# **Getting Started with Notifications**

The Notifications application is used to monitor switch activity and configure trap management tasks, including:

- Monitoring switch activity through the Trap Notifications Table.
- Handling basic Trap Management tasks, such as changing the maximum number of notifications displayed on the client, clearing entries from the Trap Notifications table, acknowledging a trap, exporting traps, etc.
- Configuring Automatic Trap Responders. OmniVista can be configured to send an e-mail or run an external process on the OmniVista server when a specified trap is received. The trap can be specified by severity level or through the use of filters.

	OmniVista 2500 - Application	n: Notifications Window:	0		
	File Applications View Help	1			
	Construction of the Local Social Soci				
		🙆 😪 💕 All	<b>•</b>	<b>a</b>	
	Notifications	Variation Variation			
	- B Responders	Notifications Switc	hes		
	- Trap Definition			TILLER	
	P SAI	Notifications for All Sw			
	• F (10.0.0.0/8)	Name warmStart	Synopsis Warm start		
	10.255.10.3	systemEvent5	Potentially fatal error occurred. Trap: 2	<b>-</b>	
	- 10.255.11.102	tempAlarm5	Temperature exceeded the threshold		-
	- 😥 10.255.11.118	moduleChange5	Module invalid inserted or removed from slot 3 subunit hsm1	_	Trap
	- 10.255.11.119	macDuplicatePort5	VLAN source port changed from 00 00 5e 00 01 02		Notification
	10.255.11.120	tempAlarm5	Temperature exceeded the threshold		Table
	10.255.11.129	moduleChange5	Module invalid inserted or removed from slot 3 subunit hsm1	-	
Notifications	10.255.11.131	powerEvent5	Power Supply 1: notPresent. Power Supply 2: 89	-	
Tree	► 10.255.11.152	1	I contraction of the second seco	• •	
	- 10.255.11.153				
	10.255.11.157	Synopsis:	Potentially fatal error occurred. Trap: 2		
	- 10.255.11.198	Description:	A systemEvent trap occurs when a potentially		
	10.255.11.201				Trap
	- 😥 10.255.11.202		fatal system error occurrs. Such as: out of FLASH/		
	- 10.255.11.207		memory space. The event type is in the var bind.		Description
			A Descriptive string MAY be present. The following		Pane
	10.255.11.225		trap numbers are defined (see xylan-trapc.mib):		
	10.255.11.227				
	10.255.11.220		10 Unspecified log event		
	10.255.11.231		11 For file full	w	
	10.255.11.240	1		•	
	- 10.255.11.251		1,000 Change Max Clear Help		
	- 10.255.11.252		1,000 Change Max Clear Help		
	10.255.11.253				
	A.T.			100000000000000	

### The Notifications Application

# **Notifications Tree**

Use the Notifications tree to navigate through the application and find the appropriate window to work from. The Notifications application has three main windows:

• Click the **Responders** icon to display the Automatic Trap Responder window. This window is used to configure the response (if any) that you want OmniVista to take when a specified trap is received on the OmniVista server. The trap can be specified by severity level or through the use of filters. The response can take the form of an e-mail sent to a user-specified address and/or the execution of an external program or script on the OmniVista server.

- Click the **Trap Definition** icon to display the Trap Definitions window. This window displays a list of all supported traps, as defined in the MIBs. It gives a brief description of each trap and allows you to edit a trap's severity level and trap synopsis if desired.
- Click the **All** icon to display the Trap Notifications window displaying the Notifications tab and the Switches tab. The Trap Notifications tab displays a list of traps received from switches that are visible to the logged-in user. The list can be configured to display notifications for a single switch, or for all switches. To learn how to configure switches to send traps, see the Configure Traps Help. The Switches tab displays a list of all the discovered switches in a tabular form.

# **Using Pop-Up Menus**

Pop-up menus are used to perform functions within the Notification application (e.g., configure traps, acknowledge traps). Pop-up menus are available in the Notifications Tree and in the Trap Notifications Table.

**Note**: You can manually poll an individual switch by right-clicking the switch in the Notifications tree or the Notifications table and selecting **Poll for Traps** from the pop-up menu. The switch will immediately be polled for traps. See the Topology application Help for a description of each pop-up menu item.

### **Notifications Tree Pop-Up Menu**

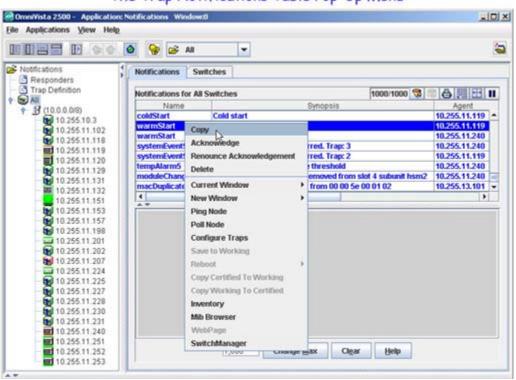
Right-click any switch in the Notifications tree to display the pop-up menu, shown below. Different menu items display on the pop-up menu for AOS switches, XOS switches, and thirdparty switches. Refer to the Topology application Help for information on individual pop-up menu commands.

OmniVista 2500 - Application File Applications View Hell		Window:0		
Elle Applications View Hel		🗧 All 💌		<b>a</b>
Notifications  Responders  Trap Definition  Solution  Trap 10.0.0.08)	Name	for All Switches	1000/100 Synopsis	Agent Agent I
In 255 1n 2     In 245 1n 2	ps ing i To Working	Temperature exec Device Status Locate on Map Health SSH Statistics Locate End-Stations Backup Configuration	eded the threshold ted or removed from slot 3 subunit hsm1 Present. Power Supply 2: 89 port 2 12 due to invalid ID or password Spanning Tree root hanged from 00 00 5e 00 01 02	10.255.11.119 no-nam 10.255.11.119 no-nam 10.255.11.119 no-nam 10.255.11.119 no-nam 10.255.11.119 no-nam 10.255.11.119 no-nam 10.255.11.119 no-nam 10.255.11.119 no-nam 10.255.13.101 UNKNO ▼

### The Notifications Tree Pop-Up Menu

# Trap Notifications Table Pop-Up Menu

Right-click any notification (or group of notifications) to display the pop-up menu, shown below. Different menu items are displayed in the pop-up menu for AOS switches, XOS switches, and third-party switches. The **Copy**, **Acknowledge**, **Renounce Acknowledgement**, and **Delete** menu items are used to manage traps.



### The Trap Notifications Table Pop-Up Menu

# The Trap Definition Window

The Trap Definition window displays a list of all the supported traps, as defined in the MIBs. Use the Trap Definitions window to:

- View detailed information about individual traps
- Edit a trap's Synopsis and Severity fields
- Reset trap Synopsis and Severity fields to the installation defaults.

To access the Trap Definitions pane, click **Trap Definition** in the Notifications tree. You can also select **Trap Definition** from the drop-down list at the top of the window.

### The Trap Definition Window

			m 🔻				0	
	Notifications	ions List				1369/1369	3 - A II II	
to open window. 🗕 🖬	Trap Definition	Name	Severity	6	Syno		Definition	
9 8	All alaDoSTrat				and the second	oS Type: \$1, Number	Default 🔺	
		alTrapAbsorbed			d \$1 trap \$5 tim		Default =	Trap
		TrapAbsorbed			d \$1 trap \$5 tim		Default	Definitions
		TrapAbsorbed		1	d \$1 trap \$5 tim		Default	1 C C C C C C C C C C C C C C C C C C C
		alTrapAbsorbed			d \$1 trap \$5 tim		Default	List
		ngTrapAbsorbed		a state that at a second state	d \$1 trap \$5 tim		Default	
		rBadMixTrap	Normal	The elem	nent identified t	iy slot \$1 will enter p	Default 👻	
	10.255.11.129							
	10.255.11.131 View Trap	Definition						
	10.255.11.132	Details						
	10.255.11.153 Name:	alaOvCriticalTra	apAbsorbed		Oid:	1.3.6.1.4.1.6486.800.	1.3.2.19.1.1.2.0.5	
	Generic Id	: 0			Specific ld:	0		l and the second
	- 10.255.11.201 Severity:	Crincal :						View/Edit
	10.255.11.202							Pane
	10.255.11.207 10.255.11.224 Suppose	Absorbed \$1 tra	ap \$5 times: \$4					Stration.
	10.255.11.224 Synopsis	:						8
	10.255.11.227							
	10.255.11.228							
	10.255.11.230							
	10.255.11.231							
	10.255.11.240							
	10.255.11.251							

The Trap Definition pane includes two sections: the Trap Definitions List and the View/Edit Pane.

### Viewing a Trap Definition

Use the scroll bar in the **Trap Definitions List** table to glance through all of the traps. If you only want to see a certain group of traps (e.g., all ATM traps, or all traps with severity level "warning"), you can do so by creating and applying a filter. For details on how to do this, see the Filter Help, which is available when you click on the Filter icon at the top of the Trap Definitions List.

To view information about a single trap, select the trap in the **Trap Definitions List** table, then view the information in the View/Edit pane. The View/Edit pane consists of two tabs, the Trap Info tab and the Details tab.

### Trap Info Tab

The **Trap Info** tab displays the trap definition fields.

Name. Name of the trap, as defined in the MIB.

**Generic ID.** Generic trap ID number. Only SNMPv1 traps make use of a generic ID. For SNMPv2 and SNMPv3 traps, this field will show a value of zero.

**Severity.** Severity level assigned to the trap as defined in the Notifications Application's Trap Definitions window. Possible values are: Normal, Warning, Minor, Major, and Critical. If desired, you can edit the Severity Level.

**OID.** Trap object identifier number.

**Specific ID.** Trap specific ID number. Only SNMPv1 traps make use of a specific ID. For SNMPv2 and SNMPv3 traps, this field will show a value of zero.

