Getting Started with 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 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 containing the IP or MAC address of the offending device. (If an IP address is received, Quarantine Manager uses its Locator function to determine the device's MAC address.) These messages trigger Quarantine Manager Rules. Depending on the rule that is written for the event, the device can be immediately quarantined or placed in a Candidate List that can be reviewed by the Network Administrator for further action.

Note: Quarantine Manager cannot quarantine any devices on the EMP subnet because the EMP port has no mobility feature.

The following sections describe the requirements for getting started with Quarantine Manager.

Hardware/Software Requirements

Quarantine Manager is an optional add-on package to OmniVista 2500. It can be installed in the OmniVista 2540 Basic Single User environment or the OmniVista 2540 Basic Multi User environment. The hardware requirements for Quarantine Manager are the same as for OmniVista 2500. Version 5.1.6 of the AOS software is required for Trap Notification to work correctly; and Fortinet software version 2.3. is supported. Quarantine Manager supports all platforms currently supported by OmniVista 2500.

External Notification Device

An external device must be set up to send notifications to the Quarantine Manager application. For example, a Fortinet IPS device must be set up to send Syslog messages to Quarantine Manager. This set up includes specifying the IP address of the OmniVista server and the port address for the OmniVista Syslog daemon (preset default is 514); and specifying what events received by the IPS will generate a Syslog Message. The message (either Syslog message or trap) must include the IP or MAC address of the offending device. In addition, the Network Administrator must create a "Quarantine" VLAN and MAC group.

Note: See the applicable user manual (e.g., Fortinet IPS) or the OmniVista Notifications Application help pages (e.g., AOS switch) for more information on configuring the external device used for Quarantine Manager.

Quarantine VLAN

You must first use the VLANs application to configure a Quarantine VLAN containing the switches you want to monitor with Quarantine Manager. In addition, because VLANs cannot be used when Group Mobility is not enabled, you must also configure an ACL by creating a Quarantined MAC group. You can access the VLANs application by clicking the VLANs button in the Configuration tab.

Note: Quarantine Manager does not support ACLs on XOS machines.

Rules

Quarantine Manager Rules are configured for dealing with Syslog events and SNMP traps. The easiest way to use Quarantine Manager is to enable one of the Built-in Rules. The Rules determine which events from an external IPS or switch are propagated through the network. For example, when the IPS notices an attack, it generates a Syslog event. After receiving a Syslog message, Quarantine Manager uses the rules to determine what device generated the event and whether or not the offending device is immediately quarantined (Banned) or placed on the Candidate List to be reviewed by the Network Administrator. The way in which a device is quarantined depends on the action that is configured for the rule.

If a device is placed in the Candidate list, all traffic to the suspect device continues. The Network Administrator reviews each event in the Candidate list and decides what action to take. If a device is placed in the Banned list, it is quarantined until it is manually removed by the Network Administrator.

Note: There are a number of important devices in a network that a Network Administrator will never want to be quarantined. Use the Never Ban List to ensure that important devices are never quarantined.

Configuring Quarantine Manager

After initial set up is complete, Quarantine Manager is configured and managed using the the tabs shown and described below. Click the link for each tab for detailed configuration instructions.

work	Candidates B	anned	Never Ba	nned	Disabled Ports	Rules	Configuration	Responders	
uration	Quarantine List							168/168	
utty	Mac Address	ID a	ddrane	1	Timestame	1		1.00.100	
	080070 701904	10 252	201 1 20	Jan 3	2006 1:49:08 PM	<161>.19	n 31349.08 Mi	on date=2008-01	035me=13:491
ลิ	000056-000101	10.252	201.138	Jan 4	2006 2:17:35 PM	<1612.12	n 4 14 17 36 toj	on dates 2006-01	04 time=14:17:
	000111 735491	10 252	201 244	Jan 4	2006 2:32:22 AM	<161×1a	n 4.02.32.20 tei	on date=2008-01	-04 time=02:32:
User-	000112 28a526	10.252	201 242	Jan 3	2006 1:10:55 PM	<161>.10	n 3131055 tei	nn date=2006-01	03 time=13:10
	000252 d48208	10 252	201 17	Jan 3	2006 9:19:42 PM	<161>.la	n 3 71 19 47 tei	on date=2006-01	-03 time=21:19
	0003ca:e4022	1 10.252	211 119	Jan 3	2006 3 33 51 PM	<161>Ja	n 3153351 tei	on date=2006-01	03 time=15 33 f
	0003ca:e85451	10.252	211.94	Jan 3	2006 7:00:13 PM	<161>.la	n 3190013tei	on date=2006-01	-03 time=19:001
	080070 012406	10.252	201.142	Jan 3	2006 4:34:54 PM	<161>Ja	n 316:34:54 tei	on date=2006-01	-03 time=16:34 5
I	080070 b41785	10 252	201.37	Jan 3	2006 5:45:51 PM	<161»Ja	n 317:45:51 tei	on date=2008-01	-03 time=17:45
	080070ccdb46	10 252	201.81	Jan 4	2006 1:19:51 PM	<161>Ja	n 413:19:51 tel	on date=2006-01-	-04 time=13:19:
l	080070:cd0515	10 252	201.63	Jan 3	2006 5:23:52 PM	<161>Ja	n 317:23:52 tei	on date=2006-01	03 time=17:23
	080070/cf255b	10.252	201.116	Jan 4	2006 9:35:31 AM	<161>Ja	n 4 09:35:31 tei	on date=2006-01	04 time=09:35:3
	080070:cf47c8	10.252	.201.128	Jan 2	2006 2:51:56 PM	<161>Ja	n 214:51:56 tei	on date=2006-01-	-02 time=14:51:5
l	080070 cf7 ae4	10.252	211.111	Jan 4	2006 8:08:31 AM	<161>Ja	n 4 08:08:31 tej	on date=2006-01-	-04 time=08:08:3
	080070:cf7c8e	10.252	.211.43	Jan 3.	2006 1:46:39 PM	<161>Ja	n 313:46:39 tel	on date=2005-01	-03 time=13:46:3
l	080070 de9235	10.252	201.25	Jan 4	2006 11:29:31 AM	<161>Ja	n 4 11:29:31 tej	on date=2006-01	04 time=11:29:3
	090070 de923	10.252	201.86	Jan 3	2006 2:51:51 PM	<161>Ja	n 314:51:51 tej	on date=2008-01-	03 time=14:51:5
	080070:e2f908	10.252	201.176	Jan 4	2006 11:59:45 AM	<161>Ja	n 411:59:45 tej	on date=2006-01-	-04 time=11:59:4
l	080070:e90d09	10.252	211.34	Jan 4	2006 1:53:00 PM	<161>Ja	n 413:53:00 tej	on date=2006-01	04 time=13:53
1	080070:465726	10.252	211.139	Jan 3	2006 8:34:21 AM	<161>Ja	n 3 08:34:21 tej	on date=2006-01-	-03 time=08:34:3
	080070:ebcfc6	10.252	201.77	Jan 3	2006 2:16:26 PM	<161>Ja	n 314:16:26 tej	on date=2006-01	-03 time=14:16:3
l	080070 :8/2900	10.252	201.115	Jan 3,	2006 2:12:07 PM	<140>Ja	n 314:12:07 20	06 [192.168.249.	6] wms[421]: <w< td=""></w<>
i	080070 946300	10.252	201 153	Jan 3	2006 1:14:56 PM	<140>Ja	n 31314:56 20	06 (192.168.249.)	6] wms[421]: <w< td=""></w<>

Quarantine Manager Tabs

Quarantine Manger tabs are described below. Click the link for each tab for detailed configuration instructions.

