03/04	Beta Release
2.3.0	U	10/27/04	GA Release
2.3.0	V	11/02/04	Post GA
2.4.0	W	01/14/05	GA Release
2.4.1	X	05/26/05	GA Release (Quarantine Manager)
2.4.1	Y	07/22/05	Release Notes update in Support Build
2.4.2	Z	09/15/05	Maintenance Release for Quarantine Manager
2.4.1	AA	11/17/05	Release Notes update
3.0	BB	02/09/06	GA Release
3.0	BC	03/08/06	Release Notes update
3.0	BD	03/31/06	Release Notes update
3.0	BE	04/12/06	Release Notes update

1 Introduction■

These Release Notes cover the basic feature set supported by OmniVista 3.0 for the following supported platforms:

- Windows Server 2003/Windows XP
- Sun Solaris 2.9
- Linux (Red Hat Linux Enterprise Workstation)
- Linux Suse Professional 9.3.

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. These Release Notes cover both versions of OmniVista:

- **OmniVista Basic 2540 Multi-User** - allows installation of the server software on a physically separate machine for support of multiple client machines.
- **OmniVista Basic 2520 Single User** - the client and server software are installed on the same machine and additional client installations are not an option.

Unless otherwise specified, all information in this document is applicable to both systems. See the table below for a summary of supported versions and platforms:

OS	OV 3.0 BSU	OV 3.0 BMU Server	OV 3.0 BMU Client**	SwitchManager
Windows Server 2003	OK	OK	OK	OK
Windows XP	OK*	Not supported	OK	OK
Solaris (32 bit and 64 bit)	OK	OK	OK	OK
Red Hat Linux	OK	OK	OK	Not supported
Suse Linux (32 bit)	OK	OK	OK	Not supported

***Note:** Users can expect better performance on Windows Server 2003 than on Windows XP.
****Note:** "Client" here refers to the BMU Client loaded on a separate machine with any of the following OS: Windows Server 2003, Windows XP, Solaris, and Linux.

1.1 Technical Support Contacts■

For technical support, contact your sales representative or refer to one of the support resources below.

Alcatel Internetworking Service and Support can be reached as follows:

- North America, Latin America, Other International
  - Phone:
    - North America: 1-800-995-2696
    - Latin America: 1-877-919-9526
    - Other International: 1-818-878-4507
  - World Wide Web: www.ind.alcatel.com/
  - Electronic Mail for Non-critical technical questions: support@ind.alcatel.com
- Europe:
  - Phone: 33-388-55-69-04
  - World Wide Web: www.businesspartner.alcatel.com/
  - Electronic Mail for Non-critical technical questions: support.center@alcatel.com

Note: For the most recent version of OmniVista Release Notes go to Alcatel Service and Support page at https://eservice.ind.alcatel.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?■

1.3.1 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 o 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 OEM 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 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.

Traps Display Enhancement

When new Traps arrived quickly, the horizontal scroll bar under "Notifications for All Switches" would reset when new trap came in, making it difficult to read the table. A "Pause" was added in the top-right corner of the panel. When the user is done checking traps, he can press the "Play" button to resume displaying the new traps.

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 OEM 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.

1.3.2 Quarantine Manager 2.4.2

Quarantine Manager - ACL Support

Quarantine Manager now supports Access Control Lists (ACL).

Quarantine Manager - Wireless Device Rules

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

Quarantine Manager - 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.

Quarantine Manager - Fortinet Event Descriptions

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

1.3.3 Release 2.4.1

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.

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.

New Implementation of STP

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

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.

MiniBoot and BootROM Information Added to Device Inventory

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

XOS 4.4.5 MIBs

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

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.

New Audit Log Size Preference Element

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

Trap Responder Includes Agent Name

Trap Responder Tables now supports a new Agent Name variable.

Support For OmniSwitch 6800L Series

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

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 AOS switch, which sends either a Syslog message or SNMP trap to Quarantine Manager when it blocks any network traffic.

1.3.4 Release 2.4.0

Support for 6800 Switches

The new OmniSwitch 6800 family of switches (OS6800-24 and OS6800-48) are now supported.

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.

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.

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.

1.3.5 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 6600-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.

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 (sold separately)	XOS-based devices: OmniStack 2000/4000/5000 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 6624, 6648 OmniSwitch 6600-U24, 6600-P24 OmniSwitch 6602-24, 6602-48 OmniSwitch 6800-24, 6800-48, 6800-U24, 6800-24L, 6800-48L OmniSwitch 7700, 7800 OmniSwitch 8800 OmniSwitch 9700	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	OmniStack 6121, 6148 OmniStack 6224, 6224P, 6248, 6248P OmniStack 6300-24 2nd Generation WLAN (OmniAccess 43xx, 6xxx, AP6x, AP70) OmniAccess WAN	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 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 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 System Requirements■

The following minimum builds are required to run OmniVista 3.0:

- AOS
  - 7000, 8800, 6000 - 5.1.6.R02 and 5.1.5.R04
  - 6800 - 5.3.1.R02
  - 9000 - 6.1.1.R01
- XOS
  - OmniSwitch, OmniSwitch Router - 4.4.5 GA
  - 4024 - 4.3.3.B
- OEM
  - 6124/6148 - 3.40.x
  - 6300 - 2.2.0.1x
- OmniVista 3.0 upgrade paths supported
  - 2.3 to 3.0

- 2.4.1 to 3.0

2.1 Requirements for All Platforms■

2.1.1 Java Requirements

OmniVista includes the Java 2 Runtime Environment (JRE) Version 1.5 for each of the following supported platforms: Windows Server 2003/ Windows XP, Solaris 2.9 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.

2.1.3 Server Platform Requirements

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

2.1.4 OmniVista Basic 2520 Single User Platform Requirements

The system requirements for OmniVista Basic 2520 Single User are the same as those for the OmniVista Basic 2540 Multi-User Server and/or the requirements for the desired Element Managers, which ever is greater.

2.2 System Requirements for Microsoft Windows■

The minimum system requirements for running OmniVista 3.0 on Microsoft Windows are:

- Windows Server 2003 or Windows XP
- Client machine:
  - Pentium IV 1 GHz minimum, 2 GHz recommended
  - 1 GB RAM minimum
  - 2 GB of free disk space on the drive on which you will be installing OmniVista.
- Server machine:
  - Pentium IV 2 GHz minimum, 3 GHz recommended
  - 2 GB RAM minimum
  - 5GB of free disk space on the drive on which you will be installing OmniVista "Server" versions of windows -Windows 2003 Server, 20 GB if managing 1,500 switches or more

Note: Minimum configuration not recommended for managing more than 500 switches. For managing more than 1,500 switches, recommend 3 GB RAM on server, 2 GB RAM on client. You can allocate up to 1280 MB of RAM to the client and/or server.