**Synopsis.** Text description of the trap. Note that certain traps have associated SNMP trap variables. If a trap synopsis includes a dollar sign symbol, this means that the trap has one or more associated variables. Right-click in the Synopsis field to see a drop-down list of the associated trap variables. The drop-down list is accessible whether you are viewing or editing a trap.

**Note**: If the **Synopsis** field of a trap displays a '?', it denotes that the trap received does not include all the variables as defined by the MIB. If this occurs, please refer to the trap details and the synopsis definition of the trap.

	<b>@</b>	Trap Definitio	n <b>-</b>					1
sponders	ap Definition	ns List				1369/1369	888	E
p Definition	N	ame	Severity		Sync	opsis	Definition	T
	aDoSTrap	a state and the second s	Normal	Detected	I DoS attack. D	loS Type: \$1, Number	Default	
(10.0.0.0/8) ala	rapAbsorbed	Critical	Absorbe	d \$1 trap \$5 tir	nes:\$4	Default	Ĩ	
		apAbsorbed	Major	Absorbed \$1 trap \$5 times: \$4			Default	
and the second se		apAbsorbed	Minor	and the second se	d \$1 trap \$5 tir		Default	
		TrapAbsorbed	Normal		d \$1 trap \$5 tir		Default	
		TrapAbsorbed	Warning	the local of the local design of the local des	d \$1 trap \$5 tir	and a standard with the second standard standard and a standard standards	Default	
	aStackMgrB		Normal	The elen	nent identified	by slot \$1 will enter p	Default	-
A TOTAL OF THE TAXABLE PROPERTY	*							0000
	New Trap D	efinition						
10.255.11.132	Trap Info	Details	Details					
10.255.11.153 N	lame:	alaOvCriticalTra	pAbsorbed		Old:	.1.3.6.1.4.1.6486.800.1	3.2.19.1.1.2.0	5
10.255.11.157 10.255.11.198 G	eneric ld:	0			Specific ld:	0		
a 10.255.11.201	everity:	Critical						
		Absorbed \$1 tra	in \$5 times: \$					Ê.
10.255.11.202			p + 0 01110 0. +		VTrapAbsorO	rightana		
10.255.11.207	And the second second			>1 ~ diau	ALL ON WHICH O	igranie .		
10.255.11.207	Synopsis:							
10.255.11.207 10.255.11.224	And the second second			\$2 = ala0	WTrapAbsorO	rigOID		
10.255.11.207 10.255.11.224 10.255.11.225	And the second second			\$2 = ala0 \$3 = ala0	wTrapAbsor0 wTrapAbsor0	rigOID 🗟 rigStamp		W.
10.255.11.207     10.255.11.224     10.255.11.224     10.255.11.225     10.255.11.227     10.255.11.228     10.255.11.228     10.255.11.230	And the second second			\$2 = ala0 \$3 = ala0	WTrapAbsorO	rigOID 🗟 rigStamp		14
10.255.11.207     10.255.11.224     10.255.11.225     10.255.11.225     10.255.11.228     10.255.11.228     10.255.11.230     10.255.11.231	And the second second			\$2 = ala0 \$3 = ala0 \$4 = ala0	≫TrapAbsorO ≫TrapAbsorO ≫TrapAbsorO	rigOID rigStamp rigSummary		145
10.255.11.207     10.255.11.224     10.255.11.225     10.255.11.225     10.255.11.228     10.255.11.228     10.255.11.230     10.255.11.231     10.255.11.240	And the second second			\$2 = ala0 \$3 = ala0 \$4 = ala0 \$5 = ala0	WTrapAbsorO WTrapAbsorO WTrapAbsorO WTrapAbsorC	rigOID rigStamp rigSummary ounter		
10.255.11.207     10.255.11.224     10.255.11.224     10.255.11.225     10.255.11.227     10.255.11.228     10.255.11.230     10.255.11.231     10.255.11.231     10.255.11.231     10.255.11.251	And the second second			\$2 = ala0 \$3 = ala0 \$4 = ala0 \$5 = ala0 \$6 = ala0	WTrapAbsorO WTrapAbsorO WTrapAbsorO WTrapAbsorC WTrapAbsorTi	rigOID rigStamp rigSummary ounter ime		
10.255.11.207     10.255.11.224     10.255.11.225     10.255.11.225     10.255.11.228     10.255.11.228     10.255.11.230     10.255.11.231     10.255.11.240	And the second	Ed	iit Upda	\$2 = ala0 \$3 = ala0 \$4 = ala0 \$5 = ala0 \$6 = ala0	WTrapAbsorO WTrapAbsorO WTrapAbsorO WTrapAbsorC WTrapAbsorTi	rigOID rigStamp rigSummary ounter		

a list of associated trap variables.

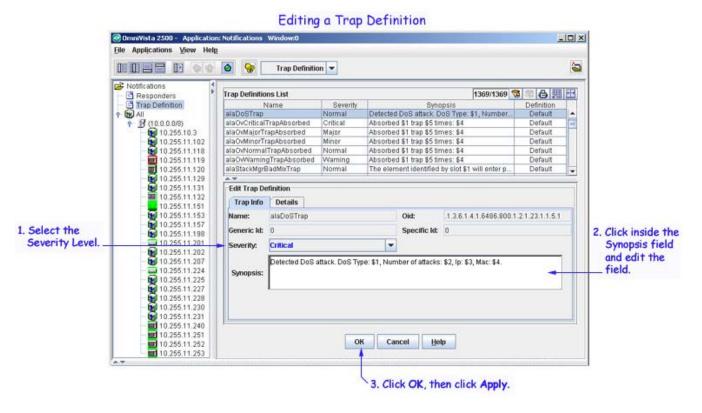
### **Details Tab**

The **Details** tab displays the description of the selected trap as defined in the MIB. It also displays the name and the description of the variables associated with that trap.

e Applications View Help				
	🙆 😧 Ti	ap Definition	1 <b>v</b>	
Notifications	Trap Definitions	List	1369/1369 🕱 🕾 🗛	
Trap Definition	Name	Sevenity	Synopsis	D
All	abortThode	Normal	ofitopolo	d
9-17 (10.0.0.0/8)	accountEvent	Normal	Accounting file, \$1, ready for collection, \$2 files are ready for collection	C
10.255.10.3	accountEvent13		Accounting file, \$1, ready for collection. \$2 files are ready for collection	10
10.255.11.102	accountEvent3	Normal	Accounting file, \$1, ready for collection. \$2 files are ready for collection	1
10.255.11.118	accountEvent5	Normal	Accounting file, \$1, ready for collection. \$2 files are ready for collection	10
- 10.255.11.119	4	4.0		11
10.255.11.120	A -			
10.255.11.129	View Trap Def	inition		
10.255.11.131	Trap Info	Details		
10.255.11.132	mapinio	Decails		
10.255.11.151	Description:	An account the switch	event is generated to signal that a new accounting file is available or	n
10.255.11.157		HIC SWITCH.		
10.255.11.198	chas Accou	utName	The fully qualified path name of the most recently terminated	
10.255.11.201			accounting file. This object is not intended to be accessed directly	
10.255.11.202			It is defined for use in accounting-related traps.	
10.255.11.224			The second of the second of the second of the	
10.255.11.225	chas Account	tFileCount	The number of terminated accounting files awaiting collection (an	d
10.255.11.227			removal) by an external accounting collection agent.	
10.255.11.228	1			
10.255.11.230				
10.255.11.231				
10.255.11.240				
10.255.11.251				
10.255.11.252		Edit	Update Reset Apply Help	
10.255.11.253		COR	Christer Reser Shink Lieth	

### **Editing a Trap Definition**

To edit a trap definition, select the trap in the **Trap Definitions List** table, then click **Edit**. The View/Edit pane changes from "View Trap Definition" to "Edit Trap Definition" and the editable fields become enabled. The only fields that are editable are Synopsis and Severity. To edit these fields you must have Administrative privileges (admin or netadmin).



For more information on editing the Synopsis and Severity fields.

# **Editing Trap Severity**

To change the severity level, select a severity level from the **Severity** drop-down list. Click the **OK** button to save the change, then click the **Apply** button to apply the changes to the server. You must have Administrative privileges to edit this field (admin or netadmin).

# **Editing a Trap Synopsis**

To edit the trap synopsis, click the Synopsis field. The value of SNMP variables contained in the trap can be displayed in the Synopsis. You can even perform simple mathematical calculations on a variable value and display the result in the Synopsis. Click the **OK** button to save the change, then click the **Apply** button to apply the changes to the server. You must have Administrative privileges to edit this field (admin or netadmin).

### **Displaying SNMP Variable Values in the Synopsis**

As previously mentioned, if a trap contains SNMP variables, a list of the variable names is displayed when you right-click the Synopsis field. The variable values for a given trap are always contained in the trap in the same order. This corresponds to the order of the variable names listed when you right-click in the Synopsis field. A variable value is referenced for display in the Synopsis by entering a dollar sign (\$) followed by the desired variable's sequence number, where one (1) is the first variable.

For example, assume an instance of the vlanChange trap (which has three SNMP variables) where:

for SNMP Variable Name:	the Sequence Number is:	the Variable Value is:
atVLANGroupId	\$1	5
atVLANId	\$2	9
atVLANAdminStatus	\$3	disabled

where the Synopsis field for this trap is:

VLAN \$2 group \$1 state changed to \$3

the Synopsis displayed for this instance of the trap in the Trap Notifications Table looks like this:

VLAN 9 group 5 state changed to disabled

### Performing Computations on SNMP Variable Values in the Synopsis

You can perform simple mathematical calculations on a variable value and display the result in the Synopsis field. The supported operations are:

Operator	Operation
*	multiplication
/	division
%	remainder
+	addition
_	subtraction

In addition, open and close parentheses can be used to change the standard Algebraic order of operations. A mathematical expression is entered in the Synopsis field enclosed by an open and a close curly brace, i.e., "{" and "}".