- **Candidates** The Candidates tab displays a list of devices that have been flagged by an IPS or switch. The Network Administrator can release a device from the list, ban a device, or configure a device to never be banned.
- **Banned** The Banned tab displays a list of all devices that have been banned and isolated from the network.
- **Never Banned** The Never Banned tab displays a list of devices that have been configured never to be banned (e.g., mail servers, IPS). Note that all switches discovered by OmniVista are implicitly on the Never Banned List even though they are not displayed.
- **Disabled Ports -** The Disabled Ports tab displays a list of all devices whose ports have been disabled.
- **Rules** The Rules tab is used to configure the conditions that will trigger Quarantine Manager notifications and actions.
- **Configuration** The Configuration tab is used to configure the "Quarantine" VLAN and MAC group, as well as the action that will be taken for the event.
- **Responders** The Responders tab enables you to specify the responses, such as run an audio program or send an e-mail to the MIS director, based on the conditions given. Quarantine Manager Logs

The Audit application can be used to access the Quarantine log and Syslog. The logs contain detailed information about Quarantine Manager and Syslog events. Currently, if Syslog is in use, when launching Quarantine Manager, a warning message is displayed in server.txt that points to the Preferences application, where you can change Syslog.

Note: Aruba default logging to Syslog produces 2,000 messages per 20 minutes.

Quarantine Manager Candidates Tab

When an external Intrusion Prevention System (IPS), such as Fortinet, detects a possible attack on the network, it generates either a Syslog Event or an SNMP Trap. A Quarantine Manager rule can be configured (Configuration Tab) to trigger an action based on these events. The action will either immediately quarantine the offending device, or place the device on the Candidates List. If the device is placed on the Candidates List, traffic to and from that device will continue until the Network Administrator decides what action should take place.

The Candidates tab, shown below, displays all of the devices that have been placed in the Candidates list by Quarantine Manager (field descriptions are provided below). The Network Administrator can:

- Release the device from the Candidates List
- Ban the device
- Place the device on the list of devices to never be banned.

🖉 OmniVista 2500 - 🛛 Application: Q	uarantine Manager Window	w:0	
Elle Applications View QM Rul	es Hel <u>p</u>		
			a
Candidates Banned Never	Banned Disabled Ports	Rules Configuration Responders	
Quarantine List		168/168 🔞 🤝	
Mac Address IP Address	Timestamp	Reason	
080070:70190e 10.252.201.139	Jan 3, 2006 1:49:08 PM	<161>Jan 3 13:49:08 tejon date=2006-01-0)3 time= 🔺
00005f :000101 10.252.201.27	Jan 4, 2006 2:17:36 PM	<161>Jan 4 14:17:36 tejon date=2006-01-0)4 time=
000111 :735491 10.252.201.244	Jan 4, 2006 2:32:22 AM	<161>Jan 4 02:32:20 tejon date=2006-01-0)4 time=
000112:26a526 10.252.201.242	Jan 3, 2006 1:10:55 PM	<161>Jan 313:10:55 tejon date=2006-01-0)3 time=
000252:d48208 10.252.201.17	Jan 3, 2006 9:19:42 PM	<161>Jan 3 21:19:42 tejon date=2006-01-0)3 time=
0003ca:e4022f 10.252.211.119	Jan 3, 2006 3:33:51 PM	<161>Jan 315:33:51 tejon date=2006-01-0)3 time=
0003ca:e85451 10.252.211.94	Jan 3, 2006 7:00:13 PM	<161>Jan 319:00:13 tejon date=2006-01-0	13 time=
080070:01240e 10.252.201.142	Jan 3, 2006 4:34:54 PM	<161>Jan 316:34:54 tejon date=2006-01-0	13 time=
080070:b41765 10.252.201.37	Jan 3, 2006 5:45:51 PM	<161>Jan 317:45:51 tejon date=2006-01-0	13 time=
080070:ccdb46 10.252.201.81	Jan 4, 2006 1:19:51 PM	<161>Jan 4 13:19:51 tejon date=2006-01-0	14 time=
080070:cd0515 10.252.201.63	Jan 3, 2006 5:23:52 PM	<161>Jan 3 17:23:52 tejon date=2006-01-0	J3 time=
080070:cf255b 10.252.201.116	Jan 4, 2006 9:35:31 AM	<161>Jan 4 09:35:31 tejon date=2006-01-0	14 time=
080070:cf47c8 10.252.201.128	Jan 2, 2006 2:51:56 PM	<161>Jan 2 14:51:58 tejon date=2006-01-0	J2 time=
080070:cf7ae4 10.252.211.111	Jan 4, 2006 8:08:31 AM	<161>Jan 4 08:08:31 tejon date=2006-01-0)4 time=
080070:cf7c8e 10.252.211.43	Jan 3, 2006 1:46:39 PM	<161>Jan 3 13:46:39 tejon date=2006-01-0	/3 time=
080070:de9235 10.252.201.25	Jan 4, 2006 11:29:31 AM	<161>Jan 4 11:29:31 tejon date=2006-01-0	J4 time=
080070:de9237 10.252.201.86	Jan 3, 2006 2:51:51 PM	<161>Jan 314:51:51 tejon date=2006-01-0	13 time=
080070:e2f906 10.252.201.176	Jan 4, 2006 11:59:45 AM	<161>Jan 4 11:59:45 tejon date=2006-01-0)4 time= 👻
•	1		F
	Release Ban	Never Ban Help	

Candidates Tab

Note: When evaluating a candidate for Ban/Release, it is recommended that the Network Administrator check the quarantine.log file in the Audit application to see if any more serious events have been logged by the same end-station.

Releasing a Device from the Candidates List

To remove a device from the Candidates list, select the device and click the **Release** button. The device is removed from the list. A device may return to the list if another event triggers a configured quarantine rule.

Banning a Device

To ban a device from the network, select the device and click the **Ban** button. The device is removed from the network and placed in the Banned list. Click here for more information on banning a device.

Placing a Device on the Never Banned List

To place a device in the Never Banned list, select the device and click the **Never Ban** button. The device is placed in the Never Banned list. An event will never trigger a quarantine rule for a device in the Never Ban list. Click here for more information on the Never Banned List.

Candidates Tab Field Descriptions

Candidates Tab field descriptions are provided below.

Mac Address - The device's MAC address. Quarantine Manager Rules extract the IP address of the device. Quarantine Manager then uses the OmniVista Locator Function to determine the MAC address.

IP Address - The device's IP address. All Quarantine Manager Rules must extract the IP address from the Syslog Message or SNMP Trap. If the IPS sends a MAC address, the IP address will have a value of 0.0.0.0.

Timestamp - The date and time the event occurred.

Reason - The reason the event triggered a Quarantine Manager rule. For all Fortinet-generated events, select the event in the table and right-click to access a detailed description of the event. Click here for more information.

Quarantine Switch List - This field contains any switches that were **not** successfully included in a "Quarantine" sub-network.

Quarantine Manager Reason Description

You can access the Fortinet web site for a detailed description of any any Fortinet event. To access the description:

1. Click on the event in the table to highlight it; then right-click on the event. The Reason window will appear.

🛔 Reason	2
<161>Jan	-
3	
14:22:54	
tejon	
date=2006-01-03	
time=14:22:54	
device_id=FGT8002604400443	
log_id=0420070000	
type=ips	
subtype=signature	
pri=alert	
attack_id=107347972	
src=128.251.40.72	
dst=198.206.187.100	
src port=3499	
dst port=8080	
src int=external	
dst_int=internal	
hatrateheeteeteeteeteeteeteeteeteeteeteeteete	
proto=6	
The second se	
http://www.fort	.com//ds/10/04/972

2. Click on the Fortinet web address button at the bottom of the Reason window. A Fortinet In-Depth Analysis page will appear describing the event in detail and providing any recommended actions.



Quarantine Manager Banned Tab

When a device is placed in the Banned List, it is quarantined from the rest of the network. Devices can automatically be added to the Banned List based on a Quarantine Manager rule or manually placed in the list by the Network Administrator. Once a device is placed in the Banned List, it remains quarantined until the Network Administrator manually releases it.

