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-Lucent 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. The application also includes the optional Quarantine Manager Remediation (QMR) feature. QMR is a switch-based application that interacts with Quarantine Manager to restrict network access of quarantined clients and provide a remediation path for these clients to regain their network access.

> **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.

Quarantine Manager Requirements

The following sections detail hardware/software and basic configuration tasks required to use Quarantine Manager.

Hardware/Software Requirements

OmniVista Hardware/Software

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. The application works with an external Intrusion Prevention System (IPS), such as Fortinet, or a network device, such as an Alcatel-Lucent AOS switch, which sends either a Syslog message or SNMP trap to Quarantine Manager containing the IP or MAC address of the offending device.

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.

Remediation Server (Optional)

On OS6250, 6400, OS6850, OS6855, and 9000 series switches, you can set up a Remediation Server that will work with Quarantine Manager to notify the user when a device is placed into the Banned List. The feature can also be configured to utilize programs/patches to debug the device and restore network access. For more information, see “Configuring a Remediation Server” on page 31.

Configuration Requirements

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.

Quarantine Manager 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.

Remediation Server (Optional)

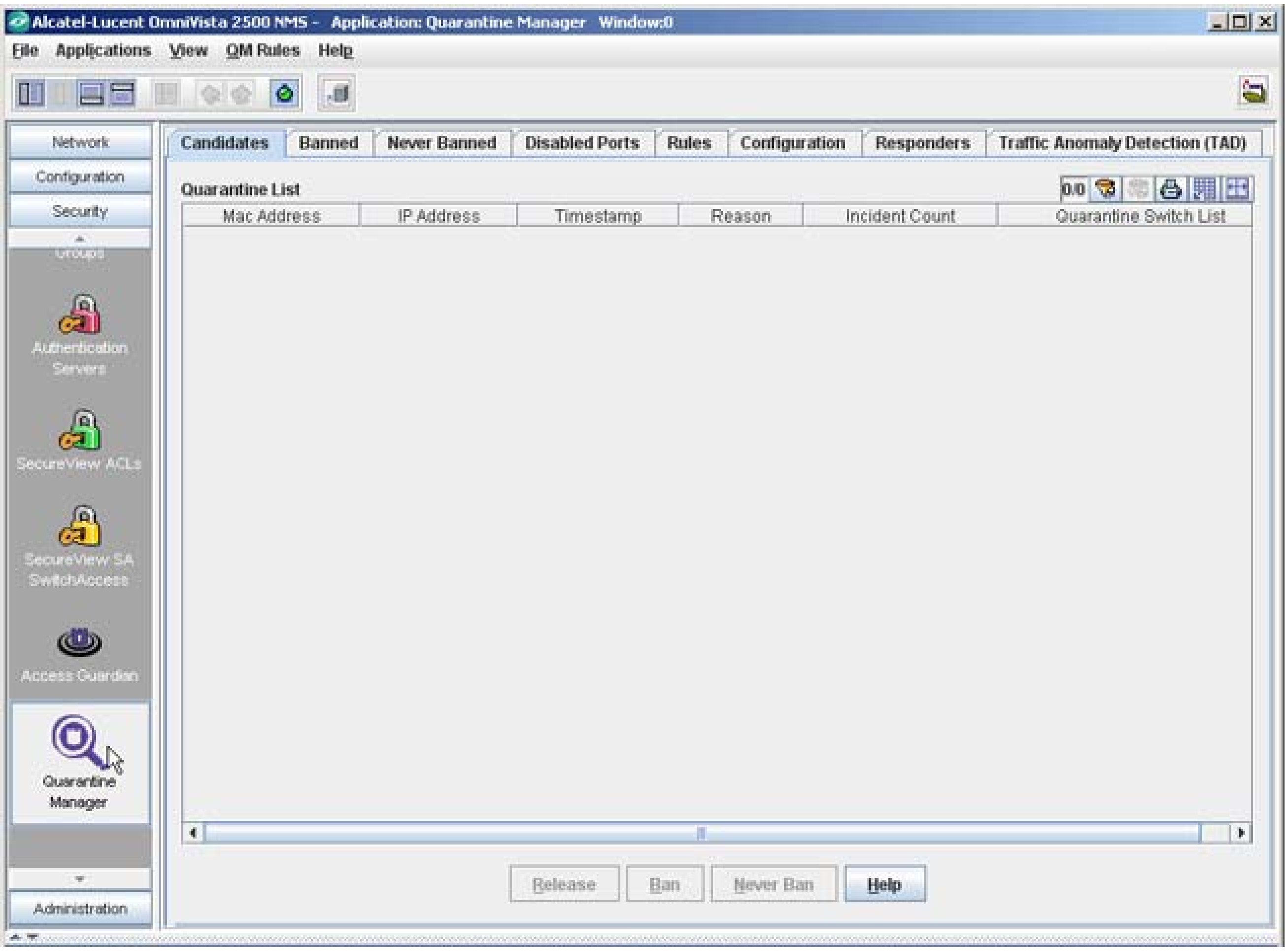
On OS6250, 6400, OS6850, OS6855, and 9000 series switches, you can set up a Remediation Server that will work with Quarantine Manager to notify the user when a device is placed into the Banned List. The feature can also be configured to utilize programs/patches to debug the device and restore network access For more information, see “Configuring a Remediation Server” on page 31.