2.2.1 PolicyView

The minimum system requirements for running PolicyView on Microsoft Windows (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

Note: When installing PolicyView on a machine with the OmniVista Multi-User Server or OmniVista Single User, this machine must NOT have multiple network interfaces, for example, dual NICs.

2.2.2 SecureView-SA

The minimum system requirements for running SecureView-SA on Microsoft Windows (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.2.3 SecureView-ACL

The minimum system requirements for running SecureView-ACL on Microsoft Windows (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.2.4 Quarantine Manager

The minimum system requirements for running Quarantine Manager on Microsoft Windows (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.
- Log size can be configured in the Preferences application.

2.3 System Requirements for Sun Solaris■

The minimum system requirements for running OmniVista 3.0 on Sun Solaris are:

- Server machine:
  - Sun Solaris 2 Workstation
  - Solaris 2.9 operating environment
  - 2 GB RAM minimum, 4 GB recommended for running 32-bit mode, 8 GB for 64-bit mode
  - 5 GB of free disk space on the drive on which you will be installing OmniVista, 20 GB if managing 1,500 switches or more
  - CD-ROM drive
  - Network interface
  - In the installation instructions in this document, you will be directed to download and apply patches to Solaris required for the Java 2 SDK.

Note: You can allocate up to 1280 MB of RAM to the client and/or server. You can also configure the server to use more memory in 64-bit mode after installation.

2.3.1 PolicyView

The minimum system requirements for running PolicyView on Sun Solaris (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.3.2 SecureView-SA

The minimum system requirements for running SecureView on Sun Solaris (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.3.3 SecureView-ACL

The minimum system requirements for running SecureView-ACL on Sun Solaris (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.3.4 Quarantine Manager

The minimum system requirements for running Quarantine Manager on Sun Solaris (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.
- Log size can be configured in the Preferences application.

2.3.5 Certified Configuration

The following server has been used to certify the configuration parameters:

- Sun V210 with 8GB memory, 2 processors
- Supporting operating / Solaris version 2.9/
- 64 bit environment - 5GB RAM allocated to the OmniVista Server
- OmniVista Server as the main and unique application used on this server.

OmniVista capabilities provided with this Configuration

- Up to 3000 switches supported (Mixed population of AOS/XOS devices)
- 300,000 traps stored on the server
- 99999 traps on client
- 6 clients

2.4 System Requirements for Linux■

The minimum system requirements for running OmniVista 3.0 on a Red Hat Linux or Suse Linux Workstation are:

- Client machine:
  - Pentium IV 1 GHz minimum, 2 GHz recommended
  - 1 GB RAM minimum
  - 2 GB of free disk space on the drive on which you will be installing OmniVista.
- Server machine:
  - Linux Workstation
  - Pentium IV 2 GHz minimum, 3 GHz recommended
  - 2 GB RAM minimum
  - 5 GB of free disk space on the drive on which you will be installing OmniVista, 20 GB if managing 1,500 switches or more
  - CD-ROM drive
  - Network interface.

Note: SwitchManager element managers are not supported on Linux. Red Hat Linux requires Enterprise Release 4, Kernel version 2.6.

2.4.1 PolicyView

The minimum system requirements for running PolicyView on Red Hat Linux Enterprise Workstation (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.4.2 SecureView-SA

The minimum system requirements for running SecureView-SA on a Red Hat or Suse Linux Workstation (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.4.2 SecureView-ACL

The minimum system requirements for running SecureView-ACL on a Red Hat or Suse Linux Workstation (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.

2.4.3 Quarantine Manager

The minimum system requirements for running Quarantine Manager on a Red Hat or Suse Linux Workstation (in addition to OmniVista requirements) are:

- 100 MB of free disk space on the drive on which you will be installing the OmniVista Basic.
- Log size can be configured in the Preferences application.

3 Installation■

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. Only OmniVista Basic application is available in Demo Mode. To test additional packages, such as Quarantine Manager or PolicyView, the customer must own valid licenses, including the license to the Core Package. Note that you can only upgrade to OmniVista 3.0 from versions 2.3 or 2.4.

3.1 Installing OmniVista on Windows Systems■

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. Change to the **OmniVistaBasic** directory (Single-User or Mulit-User).
#. Double-click the **Disk1** folder.
#. Double-click the **InstData** folder.
#. Double-click the **Windows** folder.
#. Double-click the **install_win.exe** icon.
#. 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.

#. Download and apply patches to Solaris 2.9 required for the Java 2 SDK, Standard Edition, Version 1.5.
#. Go to http://java.sun.com/j2se/1.5.0/jre/install-solaris.html and follow the instructions for determining which patches are already installed on your system, which patches are required for Solaris 2.9, and how to obtain and install the required patches.
#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. At the command prompt, change to the **OmniVistaBasic** directory (Single-User or Multi-User).
#. Change to the **Disk1** directory, then to the **InstData** directory, and finally to the **Solaris** directory on the CD. Now enter: **./install_sol.bin**.
#. 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.

3.2.1 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.

3.3 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.

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.

#. At the command prompt, change to the **OmniVistaBasic** directory (Single-User or Multi-User).
#. Change to the **Disk1** directory, then to the **InstData** directory, and finally to the **Linux** directory on the CD. Now enter: **./install_lin.bin**.
#. 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 Add-On Applications■

You must install the **OmniVista Basic Single User** or **OmniVista Basic Multi-User** system before installing add-on applications. For additional requirements, refer to the **Release Notes** document. Available Add-on Applications include:

- OmniVista PolicyView 2730
- SecureView-SA 2750
- SecureView-ACL 2760
- Quarantine Manager 2770.

3.4.1 Installing PolicyView

3.4.1.1 Installing PolicyView on Windows

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. Change to the **PolicyView** directory.
#. Double-click the **Disk1** folder.
#. Double-click the **InstData** folder.
#. Double-click the **Windows** folder.
#. Double-click the **install_win.exe** icon.
#. Follow the instructions in the installer to completion.

3.4.1.2 Installing PolicyView on Sun Solaris

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. At the command prompt, change to the **PolicyView** directory.
#. In the CD-ROM drive window, open the **Disk1** folder.
#. In the Disk1 window, open the **InstData** folder.
#. In the InstData window, open the **Solaris** folder.
#. Enter **./install_sol.bin**.
#. Follow the instructions in the installer to completion.

3.4.1.3 Installing PolicyView on Linux

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. At the command prompt, change to the **PolicyView** directory.
#. In the CD-ROM drive window, open the **Disk1** folder.
#. In the Disk1 window, open the **InstData** folder.
#. In the InstData window, open the **Linux** folder.
#. Enter **./install_lin.bin**.
#. Follow the instructions in the installer to completion.

3.4.1.4 PolicyView Post-Installation Configuration

For all platforms, in order for OmniVista to correctly determine the state of devices, you must subscribe to the following traps:

- For XOS switches: policyEvent
- For AOS switches: policyEventNotification.