The Banned tab, shown below, displays a list of all devices than have been quarantined, either by a Quarantine Manager rule, or by the Network Administrator. Field descriptions are provided below.

Applications	View QM Rules	s Help				
andidates B	anned Never B	anned Disabled Ports	Rules	Configuration	Responders	1
warantine List				1	55 😪 📾 🖨	周田口
Mac Address	IP Address	Timestamp	State	and the second	Reason	n 00.
00112:644708	10.252.201.241	Jan 3, 2006 2:22:54 PM	1202.05	<161>Jan 3	14:22:54 tejon d	ate=2006-0
80070:e85208	10.252.201.89	Jan 3, 2006 1:40:12 PM		<161×Jan 3	13:40:12 tejon d	ate=2006-0
80070:ccdb48	10.252.201.110	Jan 3, 2006 2:14:13 PM		<161×Jan 3	14:14:13 tejon d	ate=2006-1
	10 050 004 140	Iso 3, 2006 115-50 PM		<161>Jan 3	13:15:50 telon d	ate=2006-1
00252:048208	10.252.201.140	34113, 2000 1.13.30 PM		and the second second second second	of the Rent South State State State State State State	
00252:d48208 003ca:e47321	10.252.201.140	Jan 2, 2006 2:56:55 PM		<161×Jan 2	14:56:55 tejon d	ate=2008-
00252.d48208 003ca:e47321 (View Quarantin	10.252.201.24	Jan 2, 2006 2:56:55 PM		<161>Jan 2	14:56:55 tejon d	ate=2008-1
00252:d48208 003ca:e47321 (View Quarantin) IP Addres	10.252.201.24	Jan 2, 2006 2:56:55 PM		<161>Jan 2	14:56:55 tejon d	ate=2006-1

Note: In Release 3.0 and later, DHCP requests from a banned device are 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.

Note: Quarantine Manager now has the ability to ban devices connected to an OmniAccess WLAN device using the device's "Blacklist" feature. However, the 'enable' password of the device must be entered in the **Secondary Password** field of Discovery Manager Entry window in the **Topology** application.

Adding a Device to the Banned List

In addition to automatically quarantining devices based on a Quarantine Rule, you can also manually quarantine a specific device by adding it to the Banned List. To add a device to the Banned List:

1. Click the New button.

2. Select the applicable radio button and enter the device's IP Address (or host name) or MAC Address. Please note that you can enter the host name only if the **IP Address** radio button is selected.

3. Enter the reason you are placing the device on the Banned list in the Reason field.

4. Click the OK button. The device will appear in the list.

Editing a Device on the Banned List

You can edit the Reason field for a device in the Banned list. To edit the Reason field:

1. Select the device in the list.

2. Click on the Edit button and edit the Reason field.

3. Click the OK button. The new information will display in the device's Reason field.

Releasing a Device from the Banned List

To release a device from the Banned List:

1. Select the device in the list. (You can select multiple devices using the SHIFT or CTRL keys.)

2. Click the Release button. The device will be deleted from the list.

Redo Ban

Click the **Redo Ban** button to poll the network for banned switches. This is useful if you have banned switches without first creating a Quarantine VLAN or MAC Group.

Banned Tab Field Descriptions

Banned tab field descriptions are provided below.

Mac Address - The device's MAC address. Quarantine Manager Rules extract the IP address of the device. Quarantine Manager then uses the OmniVista Locator function to determine the MAC Address.

IP Address - The device's IP address or the host name. All Quarantine Manager rules must extract the IP address from the Syslog Message or SNMP Trap.

Timestamp - The date and time the event occurred.

State - The state of the banning action:

- Scheduled to be Banned (Ban is in process)
- Completed (Ban is complete)
- Partially Banned (Ban not completed for all devices)
- Scheduled to Be Released (Release is in process)
- Partially Released (Release not completed for all devices).

Reason - The reason the event triggered a Quarantine Manager rule. For all Fortinet-generated events, select the event in the table and right-click to access a detailed description of the event. Click here for more information.

Partial Results - The devices where the ban has either succeeded, or for which the user has not configured/enabled Quarantine Manager.

VLAN Name - The user-configured name for the Quarantine VLAN.

Mac Group Name - The user-configured name for the Quarantine Mac group.

Quarantine Switch List - This field contains any switches that were **not** successfully included in a "Quarantine" sub-network.

Quarantine Manager Never Banned Tab

A device placed on the Never Banned list can never be banned, either manually or automatically, by Quarantine Manager. Important network servers should be placed in the Never Ban list. The Never Banned tab, shown below, displays a list of all devices that have been added to the Never Banned list by the Network Administrator. Field descriptions are provided below.

Note: The OmniVista server and all switches discovered by OmniVista are implicitly placed in the Never Banned list. Even though these devices do not appear in the list, they cannot be banned.

Never Renned Teh

andidates Ba	nned Never Ban	ned Disabled Ports Rul	les Configuration	Responders	
uarantine List			35	35 🐄 📾 📰 🖽	I
Mac Address	IP Address	Timestamp	Reason	Quarantine Switch List	Т
80070:b41768	10.252.201.172.	Jun 29, 2005 7:47:19 AM	Pubs3		1
003ca:e2f915	10.252.201.129	Nov 18, 2005 8:44:17 AM	Genoa		1
80070:de9726	10.252,201.76	Aug 16, 2005 11:03:31 AM	Gohira		1
003fe:cf7ae6	10.252.201.232	Aug 16, 2005 9:21:21 PM	Delphi1		1
80070:cf254b	10.252.201.197	Mar 23, 2005 8:16:33 AM	Larry's Computer		1
00111:d47316	10.252.201.121	Jun 24, 2005 5:30:58 PM	Storage		1
80070:cf7ae2	10.252.201.100	Oct 28, 2005 2:57:57 PM	AINDBDC1		1
80070:ccdb46	10.252.211.157	Oct 19, 2005 11:23:05 AM	Olympus		1
80070:7224fe	10.252.201.222	Jun 24, 2005 8:57:13 AM	Warehouse		1
003ca:e4022f	10.252.201.121	Jul 14, 2005 11:34:36 AM	Ares		1
80070:70190e	10.252.211.6	Oct 19, 2005 1:25:21 PM	Insight		1
00252:d48216	10.252.211.111	Dec 5, 2005 8:27:22 AM	Salem-NT01		1
00112:26a453	10.252.201.89	Jun 24, 2005 1:58:38 PM	Sql1		1
0005f;735491	10.252.201.244	Jul 14, 2005 11:46:13 AM	Fax1		T
View Quarantine IP Address Mac Address 	object	Reason			

Adding a Device to the Never Banned List

To add a device to the Never Banned List:

1. Click the New button.

2. Select the applicable radio button and enter the device's **IP Address** (or host name) or **MAC Address**. Please note that you can enter the host name only if the **IP Address** radio button is selected. If you ban a device by the MAC address, the IP address will display a value of 0.0.0.0. If you ban a device by its IP address, Quarantine Manager will use its Locator function to determine the MAC address.

3. Enter a reason for placing the device on the Never Banned List in the Reason field.

4. Click the OK button. The device will appear in the list.

Editing a Device in the Never Banned List

You can edit the Reason field for a device in the Never Banned list. To edit the Reason field:

1. Select the device in the list.

2. Click on the Edit button and edit the Reason field.

3. Click the OK button. The new information will display in the device's Reason field.

Deleting a Device from the Never Banned List

To delete a device from the Never Banned List:

1. Select the device in the list. (You can select multiple devices using the SHIFT or CTRL keys.)

2. Click the Delete button. The device will be deleted from the list.

Never Banned Tab Field Descriptions

Never Banned Tab field descriptions are provided below.

Mac Address - The device's MAC address.

IP Address - The device's IP address or host name. If an Intrusion Prevention System (IPS) sends a MAC address, the IP address will have a value of 0.0.0.0.