Quarantine Subnets (Optional)

If a device is banned either by the Network Administrator if Quarantine Manager, 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). For more information, See “Creating Quarantine Subnets” on page 32.

Configuring Quarantine Manager

After initial configuration is complete, Quarantine Manager is configured and managed using the tabs shown and 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. It is also used to configure the optional Remediation Server.
- **Responders -** The Responders tab is used 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
- **Traffic Anomaly Detection (TAD) -** The Traffic Anomaly Detection (TAD) tab is used to configure the TAD feature. TAD is a network monitoring feature that detects anomalies in the network traffic by monitoring the difference in the rate of ingress and egress packets on a port, matching a specific traffic pattern.

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.

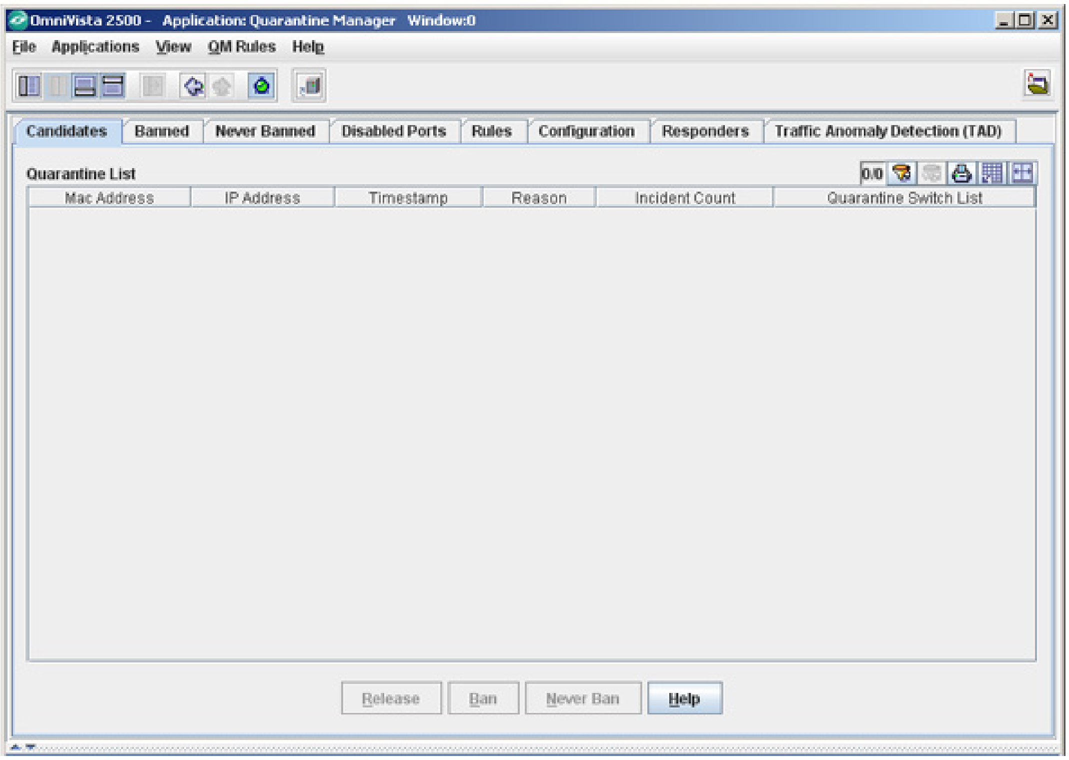
Quarantine Manager Candidates Tab

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.

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.

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.

Candidates Tab Field Descriptions

Candidates Tab field descriptions are provided below.

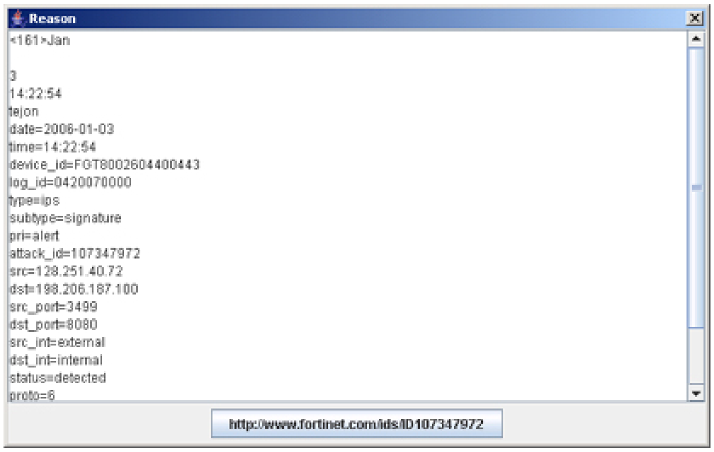
Mac Address - The device's MAC address. Quarantine Manager Rules extract the IP address of the device. Quarantine Manager then uses the OmniVista Locator Function to determine the MAC address.

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

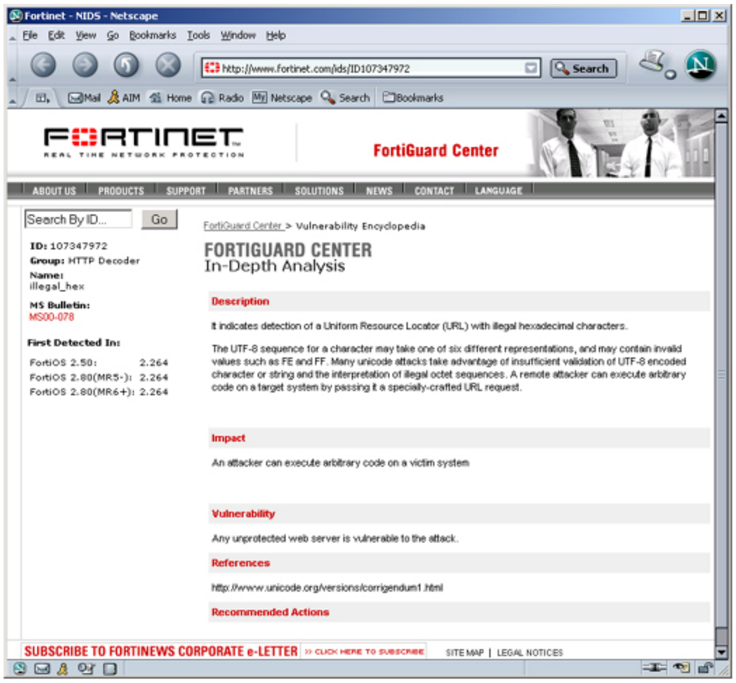
Click on the event in the table to highlight it; then right-click on the event. The Reason window will appear.



```
<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
status=detected
proto=6
```

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.