Trap Configuration can be performed in the Topology and Notifications applications; just click the bell icon on the tool bar and refer to the online help using the Help button that appears on each dialog of the Trap Configuration wizard.

Note: On UNIX systems, it is recommended that you modify a startup script to launch the Netscape Directory Server automatically when you turn on or restart the computer.

3.4.2 Installing SecureView-SA

3.4.2.1 Installing SecureView-SA on Windows

To install SecureView-SA on Windows, you must log on with a User Profile that has administrative rights.

# . Insert the **OmniVista NMS** CD into the CD-ROM drive.
# . change to the **SecureView** directory.
# . Double-click the **Disk1** folder.
# . Double-click the **InstData** folder.
# . Double-click the **Windows** folder.
# . Double-click the **install_win.exe** icon.
# . Follow the instructions in the installer to completion.

3.4.2.2 Installing SecureView-SA on Sun Solaris

To install SecureView-SA on Sun Solaris, you must log on with a User Profile that has administrative rights.

# . Insert the **OmniVista NMS** CD into the CD-ROM drive.
# . At the command prompt, change to the **SecureView** directory.
# . In the CD-ROM drive window, open the **Disk1** folder.
# . In the Disk1 window, open the **InstData** folder.
# . In the InstData window, open the **Solaris** folder.
# . Enter **./install_sol.bin**.
# . Follow the instructions in the installer to completion.

3.4.2.3 Installing SecureView-SA on Linux

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

# . Insert the **OmniVista NMS** CD into the CD-ROM drive.
# . At the command prompt, change to the **SecureView** directory.
# . In the CD-ROM drive window, open the **Disk1** folder.
# . In the Disk1 window, open the **InstData** folder.
# . In the InstData window, open the **Linux** folder.
# . Enter **./install_lin.bin**.
# . Follow the instructions in the installer to completion.

3.4.2 Installing SecureView-ACL

3.4.2.1 Installing SecureView-ACL on Windows

To install SecureView-ACL on Windows, you must log on with a User Profile that has administrative rights.

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. change to the **SecureView** directory.
#. Double-click the **Disk1** folder.
#. Double-click the **InstData** folder.
#. Double-click the **Windows** folder.
#. Double-click the **install_win.exe** icon.
#. Follow the instructions in the installer to completion.

3.4.2.2 Installing SecureView-ACL on Sun Solaris

To install SecureView-ACL on Sun Solaris, you must log on with a User Profile that has administrative rights.

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. At the command prompt, change to the **SecureView** directory.
#. In the CD-ROM drive window, open the **Disk1** folder.
#. In the Disk1 window, open the **InstData** folder.
#. In the InstData window, open the **Solaris** folder.
#. Enter **./install_sol.bin**.
#. Follow the instructions in the installer to completion.

3.4.2.3 Installing SecureView-ACL on Linux

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. At the command prompt, change to the **SecureView** directory.
#. In the CD-ROM drive window, open the **Disk1** folder.
#. In the Disk1 window, open the **InstData** folder.
#. In the InstData window, open the **Linux** folder.
#. Enter **./install_lin.bin**.
#. Follow the instructions in the installer to completion.

3.4.3 Installing Quarantine Manager

3.4.3.1 Installing Quarantine Manager on Windows

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. Change to the **QuarantineManager** directory.
#. Double-click the **Disk1** folder.
#. Double-click the **InstData** folder.
#. Double-click the **Windows** folder.
#. Double-click the **install_win.exe** icon.
#. Follow the instructions in the installer to completion.

3.4.3.2 Installing Quarantine Manager on Sun Solaris

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. At the command prompt, change to the **QuarantineManager** directory.
#. In the CD-ROM drive window, open the **Disk1** folder.
#. In the Disk1 window, open the **InstData** folder.
#. In the InstData window, open the **Solaris** folder.
#. Enter **./install_sol.bin**.
#. Follow the instructions in the installer to completion.

3.4.3.3 Installing Quarantine Manager on Linux

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

#. Insert the **OmniVista NMS** CD into the CD-ROM drive.
#. At the command prompt, change to the **QuarantineManager** directory.
#. In the CD-ROM drive window, open the **Disk1** folder.
#. In the Disk1 window, open the **InstData** folder.
#. In the InstData window, open the **Linux** folder.
#. Enter **./install_lin.bin**.th
#. 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. You may upgrade your old installation of OmniVista 2.4.1 or 2.4.2 by installing the new package over the old installation. Performing an upgrade installation 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 (2.3, 2.4) 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\Alcatel OmniVista 2500\data").

3.5.1 Copying the "Data" Directory from OmniVista 2.3 or 2.4 to 3.0

To upgrade without giving up the current working configuration, copy the data directory and all of its files from an OmniVista 2.3 or 2.4 server to an OmniVista 3.0 server.

#. Stop the OmniVista 2.3/2.4.server.
#. Rename the data directory located in the C:\Program Files\OmniVista 2500\ directory on the OmniVista 2.4. server to something other than "data" (e.g., "data2_4_1").
#. Copy the data directory located in the C:\Program Files\OmniVista 2500\ directory on the OmniVista 2.4 server to the C:\Program Files\OmniVista 2500\ directory on the OmniVista 3.0 server.
#. On the OmniVista 2.3/2.4 server, copy the openldapdb folder and all of its contents from the directory you created in Step 2 (e.g., "data2_4_1") to the C:\Program Files\OmniVista 2500\data\ directory on the OmniVista 3.0 server.
#. Remove the data\mibs\mibsets.txt file. (Any third-party MIB sets must be re-imported.)
#. Restart the OmniVista 2.3/2.4 server.
#. Restart OpenLDAP on the OmniVista 3.0 server.

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.

#. 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).
#. 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.
#. Close the client and shutdown the server.
#. 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.
#. 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.

3.5.3 Upgrading PolicyView from 2.3 or 2.4 to 3.0

When you upgrade to PolicyView 3.0, user authentication configuration in the LDAP database is preserved. No reconfiguration is required.

3.5.4 Upgrading SecureView-SA from OmniVista 2.3 or 2.4 to 3.0

When you upgrade to SecureView-SA 3.0, 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 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. 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.

#. Purchase a licensed OmniVista product. You will receive a License Card that contains a serial number.

#. Once you receive your License Card, log onto the Customer Support website at http://license.ind.alcatel.com. A screen requiring information from you displays.

#. Enter your name, company, phone number, email address, and serial number in the required fields. The email 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.

#. Select the product for which you want a key. The core set of OmniVista applications is called OmniVista 2500 BMU-3.0 or OmniVista 2500 BSU-3.0. BMU stands for Basic Multi-User and BSU stands for Basic Single User.

#. 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:

Product: OV20S
Registration Number: OV203233-1916
License Contact: License@ind.alcatel.com
License Key: xxxxxxxx-yyyyyyyy-zzzzzzzz-aaaaaaaa

#. Make a note of the License Key.