Timestamp - The date and time the device was placed on the Never Banned list.

Reason - The reason the device is in the Never Banned list.

Quarantine Switch List - This field contains any switches that were **not** successfully included in a "Quarantine" sub-network.

Quarantine Manager Disabled Ports Tab

When a port is disabled, an entry appears in the Disabled Ports List table. If you attempt to ban multiple MAC addresses for the same switch's slot/port, multiple entries will appear in the table. The Disabled Ports tab shown below, displays a list of all devices whose ports have been disabled, either by a Quarantine Manager Rule or by the Network Administrator. Field descriptions are provided below.

umniVista 2500 -	Application: Quara	intine M	anåger Wir	0.wob			_ [
Applications	/iew QM Rules	Help					
		,					
Candidates Bar	ned Never Ban	ned C	isabled Por	ts Rules	Configuration	Responders	1
isabled Ports List)	0.0 😨 🗟	
Switch Addre	ss Slot	Port	IfIndex	Tì	mestamp	Mac A	ddress
6							
1			1				1
() View Disabled Po	rt Object		n				1
View Disabled Po View Disabled Po	rt Object		H	Slot:			
View Disabled Po Switch Address: Port:	rt Object			Slot: Mndex:			
View Disabled Po Switch Address: Port: Timestamp:	rt Object Jan 4, 2006 3:30:0	00 PM		Slot: Mindex: Mac Address	R :		
↓ View Disabled Po Switch Address: Port: Timestamp: Reason:	rt Object Jan 4, 2006 3:30:0	00 PM		Slot: Mndex: Mac Address State:	c : Scheduled t	o Disable	

Note: If you disable the port, that was already disabled, there will be two entries in the table. The first entry will contain the MAC address of the offending end station. The second entry will contain a null (possibly 000000:000000) MAC address. The reason for this second entry is that when you use the Banned tab to release a MAC address, the port will **not** be re-enabled. The Network Administrator will have to manually re-enable the port by releasing the port from the Disabled Ports tab.

Note: When you delete an entry from the Disabled Ports List table, the item will be removed. If it is the last item with the specified IP address and slot/port combination, then that port will be enabled. That is, the port will not be enabled until every device that caused it to be banned has been released.

Note: Use the **Configuration** tab to turn on port disabling; then use the Topology application to enable port disabling for each switch.

Editing a Device in the Disabled Ports List

You can edit the Reason and the Timestamp fields for a device in the Disabled Ports list. To edit the Reason and the Timestamp fields:

- **1.** Select the device in the list.
- 2. Click on the Edit button and edit the Reason and the Timestamp fields.
- 3. Click the OK button. The new information will display in the device's Reason and Timestamp fields.

Releasing a Device from the Disabled Ports List

To release a device from the Disabled Ports list:

- 1. Select the device in the list. (You can select multiple devices by using the SHIFT or CTRL keys.)
- 2. Click the Release button. The device will be deleted from the list.

Retry the Failed Operation

To retry the failed operation during the enabling/disabling of a port:

- **1.** Select the device in the list.
- 2. Click the Retry button. The failed operation will be retried.

Disabled Ports Tab Field Descriptions

Disabled Ports tab field descriptions are provided below.

Switch Address - The device's IP address. Quarantine Manager Rules extract the IP address from Syslog Message or SNMP trap.

Slot - The disabled slot number.

Port - The disabled port number.

IfIndex - The value of the slot/port numbers of the offending device that are disabled, which equals 1000 times the slot number plus the port number. This calculated value is applicable for Alcatel switches only.

Timestamp - The date and time the event occurred.

Mac Address - The device's MAC address. Quarantine Manager Rules extract the IP address of the device. Quarantine Manager then uses the OmniVista Locator function to determine the MAC address.

State - The state of the disabling or enabling action:

- Completed (Disabling is complete)
- Failed (Disabling/enabling of a port failed)

Reason - The reason a port was disabled.

Quarantine Manager Rules Tab

Quarantine Manager Rules determine which Syslog events or SNMP traps cause a device to be placed in the Candidates list or Banned list. A rule consists of:

- A name
- A description of the rule
- A trigger expression that specifies the event or trap that will trigger an action
- An extraction expression that is used to extract the source address from the event or trap
- An action to be taken when the event or trap is received (device is placed in the Candidates list or Banned list).

		jā.
andidates Bar	ned Never Banned Disabled Ports Rules	Configuration Responders
tule List		12/12 🕱 🕽 🖨 🔢 🖽 🛄
Name	Description	Trigger Expression
alaDoSTrap	Alcatel Denial of Service Trap	TrapName=alaDoSTrap
Arruba 1	The switch has classified an AP as a Rogue AP	FLAGGING AP with BSSID."as an Unsecure A
krruba 2	The AP/AM has detected a rogue AP as being active	Unsecure AP detected BSSID
krruba 3	The AP/AM has detected a rogue AP as being active	STA with MAC.*associating with Rogue AP BS
ortinet	Fortinet Signature	log_id=0420070000
ortinet Anomaly	Fortinet IDS Anomaly	log_id=0421073001.*status=[*t]
fortinet Signature	Fortinet IDS Signature	log_id=0420070000.*status=_[*t]
Fortinet Virus	Fortinet Virus Attack	log_id=0211060001
DA WLAN: Rogu	The switch has classified an AP as a Rogue AP	FLAGGING AP with BSSID.*as an Unsecure A
DA WLAN: Rogu	The AP/AM has detected a rogue AP as being active	Unsecure AP detected BSSID
(II. III. III. III. III. III. III. III.	•
View Quarantine	Rules	
lamo	Descriptions	
warne:	Description	
Trigger Expressio	en: Extraction Extract	xpression:
Action:	Candidate List. 💌 Enabled:	false
Event Type:	Syslog	

Note: Banned rules have precedence over Candidate rules. If an event matches more than one rule, Quarantine Manager will match the first rule that places a device on the Banned list. If there is no rule that places the item on the Banned list, Quarantine Manager will match the first rule that places the device on the Candidate list.

Rule Types

There are two types of rules: Built-In Rules and Custom Rules. The Built-In Rules cannot be deleted (although they can be modified or disabled). Custom Rules are rules that the Network Administrator creates. The Network Administrator can create a new rule, edit a rule, delete a rule, or import a rule.

Built-In Rules

There are seven Built-In Rules that come with Quarantine Manager. You must change the "Enabled" status to "True" to enable these rules. The default action configured for all of the Built-In Rules is to send the device to the Candidates list for review by the Network Administrator. Although the rules are preconfigured, the Network Administrator can modify the them. Built-In Rules are initially configured in the Disabled state. The Built-In Rules are:

- Alcatel DOS Trap Rule Triggers an action based on an AOS trap (AlaDosTrap). The rule triggers an action in response to a Teardrop, Ping of Death, or Port Scan attack.
- Fortinet Anomaly Triggers an action on a Fortinet Attack Anomaly Event. Ignores Anomaly attacks configured to "Pass" on Fortigate.
- Fortinet Signature Triggers an action on a Fortinet Syslog Signature event. Ignores Signature attacks configured to "Pass" on Fortigate.
- Fortinet Virus Triggers an action on a Fortinet Virus Detection event. Only triggers on sub-type "infected".
- OA WLAN: Rogue AP Active Triggers an action when the switch classifies an Access Point as a "Rogue AP."
- OA WLAN: Rogue AP Detected Triggers an action when the Access Point detects an active "Rogue AP."
- OA WLAN: Station w/ Rogue AP Triggers an action when the Access Point detects traffic from a client through a "Rogue AP."

Fortinet Anomaly and Signature attack events include a "status=" attribute that can be "clear_session", "pass_session", "dropped", "reset", or "detected". When Fortigate is configured to allow a particular attack (using the GUI to set its action to "Pass"), a Syslog event is still sent out for that attack, but its status is "detected"; meaning it is detected but not acted upon. Our built-in triggers are therefore designed to act on any value of "status=" EXCEPT for "detected". This means you can use the Fortigate control panel to selectively enable or disable attack actions and Quarantine Manager will behave consistently, without the need to change any of these triggers.