Fortinet - NIDS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.fortinet.com/ids/ID107347972
Search
Mail AIM Home Radio Netscape Search Bookmarks
FORTINET
REAL TIME NETWORK PROTECTION
FortiGuard Center
ABOUT US PRODUCTS SUPPORT PARTNERS SOLUTIONS NEWS CONTACT LANGUAGE
Search By ID...
Go
FortiGuard Center > Vulnerability Encyclopedia

FORTIGUARD CENTER
In-Depth Analysis

ID: 107347972
Group: HTTP Decoder
Name: illegal_hex
MS Bulletin: MS00-078

First Detected In:

FortiOS 2.50:	2.264
FortiOS 2.80(MR5-):	2.264
FortiOS 2.80(MR6+):	2.264

Description

It indicates detection of a Uniform Resource Locator (URL) with illegal hexadecimal characters.

The UTF-8 sequence for a character may take one of six different representations, and may contain invalid values such as FE and FF. Many unicode attacks take advantage of insufficient validation of UTF-8 encoded character or string and the interpretation of illegal octet sequences. A remote attacker can execute arbitrary code on a target system by passing it a specially-crafted URL request.

Impact

An attacker can execute arbitrary code on a victim system

Vulnerability

Any unprotected web server is vulnerable to the attack.

References

http://www.unicode.org/versions/corrigendum1.html

Recommended Actions

SUBSCRIBE TO FORTINEWS CORPORATE e-LETTER
>> CLICK HERE TO SUBSCRIBE
SITE MAP | LEGAL NOTICES

Incident Count - The number of times an anomaly has been seen for the candidate device.

Quarantine Switch List - This field contains a list of switches that will be included in a quarantine if the network administrator decides to ban a device.