#. Under the OmniVista main **Help** menu, select **Licenses**.

#. Select **OV2500-CORE** and click **Relicense**.

#. 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.

3.7 Upgrading Licenses for Optional OmniVista Applications■

OmniVista is a suite of software applications. Some of these applications, such as PolicyView and SecureView, are purchased separately and require separate license keys. In configurations that include the OmniVista base application and one or more optional applications, you need to upgrade the licenses for add-on applications as described above in Section 3.6. However, select the add-on product you are upgrading in **Step 8** (e.g., OV2750-SV-SA).

4 Launching OmniVista■

When launching OmniVista Basic 2500 Multi-User, 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 Server 2003/Windows XP ■

For the OmniVista Basic **Multi-User** version, 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:

OVServer. There are two ways to launch a Client (or OmniVista Basic 2520 Single User) on Windows:

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

for **OmniVista Basic Multi-User**:

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

for **OmniVista Basic Single User**:

Select **Start** > **Programs** > **Alcatel OmniVista 2500 Single User** > **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 server does not run automatically and therefore must be launched manually after installation or a system restart.

You can make the OmniVista server a UNIX daemon that runs at boot time. 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 (or OmniVista Basic 2520 Single User) on Sun Solaris:
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.

Note that, after a standard installation on a Linux platform, the server does not run automatically and therefore must be launched manually after installation or a system restart.

You can make the OmniVista server a Linux daemon that runs at boot time. 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 (or OmniVista Basic 2520 Single User) on Linux:
At the command prompt, change to the directory in which you installed OmniVista, then enter: **./OmniVista**.

5 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 Server 2003/Windows XP■

5.2.1 Uninstalling OmniVista

For **OmniVista Basic Multi-User**:

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

For **OmniVista Basic Single User**:

> Select **Start** > **Programs** > **Alcatel OmniVista 2500 Single User** > **Uninstall OmniVista Basic**.

5.2.2 Uninstalling PolicyView

For **OmniVista Basic Multi-User**:

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

For **OmniVista Basic Single User**:

Select **Start** > **Programs** > **Alcatel OmniVista 2500 Single User** > **Uninstall PolicyView QoS**.

5.2.3 Uninstalling SecureView-SA

For **OmniVista Basic Multi-User**:

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

For **OmniVista Basic Single User**:

Select **Start** > **Programs** > **Alcatel OmniVista 2500 Single User** > **Uninstall SecureView SA**.

5.2.4 Uninstalling SecureView-ACL

For **OmniVista Basic Multi-User**:

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

For **OmniVista Basic Single User**:

Select **Start** > **Programs** > **Alcatel OmniVista 2500 Single User** > **Uninstall SecureView ACL**.

5.2.5 Uninstalling Quarantine Manager

For **OmniVista Basic Multi-User**:

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

For **OmniVista Basic Single User**:

Select **Start** > **Programs** > **Alcatel OmniVista 2500 Single User** > **Uninstall Quarantine Manager**.

5.3 ■Uninstalling on Sun Solaris

5.3.1 Uninstalling OmniVista

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

5.3.2 Uninstalling PolicyView

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

5.3.3 Uninstalling SecureView-SA

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

5.3.4 Uninstalling SecureView-ACL

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

5.3.5 Uninstalling Quarantine Manager

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

5.4 Uninstalling on Linux■

5.4.1 Uninstalling OmniVista

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

5.4.2 Uninstalling PolicyView

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

5.4.3 Uninstalling SecureView-SA

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

5.4.4 Uninstalling SecureView-ACL

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

5.4.5 Uninstalling Quarantine Manager

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

6 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: The maximum number of clients for Single Server is six (6).

6.1.1 Changing the Maximum Number of Traps Logged on the Server

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 MB 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 **Switches** tree node. Select the tree node for an individual switch to display traps for that switch. 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 Maintenance and Disk Usage

The Audit application displays and maintains log files that record the activity of various applications and users in the system. With the exception of the server.txt file, logs can be 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. Log files can also be manually archived or exported as a .txt file.

6.1.3.1 server.txt Disk Usage and Maintenance

The server.txt file does not require manual file maintenance. However, the Preferences application will not allow you to set the maximum log size for the server.txt file to anything over 10 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 2001 10:58:01 INFO  : ----------------------------------------------------------------------
15 Mar 2001 10:58:01 INFO  : Starting OmniVista Server 1.0GA (Build 122, 3/12/2001)
15 Mar 2001 10:58:01 INFO  :     Server Location: 10.255.12.163
15 Mar 2001 10:58:01 INFO  :     Server Port    : 1127
15 Mar 2001 10:58:01 INFO  : Starting Security Services...
15 Mar 2001 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

Possible 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.

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. Known Problems■

7.1 Known General Problems■

7.1.1 OmniVista Server Must Be Run As "ROOT"

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). So, the OmniVista server must be run on UNIX as root to receive traps properly.

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

PR# 38215

7.1.2 ESC Used in Progress Dialogs Does Not Select the Cancel Button in the Progress Dialog

Pressing "ESC" in Progress Dialogs does not select the Cancel button in the Progress Dialog.

Workaround: Use the Cancel button rather than pressing the ESC key.

PR# 66257

7.1.3 Audit Tables Only Autoscroll to Second to the Last Row

If you're viewing a log with the Audit application, and a new row gets added to the log, the table doesn't autoscroll so that the new row is visible. If another row gets added, the table autoscrolls down one row, but the last row is still hidden.

Workaround: Click on the scroll arrow to see the last entry in the list.

PR# 72113

7.1.4 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 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

7.1.5 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'd 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

7.1.6 Firmware Backups Performed Using Previous Versions of OmniVista Are Not Compatible After Upgrades to OmniVista 2.3

After a backup to OmniVista 2.3, firmware backups performed using previous versions of OmniVista are not compatible and cannot be seen/restored using OmniVista 2.3. However, these files are not erased and use extra disk space.

Workaround: As soon as the upgrade to OmniVista 2.3 is complete, backups of all switches deemed important must be performed. These new backup files will, of course, be fully compatible with OmniVista 2.3, allowing successful restore operations to be performed. Old files must be manually removed from [OmniVista Root Directory]/data/configadmin/snaphosts/

PR# 74984

7.1.7 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: If you want to change the server's maximum memory on Windows, you must modify the OVServer.lax file, run bin\regsync.exe, and finally restart the service. To change the server's maximum memory on other platforms, you must modify the RunOVServer.lax file and restart the server.

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

7.1.8 Upgrade OV2.0->OV2.3: Errors in Server Log From Scheduled "configadmin" Tasks

Upgrade OV2.0->OV2.3: Errors in server log from Scheduled "configadmin" tasks

Workaround: Delete all the entries from the data/configadmin directory and remove the configadmin directory before upgrading to 2.3.