For example, for some Alcatel object IDs, the linkDown trap's ifIndex SNMP variable value is equal to the slot number times 1000, plus the port number. Assume an instance of this trap where ifIndex is equal to 5009 and the Synopsis field:

Link Down: slot {\$1/1000} port {\$1%1000}

the Synopsis displayed for this instance of the trap in Notifications List looks like this:

Link Down: slot 5 port 9

### When Does an Edited Synopsis Take Effect?

Changes made to Synopsis are effective immediately. Notifications logged on the OmniVista server are stored in raw data format. Each time the Notifications List is displayed, the traps are formatted for display using the current Synopsis. Therefore, if, for example, you edit the vlanChange trap Synopsis after vlanChange traps were logged on the server, they will be displayed using the new Synopsis format.

### **Resetting a Trap Definition to the Installation Default**

If you wish to reset one or more trap definition to the factory-installed defaults, select the trap(s) in the Trap Definitions List and click the **Reset** button. Then, click the **Apply** button to write the changes to the OmniVista server. Changes that you made to other trap definitions will remain in effect.

# The Trap Notifications Window

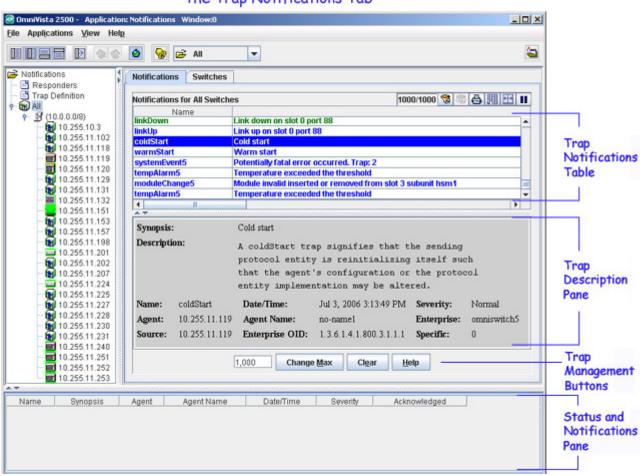
The Trap Notifications window consists of two tabs, **Notifications** and **Switches**. The Notifications tab displays alarms and traps (more generically referred to as "notifications"). The Switches tab displays a list of all the discovered switches with a trap count total for each switch.

### The Notifications Tab

In the Notifications tab, you can view notifications for all switches, switches in a subnet, or a single switch by selecting the option in the Notifications tree.

- To display notifications for all known switches, click **All** in the Notifications tree (as shown below).
- To display notifications for all switches in a subnet, click the subnet in the Notifications tree.

• To display notifications for an individual switch, click on the switch in the Notifications tree. OmniVista displays all traps received from any of the switch's valid IP addresses.



The Trap Notifications Tab

**Note:** If the Trap Notifications table is not displaying any notifications, it may be that none of your discovered switches have been configured to send traps to the OmniVista server. For information on how to configure switches to send traps to the server, see the Configure Traps Help.

The Trap Notifications window consists of four main areas:

- The **Trap Notifications Table** can display alarms and traps for a single switch, for all the switches in a selected subnet, or for all known switches. For more information, see Trap Notifications Table.
- The **Trap Description Pane** provides details about an individual alarm or trap that is selected in the Trap Notifications Table. For more information, see Trap Description Pane.
- The **Trap Management Buttons** give you access to basic trap management functions, such as changing the maximum number of notifications displayed on the client (**Change Max**), and deleting all entries from the notifications table (**Clear**).

• The **Status and Notifications Pane** can be displayed from any OmniVista application, making it possible to view notifications at any time, without having to return to the Notifications application. To view notifications from the Status and Notifications pane, click the **Notifications** tab at the bottom of the OmniVista window. The same information that displays through the Trap Notifications table also displays here. If the Status and Notifications pane is not currently displayed, click the **View** Menu and select **Status Panel**.

### Trap Notifications Table

The Trap Notifications table displays a list of the received alarms and traps. Each row in the table displays in the color that represents the trap's severity level. For example, in the illustration below, all rows display in blue, because blue is the color used to represent a trap with severity level "Normal." The columns headings and severity level color coding are described below.

**Note:** A new "Switch Down" trap was added for Release 3.3. The trap is generated by OmniVista when a switch status is changed to "down" because the switch stops responding to SNMP polling.

Notifications for Switch Kite		29/29 🔞 🔍	883	
Name	Synopsis	Agent	Agent Nan	ne
chassisTrapsAlert	fansOk All fans OK, Object: fan 0, Index: 65	10.255.11.59	Kite_59	
chassisTrapsAlert	psOperational Power supply is OK, Object: p	10.255.11.59	Kite_59	
chassisTrapsStateChange	ni 1 (index 1) state changed to down	10.255.11.59	Kite_59	
coldStart	Cold start	10.255.11.59	Kite_59	
chassisTrapsAlert	cmmStartupCompleted CMM startup compl	10.255.11.59	Kite_59	
chassisTrapsStateChange	ni 1 (index 1) state changed to down	10.255.11.59	Kite_59	
chassisTrapsStateChange	ni 1 (index 1) state changed to up	10.255.11.59	Kite_59	
stpNewRoot	New root for spanning tree 999	10.255.11.59	Kite_59	
stpNewRoot	New root for spanning tree 1	10.255.11.59	Kite_59	
4				•

### **Trap Notifications Table**

### **Column Definitions**

### Name

The name of the trap as defined in the MIB.

### Synopsis

A brief description of the trap.

### Agent

The IP address of the switch that generated the trap.

### Agent Name

The name of the switch that generated the trap.

### Date/Time

The date and time the trap was received by the OmniVista server, using the OmniVista server's system clock.

### Severity

The severity level assigned to the trap in the Notifications Application's Trap Definitions Window. If desired, you can edit the severity level.

Normal	Blue
Warning	Green
Minor	Magenta
Major	Yellow
Critical	Red

#### Acknowledged

Indicates whether or not the trap has been acknowledged. Acknowledged traps ("true") display in plain type. Traps that have not yet been acknowledged, or whose acknowledgement has been renounced ("false"), display in bold type.

### **Trap Description Pane**

The Trap Description pane displays a detailed description of the selected trap. Click a row in the Trap Notifications table to view the corresponding information in the Trap Description pane. When a trap has variables associated with it, those variables are presented in a Trap Variables Table located in the bottom half of the Trap Description pane (as shown below).

	Trap De	scription F	Pane		
Synopsis:	Authentication failed due to unk	nownUser. IP: 128.2	51.19.109, User: admin, Access Type: http		
Description:	Authentication Failure authentication is refu		ach time a user		
Name: sessionAuthenticatio	nTrap Date/Time: Nov 28, 2	005 5:29:48 PM	Severity: Normal		
Agent: 10.255.11.59	Agent Name: Kite_59		Up Time: 5 days, 6 hours, 35 minutes, 16 seconds.		
Source: 10.255.11.59	Trap OID: .1.3.6.1.4	1.6486.800.1.3.2.11	1.0.1		
sessionAccessType	http	The access ty	me of the session.		
sessionUserName	admin	The user name	of the user logged-in.	Trap Variables	
sessionUser IpAddress	128.251.19.109	The IP addres	he IP address of the user logged-in.		
sessionAuthFailure	unknownUser	The reason wi	The reason why the user authentication failed.		

The information in the Description pane will vary depending on whether it is displaying an SNMPv1 trap, or an SNMPv2/SNMPv3 trap. OmniVista supports receipt of SNMPv1 traps from AOS devices.

### Synopsis

A brief description of the trap. When a trap has variables associated with it, the values of some or all of the variables may appear in the synopsis. For example, in the trap synopsis "Link down on slot 6 port 2," the numbers "6" and "2" are trap variable values for the link down trap. The values of all variables in a trap are presented in a Trap Variables Table located in the bottom half of the Description Pane. If desired, the synopsis can be edited to include or exclude trap variable values.

### Description

A detailed description of the trap as it appears in the MIB.

### Name

The name of the trap as defined in the MIB.

### Date/Time

The date and time the trap was received by the OmniVista server, using the OmniVista server's system clock. However, for traps received that are "replays" of previously-generated traps, the date/time will be adjusted to the time that the original trap was sent. This is calculated by adjusting the time received by the difference between the current upTime of the source device and the upTime contained within the trap itself. Therefore, it is possible for new traps to be added to the display with old timestamps. So, if the network was down for hours, you may suddenly see traps appear from hours ago.

### Severity

The severity level assigned to the trap in the Trap Definitions Window. Possible values are: Normal, Warning, Minor, Major, and Critical. If desired, you can edit the Severity Level.

### Agent

The IP address of the agent.

### Agent Name

The name of the switch that generated the trap.

### Up Time

The length of time the switch that sent the trap has been up (or the amount of time since the last reset), specified in days, hours, minutes, and seconds. This only applies to SNMPv2 and SNMPv3 traps.

### Source

The IP address of the switch that generated the trap.

### Trap OID

The trap object identifier number. This only applies to SNMPv2 and SNMPv3 traps.

### Enterprise OID

The enterprise object identifier number. This only applies to SNMPv1 traps.

### Enterprise

The enterprise name. This only applies to SNMPv1 traps.

### Specific

The enterprise trap number. This only applies to SNMPv1 traps.

### **Trap Variables Table**

When a trap has variables associated with it, those variables are presented in a Trap Variables table (as shown above). For each variable, there is a row in the table.

- The first column is the name of the variable as defined in the MIB.
- The second column is the variable value.
- The third column is a description of the variable as it appears in the MIB.