The Canned rules in Quarantine Manager for Fortigate have been modified as such, in both the anomaly and signature rules.

log_id=0421073001.*status=[^p].[^t]

log_id=0420070000.*status=[^p].[^t]

The [^p] was added to exclude any Syslog message starting with a "p" character, as well as a "t" character. This prevents quarantine for both "detected" and "pass_session" status.

The "pass_session" state was previously unknown.

Note: The Audit application can be used to access the Quarantine log and Syslog. The logs contain detailed information about Quarantine Manager and Syslog events.

Custom Rules

The Network Administrator can create Custom rules using Regular Expressions to configure the trigger event and extraction expression. The rules can be based on an Intrusion Prevention System (IPS) event or an AOS SNMP trap notification.

Note: You must be careful when creating a rule since a misconfigured rule could cause an important service to be inadvertently banned.

Creating a New Rule

To create a new rule, click the **New** Button and complete the Quarantine Rules Parameters. When you have completed all the fields, click the **OK** button, then click the **Apply** button to write the rule to the server.

Editing an Existing Rule

To edit an existing rule, select the rule and click the **Edit** button. Edit the applicable Quarantine Rules Parameter(s), click the **OK** button, and then click the **Apply** button to write the changes to the server.

Deleting a Rule

To delete a rule, select the rule (use the **SHIFT** or **CTRL** keys to select multiple rules), click the **Delete** button, and then click the **Apply** button.

Importing a Rule

You can import a new rule from Alcatel without having to update the Quarantine Manager code. New rules are sent by Alcatel as .xml files.

1. Save the .xml file on your machine.

2. Select Import from the QM Rules drop-down menu or click the Import icon.



An Import window will open in the OmniVista directory.

Open		
Look in: 📑	Alcatel OmniVista 2500	
📑 bin		C UninstallerData_PolicyView_QoS
📑 classes		📑 UninstallerData_Quarantine_Manage
📑 clientdata		UninstallerData_SecureView_ACL
📑 data		UninstallerData_SecureView_SA
📑 jre		🗋 backuprestore.xml
📑 openidap		
📑 Uninstalle	rData	
the Manual		
nie Mame:		
Files of Type:	XML files (*.xml)	
		Onen Concol

Use the Look In pulldown menu to browse and locate

Click the Open button.

3. Browse to the .xml file that you saved, select the rule and click the **Open** button. The Import window will close and the new rule will appear in the Rules table.

Note: Imported rules are initially configured in the Disabled state. You must change the "Enabled" status to "True" to enable the rules.

Rule Parameters

The Quarantine Manager Rule parameters are described below.

Name - The user-defined name for the rule.

Description - The user-defined description for the rule.

Trigger Expression - A regular Java expression that is used to determine if a Syslog message or SNMP trap should trigger a quarantine action. If a Syslog message or SNMP Trap matches this regular expression, the action is performed. The regular expressions used by OmniVista are very similar to those used by programs such as PERL and AWK. See http://java.sun.com/docs/books/tutorial/extra/regex/intro.html for more information on using regular expressions. Click here for more information on Regular Expressions.

Extraction Expression - A regular Java expression that specifies the source address of the suspect device. Use the () expression to capture the source IP or MAC address. (Quarantine Manager also supports the hex form of IP addresses.) Once Quarantine Manager receives a Syslog message or SNMP trap that matches a Trigger Expression, it must extract from it the source address of the suspect end station. Click here for more information on Regular Expressions.

Note: You can check the **server.txt** file to verify that your Extraction Expression is functioning properly.

Action - The action to be taken when the rule is triggered:

- **Candidate List** The device is added to the Candidates list. The device can still send and receive traffic. The Network Administrator reviews the list and determines what action to take (e.g., remove the device from the list, ban the device)
- **Quarantine** The device is moved to the Quarantined VLAN and/or MAC Group, and added to the Banned list. While on the Banned list, the device cannot send or receive traffic. The device remains on the list until it is manually removed by the Network Administrator.
- **Release** The device is released from the Quarantined VLAN and/or MAC Group. This can be used to allow an external system (e.g., Trouble Ticket System) to send a syslog message or trap to OmniVista to automatically release a quarantine without having to access OmniVista.

Note: The Quarantine VLAN or MAC group must be properly set up for traffic to be quarantined. If you do not first configure a Quarantine VLAN or MAC group, even a device on the Banned list could still pass traffic. The Quarantine VLAN or MAC group is configured in the Configuration tab.

Enabled - Administrative state of the rule:

- **True** The rule is enabled.
- False The rule is disabled.

Event Type - The type of triggering event (Syslog or Trap).

Regular Expressions Overview

Trigger Expressions

As stated earlier, a Trigger Expression is a regular Java expression that is used to determine if a Syslog message or SNMP Trap should trigger a quarantine action. If a Syslog Message or SNMP Trap matches this regular expression, the action is performed. For example, let's say that we are interested in a Fortinet Syslog Event that looks something like:

Fortinet Anomaly 03-08-200 14:09:34 device_id=FG36002805033253 log_id=0421073001 type=ips subtype=anomaly pri=critical attack_id=102039582 src=90.0.0.10 dst=10.10.10.100 src_port=2370 dst_port=139 src_int=internal dst_int=external status=dropped proto=6 service=139/tcp msg="netbios: SMB.NTLMSSP.Attempt.B

Many Syslog messages appear similar. However, each message may have a different date, device ID, source and destination address, etc. What is unique about each Syslog message is the log_id value. If you are interested in all Fortinet Syslog messages with a log_id of 0421073001, then the regular expression is easy - you can simply search for any message that contains the String log_id=0421073001. In the Trigger Expression Field you would type the value

log_id=0421073001.

Extraction Expressions

As stated earlier, an Extraction Expression is a regular Java expression that specifies the source address of the offending device. Once a Syslog message matches a Trigger Expression, Quarantine Manager must extract the source address of the suspect end station from the message. In our the Fortinet example above, the source address is preceded by the string "src=" and then an IP address. An IP address consists of 4 sets of numbers separated by the "." character. Each set is 1 to 3 characters in length and the numbers are decimal (0-9) digits. One way to express this is with the regular expression

 $src=([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}]$

Because we are only interested in the IP address and not the characters "src=", place () around the IP address to indicate which part you want to capture. The [0-9] means any single character from 0-9, the $\{1,3\}$ means that you are looking for a set of 1 to 3 numbers. The \. says that you are looking for a "." character. The backslash is an escape character that says take the "." literally (normally "." is a special character that means any character.

Often there are a number regular expressions that you can use to achieve the same results. In the Fortinet example above, there is the string "src=" followed by the IP address, followed by either a space or a tab character. The regular express for getting the IP address could be

 $src=([^]*)$

The characters between the [] are $^$, a space character and a tab character. This expressions says: the string "src=" followed by a sequence of characters that are not spaces or tabs. This expression works well, but is can be difficult to read because the space and tab character are not "visible".

Another way to extract the IP address would be

src=([0-9.]*)

This says, the string "src=" followed by a sequence of characters that contain only numbers and the "." (a "." inside of [] does not need to be escaped).

Note: If an extraction expression is not working, check the server.txt file to troubleshoot the problem.

Useful Operators for Quarantine Manager Rules

^ the "not" operator

[start of character list] end of character list

(beginning of an expression) end of an expression

[.] useful for escaping characters used as operators in regular expressions

Basic Regular Expressions

. Matches any single character

[...] Matches any one of the characters enclosed between the brackets. If the first character is a circumflex (^), then it matches any one character Not enclosed between the brackets. A hyphen (-) is used to indicate a range of characters.