PR# 76160

7.1.9 Installer Will Not Upgrade an Existing 2.0 or 2.1 "Single User" Version to 2.3

The installer will not upgrade an existing 2.0 or 2.1 "Single User" version to the 2.3. Even though the new 2.3 version being installed is a single-user version, it will say "Cannot install Client-only or Multi-user over an Existing Single-user installation".

Workaround: Uninstall the earlier version and install 2.3 Single-user into the same directory.

PR# 76233

7.1.10 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

7.1.11 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

7.1.12 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 1440m. The maximum memory allocation for a windows platform should be 1.4 GB, or "-Xmx1440m" when editing the command line.

> **Note:** For Windows installations, do not set the server memory higher than 1280 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 7.1.7.

PR# 91414

7.1.13 Firmware Cannot Be Backed Up When Backing Up OS-6100 Series Switches

When backing up OEM OmniStack 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

7.1.14 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

7.1.15 Alcatel Router 7750 and Fortigate Have "Unknown" Type in OmniVista

Fortigate devices that are discovered as third-party devices will display "unknown" in the "Type" column of the device table in the Topology application.

Workaround: Select the individual device display to show additional information about this device.

PR# 92305

7.1.16 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

7.1.17 GUI Temporarily Freezes When Receiving Traps if Max Display is Larger Than Max Stored

If your Max Display setting in the Notifications application is larger than the number of traps being stored on the server, the client GUI freezes up for a couple of seconds when new traps are received.

Workaround: If the Max Stored and Max Displayed are the same (e.g., both 30,000), the client does not have the freezup problem. You can also enable the "Show New Traps at Top" option on the Notifications Display screen in the Preferences application.

PR# 92310

7.1.18 Client GUI Freezes for Long Periods When Deleting Many Devices

When selecting a very large number of managed devices to delete at the same time, the client GUI will take a long time for the operation, and appear frozen during that time. For over a thousand switches, this can be many minutes.

Workaround: The simplest solution for now is to delete smaller numbers of switches at a time.

PR# 90358

7.1.19 Failures if Server IP Changed After Installation

The IP address of the PC is changed after the installation, the LDAP server would not start. After re-installing the basic package over the top of the first installation (same Build 28), the LDAP server starts, and OV Server starts, but there is this display problem in the Audit Application.

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. If you modified the IP address, you will probably want to modify the IP address of the OpenLDAP server.
4. Restart the OpenLDAP server and the OmniVista Server.

PR# 92921

7.1.20 "Out Of Memory" Problem After Stopping syslogd on Some UNIX Configurations

On UNIX, if a user terminates the native syslog daemon to allow the OV Syslog Listener to use port 514, some configurations may encounter “Out of Memory” problems. In some UNIX configurations, there's a background process called minilogd that detects that the native syslog daemon is not running, and buffers all of the incoming syslog messages in memory until the syslog daemon starts up again. Since the native syslog daemon does not start again, minilogd keeps using more and more RAM until the system eventually runs out of memory.

Workaround: If a user manually kills the syslogd process, or configures it to not start up, the user must also kill the minilogd process. If not, the minilogd process will cache all incoming syslog messages in memory, and eventually use up all of the available memory.

PR# 97852

7.1.21 OV 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

7.1.22 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

7.1.23 Client Received OutOfMemory Error Messages

Setting the number of lines in the Audit Log File to a very large number can cause the client or server to run out of memory.

Workaround: Customers with more than 1,000 switches running OmniVista Server on Windows should probably not increase the default "Maximum Audit Entries" much past the 2,000-line default. Customers running Linux and 32-bit Solaris machines that have at least 2GB of memory should be able to increase this number to 4,000 lines without trouble.

Note that there is no memory penalty for setting the "Maximum Audit File Copies" to a large number. This only increases the amount of disk space consumed, to store the additional rolled-out log files, which are still available for viewing in Audit View. This can be a good workaround to make a longer audit trail available on machines with limited memory.

PR# 99142

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 Statistics Does Not Limit the Size of the Profile

Statistics does not limit the size of the profile.

Workaround: The maximum recommended load times for different profile parameters are shown below. These guidelines are for machines running the Statistics application only. If additional applications are running, the recommended memory requirements increase.

- 1 variable * 1 day = 1.09 MB
- 1 variable * 10 days = 10.92 MB
- 1 variable * 30 days = 32.75 MB
- 10 variables * 1 day = 10.92 MB
- 10 variables * 10 days = 109.19 MB
- 10 variables * 30 days = 327.23 MB
- 100 variables * 1 day = 109.18 MB
- 100 variables * 10 days = 1,091.77 GB
- 100 variables * 30 days = 3,275.30 GB

Remember that this table is normalized to a single series profile. For example: with 2024 MB setting, a client should not load more than of 1760 days of a profile with a single series @ 25 sec poll rate. If there are 5 series in the profile, one should load no more than 1760/5= 352 days

PR# 82830

7.2.4 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.

- 1 variable * 1 day = 1.09 MB
- 1 variable * 10 days = 10.92 MB
- 1 variable * 30 days = 32.75 MB
- 10 variables * 1 day = 10.92 MB
- 10 variables * 10 days = 109.19 MB
- 10 variables * 30 days = 327.23 MB
- 100 variables * 1 day = 109.18 MB
- 100 variables * 10 days = 1,091.77 GB
- 100 variables * 30 days = 3,275.30 GB

Note: Discovery List Items also use memory.

Workaround: The following is a breakdown of how much extra memory is required to open a statistics profile, based 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

7.3 Known Topology Problems■

7.3.1 AMAP links for 6148/6124 Stack to 6300-24 Do Not Show Up in Topology Map

AMAP links for 6148/6124 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 Client/Server Out of Memory Rearranging a Large Number of Switch Icons on Topology Map

The topology GUI application may run out of memory if too many switches are included in a single topology map.

Workaround: Limit the number of switches on a single topology map to 600 or less.

PR#s 91020, 91837

7.3.3 Arranging a Hub of Switches as Networked Does Not Work The First Time

If group of devices are connected and their initial placement is in same straight line horizontally or Vertically, then using the "Arrange Icon" Networked doesn't work.

Workaround: This initial alignment is possible only for very small networks but if it happens using the "Arrange Icon" Circular before using the "Arrange Icon" Networked will resolve the problem.

PR# 86618

7.3.4 Cannot Edit Manual Links Slot/Port Fields

When editing manual links using the Topology application, only the LAG fields are open for Edit.

Workaround: Remove the link and add it again, specifying the slot/port fields.

PR# 91573

7.3.5 Toolbar in Topology Physical Map Refers to Mobility Drop-Down from VLANs

When a device is selected in the VLANs application and one of its children nodes is selected ('Mobility)', if the user switches to another application and the information pertaining to this device is refreshed, the navigation drop-down at the top of OmniVista's screen will be mistakenly refreshed to display the currently selected VLAN node.

Workaround: To avoid this behavior, make sure that no tree node under a switch node is selected in VLANs when using another OmniVista application.

PR# 98497

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.