For some traps, a variable may contain multiple data embedded in the variable value in a manner that prohibits separation of the individual values based solely on the MIB definition of the variable. For this type of variable, an additional table appears after the Trap Variables table. This additional table is preceded by the label "Details of: <SNMP variable name>" and has a row for

each embedded datum where the first column is the name or brief description of the datum and the second column is the data value.

## The Switches Tab

The switches tab displays a list of all discovered switches with an additional **Trap Count** column that displays the total number of traps received on each switch. Like all Lists of Discovered Switches, this list of switches enables you to perform functions on a single switch or multiple switches simultaneously. To do so, select a switch (or multiple switches) in the list and right-click to display a popup menu of the functions available. You can also filter the list, not only by switch, but by trap type.

OmniVista 2500 - Application	c Notifications	Window:0					_10
e Applications View Help							
	۵ 💊 ۵	al 🗸					
		🕹 All 🔽					
Notifications	Notifications	Switches					
Responders						26.0	5 🐨 🖨 🛄
Trap Definition	Trap Count	Name	Address	DNS Name	Туре	Version	Last Upgrade Stat
		no-name1	10.255.11.119	Divo realitie	OmniSR-5	4.5.2	cast opgrade orat
10.255.10.3	6	Unset	10.255.11.253		Omni-5WX	4.4.3	
10.255.11.102	2	no-name	10.255.11.252		OmniSR-5	4.3.3.176	
10.255.11.118		DCTestnetCore	10.255.10.3		059600	6.1.1.154.R02	
- 10.255.11.119		NMS_HAWK_102	10.255.11.102		0\$6624	5.1.6.32.R03	
- 10.255.11.120	0	HAWK_118	10.255.11.118		OS6648	5.1.6.200.R02	
10.255.11.129	0	no-name	10.255.11.120		OmniS/R-3	4.5.2	
10.255.11.131	0	🙀 Fuji_129	10.255.11.129		0S9700	6.1.1.154.R02	
10.255.11.132	0	HAWK_131	10.255.11.131		OS6648	5.1.6.200.R02	
10.255.11.151	0	OS6248	10.255.11.132		0S6200-48LS		
10.255.11.153	0	QAW-4308_nms	10.255.11.151		OAW-4308		
10.255.11.157	0	HAWK_153	10.255.11.153		OS6648	5.1.6.200.R02	
- 10.255.11.198		AOS_Hawk_157_alias	10.255.11.157		0S6624	5.1.6.173.R02	
- 20 10.255.11.201		OmniSwitch_198_xyz	10.255.11.198		OS7800	5.1.6.32.R03	
- 10.255.11.202	0	OmniStack 8008_201	10.255.11.201		08-8008	V2.50.09	
10.255.11.207		🖬 Fuji9600_202	10.255.11.202		0\$9600	6.1.1.138.R02	
10.255.11.224		💓 OS6602-24	10.255.11.207		OS6602-24	5.1.6.393.R01	
- 10.255.11.225	0	🚃 test	10.255.11.224		08-6124	V3.40.31	
- 10.255.11.227		MNS_HAWK_102	10.255.11.225		OS6624	5.1.6.170.R02	
- 10.255.11.228		😥 Hawk151	10.255.11.227		0S6624	5.1.6.288.R01	
- 10.255.11.230		😥 OmniSwitch	10.255.11.228		0S6648	5.1.5.114.R04	
- 10.255.11.231		😥 lanswitch	10.255.11.230		OS6600-P24	5.1.6.143.R02	
- 10.255.11.240		🔂 Hawk197	10.255.11.231		OS6648	5.1.6.143.R02	
- 10.255.11.251		240-osr-mpx10	10.255.11.240		OmniS/R-5	4.5.2.82	
10.255.11.252	0	no-name	10.255.11.251		OmniSR-5	4.4.4	

The Trap Switches Tab

The **All** icon in the Notifications tree lists each known subnet. Click a subnet, and then click the Switches tab, to view the list of all the discovered switches in that subnet. Popup menus available in the tree provide additional functionality. You can only select one switch at a time in the tree.

### **Information Fields in the List**

### **Trap Count**

Displays the number of traps that belong to the switch (corresponding trap names are shown in the Notifications tab). This field is periodically updated as new traps arrive. The **Trap Count** field initially sorts the list of discovered switches in descending order.

### Name

The name of the device.

### Address

The address of the device.

### DNS Name

The DNS name of the device.

### Туре

The type of the device chassis.

### Version

The version number of the device firmware. Version numbers are not displayed for certain non-XOS devices.

### Last Upgrade Status

The status of the last firmware upgrade on the switch.

- "Successful" Successful BMF and Image upgrade performed.
- "Successful (BMF)" Successful BMF upgrade performed.
- "Successful (Image)" Successful Image upgrade is performed.
- "Failed (BMF, Image)" BMF and Image upgrade failed.
- "Failed (BMF)" BMF upgrade failed.
- "Failed (Image)" Image upgrade failed.

In all "Failed" cases, "Reload From Working" will be disabled on the switch until a successful upgrade is performed.

### Backup Date

The date that the device's configuration and/or image files were last backed-up to the OmniVista server.

### **Backup Version**

The firmware version of the configuration and/or image files that were last backed-up to the OmniVista server

### Last Known Up At

The date and time when the last poll was initiated on the device.

### Description

A description of the device, usually the vendor name and model.

### Status

This field displays the operational status of the device. It displays **Up** if the device is up and responding to polls. (When a device is up, it displays green in both the List of All Discovered Devices and the tree.) It displays **Down** if the device is down and not responding to polls. (When a device is down, it displays red in both the List of All Discovered Devices and the tree.) This field displays **Warning** if the switch has sent at least one warning or critical trap and is thus in the warning state. (When a device is in the warning state, it displays orange in both the List of All Discovered Devices and the tree.)

### Traps

This field indicates the status of trap configuration for the device. **On** means that traps are enabled. **Off** means that traps are disabled. **Not Configurable** means that traps for this device

are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.) **Unknown** means that OmniVista does not know the status of trap configuration on this switch. OmniVista will read the switch's trap configuration when traps are configured for the switch via the Configure Traps Wizard.

### Seen By

This field lists the Security Groups that are allowed to view the device. (The Security Groups that are allowed to view a device can be defined when devices are autodiscovered, added manually, or edited.) The default Security Groups shipped with OmniVista are as follows:

- **Default** group. This group has read-only access to switches in the list of All Discovered Devices that are configured to grant access to this group.
- Writers group. This group has both read and write access to switches in the list of All Discovered Devices that are configured to grant access to this group. However, members of this group cannot run autodiscovery nor can they manually add, delete, or modify entries in the list of All Discovered Devices.
- Network Administrators group. This group has full administrative access rights to all switches on the network. Members of this group can run autodiscovery and can manually add, delete, and modify entries in the list of All Discovered Devices. Members of this group also have full read and right access to entries in the Audit application and the Control Panel application. Members of this group can do everything EXCEPT make changes to Security Groups.
- Administrators group. This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to make changes to Security Groups.

Note that other Security Group names may display in this field if custom Security Groups were created. Refer to help for the Security application *Users and Groups* for further information on Security Groups.

### **Running From**

For AOS devices, this field indicates whether the switch is running from the **certified** directory or from the **working** directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:

- The certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory. (Note that you can specifically command a switch to reboot from either directory.)
- The working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

### Changes

For AOS devices, this field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:

- **Unsaved**. Changes have been made to the running configuration of the switch that have not been saved to the working directory.
- **Uncertified**. Changes have been saved to the working directory, but the working directory hasn't been copied to the certified directory. The working directory and the certified directory are thus different.
- Blank. When this field is blank for an AOS device, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.

OmniVista is now capable of tracking AOS configuration changes made through CLI commands or WebView, and so will reflect configuration changes made outside of OmniVista through these two interfaces in the Changes field. Information in the Changes field will be accurate as long as OmniVista has polled the switch since the last change was made (through any interface).

Note that it is possible a switch could be in a state where it is both Unsaved and Uncertified. In this situation **Unsaved** displays in the Changes field. Whenever an AOS device is in the Unsaved or Uncertified state, a blue exclamation mark displays on its icon (

### Discovered

This field displays the date and time when OmniVista successfully pings or polls the switch for the first time. This value remains unchanged until the switch entry is deleted. This field will remain blank if OmniVista does not ping or poll the switch at all.

# Trap/Switch Filtering

In addition to the standard switch table filter functions, you can use the Notifications Tab and the Switches Tab to filter by trap type and switch. When you create a trap filter using the Notifications Tab, the Switches Tab is automatically filtered to display the switches generating the filtered trap. After applying the filter in the Notifications Tab, click on the Switches Tab. The switches generating that trap will be displayed at the top of the list. If you have previously applied a filter to the Switches Tab, the list will also be filtered by that Switch Filter; or you can apply a different/new filter.

# **Trap Archiving**

When traps are received, OmniVista logs the information about a trap to a trap archive log file (**traps.txt**) located in the installation directory/data/logs folder. The **traps.txt** file will not be listed under **Current Log Files** in the **Audit** application like other log files.

When the **traps.txt** file reaches the configured maximum file size, OmniVista automatically archives a copy of the file under **Archived Log Files** of the **Audit** application. The number of trap archived files cannot exceed the maximum number of audit file copies configured in the **Preferences** application.

**Note:** You can set the maximum number of archived files and the maximum trap archive file size using the **Preferences** application.

The archived log file of **traps.txt** will have the same filename, but the date and time the file was archived is appended to it (e.g., traps\_05-16-2006\_043715PM.bak).

# **Trap Management**

The Notifications application is used to handle basic Trap Management tasks. Depending on user privileges, you can perform the tasks listed below.

All Users can perform the following:

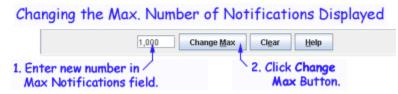
- Change the maximum number of Notifications displayed on the Client
- Change the maximum number of Notifications logged on the Server
- Copy traps to the clipboard
- Export traps to a .csv (comma-separated value) file.