- \Escape the special character that follows.
- * Matches any number (including none) of the single character that immediately precedes it.
- + Matches one or more occurrences of the preceding regular expression.
- ? Matches zero or one occurrences of the preceding regular expression.

For example:

- [abc] Matches either an 'a', 'b' or 'c'
- **[a-z]** Matches all lower case letters
- [a-zA-Z] Matches all letters
- [0-9a-fA-F] Matches all hex digits
- [^0-9] Matches any character that is not a digit

Quarantine Manager configures a maximum of 32 MAC rules when it is trying to ban 100 IP addresses on XOS devices. Quarantining using XOS devices is limited by the number of MAC rules supported by these devices, which is 32. This means that even if you attempt to quarantine 100 end-stations, only the first 32 will be quarantined on the XOS switches in the management domain. To avoid this limitation, release quarantines as soon as possible.

Quarantine Manager Configuration Tab

The Configuration tab is used to configure the Quarantine VLAN and Quarantine MAC groups. By default, the name of the Quarantine VLAN is "Quarantined". However, you can change the name as desired. The VLAN is created using the OmniVista **VLANs** application, which opens when you click the **VLANs...** button at the bottom of the page. The Quarantine MAC group is created using the Omnivista **Groups** and **SecureView ACLs** applications.

In order for Quarantine Manager to use SecureView ACL, you first create an L2 MAC group (which has a MAC group that matches the MAC group name specified in the Configuration tab of Quarantine Manager) using the **Groups** application. After creating the MAC group, you create an ACL rule using the **SecureView ACLs Expert Wizard**, which drops traffic if it finds a matching MAC address. For instructions on setting up an ACL using the **SecureView ACLs** application, click here.

Note: The Quarantine Manager ACL feature is not currently supported for OS6200 devices. Quarantine Manager support for these devices is based on creating VLAN MAC Rules. The user creates a Quarantine VLAN and an associated MAC Group. If Quarantine Manager needs to ban a MAC Address on the device, it adds the new MAC Address to the Group specifying the Quarantine VLAN ID. This will result in traffic moving to Quarantine VLAN based on the MAC Rule.

ACL has been extended to include ACL rules that have been stored in the OmniVista LDAP server through the **SecureView ACLs** application. When Quarantine Manager attempts to quarantine a device, it first checks the LDAP server for a MAC group with a specified name. If the MAC group exists, Quarantine Manager quarantines the device by adding the MAC address to the MAC group on the LDAP server. If the MAC group does not exist, Quarantine Manager adds the MAC address to the Quarantine MAC group you have created on the switch. Note that Quarantine Manager does not support ACLs on XOS machines.

Note: Quarantine Manager now has the ability to ban devices connected to an OmniAccess WLAN device using the device's "Blacklist" feature.

When devices are banned, either through a Quarantine Manager rule or by the Network Administrator, they are added to the Quarantined VLAN and/or Quarantine MAC group. These devices no longer route traffic. The devices remain in the Banned list until removed by the Network Administrator.

Note: You can create a logical "Quarantine" subnet to limit Quarantine Manager actions to a specific set of switches.

Applications View QM	Rules Help	
andidates Banned New	ver Banned Disabled Ports Rules Con	figuration Responders
uarantine Action		1/1 🥵 📾 🛃 🎞 🗉
VLAN Name	Mac Group Name	Allow Port Disabling
View Object		
View Object /LAN Name:	Mac Group Nam	BC
View Object VLAN Name:	Mac Group Nam	BC

Configuration Tak

Configuring the Quarantine VLAN/MAC Group

You must first use the VLANs application to configure a Quarantine VLAN containing the switches you want to monitor with Quarantine Manager. In addition, because VLANs cannot be used when Group Mobility is not enabled, you must also configure an ACL by creating a Quarantined MAC group.

1. Create the Quarantined VLAN using the OmniVista VLANs application.

- Click the VLANs... button to open the VLAN application and the VLAN wizard. •
- Create the "Quarantined" VLAN following the steps in the VLAN wizard. You can accept the next available VLAN number or enter a new VLAN number; however, you cannot use a number for the VLAN. You must give the VLAN a name (e.g., Quarantined). When adding devices to the VLAN, you must add all the devices that you want to monitor with Quarantine Manager.

2. Create the Quarantined MAC group using the **Groups** application. Create a **Source** MAC group and associate it with a QoS rule to **Deny** any traffic originating from MAC addresses in this group using the SecureView ACLs application. When a rule extracts an IP address from a device, OmniVista uses the Locator function to determine the MAC address of the device. The device is then automatically added to the Quarantined MAC group.

Note: For instructions on setting up an ACL using the SecureView ACLs application, click here.

3. Click the VLAN name in the Quarantine Action table, and then click the Edit button.

4. If necessary, edit the name of the VLAN to match the name of the VLAN you created in Step 1. Then, add or edit the MAC group name to match the name of the MAC group you created in Step 2.

5. Click the Apply button to write the changes to the server.

Note: Quarantine Manager cannot quarantine any devices on the EMP subnet because the EMP port has no mobility feature.

Editing the Quarantine VLAN/MAC Group

You can change the name of your Quarantined VLAN/MAC group by selecting the name in the list and clicking the **Edit** button. When you have completed the name change, click the **Apply** button to write the change to the server.

Note: The names you configure in this tab must match the names you use when you create the VLAN/MAC group. In Quarantine Manager, VLAN names are case-insensitive.

Please note that switches discovered after the 'Quarantined' VLAN is created cannot be added via VLANs. Also, there will be no warning message when you add the VLANs manually to the switches. Add 'Quarantined' VLAN to switches to protect them. It is not necessary that all the switches should be included in the 'Quarantined' VLAN. It is a decision that is up to the Network Administrator. If you want to include all the discovered switches in the 'Quarantined' VLAN, create a CLI script and run it periodically.

Configuring Quarantine Manager on OmniAccess WLAN Devices

Quarantine Manger can ban wireless devices connected to an OmniAccess WLAN device by placing them in the OmniAccess "Blacklist". If wireless device(s) is found in a Quarantine Segment, the MAC address of the Quarantined device is placed in the blacklist. Due to limitations in the current OmniAccess device's SNMP implementation, the banned device is placed on the blacklist using SSH to send CLI commands to OmniAccess. SSH must be able to login to the OmniAccess device. In addition, the OmniAccess device's 'enable' command must be executed and a secondary password is required to entry the privileges commands necessary to perform the blacklist. To enable automatic login, configure a valid user name and password for the OmniAccess device using the **Topology** application.

1. Open the **Topology** application, click on the **Switches** node, right click on the device you want to configure and select **Edit**. The **Edit Discovery Manager Entry** window appears.

		😵 😂 Switches 💌	6
Devices Manual Links Active Links Subnets Switches Cogical Network	Edit Discovery Manager Entry General SNMP Settings Name: Telnet/FTP User Name: Can Be Seen By Administrators Default Network Administrators Writers OK	IP Address: ID 255 11 111 Telnet/FTP Password: Intervention Secondary Password: Intervention SNMPv2 Intervention Links Discovery Intervention Handle as an OEM Device Intervention Shell Window Intervention Quarantine Intervention Allow Port Disabiling Intervention	Sta

Configuring OmniAccess for Quarantine Manager

- 2. Enter a user name in the Telnet FTP User Name field.
- 3. Enter a password in the Telnet/FTP Password field.
- 4. Enter a secondary password in the Secondary Password field.
- 5. Click the OK button.

Creating Quarantine Subnets

If a device is banned either by the Network Administrator or Quarantine Manger, the ban is applied to all devices in the network. However, you can segment your network by creating a logical "Quarantine" Network. This will limit Quarantine Manager actions to only those switches in the "Quarantine" subnetwork(s).

1. Use the Topology application to create a Logical Network named "Quarantine".

2. Create a sub-network or networks to segment the "Quarantine" network (e.g., "Quarantine Test", "Quarantine Engineering").