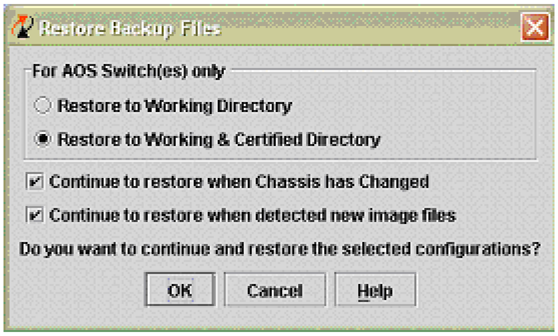
PR# 86393

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 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 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.



For AOS Switch(es) only

○ Restore to Working Directory

● Restore to Working & Certified Directory

☑ Continue to restore when Chassis has Changed

☑ Continue to restore when detected new image files

Do you want to continue and restore the selected configurations?

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 Cannot View or Modify Scheduled Backup Settings

Cannot view or modify scheduled backup settings.

Workaround: The user can view, modify, or delete the backup settings using the Schedule application. There is no way to change the backup settings after the backup has been scheduled. The workaround is to delete the backup schedule using the Schedule application and then reschedule it.

PR# 75215

7.5 Known Locator Problems■

7.5.1 Wrong Slot/Port Datatype When Exporting Search Results for Locator Browser

Wrong Slot/Port datatype when exporting Search Results for Locator Browser.

Workaround: This is an Excel limitation. currently, the only workaround available is:
1. Rename the file (change the .csv extension to .txt.
2. Open the file in Excel. Excel prompts the user for column delimiters and types.
3. Select the type "text."

PR# 82735

7.5.2 Live Search with Big Discovery List Can Fill up Polling.log and All 10 Copies with Meaningless Information

If you have a large discovery list, and you perform a Live Search in Locator that doesn't stop on the first match, tens of thousands of meaningless "Frequent poll started" and "Frequent poll finished" messages get written to the polling.log.

Workaround: None

PR# 91855

7.5.3 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

7.5.4 Cannot Restart Locator Browse After It's Been Canceled

If a Locator Browse function is canceled by selecting the Search tab while the browse is underway and clicking the Cancel button, the browse function cannot be properly restarted.

Workaround: If a Locator Browse must be canceled in this manner, closing and reloading the Locator application will re-enable the browse function.

PR# 100093

7.5.5 Locator Browse Results Table Shows Previous Results Until New Search Is Complete

Locator browse results panel may show previous results until the current browse has been completed.

Workaround: Wait for the current browse operation to complete, and the old data will be replaced.

PR# 99837

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

7.7 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 SNMPv3 Not Working for 6300-24 - Chassis Information Table SNMPv3 Get Request Timeout

When the 6300-24 is configured to use snmpv2 or snmpv3 with OmniVista, the default settings for the getbulk option will not work well. Most snmp requests will time out and produce errors.

Workaround: When selecting the "getbulk" snmpv2/snmpv3 option for the 6300-24, set the "max repetitions" value to 2 instead of the default of 10. If problems persist, turn off the getbulk option.

PR# 86489

7.7.6 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: None.

PR# 91804

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

On Unix platforms, the OmniVista 3.0 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

7.7.8 Trap Table is Much Slower with Replayed Traps

Notifications application may be unresponsive for 15-second periods while updating displays of large numbers of traps..

Workaround: If this is a problem on your system, consider going to the "Notifications Displayed" panel under "Preferences", and selecting "Show new traps at top". This can make the application much more responsive.

PR# 99731

7.7.9 Traps Sent to Clients Fall Behind When the Server Rewrites the Trap Cache File

A busy OmniVista server, with a large number of traps saved on the server, can occasionally delay delivering new trap notifications to clients. The delay can be as great as several minutes.

Workaround: During the busy time, while traps are not being delivered to clients, traps are still being received by the OmniVista server, and when ultimately posted to clients, are displayed with the correct original date/time stamps.

PR# 99905

7.7.10 OV 3.0 Notifications Are Purged on "Oldest Received" but Displayed in "Adjusted Time" Order

Traps do not expire from the OmniVista client and the OmniVista server in the same way. When OmniVista receives more traps than it has been configured to retain, the traps are expired. Traps expire from the OmniVista server in the order that they were received, while they expire from the OmniVista client by oldest date/time. These are usually the same, or nearly the same, but not always (especially because of Trap Replay). In both cases, however, it is very nearly the oldest trap that is expired.

Workaround: None.

PR# 99204

7.7.11 The Trap Replay Feature Has the Wrong Default Setting in OmniVista 3.0 GA

Trap Replay is documented as being enabled by default. However, in OmniVista 3.0 GA, it is actually disabled by default.

Workaround: The setting can be configured via the Preferences application in the OmniVista client, in the System-Wide Notifications preference panel, by selecting the Trap Replay Polling checkbox..

PR# 100228

7.7.12 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 o3 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

7.7.13 Deleted Traps Are Not Removed from Paused Trap Table

If traps are deleted while the trap display is in "paused" mode, the traps will not be deleted until the trap display is "resumed".

Workaround: Resume the trap display and the traps will be deleted.

PR# 99551

7.7.14 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

7.8 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 recache policies using PolicyView. This will ensure the correct LDAP server entry is written to the device so that it may recache 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.
- Disable the firewall

PR# 85026

7.8.5 Source MAC Address Radio Option for MAC Groups May Not Show up Until Window is Expanded on Linux

On Linux, when running SecureView ACL or PolicyView, when the "L2 MACs" screen is displayed, the "Source MAC Addresses Group" option is not displayed.

Workaround: Resize the application window until the option group has enough room to be displayed.

PR# 98755

7.9 Known SecureView-SA Problems■

7.9.1 User Should Not Be Allowed to Modify Bundled Open LDAP Credentials from SecureView

SecureView-SA allows the user to modify the LDAP server setting it expects the switches to use. If the user does this, without actually changing the OpenLDAP servers' configuration, then the switches will fail to authenticate with the target LDAP server and therefore will not be able to read their security information.

Workaround: When a password change is required for the OpenLDAP server, the user must modify the following to ensure all parts of the system will be in sync and can continue to communicate: alcatel.conf, NetscLdapConfig.xml
- alcatel.conf: change the 'rootpw' value to the new one of the users choice; this file is found within <OmniVista root directory>/openldap
- NetscLdapConfig.xml: change the 'rootDNpw' value to the same value as used in alcatel.conf above; this file is found within <OmniVista root directory>/classes/com/alcatel/ov1/ldap/server/resource

After modification of the previously mentioned files, the user will have to take the following action:
- restart the OpenLDAP server
- restart the OmniVista server

PR# 86923

7.9.2 aaas Retries Can Only Be Set from 0 - 5 Documentation says 0 - 32

aaasRetries can only be set from 0 - 5 documentation says 0 - 32.