If you have Administrative privileges (admin or netadmin), you can also perform the following:

- Clear all entries from the Trap Notifications table
- Acknowledge a trap
- Delete a trap.

# Changing the Maximum Number of Notifications Displayed

On the Client side, the default maximum number of notifications that can be displayed in the Trap Notifications table is 1,000. To change this value, enter a new number in the Max Notifications field, then click the **Change Max** button, as shown below.



There is no restriction on the number that can be entered in the Max Notifications field. However, the default maximum number of notifications that can be logged on the server is 30,000. If a number higher than 30,000 is entered in the Max Notifications field on the client, but the server has not been configured to log more than 30,000 notifications, the client will display no more than 30,000 notifications.

As the Trap Notifications table becomes filled, the oldest entries in the table are deleted to make room for the new alarms and traps that are received.

**Note**: Editing the number in the Max Notifications field on the Client does not result in any permanent change. If you close the Notifications application, then reopen it, the number in the Max Notifications field will return to its default value of 1,000. However, while the Notifications application is open, the maximum number of notifications will remain at the number that was set.

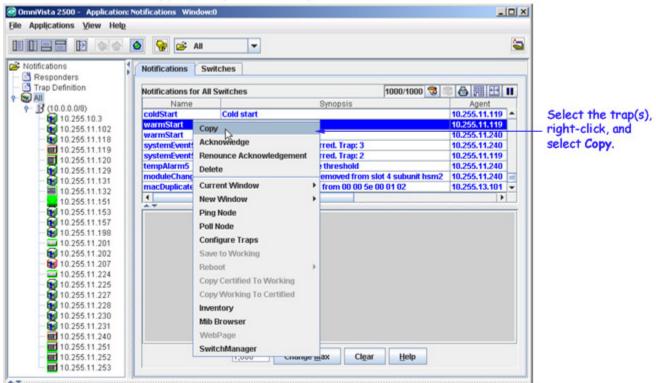
## Changing the Maximum Number of Notifications Logged

The maximum number of Notifications logged on the server is specified by the **Notifications Preferences** window in the Preferences application. The Preferences application is part of the Administration group of applications and can be opened from the Taskbar or by selecting **Preferences** on the **File** menu.

### **Copying Traps to the Clipboard**

To copy one or more traps to the clipboard, select the corresponding row(s) in the Trap Notifications Table, right-click to bring up the pop-up menu, then click **Copy** (as shown below).

**Note**: To select multiple rows, click on the rows while holding down the **CTRL** or **SHIFT** keys.



Copying Traps to the Clipboard

This feature is useful for copying a single trap into a text editor or pasting it into an e-mail. When copied into a spreadsheet file, the trap information displays in a single field; this is in contrast to exporting traps, where all the field information is retained

### **Exporting Traps to a .CSV File**

Use the Export function to save trap information to a \*.csv (comma-separated value) file, then view it through a text editor, spreadsheet, or database program. Because trap information is eventually written over as the Max Notifications value is reached, the Export function is useful when you want to archive trap information for later use.

You can export traps for all switches, for all switches in a selected subnet, or for a single switch. Display the traps that you want to export by clicking on **All**, a subnet or an individual switch in the Notifications tree; then select **Export Traps** from the **File** menu or click the Export Table icon. In the example below, a subnet was selected, so all of the traps for all of the switches in that subnet are displayed.

In the state of th	File Applications View H	leip			
lect Switches, subnet, or a	Logout Preferences	o o 😡 🔄	10.255.11.119	<b>a</b>	Exp
igle switch, then lect Export	Glose Notifications	Notifications 1	Switches		Tab
aps from the	₽ Polling	Notifications for 5	Switch no-name1 (10.255.11.119) 1000/100	10 🤝 💷 🔂 🗐 🚾 👭	-
e Menu.		Name	Synopsis	Agent Agent I	
e menu.	- Export Traps	coldStart warmStart	Cold start Warm start	10.255.11.119 no-nam  10.255.11.119 no-nam	
	Exit 402	systemEvent5	Potentially fatal error occurred. Trap: 2	10.255.11.119 no-nam	
	10.255.11.118	temnAlarmS	Temperature exceeded the threshold	10.255.11.119 no-nam	
	10.255.11.119	moduleChange5		10.255.11.119 no-nam	
	10.255.11.120	tempAlarm5	Temperature exceeded the threshold	10.255.11.119 no-nam	
	10.255.11.129	moduleChange5	Module invalid inserted or removed from slot 3 subunit hsm1	10.255.11.119 no-nam	
	10.255.11.131	powerEvent5	Power Supply 1: notPresent. Power Supply 2: 89	10.255.11.119 no-nam •	
	10.255.11.151	4			
	10.255.11.153				
	10.255.11.157	Trap Configurat	ion Status: On		
	10.255.11.198				
	10.255.11.201				
	10.255.11.202				
	10.255.11.207				
	10.255.11.224				
	10.255.11.225				
	10.255.11.228				
	10.255.11.230				
	10.255.11.240				
	10.255.11.240				
			1,000 Change Max Clear Help		

When you select **Export Traps** or click the Export Table icon, the Export Traps window appears. Navigate to the directory where you want to save the information, enter a file name, then click **Save**.

1 Nevineta to the	Export Traps Window
<ol> <li>Navigate to the directory where</li> </ol>	Export Traps
server and the server	Save In: My Documents
	Adobe
	My Data Sources My eBooks
	My Pictures
	OmniVista
2. Enter a file name	File Name:
	Files of Type: comma separated value file (.csv)
	Save Cancel
	3. Click Sov

**Note**: You do not need to include .csv to the filename; the file extension is automatically added.

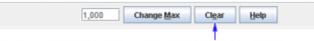
The .csv file can be opened using any text editor, spreadsheet, or database program. The following is an example of what you would see when the file is viewed through a spreadsheet application:

SI M	licrosoft Excel -	Engineering Tra	aps 12-12-05.csv				d,
8	Ele Edit Vie	w Insert For	mat <u>T</u> ools <u>D</u> ata <u>W</u> indow	Help Acrobat	Type a qu	estion for help 🔹 🗕 🗗	1
D	😂 🖬 😢 (	5 🗟 🖤  🕷	🗈 💼 • 🛷 🗠 • Σ •	21 🛍 🕐 🗄	Arial	• 10 • 🚍	
-							
찐	12 -						
_	A22 💌		55.11.59				_
	A	В	C	D	E	F	1
1	Source	Agent	Name	GenericTrap	SpecificTrap	Time	_
2	10.255.11.59	10.255.11.59	chassisTrapsAlert	0		Wed Nov 23 10:55:32	_
3	10.255.11.59	10.255.11.59	chassisTrapsAlert	0	0	Wed Nov 23 10:55:32	1
4	10.255.11.59	10.255.11.59	chassisTrapsStateChange	0	0	Wed Nov 23 10:55:32	1
5	10.255.11.59	10.255.11.59	coldStart	0	0	Wed Nov 23 10:55:32	1
6	10.255.11.59	10.255.11.59	chassisTrapsAlert	0	0	Wed Nov 23 10:55:39	1
7	10.255.11.59	10.255.11.59	chassisTrapsStateChange	0	0	Wed Nov 23 10:55:49	1
8	10.255.11.59	10.255.11.59	chassisTrapsStateChange	0	0	Wed Nov 23 10:55:51	I
9	10.255.11.59	10.255.11.59	stpNewRoot	0	0	Wed Nov 23 10:55:54	1
10	10.255.11.59	10.255.11.59	stpNewRoot	0	0	Wed Nov 23 10:55:56	Ĩ
11	10.255.11.59	10.255.11.59	stpNewRoot	0	0	Wed Nov 23 10:55:57	1
12	10.255.11.59	10.255.11.59	stpNewRoot	0	0	Wed Nov 23 10:55:57	1
13	10.255.11.59	10.255.11.59	stpRootPortChange	0	0	Wed Nov 23 10:56:04	Ī
14	10.255.11.59	10.255.11.59	aipAMAPStatusTrap	0	0	Wed Nov 23 10:56:29	ũ
15	10.255.11.59	10.255.11.59	stpRootPortChange	0	0	Wed Nov 23 15:08:54	Ī
16	10.255.11.59	10.255.11.59	chassisTrapsAlert	0	0	Sat Nov 26 12:28:12 F	p
17	10.255.11.59	10.255.11.59	chassisTrapsAlert	0	0	Sat Nov 26 12:28:18 F	þ
18	10.255.11.59	10.255.11.59	stpRootPortChange	0	0	Mon Nov 28 08:57:26	F
19	10.255.11.59	10.255.11.59	chassisTrapsAlert	0	0	Mon Nov 28 14:17:54	F
	Enginee	ring Traps 12-1	1	1.	1		i
lead				1.1			1

### **Clearing All Entries from the Trap Notifications Table**

To remove all alarms and traps currently displayed in the Trap Notifications table, click the **Clear** button at the bottom of the log. Once you have cleared the entries, they are permanently deleted from the OmniVista server and will no longer be displayed on any OmniVista client.

Clearing All Entries from the Notifications Table



To clear all entries from the Notifications table, click **Clear**.

### Acknowledging a Trap

To acknowledge a trap or renounce a trap acknowledgement, follow the steps below:

**1.** Select one or more traps from the Trap Notifications table.

**2.** Right-click to bring up the pop-up menu.

### 3. Select either Acknowledge or Renounce Acknowledgement.

Acknowledged traps appear in plain type. Traps that have not yet been acknowledged and traps for which you have renounced acknowledgement are displayed in bold type.