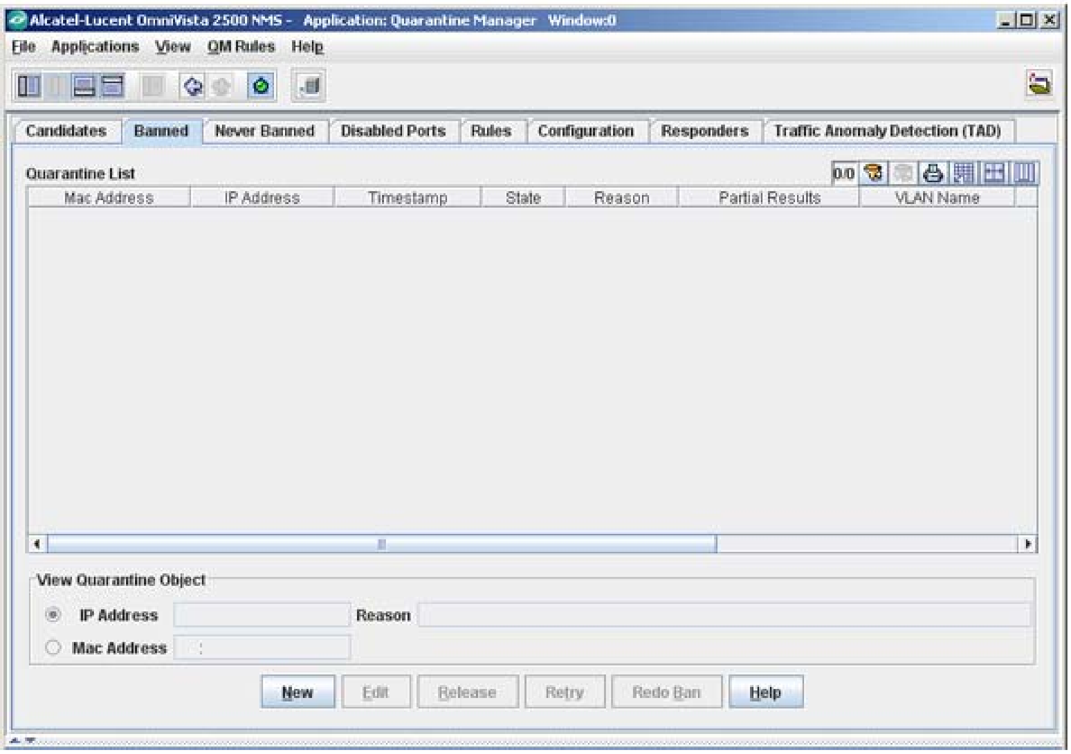
Quarantine Manager Banned Tab

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.

> **Note**: A Network Administrator can also set up a Remediation Server that will work with Quarantine Manager to notify the user when a device is placed into the Banned List. The feature can also be configured to utilize programs/patches to debug the device and restore network access. This feature is currently available only on OS6400, OS6850, and OS6855 devices.

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.

Banned Tab



> **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 can 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.

Note: Quarantine Manager uses a new "Fast Re-Cache" mechanism. With the new mechanism, the switch will look through LDAP only for the existence of quarantine MAC groups. The contents of the MAC group are added to the quarantine settings without flushing any other policies. This feature is only available on the 6400, 6850, and 6850 Series Switches running 6.3.1.R01 or later.

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

Certain information about a banned device may not be picked up by a QM Rule. An Administrator is allowed to edit the IP Address and Reason for an entry in the Banned List to make it more closely match what the Administrator knows to be the best information about a Banned device. Follow the steps below to edit this information.

1. Select the device in the list.

2. Click on the **Edit** button and edit the appropriate fields.

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.

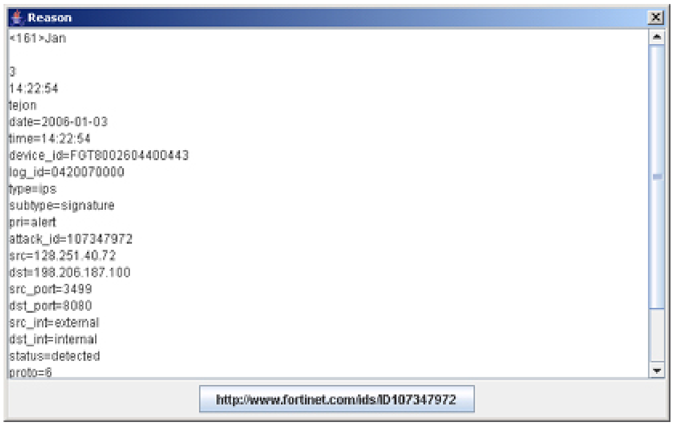
Timestamp - The date and time the event occurred.

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

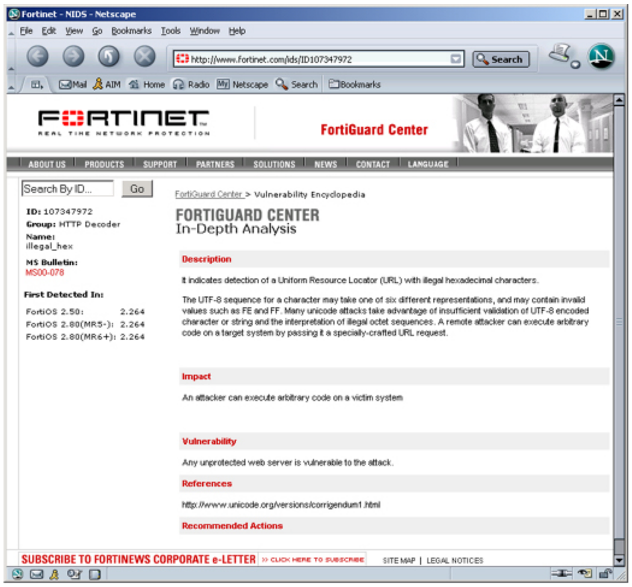
Click on the event in the table to highlight it; then right-click on the event. The Reason window will appear.



```
<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
status=detected
proto=6
```

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.