When Quarantine Manager is notified of an offending end station, Quarantine Manager determines the device directly connected to that end station and applies the ban to all switches in that switch's Quarantine subnet(s). For example, if a switch in the "Quarantine Test" subnet is connected to an offending device, Quarantine Manager will apply the ban to all of the switches in the "Quarantine Test" subnet.

Note: Network segmentation does not work if the **SecureView ACLs** application is used to create the ACLs for Quarantine Manager. The **SecureView ACLs** application overrides the Quarantine Manager network segmentation setup.

Enabling/Disabling the Quarantine Port

You can enable or disable a port rather than create a VLAN or ACL rule. In addition to the VLAN name and Mac group name, an **Allow Port Disabling** check box is available for enabling or disabling a port in the Configuration tab. By default, this checkbox is disabled. If the checkbox is checked, it means that you want to disable the port when a Quarantine rule is matched. Please note that you must turn on port disabling for each switch in addition to turning on global port disabling.

Note: Port disabling looks for Locator Live Search information and does not look for historical information.

🖉 Omni¥ista 2500 -	Application: Quarantine N	1anager Window:	0			
Elle Applications	View QM Rules Help					
						a
Network	Candidates Banned	Never Banned	Disabled Ports	Rules	Configuration	Responders
Configuration	Quarantine Action					
Security	VLAN Name		Mac Group N	lame		Allow Port Disabling
0	Quarantined	QM M	AC Group			true
6						
Users and User						
Groups						
0						
a						
Authentication						
Servers						
0						
i						
SecureView ACLs						
~						
SecureView SA						
	View Object					
	VLAN Name:			Mac Gro	up Name:	
w w					- ap trainer	
Quarantine Manager	Allow Port Disabling:	Talse				
manager ▼		Edi	VLANS	Appt	Help	
Administration				- Carded	Ted.	

Configuration Tab

To enable port disabling, click the Allow Port Disabling checkbox.

You can also enable/disable a port from the Topology application. To do this, right-click the desired switch in the Topology application and select **Edit**. The **Edit Discovery Manager Entry** window appears. To enable port disabling, check the **Allow Port Disabling** checkbox.

General SNMP Settings	1	
Name: [Telnet/FTP User Name: [Trap Station User Name: [0x2_NM3	IP Address: 10.255.11.144 Tetnet/FTP Password: Secondary Password:
Can Be Seen By Administrators Default Network Administrator Writers	5	SNMP Version SNMPv2 IIInks Discovery Handle as an OEM Device Shell Window Prefer SSH Quarantine Allow Port Disabling

To enable port disabling, click the Allow Port Disabling checkbox.

You can disable the ports for a switch that is on the "Quarantine" logical network and allows ports to be disabled. By default, all switches prohibit port disabling. You must specifically enable this feature for all ports to be disabled.

Setting up an ACL

To set up an ACL using the SecureView ACLs application, follow the steps given below:

- 1. Start the Groups application and click the L2 MAC Groups tab.
- 2. Click the New button. The Create a MAC Group dialog box is displayed.

ork	Set Groups
ration	L2 MAC Groups L3 Network (IP) Groups L4 Service Groups
Manager	MAC Group Definition MAC Group Name MAC Group Status
	MAC Group Name: Ouarantined
e e	Group Member MAC Address
* 005	
8	New Edit Delete Apply Help

3. In the **MAC Group Name** field, enter the name that is displayed in the **MAC Group Name** field of the **Configuration** tab in Quarantine Manager.

Note: The MAC group names created in both the Quarantine Manager and Groups applications must match.

- 4. In the Create a MAC Group dialog box, click the New button.
- 5. Enter a MAC address in the Group Member MAC Address field.
- 6. Click the Apply button to apply the changes to the LDAP repository.
- 7. Click the **OK** button to dismiss the dialog box.

8. To create an ACL rule to drop traffic, start the SecureView ACLs application and click the Expert tab.

9. In the Existing ACL Policies panel, click the New button to display the SecureView ACL Expert Wizard window.

ubbications Ten unifi	-						
	0						
Network One Touct	Expert						
SecureView AEL Expert Wiz	ard						ļ
Configuration for Policy							
Policy Na	me: Quarantine	d	Policy	Precedence:	30,001		
			nable 🗌 🖌 Impor	e Dolicy Enable			
				er oney chaine			
			Save 🔄 🗹 Ignor	e Policy Save			
		Log Ma	tches 🗌 🗹 Ignor	e Policy Log M	atches		
		Dat	Institute Concerning	a Dolicy Deflay			
		1983	iesave 🗌 💌 ignori	e Policy Reliex	we		
Configuration for Devices -							
Devices available for this P	olicy Configurati	ion		Devices to r	ecelve t	his Policy Confir	uration
Conces available for this r	oncy comigniou			Devices to i	occive i	ins roncy coming	
Name	Address	DNS Name		Nam	0	Address	DNS Name
DCTestnetCore	10.255.10.3	CITE ITALIE		WW FUL	12 129	10.255.11.129	arts rearies
NMS_HAWK_102	10.255.11.102			Hawk_1	51_sw1	10.255.11.151	
no-name	10.255.11.111		Addass	0mniSw	ritch	10.255.11.244	
Kite	10.255.11.112		Add >>	A CONTRACTOR OF STREET			
AOS_Hawk_157_alias	10.255.11.157		ee Domean	1			
lanswitch	10.255.11.172		22 Dramoon				
CmniSwitch_198_xyz	10.255.11.198		0.000 000 000				
B OS6602-24	10.255.11.207	1	Constraint of the second				
to lanswitch	10.255.11.252		<< Remove All				
		80					
215		1.1.1					
4	- T	1.		4			

10. In the Policy Name field, enter a policy name such as "Quarantined".

11. Select the switches to which you want to apply this policy and then click the Add button.

12. Click the **Next** button to create a policy condition.

13. Click the L2 MACs tab.

🛃 Omni	Vista 2500 - App	lication: Sec	ureYiew ACLs Wind	0wc0			_10);	×
Elle Ap	oplications View	Help						
							6	
Net	twork One	e Touch	Expert					1
Cor	SecureView AE	L Expert Wiz	ard				×	1
5	Set Conditions fo	r Policy Qua	rantined	No.	1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -		<u>^</u> P	
	L1 Interfaces	L2 MACs	L2 VLANS L31	Ps L4 Services	Validity Period			
User		ſ	Source MAC Addre	sses				
ALD			 Single 	1	. Group			
4			MAC Address:		MAC Group:	Quarantined		
			Ignore Source I	MACs in defining Po	licy Condition		- E	
Securi		Ĩ	Destination MAC Ad	ldresses				
			(8) Single		O Group			
Secu			MAC Address	÷ [MAC Group:			
			🗹 Ignore Destinat	ion MACs in definin	g Policy Condition		-	
Adh		Ļ						
EtiMa	•							
State			< Back	Next > Einis	h Cancel He	lp		-1
2-	an secures	WINCLS				au 2 0		

14. In the Source MAC Addresses panel, uncheck the **Ignore Source MACs in defining Policy Condition** checkbox. This will enable the other controls in this section.

15. Click the **Group** radio button.

16. In the **MAC Group** dropdown list select the Quarantined MAC group. This name should be the same as that entered in Step 3.

17. Click the **Next** button to create a policy action.

Note: If you select a switch in Step 11 that does not support the MAC group, an error will be displayed. You must go back and remove the switch from the selection list.