Workaround: The firmware to the switch must be update (5.1.6.197) or the user may receive an error if the retries is set to greater than 5.

PR# 88567

7.9.3 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

7.11 Known VLAN Problems■

7.11.1 Spanning Tree Status Changes Fail for OEM OmniStack 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

7.12 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 when using FTP. For larger backups local file system should be used.

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

8. Problems Fixed Since 2.4.2■

8.1 Combination of Spacebar and Enter Keys Automatically Logs Off AOS Telnet Sessions (PR 86252)

8.2 SSH Scripting Hangs for Switches Discovered via EMP Port (PR 91315)

8.3 No Canned Scripts for OV Admin Users Other Than Default (Admin, Switch) (PR 88887)

8.4 "Show Traps State In Switch..." is a Per-User Preference, Not System-Wide (PR 80956)

8.5 Loading from Certified Directory and Rebooting the Entire Switch Causes OmniSwitch 9000 to Fail (PR 96347)

8.6 Discovery Loses its Progress Reporting After Being Canceled and Restarted (PR 91788)

8.7 If Recurrence Time Equal or Exceeds 4 Weeks, Then Scheduled Profile Will Not Start Again (PR 85096)

8.8 SwitchManager not Working with OmniStack 63xx (PR 78593)

8.9 For Upgrade Installs, Fields Should be Pre-Filled with Existing Settings, Rather than Default Values (PR 91805)

8.10 Cryptic Error Message Return When Trying to Set a Rule for 127.0.0.0/8 (PR 88831)

8.11 Cryptic Error Message When Setting a Rule for Host 155.14.12.1/255.255.255.255 (PR 88832)

8.12 QM Should Replace Existing MAC Rule So it Can Create a New MAC Rule in Quarantined VLAN (PR 93110)

8.13 QM Should Replace Existing DHCP MAC Rule So it Can Create a New DHCP MAC Rule in Quarantined VLAN (PR 93111)

8.14 After Notifying a AOS Switch to Load New Policy, the Status Panel Displays Inappropriate Error Message (PR 80468)

8.15 For Invalid SMTP Server, the server.txt Error Should Name the Invalid Server Rather Than 'Mailhost' (PR 92156)

8.16 OV Server Does Not Shutdown Gracefully When Solaris Box is Rebooted (PR 91710)

8.17 Setting OV Server's -Xmx Setting to the Maximum When Installing in 32-bit Environments Can Cause "OutofMemory" Errors (PR 96104)

8.18 Vertical Scrollbar Does Not Track for Extremely Large Data Values (PR 75433)

8.19 Unsaved Changes to a Map Are Lost If Additional Changes Are Made By Another and Saved at the Same Time (PR 75257)

8.20 OmniVista Topology Switch Connection is Lost When a Redundant Link Goes Down (PR 91182)

8.21 Topology Links Do Not Show for the 6124 Release 3.40.31 (W 97464) (PR 97307)

8.22 Locator Does Not Display the Correct VLAN ID for a Corresponding MAC Address (PR 94010)

8.23 OmniVista Trap Configuration is Not Available for the OmniStack 6024, 6124, 6148, and 8008 (PR 69126)

8.24 Exceeding Maximum LDAP Server Entries on Switch Produces "general failure" or "not writeable" SNMP Error (PR 61920)

8.25 PolicyView Unable to Launch Due to Port Conflict (PR 96800)

8.26 aaas Retries Can Only Be Set from 0 - 5 Documentation says 0 - 32 (PR 88567)

8.27 QM Configures max 32 MAC Rules When Trying to Ban 100 IP Addresses on XOS Devices (PR 92098)

9. Problems Fixed Since 2.4.1■

9.1 Combination of Spacebar and Enter Keys Automatically Logs Off AOS Telnet Sessions (PR 86252)

9.2 SSH Scripting Hangs for Switches Discovered via EMP Port (PR 91315)

9.3 No Canned Scripts for OV Admin Users Other Than Default (Admin, Switch) (PR 88887)

9.4 Telnet logs-Out User With Up-Arrow for AOS Switches (PR 92083)

9.5 'ls' <ent> Key Combination in Telnet AOS Sometimes Causes Session to Disconnect (PR 91473)

10. Problems Fixed Since 2.4.0■

10.1	**Filtering Not Allowed On All Columns Displayed in the "All Discovered Devices" Table in Topology View (PR 70450)**
10.2	**Background Image Listbox is not Updated when Image is Imported from Remote Client (PR 83828)**
10.3	**All Discovered Devices Table Shows Microcode Loaded not Microcode Working (PR 845200)**
10.4	**Resource Manager Backup File Disappears After Upgrading from OV2.2.5 to OV2.3 for Solaris 2.9 Only (PR 86452)**
10.5	**Add Item Dialog Takes Almost 4 Minutes to Come Up with 2,000 Switches (PR 86573)**
10.6	**Y-Axis Max is Miscalculated When Different Variables Have Different Scale Multipliers (PR 87201)**
10.7	**OmniVista Creating a IP VLAN with Switch Running 5.1.6 Code Fails (PR 88364)**
10.8	**OutOfMemory on Server Receiving and/or Replaying Traps (PR 88483)**
10.9	**OV 2.3 shows AOS devices as unsaved after taking backup (W88640) (PR 88589)**
10.10	**After switch reboot, new traps get inserted after oldest available seq # instead of current seq # (PR 88676)**
10.11	**OV2.4 client times out with an "Error processing Discovery Events" message (PR 88761)**
10.12	**SSH gets stuck in double-strike mode frequently (PR 88943)**
10.13	**OmniVista inventory says product description not available for GSX-K-FM-2W/K3 module (PR 89258)**
10.14	**Discovery Wizard menu item is disabled for Writer and Read-Only users (PR 89287)**
10.15	**Closing Statistics with unsaved profile gives NullPointerException (PR 89360)**
10.16	**Launching Mib browser generates error after importing new MIBs (PR 89385)**
10.17	**Inventory from OmniVista changes the switch status to UNSAVED (W88649) (PR 89528)**
10.18	**OmniVista server outofmemory with 2.4 release during discovery (PR 90228)**
10.19	**OV exported statistics data not having slot and port information (PR 90278)**
10.20	**Server won't run as a service anymore after regsync (PR 90844)**

11. Problems Fixed Since 2.3.0■

11.1	**When subnets overlap, traps display in both subnets (PR 81239)**
11.2	**OmniSwitch 6800, 6600 stack 2nd CMM not showing in Chassis Table on General Tab, Topology app (PR 86825)**
11.3	**OmniVista SNMPv3 setting does not work after a takeover on a stack of two 6600s (PR 87406)**
11.4	**OpenLDAP server as installed allows anonymous binds (PR 87649)**
11.5	**SNMPv3 Discovery of non-existent switches breaks OV polling of existing SNMPv3 switches (PR 87651)**
11.6	**OV 2.3 not displaying SNMP v1 Traps (PR 88877)**
11.7	**Source IP of one switch is being replaced with other switch's IP during trap display on OmniVista (PR 89482)**