Fortinet - NIDS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.fortinet.com/ids/ID107347972
Search
Mail AIM Home Radio Netscape Search Bookmarks
FORTINET
REAL TIME NETWORK PROTECTION
FortiGuard Center
ABOUT US PRODUCTS SUPPORT PARTNERS SOLUTIONS NEWS CONTACT LANGUAGE
Search By ID...
Go
SUBSCRIBE TO FORTINEWS CORPORATE e-LETTER
>> CLICK HERE TO SUBSCRIBE
SITE MAP | LEGAL NOTICES

ID: 107347972
Group: HTTP Decoder
Name: illegal_hex
MS Bulletin: MS00-078

First Detected In:

FortiOS 2.50: 2.264
FortiOS 2.80(MR5-): 2.264
FortiOS 2.80(MR6+): 2.264

FortiGuard Center > Vulnerability Encyclopedia

FORTIGUARD CENTER
In-Depth Analysis

Description

It indicates detection of a Uniform Resource Locator (URL) with illegal hexadecimal characters.

The UTF-8 sequence for a character may take one of six different representations, and may contain invalid values such as FE and FF. Many unicode attacks take advantage of insufficient validation of UTF-8 encoded character or string and the interpretation of illegal octet sequences. A remote attacker can execute arbitrary code on a target system by passing it a specially-crafted URL request.

Impact

An attacker can execute arbitrary code on a victim system

Vulnerability

Any unprotected web server is vulnerable to the attack.

References

http://www.unicode.org/versions/corrigendum1.html

Recommended Actions

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.

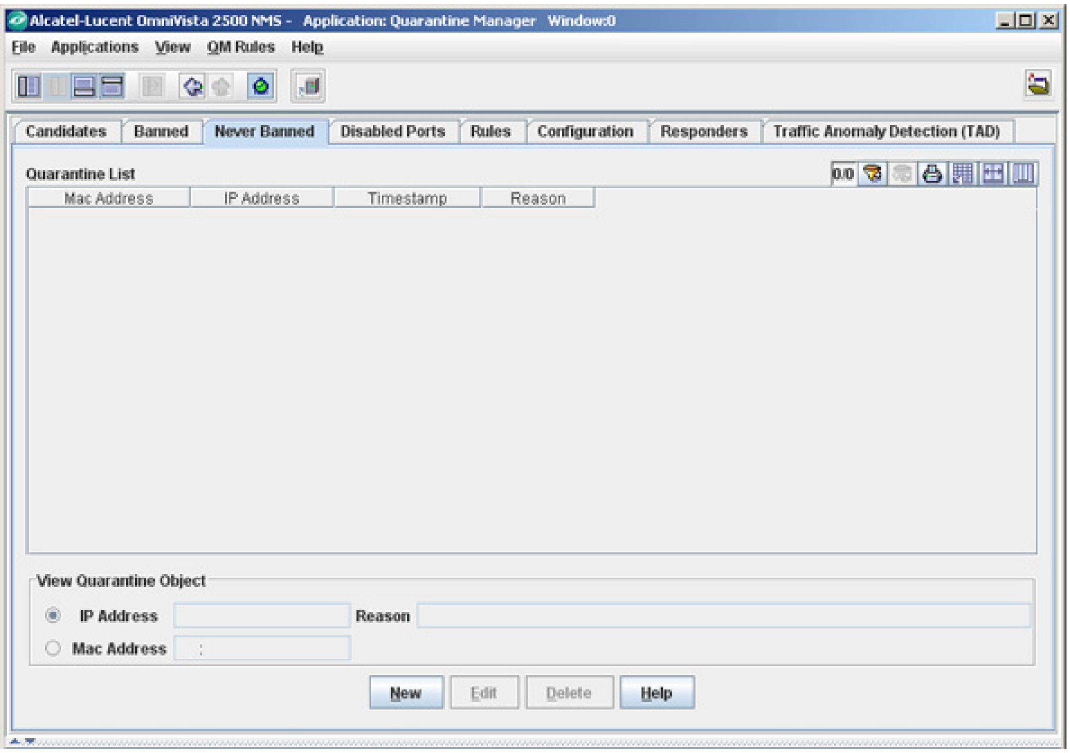
Quarantine Switch List - This field contains a list of switches that will be included in a quarantine of the banned device..