### **Deleting a Trap**

To delete a trap, follow the steps below:

**1.** Select one or more traps from the Trap Notifications table.

**2.** Right-click to bring up the pop-up menu.

**3.** Select **Delete**. No confirmation is requested. The trap is permanently deleted from the OmniVista server and will no longer be displayed on any OmniVista client.

**Note**: Refer to the Topology Help for information on pop-up menu commands not related to trap management.

# The Trap Responders Window

The Trap Responders window enables you to specify the response (if any) that you want OmniVista to make when specified traps are received by OmniVista. You can specify the traps to which OmniVista will respond by severity level; or, you can specify the traps using filters. You can also specify the trap origin by logical regions, physical subnets, or IP address range. OmniVista can make the following responses to receipt of a specified trap:

- OmniVista can send an e-mail to any address you specify. You can specify the information you want included in the e-mail through the use of variables. Variables exist for information such as the trap name, synopsis, description, etc.
- OmniVista can execute an external program or script on the OmniVista server
- OmniVista can forward traps to a specific IP address.

To configure an OmniVista trap response, select **Responders** in the Notifications tree. The **Automatic Trap Responders** table displays any configured Trap Responders. The **Trap Condition and Response** area is used to configure the traps that OmniVista will respond to and what that response will be. The area contains three tabs:

- Agent The Agent tab is used to specify trap origin.
- **Trap Type** The Trap Type tab is used to specify trap by severity level or trap type.
- **Response** The Response tab is used to configure the action OmniVista will take when it receives a trap that matches the specified trap criteria.

The **Agent** and **Trap Type** tabs are used to specify which traps that OmniVista will respond to. The **Response** tab is used to configure how OmniVista will respond to the traps.

ders III		🙆 🎯 Responders 🔽		
g up idow.	fications	Automatic Trap Responders Agent From range 10.255.10.1-10.255.10.254	Trap Type Severity any of (Major) Severity any of (Critical)	Response Descript E-Mail Trap Forward
	- 10.255.11.155 10.255.11.156 10.255.11.176 10.255.11.194 10.255.11.196 10.255.11.197 10.255.11.199 10.255.11.201 10.255.11.218 10.255.11.223 10.255.11.223 10.255.11.225 10.255.11.255 10.2	View Trap Conditions and Response           Agent         Trap Type         Response           sps from one of these topology ro         (10.0.0.0 €           Agent Regions:         (14.0.0.0 €	Agent Start IP	s IP address range:
	- 10.255.11.252 - 10.255.11.253 - 10.255.73.1 - 10.255.73.12 - 10.255.73.13 - 10.255.73.13 - 10.255.73.15			

#### condition and response.

### How to Configure a Trap Responder

To configure a new trap responder, click the **New** button at the bottom of the Trap Responders pane and refer to the sections below.

### The Agent Tab

You can limit the traps you receive to a specific Topology Region or IP address range. Only those traps originating in the specified area will generate a response. You can specify a trap by multiple regions; however, you cannot specify a trap by both Topology Region and IP address range. (In other words, you cannot "AND" a Topology Region and IP address range to create an expression.) When the origin is specified, click on the **Trap Type** tab to configure a severity level or Trap Filter.

**Note:** Although you cannot specify traps by Topology Region **and** IP address ranges, the conditions configured in the Agent tab can be combined with the condition you specify in the Trap Type tab.

-	0.52	A	1000	4.1		1.5
	ne	Ag	en	T	a	D
						-

	Responders 💌
Notifications Responders Trap Definition All P (10.0.0.08) - 10.255.11.121 - 10.255.11.123 - 10.255.11.125 - 10.255.11.125 - 10.255.11.125 - 10.255.11.125 - 10.255.11.126 - 10.255.11.194 - 10.255.11.194 - 10.255.11.194 - 10.255.11.199 - 10.255.11.218	Automatic Trap Responders           Agent         Trap Type         Response Description           From range 10.255.10.1-10.255.10.254         Severity any of (Major)         E-Mail           From any region of (44.0.0.008)         Severity any of (Critical)         Trap Forward             Create Trap Conditions and Response           Agent         Trap Type         Response           raps from one of these topology regione        OR from this IP address range:           (10.0.0.08)         Agent Start IP;
10.255.11.223     10.255.11.224     10.255.11.225     10.255.11.229     10.255.11.252     10.255.11.252     10.255.73.1     10.255.73.1     10.255.73.15     10.255.73.15     10.255.73.15     10.255.73.98	Agent Regions: (33.0.0.08) (44.0.0.08) Agent End IP: OK Default Cancel Help

### The Trap Type Tab

In the Trap Type tab, you can specify the traps to which OmniVista will respond by severity level; or, you can specify the traps using filters. Note that you can specify traps by severity level or filters, but you cannot specify traps using both severity levels and filters. (In other words, you cannot "AND" specified severity levels and specified filters to create an expression.) If you create a trap responder that specifies both severity level and filters, the trap responder will respond to all traps with the specified severity (even if they do not match the filter), and all traps that match the specified filters (even if they do not have the specified severity).

**Note:** Although you cannot specify traps by Severity Level **and** Filters, the conditions configured in the Trap Type tab can be combined with the condition you specify in the Agent tab.

### The Trap Type Tab

Agent       Trap Type       Response to the second	Responders	Automatic Trap Re	enondere			
Agent       Trap Type       Response I         All       From range 10.255.10.254       Severity any of (Maior)       E-Mail         From any region of (44.0.0.0/8)       Severity any of (Critical)       Trap Forward         10.255.11.21       10.255.11.22       Severity any of (Critical)       Trap Forward         10.255.11.225       10.255.11.23       Create Trap Conditions and Response       Severity any of (Critical)       Trap Forward         10.255.11.125       10.255.11.126       Severity any of (Critical)       Trap Forward       Severity any of (Critical)       Trap Forward         10.255.11.25       10.255.11.26       Magent       Trap Type       Response       Severity any of (Critical)       Trap Forward         10.255.11.201       Trap Swhich match these severities:      OR which match these filters         10.255.11.225       Normat:       Ignore       Must Match:       Any Selected Filter         10.255.11.225       Minor:       Ignore       Engineering       Test Lab			cohomero			8 H H
All       From range 10.255.10.254       Seventy any of (Major)       E-Mail         I 10.255.11.121       From any region of (44.0.0.008)       Seventy any of (Critical)       Trap Forward         I 10.255.11.123       10.255.11.125       I 10.255.11.125       I 10.255.11.126         I 10.255.11.124       I 10.255.11.125       I 10.255.11.126         I 10.255.11.126       I 10.255.11.126         I 10.255.11.126       I 10.255.11.126         I 10.255.11.126       I 10.255.11.126         I 10.255.11.127       Reponse         I 10.255.11.128       Agent Trap Type Response         I 10.255.11.201       I 10.255.11.223         I 10.255.11.223       Normat gnore         I 10.255.11.224       Warning: gnore         I 10.255.11.225       Minor: ignore         I 10.255.11.225       Minor: ignore				-		Response Description
I (10.0.0.00)       I (10.255.11.121)         I (10.255.11.121)       I (10.255.11.124)         I (10.255.11.124)       I (10.255.11.124)         I (10.255.11.125)       I (10.255.11.124)         I (10.255.11.125)       I (10.255.11.126)         I (10.255.11.126)       I (10.255.11.126)         I (10.255.11.126)       I (10.255.11.126)         I (10.255.11.127)       I (10.255.11.127)         I (10.255.11.127)       I (10.255.11.127)         I (10.255.11.127)       I (10.255.11.127)         I (10.255.11.127)       I (10.255.11.127)         I (10.255.11.127)       I (10.255.11.227)         I (10.255.11.127)       I (10.255.11.227)         I (10.255.11.227)       I (10.255.11.227)         I (10.255.11.228)       I (10.255.11.228)         I (10.255.11.229)       I (10.255.11.228)         I (10.255.11.229)       I (10.255.11.228)	IIA					
10.255.11.121         10.255.11.123         10.255.11.124         10.255.11.125         10.255.11.125         10.255.11.125         10.255.11.125         10.255.11.126         10.255.11.126         10.255.11.194         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.201         10.255.11.218         Normal:       gnore         10.255.11.224         Warning:       ignore         10.255.11.225         Ninor:       ignore         Filter Names:       Filter Names:	B (10.0.0.0/8)	From any region of	1(44.0.0.0/8)	Sever	ity any of (Critical)	Trap Forward
10.255.11.124         10.255.11.125         10.255.11.135         10.255.11.135         10.255.11.195         10.255.11.196         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.201         10.255.11.218         Normal:       gnore         10.255.11.224         Warning:       ignore         10.255.11.225       Engineering         10.255.11.225       Filter Names:						
10.255.11.125         10.255.11.135         10.255.11.135         10.255.11.135         10.255.11.194         10.255.11.194         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.197         10.255.11.201         10.255.11.218         Normal:       gnore         10.255.11.224         Warning:       ignore         10.255.11.225         10.255.11.225         Ninor:       ignore         Filter Names:						
ID 255.11.135       ID 255.11.135         ID 255.11.165       ID 255.11.165         ID 255.11.194       ID 255.11.194         ID 255.11.197       ID 255.11.197         ID 255.11.197       ID 255.11.197         ID 255.11.197       ID 255.11.197         ID 255.11.201       ID 255.11.201         ID 255.11.218       Normal:         ID 255.11.224       ID 255.11.224         ID 255.11.225       ID 255.11.225         ID 10.255.11.225       ID 255.11.225         ID 10.255.11.225       ID 255.11.225         ID 10.255.11.225       ID 255.11.225						
10.255.11.155         Create Trap Conditions and Response           10.255.11.194         Agent Trap Type Response           10.255.11.197         Traps which match these severities:           10.255.11.201         Normal: ignore           10.255.11.223         Warning: ignore           10.255.11.224         Minor: ignore           10.255.11.229         Filter Names:						
10.255.11.176       Create Trap Conditions and Response         10.255.11.194       Agent Trap Type Response         10.255.11.197       Traps which match these severities:         10.255.11.218       Normal: ignore         10.255.11.224       Warning: ignore         10.255.11.225       Filter Names:         10.255.11.225       Minor: ignore						
In 10.255.11.194       Create Trap Conditions and Response         In 10.255.11.195       Agent Trap Type Response         In 10.255.11.197       Traps which match these severities:         In 10.255.11.201       In 255.11.201         In 10.255.11.218       Normal:         In 10.255.11.224       Warning:         In 10.255.11.225       Ignore         In 10.255.11.225       In 10.255.11.225						
I 0.255.11.196       Agent Trap Type Response         I 0.255.11.197       Traps which match these severities:      OR which match these filters         I 0.255.11.201       Normal:       Ignore       Must Match:       Any Selected Filter         I 0.255.11.225       Warning:       Ignore       Engineering       Test Lab		-Croate Tran Con	ditions and Desnen			
10.255.11.197       Image Trap Type       Traps which match these severities:      OR which match these filters         10.255.11.218       Normal:       Ignore       Must Match:       Any Selected Filter         10.255.11.223       Warning:       Ignore       Engineering         10.255.11.225       Minor:       Ignore       Filter Names:		create trap con		Pe -		
Image: Constraint of the sector in		Agent Trap	Type Response			
4     10.255.11.201     Image which match these sevenines.     Image which match these sevenines.       4     10.255.11.218     Normal:     ignore       4     10.255.11.224     Warning:     ignore       5     10.255.11.225     Minor:     ignore       6     10.255.11.225     Minor:     ignore						
Image: Second		Traps v	which match these s	everities:	OR which	match these filters:
•••••••••••••••••••••••••••••		332550	1.00		100000000000000000	
Warning:         Ignore         Engineering           10.255.11.225         Minor:         Ignore         Filter Names:		Normal:	ignore	-	Must Match:	Any Selected Filter
10.255.11.225 10.255.11.229 Minor: Ignore Vial International Action of the Internation		Marning	Importo	-		Engineering
- 🔂 10.255.11.229 Minor: ignore 👻 Filter Names:		warning	r ignore		12.12.12 C	
10 355 11 352		Minor:	ignore	-	Filter Names:	
	10.255.11.252					
10.255.11.253 Major: ignore	- 10.255.11.253	Major:	ignore	-		
10.255.73.1 Criticat ignore  Edit Filter List	10.255.73.1	Cultingh	Image			Edit Filter List
to 255.73.12 Critical: ignore Edit Fifter List	10.255.73.12	Criticac	ignore			Lon Chevr Line
10.255.73.13	- 🔂 10.255.73.13	-	117			
10.255.73.15	10 255 73 15					
			OK	Default	Cancel He	lp
	10.255.73.96 💌					