A Constant I man			
Cone Touch Expert			
SecureView ACL Expert Wizard			
tions for Policy Quarantined			
Access Control			
A	cessibility: ACCEPT 🔻		
	ACCEPT		
205 Parameters	DROP		
Shared Queue:	🗌 🗹 Ignore sharëd qu	ueue on egress	
aress Values			
Output Flow Setting			
Min Output Rate (kbits/sec):	🗹 Ignor	re minimum limit on egr	ess
Max Output Rate (iduits/sec);	🔽 lanor	re maximum limit on eq	ress
	1.2		1000 A
Output Mapping			
002 to Drively Laure	1 Immere 002 4	In on Farmer	
ouz. ip Prinniy Leves	· · · · · · · · · · · · · · · · · · ·	ip on cyress	
Differentiated Services Code Point	gnore DSCP	in defining Policy Actio	n
O TOS Precedence	gnore TOS	Precedence in defining !	Policy Action
O TOS Precedence	÷ Ignore TOS I	Precedence in defining I	Policy Acti

18. In the Access Control panel, select "DROP" in the Accessibility field.

19. Click the **Next** button.

20. Review the policy and then click the **Finish** button to save the policy to the LDAP repository. You will be returned to the **Expert** tab.

21. Click the **Notify** button to allow the switches to recache their policies.

Quarantine Manager Responders Tab

The Responders tab enables you to specify the response, such as external emails or scripts to be run (if any) that you want OmniVista to provide when quarantine actions are taken. This will provides a method to integrate with trouble-ticket systems. You can specify the events to which OmniVista will respond by using a trigger level. OmniVista can make the following responses to the receipt of a specified event:

- OmniVista can send an e-mail to any address you specify. You can use variables to specify the information you want to include in the e-mail. Variables exist for information, such as action, reason, MacAddress, etc.
- OmniVista can execute an external program or script on the OmniVista server.

To configure an OmniVista event response, select **Responders** in the Quarantine Manager window. The **Automatic Event Responders** panel is displayed, as shown below. The upper part of the panel contains a table with all the current responders. The lower part of the panel contains two tabs, the **Condition** tab and the **Response** tab. The **Condition** tab is used to specify the events that will trigger OmniVista's response; and the **Response** tab is used to configure the response. The user can create, modify, or delete the responders.

and the second sec

ndidates Ban	med Neve	r Banned	Disable	ed Ports	Rules	Confi	guration	Respo	onders	
tomatic Event Re	esponders							1	A	
Banned	1	Relea	sed			Res	ponse De	escription	1	
iew QM Conditio Condition Re	n and Respo	nse								
fiew QM Conditio Condition Re	n and Respo	nse Eve	nts whic	ch match	these trip	ggers:				
iew QM Conditio Condition Re Banned:	n and Response	nse Eve	nts whic	ch match	these trip	ggers:				_
Tiew QM Conditio Condition Re Banned: Released:	n and Respo sponse	nse Eve	nts whic	ch match	these trip	ggers:				
iew QM Conditio Condition Re Banned: Released:	n and Respo sponse	nse Eve	nts whic	ch match	these trip	ggers:				v

For example, when a specified event is received, you can configure the following responses:

- OmniVista can automatically send an e-mail to the MIS director. The body of the e-mail can contain the details of the event.
- OmniVista can automatically run an audio program that announces out loud: "You have received an event."

Note: You must set the mail server in the Preferences application.

How to Configure an Event Responder

To configure a new event responder, click the **New** button at the bottom of the Event Responder window and refer to the sections below.

The Condition Tab

You can specify the events to which OmniVista will respond based on the trigger level. The **Condition** tab allows you to select whether you want to be notified when devices are banned, or released, or both banned and released.

Applications y	jew QMR	Ø	, III						
ndidates Banı	ned Neve	er Bann	ed Disa	abled Ports	Rules	Configuratio	n I	Responders	1
omatic Event Re Banned	sponders	I	Released			Response	Desc	ription	
reate OM Conditi	ion and Res	nonse							
reate QM Condition	ion and Res	ponse							
reate QM Conditi Condition Re	ion and Res sponse	ponse	Events v	which matc	h these trij	Igers:			
reate QM Conditi Condition Res Banned:	ion and Res sponse ignore	ponse -	Events v	which mate	h these tri	igers:			•
reate QM Conditi Condition Res Banned: Released:	ion and Res sponse ignore ignore	ponse -	Events v	which matc	h these tri	igers:			v
reate QM Conditi Condition Re Banned: Released:	ion and Res sponse Ignore ignore	ponse -	Events v	which matc	h these tri	igers:			•

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** or to **Run an application on the server**. Continue as described in the appropriate section below.

	6 6	1				4
		n Variante da sera	Value	Vara	Va	-
andidates Banned	Never Banned	Disabled Ports	Rules	Configuration	Responders	
utomatic Event Respon	ders				8	[]]][]]][]]][]]][]]][]][]][]][]][]][]][
Banned	Re	leased		Response De	escription	
Create QM Condition a	nd Response					
Create QM Condition a Condition Respon Response Description:	nd Response					
Create QM Condition a Condition Respon Response Description: Response Action:	nd Response se Send an e-mai	đ				
Create QM Condition a Condition Respon Response Description: Response Action: E-mail To:	nd Response se Send an e-mai	a and a second sec				
Create QM Condition a Condition Respon Response Description: Response Action: E-mail To: E-mail Subject:	nd Response	ı 				

Response Tab

To Send an E-Mail

If you set the Response Action field to **Send an e-mail**, follow the steps below to define the email to be sent. It is important to note that all fields in the Sending E-Mail window in the Preferences application MUST be complete, or the emails you define will not be sent. To display the Sending E-Mail window, select **Sending E-Mail** in the Preferences application, which is part of the Administration group of applications.

Jmni¥ista 2500 - Applic	ation: Quarantine	Manager Window	v:0			
Applications View	QM Rules Help					
						4
andidates Banned	Never Banned	Disabled Ports	Rules	Configuration	Responders	1
utomatic Event Respon	lers				8	JE 1999 1000
Banned	Rele	ased		Response De	scription	
Create QM Condition an	d Response					
Create QM Condition an Condition Respons	d Response					
Create QM Condition an Condition Respons Response Description:	d Response					
Create QM Condition an Condition Respons Response Description: Response Action:	d Response e Send an e-mail					
Create QM Condition an Condition Respons Response Description: Response Action: E-mail To:	d Response e Send an e-mail					
Create QM Condition an Condition Respons Response Description: Response Action: E-mail To: E-mail Subject:	d Response					
Create QM Condition an Condition Respons Response Description: Response Action: E-mail To: E-mail Subject: E-mail Body:	d Response					
Create QM Condition an Condition Respons Response Description: Response Action: E-mail To: E-mail Subject: E-mail Body:	d Response	Default	Cancel	Help		

Response Tab

1. Enter a response description.

2. Enter the address to which the email will be sent in the **E-mail To** field. (The "From" address in the responder emails is determined from the entry in the **Use "From" Address** field in the Sending E-mail window of the Preferences application.)

3. Enter a subject for the email that is to be sent in response.

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

5. Click on the OK button. The new automatic event responder is saved to the session memory and is listed in the Automatic Event Responders table as an unsaved change. Click on 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.

andidates E	Banned	Never Ban	ned Disabl	ed Ports	Rules	Configuration	Responders	
utomatic Even	Responde	ers					6	
Ban	ned	Sach	Released			Response De	scription	ana ana
Response Acti Command: Arguments:	onc	Run an app \$MacAddre	dication on the	server				
Start Directory	c							
		\$Details\$	Į.					ŝ

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, which is the variable \$MacAddress\$ (explained in the Event 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, which is the variable \$Details\$ (explained in the Event Variables section below).

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

Event Variables

When sending an email, you can specify the following variables in the E-mail Body field:

\$Action\$
The action being taken, a ban or a release.
\$Reason\$
The Reason field from the QM object.
\$MacAddress\$
The MAC address of the device being banned or release.
\$IpAddress\$
The IP address of the device being banned or release. If the IP address is unknown it will be displayed as 0.0.0
\$VlanName\$
The name of the vlan that the device was banned to or released from.
\$MacGroupName\$
The MAC group that the device was banned to or released from.
\$Details\$
Contains a message with the Action, Mac, IP address, Vlan, and MacGroupName.