12. Problems Fixed Since 2.2.5■

12.1	**CLI Warning Sent When the Number of Protocol Rules Exceeds Its Limits on OS7700/7800 and OS8800 (PR 68605)**
12.2	**The "Context Name" and "Context ID" Fields in the SNMP Settings Dialog Cannot be Used for Alcatel AOS Switches (PR 70692)**
12.3	**Displaying Large Data Values on Chart May Get Corrupted When Changing the Horizontal Scale Value From Minutes to Hours (PR 74389)**
12.4	**"Delete Previous Links" Check Box in the Discovery Wizard Has No Effect on the Links Discovered (PR 74497)**
12.5	**Right-Click Menu Stays On the Screen Until Save Process Has Completed (PR 74826)**
12.6	**User Not Instructed to Manually Reboot AOS Switches After Restore/Install (PR 74891)**
12.7	**Links Do Not Immediately Change to Green When the Switch Comes Online After Going Down (PR 75187)**
12.8	**Configuring Traps Will Fail For AOS Devices If Telnet/FTP Username Specified in OmniVista Does Not Have SNMP Access (PR 75238)**
12.9	**Using the "Profile Manager" Dialog When Renaming a Profile May Cause Some Profiles to Stop Collecting New Data (PR 75378)**
12.11	**"Time Zone Not Found" box comes up after opening the backup window (PR 79757)**
12.12	**OmniVista does not Discover OmniAccess 4012/4024/4102 device unless it is enabled for snmpv1 (PR 79764)**
12.13	**Server is having out of memory problem (PR 82369)**
12.14	**Out of Memory Error in OmniVista Statistics Client (PR 83839)**

13. Problems Fixed Since 2.2.4■

13.1	**OmniVista client crash with Polling service on (PR 84505)**

14. Problems Fixed Since 2.2.3■

14.1	**Client PC locks up during importing notifications, etc. (PR 82710)**

15. Problems Fixed Since 2.2.2■

15.1	**After installing OmniVista 2.2 the client PC gets locks-up for almost 5 minutes during the polling (PR 77198)**

15.2	**OmniVista 2.2 can not discover more than 600 switches (PR 81220)**

15.3	**Topology "Switches" table sorts "Type" extremely slowly, especially over laggy client-server link (PR 81854)**

15.4 OmniVista 2.2.3 uses a new API. Show a dialog at login time if the client ver. <> server ver (PR 81855)

15.5 Tried to change write community on 1765 switches and got errors. Server finally shutdown (PR 81963)

15.6 The upgrade installer doesn't find previous copy of OmniVista 2.2 on a PC with a German Windows (PR 79913)

16. Problems Fixed Since 2.2.1■

16.1 Cannot add 802.1Q port numbers >32 to VLANs on OmniSwitch 6600 using OmniVista

16.2 Physical port statistics of 66xx switches gives "Error decoding XML file for Category Tree: null"

16.3 After enabling the FTP banner the backup configuration feature doesn't work from OmniVista

16.4 Symbol not removed in OV Wizard Checkbox (PR 79667)

16.5 Port Operational State for 6300-24 shows as '7' instead of LowerLayerDown for Interfaces Table (PR 79714)

16.6 Select backup configuration and click X from the warning window and the backup starts (PR 79728)

16.7 Select X from the main backup window and from the exit wizard window select no (PR 79729)

16.8 Deleting entries from the backup. Select X from the delete backup warning window (PR 79728)

16.9 Client Only Install: installer displays warning message on the last screen (PR 79788)

16.10 After deleting a imported file it leaves a file detail in the lower upgrade image window (PR 79805)

16.11 OmniVista drop down view, task. Click on a running task and click end task (PR 79809)

16.12 Missing 'Type' information in All Discovered Devices Table for OmniAccess 4012/4024/4102 - sysDescr (PR 79833)

16.13 MIB browser loads AOS MIBs when pointed to a new mib directory (PR 79876)

16.14 MIBs imported into a standard directory do not show up in mib browser (PR 79901)

16.15 Install images upgrade images window. Click X and you get a install image message in the lower box (PR 79943)

16.16 OmniVista doesn't realize that OmniStack 6xxx V3.30.05 supports AMAP (PR 80099)

17. Problems Fixed Since 2.2.0■

17.1 Reverse DNS lookup causes client running Control Panel to temporarily freeze up (PR 76231)

17.2 Canceling a multiple-switch restore only cancels one switch (PR 76258)

17.3 Resource Manager slow, issues many discovery client requests if backup row is selected when polling occurs (PR 76239)

17.4 "Completed Reading Backup Files" message displays before table finishes displaying (PR 76244)

17.5 All rows not removed from Backup/Restore table when deleting multiple backups (PR 76269)

17.6 Memory leak switching tabs in Resource Manager (PR 76243)

17.7 Resource Manager unable to backup an XOS switch (PR 76556)

17.8 Client is not notified if OEM OmniStack Restore (or Install) exceeds retransmit limit (PR 76314)

17.9 Expert Mode: MAC wildcards not written to LDAP as colon separated value - Policy Manager rejects (PR 76610)

17.10 Server can run out of memory if it can't send Discovery Events to Logged-In Client (PR 76840)

17.11 Reload from OmniVista 2.2 of a 6600 does not work (PR 76811)

17.12 Topology takes a long time to load when the discovery list has many switches (PR 77241)

17.13 Ports OmniStack tab calls up the XOS tab help instead of OmniStack tab help

17.14 Click on OS device to display VLAN definitions, then Help and wrong help file displays

17.15 OS Ports dot1qPortVlan table help displays Mobility help file

18. Problems Fixed in PolicyView■

18.1 PolicyView OneTouch Voice Sets Both Layer2 and Layer3 Policies in the Switch(es) (PR 69198)

18.2 PolicyView OneTouch Data Will Not Be Applied Unless Classify Layer3 Bridge is Enabled (PR 69199)

18.3 Protocol TCP/UDP Ports Cannot be Modified or Deleted (PRs 57684, 61223)

18.4 Intermittent LDAP Access (SNMP Timeout) Errors If You Install, Uninstall, and Then Reinstall (PR# 61141)

18.5 One Touch Policy Actions for XOS 4.5 or Less Cannot Contain 802.1p Priority (PR# 61629)

18.6 Environment Unstable After PolicyView Install is Updated (PR# 61918)

18.7 LDAP Database May Be Left with Unused Roles (PR# 65052)

18.8 In Expert Mode, A Canceled Policy Still Shows Up in the "Switches Pending Notification" Screen (PR# 75592)

18.9 Additional LDAP Server Set-Up is Required When Upgrading to PolicyView or SecureView-SA 2.2 (PR# 76285)

18.10 Changing Computer Name Fails PolicyView to Launch (PR# 86923)