#### **Specifying Traps by Severity**

The Trap Type tab lists each possible trap severity level - Normal, Warning, Minor, Major, and Critical - and provides a drop-down menu for each level. Each level can be set to either **ignore** or **respond**. When a level is set to **respond**, receipt of a trap with that severity level will trigger the response specified in the Response tab. When a drop-down box is set to **ignore**, receipt of a trap with that severity level will not trigger the response specified in the Response Tab.

If you want to specify traps using one or more severity levels, set the desired trap severity levels to **respond**. For example, you might want to set the Major severity level and the Critical severity level to **respond** and leave other severity levels set to **ignore**. In this case, the response specified in the Response Tab will occur when a trap of Major severity or Critical severity is received. If you specify traps using severity levels, ensure that no filters are selected in the **Filter Names** box.

When the severity level is specified, click the Response Tab to configure the response.

Notifications		onders 💌		<b>a</b>	-
- C Responders	Automatic Trap Res			8 III III III	
- 📑 Trap Definition		Agent	Trap Type	Response Description	
	From range 10.255. From any region of (		Severity any of {Major} Severity any of {Critical}	E-Mail Trap Forward	
- 10.255.11.121 - 10.255.11.123 - 10.255.11.124 - 10.255.11.125 - 10.255.11.125 - 10.255.11.155 - 10.255.11.155 - 10.255.11.196 - 10.255.11.196 - 10.255.11.197 - 10.255.11.199 - 10.255.11.218 - 10.255.11.218 - 10.255.11.218	Agent Trap Ty	tions and Response pe Response hich match these sever		match these filters: Any Selected Filter 🔽	Make sure no
- 🚜 10.255.11.224 📑	Warning:	ignore	-	Engineering	Filters are
10.255.11.225	Minor:	ignore	Filter Names:	Test Lab 🔫	selected.
10.255.11.252			-		
- 10.255.11.253	Major:	ignore	-		
- 🙀 10.255.73.1	Critical:	ignore	-	Edit Filter List	
10.255.73.12	Grinden	ignore			
10.255.73.13 10.255.73.15 10.255.73.96		To specify tr specify wheth	Default Cancel Hel aps by severity level her or not you want respond to each leve		

### Specifying Traps by Severity Level

### **Specifying Traps by Filter**

Create filters by clicking the **Edit Filter List** button, which displays the Edit Filters Window. The Edit Filters Window enables you to create, edit, and delete the filters listed in the **Filter Names** field.

To specify traps by one or more filters, set the **Must Match** drop-down menu to **Any Selected Filter** (which will OR the filters that you select) or to **All Selected Filters** (which will AND the filters that you select). Select the desired filters in the **Filter Names** box. A filter is selected when it is checked. Ensure that the severity levels are set to **ignore**.

When the filter is specified, click on the Response Tab to configure the response.

Specifying Trap	s by Filt	er
-----------------	-----------	----

OmniVista 2500 - Application: No	tifications Windows	0			×
Ele Applications View Help	De Derer	onders 👻			
	Respo	onders 💌			
A Notifications	Automatic Trap Res	nondere		6 III III	n
- Responders	a balance in the second s	Agent	Trap Type	Response Description	4
- 🗳 Trap Definition - 🕤 All	From range 10.255.		Severity any of (Major)	E-Mail	
P S All	From any region of {		Severity any of (Critical)	Trap Forward	
	i rom any region or	++.0.0.0.00	derenty any or (ormeal)	Trap I armara	
- 10.255.11.121					
10.255.11.123					
10.255.11.124					
10.255.11.125					
10.255.11.194	Create Trap Condi	tions and Response			1
10.255.11.196					
10.255.11.197	Agent Trap Ty	pe Response			A 1.411 C 114
- 10.255.11.199	Transat		on which and the second s	h match the set filler as	Set this field to
- 3 10.255.11.201	Traps wi	hich match these seve	rities:OR whic	h match these filters:	Any Selected Filter
- 10.255.11.218		-		a contraction of the	or All Selected Filters.
- 3 10.255.11.223	Normal:	ignore	Must Match:	Any Selected Filter 💌 <	of All Selected Fillers.
- 36 10.255.11.224	Warning:	ignore	-	✓ Engineering	Contract Contract Contractor
- 🗑 10.255.11.225	e e a marga	-guore		Test Lab	—— Select Filter(s)
- 😥 10.255.11.229	Minor:	ignore	Filter Names:		The second s
- 10.255.11.252					
- 10.255.11.253	Major:	ignore	-		
- 📷 10.255.73.1	Critical:	ignore	-	Edit Filter List	Click Edit Filter List
- 💓 10.255.73.12	CI IOCOIL	ignore			
- 🙀 10.255.73.13		+			button to create, edit,
- 🙀 10.255.73.15		OK	Default Cancel H	elp	or delete a filter.
- 🗑 10.255.73.96 💌		On	Deraux Cancel H	eip	
* <b>*</b>					
		Make sure a	Sevenity		
		levels are se	T TO Ignore.		

#### The Response Tab

To create the response, first enter a description of the response in the **Response Description** field. Set the **Response Action** field to **Send an e-mail**, **Run an application on the server**, or **Forward traps**. Continue as described in the appropriate section below.

	Respond	ters 💌	
Notifications     Responders     Trap Definition     Trap Definition     10.255.10.3     10.255.11.102     10.255.11.119     10.255.11.129     10.255.11.129     10.255.11.131     10.255.11.131     10.255.11.151     10.255.11.151     10.255.11.151     10.255.11.151     10.255.11.151     10.255.11.151     10.255.11.151     10.255.11.151     10.255.11.199     10.255.11.199     10.255.11.199	and the second sec	Minor Major Critical Must Match Fitter Names Response Description inore ignore Any Selected Fitter Switch 242	Enter a description for the Response. Set the Response
10.255.11.202 10.255.11.207 10.255.11.224 10.255.11.225 10.255.11.225 10.255.11.229 10.255.11.230 10.255.11.231 10.255.11.231 10.255.11.251 10.255.11.251 10.255.11.252 10.255.11.253	E-mail To:	Spetial all 6-mail	Action.

#### The Response Tab

### To Send an E-Mail

If you set the Response Action to **Send an e-mail**, follow the steps below to define the e-mail to be sent. It is important to note that all fields in the Sending E-Mail Preferences Window in the Preferences Application MUST be completed or the e-mails you define will not be sent. To display the Sending E-Mail Preferences Window, select **Sending E-Mail** in the Preferences Application, which is in the Administration Group of applications.

	🙆 😵 Respon	fers 💌	2
Notifications Respondent Trap Definition 10 255 11 102 10 255 11 202 10 255	and a state of the	Minor Major Critical Must Match Fitter Names Response Description more lignore lignore Any Selected Fitter Switch 242	Enter a Response Description. Enter the address to which the e-ma will be sent. Enter the text fo the body of the e-mail, or enter a variable.
10.255.11.253			_

Response Tab - Send an E-Mail

**1.** Enter a Response description.

**2.** Enter the address to which the email will be sent in the **Email To** field. (The "From" address on responder e-mails is determined by the entry in the **Use 'From' Address** field in the Sending E-mail pane n the Preferences application.)

**3.** Define the body of the email in the **E-mail Body** field by typing the desired text and/or the desired variables. The variables you can use are explained in the Trap Variables section below. You can also accept the default e-mail body, which is the variable \$Details\$ (explained below).

**4.** Click the **OK** button. The new automatic trap responder is saved to the session memory and is listed in the **Automatic Trap Responders** table as an unsaved change. Click the **Apply** button to save the new responder to the server.

### To Run an Application on the Server

If you set the Response Action to **Run an application on the server**, follow the steps below to define the application to be run.

idee e 💩	🙆 😵 Respond	ers 💌	la
Notifications	Automatic Trap Respond	ers 🛛 🔠	TERTOUT
Trap Definition	procession and an and an and an approximation of the second secon	Minor Major Critical Must Match Filter Names Response Desc	
Trap Definition	ignore ignore ig	nore ignore Any Selected Filter Switch 242	
10.0.0.0/8)			
10.255.10.3			
10.255.11.102			
- 10.255.11.118			
10.255.11.120			
10.255.11.129			
10.255.11.131	4	1	•
- 10.255.11.132	Create Trap Condition a	nd Dogungero	
- 10.255.11.151			Enter a Response
10.255.11.153	Condition Respons	8	
10.255.11.157	Response Description:		Description.
10.255.11.201	Decemence Actions	Due as application on the context	Enter a command.
10.255.11.202	Response Action:	Run an application on the server	
10.255.11.207	Command:		Enter the Argument
10.255.11.224	Arguments:	\$Synopsis\$	
- 😥 10.255.11.225		(aphobalat	Enter directory whe
10.255.11.227	Start Directory:		command should star
10.255.11.228		\$Details\$	
- 10.255.11.230	Standard Input:		Enter the Standard
10.255.11.240			Input for the commo
10.255.11.251			Input for the comme
10.255.11.252		OK Default Cancel Help	
10.255.11.253			

Response Tab - Run an Application

**1.** Enter a Response description.

**2.** Enter the command to be executed in the **Command** field.

**3.** Enter the arguments to the command specified above in the **Arguments** field, or accept the default argument, the variable \$Synopsis\$ (explained in the Trap Variables section below).

4. Enter the directory in which the command should be executed in the **Start Directory** field.

**5.** Enter the standard input for the command in the **Standard Input** field, or accept the default standard input, the variable \$Details\$ (explained in the Trap Variables section below).

6. Click the OK button. The new automatic trap responder is saved to session memory and is listed in the Automatic Trap Responders table as an unsaved change. Click the Apply button to save the new responder to the server.

### **To Forward the Traps**

If you set the Response action to **Forward traps**, follow the steps below to forward the traps to a specific IP address.

**Note:** If you have enabled Trap Absoprtion for non-AOS devices through the Preferences application, all traps will still be forwarded for this response option.

IIIII III P 🐼 🙆 🚱 Responders 🔻			
Responders	Automatic Trap Responders		
Trap Definition	Normal Warning	linor Major Critical Must Match Filter Names Response Description	
Trap Definition	ignore ignore ig	nore ignore Any Selected Filter Switch 242	
10.0.0/8			
10.255.10.3			
- 10.255.11.102			
10.255.11.118			
- 10.255.11.119			
10.255.11.120			
10.255.11.129			
- 10.255.11.131	4		
10.255.11.132			
10.255.11.151	Create Trap Condition a	nd Response	1 100 100 100 100 100 100 100 100 100 1
10.255.11.153	Condition Respons	0	Enter a Response
10.255.11.157			
10.255.11.198	Response Description:		<ul> <li>Description.</li> </ul>
	Response Action:	Forward traps	
10.255.11.202	response rectors		Enter the Destination
10.255.11.207	Destination IP:		
	Destination Dest	162	_ IP address for the tr
10.255.11.225	Destination Port:	102	
10.255.11.227			
10.255.11.228			Enter the Destination
10.255.11.230			UDP Port Number
10.255.11.231			
- 10.255.11.240	2		(Default = 162).
10.255.11.251			(0010011 - 101).
10.255.11.252		OK Default Cancel Help	
10.255.11.253		terrational terrational terrational terrational	
10.200.11.200		T	

Response Tab - Forward Traps

Then click Apply to save the Responder to the server.

**1.** Enter a Response description.

**2.** Enter the destination IP address in the **Destination** IP field. Only one IP address can be entered per Responder. However, you can create multiple Responders to forward the trap to multiple recipients.

**3.** Enter the destination UDP port number (Default = 162) in the **Destination Port** field.

**4.** Click the **OK** button. The new automatic trap responder is saved to the session memory and is listed in the **Automatic Trap Responders** table as an unsaved change. Click the **Apply** button to save the new responder to the server.

**Note:**You can forward traps between two servers to provide a backup for trap logs. However, forwarding traps between more than two servers is not supported.

### **Facts About Responder E-Mails**

To prevent e-mail storms that would result from receipt of multiple traps, OmniVista does NOT send one e-mail per trap received. Rather, OmniVista "coalesces" (i.e., combines) responder e-mails to prevent storms. OmniVista will send a coalesced responder e-mail when:

- a minute has passed since the first trap was received for which an e-mail was not generated, OR
- a minimum of 100 traps have been received.

**Note:** These default values can be re-defined using the Trap E-Mail pane of the Preferences application, which is in the Administration group of applications.

The subject of responder e-mails takes the following form:

### OmniVista: Traps Received (2 Critical, 2 Major, 5 Minor)

The "From" address in the responder e-mails is determined by the entry in the Use 'From' Address field in the Sending E-Mail pane of the Preferences application.

### **Trap Variables**

You can use the following variables when you configure an automatic trap responder. There are two types of variables: generic variables (which currently apply only to traps) and trap-specific variables.

### **Generic Variables**

### **\$Details\$**

For traps, this variable is equivalent to the following combination of text and trap-specific variables (trap-specific variables are described in the following section):

Trap Received: \$TrapName\$ Severity: \$TrapSeverity\$ Synopsis: \$TrapSynopsis\$ Agent: \$TrapAgent\$ Variables: \$TrapVariables\$

### Output Example:

Trap Received: portPartitioned Severity: Minor Synopsis: Port jabber on slot 7 frtrunking port 1 instance 156 (port state alternated between enabled and disabled more than 50 times in 200 ms) Agent: 128.251.30.27

### \$Synopsis\$

For traps, this variable is equivalent to the trap-specific variable \$TrapSynopsis\$, which is a brief description of the trap.

*Output Example:* Port jabber on slot 7 frtrunking port 1 instance 156 (port state alternated between enabled and disabled more than 50 times in 200 ms)

### **Trap-Specific Variables**

### \$TrapName\$

The name of the trap (as defined in the MIB)

Output Example: portPartitioned

### TrapSynopsis

A brief description of the trap.

*Output Example:* Port jabber on slot 7 frtrunking port 1 instance 156 (port state alternated between enabled and disabled more than 50 times in 200 ms)

### **\$TrapDescription\$**

A detailed description of the trap (as it appears in the MIB)

*Output Example:* A portPartitioned trap occurs when the physical port has transitioned through enable/disable states faster than 10 times in the past second...indicative of a flaky cable.

#### **\$TrapSeverity\$**

The severity level assigned to the trap in the Notifications application's Trap Definitions pane. The severity level can be Normal, Warning, Minor, Major, or Critical.

#### *Output Example:* Minor

#### \$TrapSeverityInt\$

The severity level assigned to the trap in the Notifications application's Trap Definitions pane, expressed as an integer. The severity level integer can be 1 (Normal), 2 (Warning), 3 (Minor), 4 (Major), or 5 (Critical).

### Output Example: 3

### \$TrapSnmpVersion\$

The version of the trap request, either 1 (version 1) or 2 (version 2).

All traps sent with SNMP version 1 protocol are "version 1" trap requests. All traps sent with SNMP versions 2, 2c, or 3 protocol are "version 2" trap requests. There are actually two different types of trap requests (not three). The message packet in which trap requests are sent can be one of four different versions: 1, 2, 2c, or 3. When you use the AOS CLI to create a version 1 trap station, version 1 traps in version 1 protocol are sent to that station. When you use the AOS CLI to create a version 2 trap station, version 2 traps in version 2 c protocol are sent to that station. When you use the AOS CLI to create a version 3 protocol are sent to that station. The version 2 trap station, version 2 traps in version 3 protocol are sent to that station. The version 2 trap request itself is identical whether wrapped in a version 2 or version 3 packet.

### **Output Example:** 1

### **\$TrapSource\$**

The IP address of the switch that generated the trap.

### Output Example: 127.0.0.1

### **\$TrapUpTime\$**

The length of time the switch that sent the trap has been up (or the amount of time since the last reset).

### Output Example: 21 hours, 35 minutes, 49 seconds

### **\$TrapAgent\$**

The IP address of the SNMP agent.

### *Output Example:* 128.251.30.27

#### **\$TrapV1Enterprise\$**

The enterprise name. This only applies to SNMP Version 1 traps.

### Output Example: xylanSwitchDevice

### **\$TrapV1EnterpriseOID\$**

The enterprise object identifier number. This only applies to SNMP Version 1 traps.

### Output Example: .1.3.6.1.4.1.800.3.1.1

### **\$TrapV1GenericID\$**

The generic trap number. This only applies to SNMP Version 1 traps.

### **Output Example: 6**

**\$TrapV1SpecificID\$** The enterprise trap number. This only applies to SNMP Version 1 traps.

### Output Example: 10

**\$TrapVariables\$** Describes all of the variables in the trap.

**\$TrapVariable[1]\$, \$TrapVariable[2]\$...** Accesses the first (second, etc.) variable in the trap.

### \$TrapVariable[someVariableName]\$

Accesses the trap variable by its name.