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 Banned Tab



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.

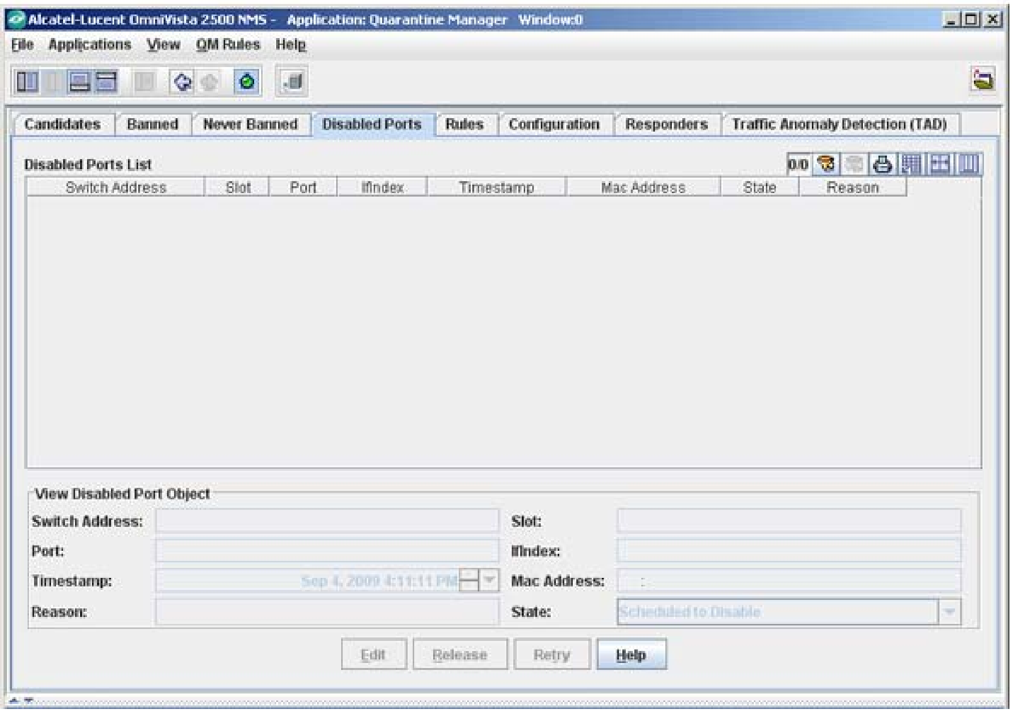
Reason - The reason the device is in the Never Banned list.

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.

Disabled Ports Tab



Disabled Ports List

Switch Address	Slot	Port	IfIndex	Timestamp	Mac Address	State	Reason

View Disabled Port Object

Switch Address:

Slot:

Port:

IfIndex:

Timestamp: Sep 4, 2009 4:11:11 PM

Mac Address: :

Reason:

State: Scheduled to 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)

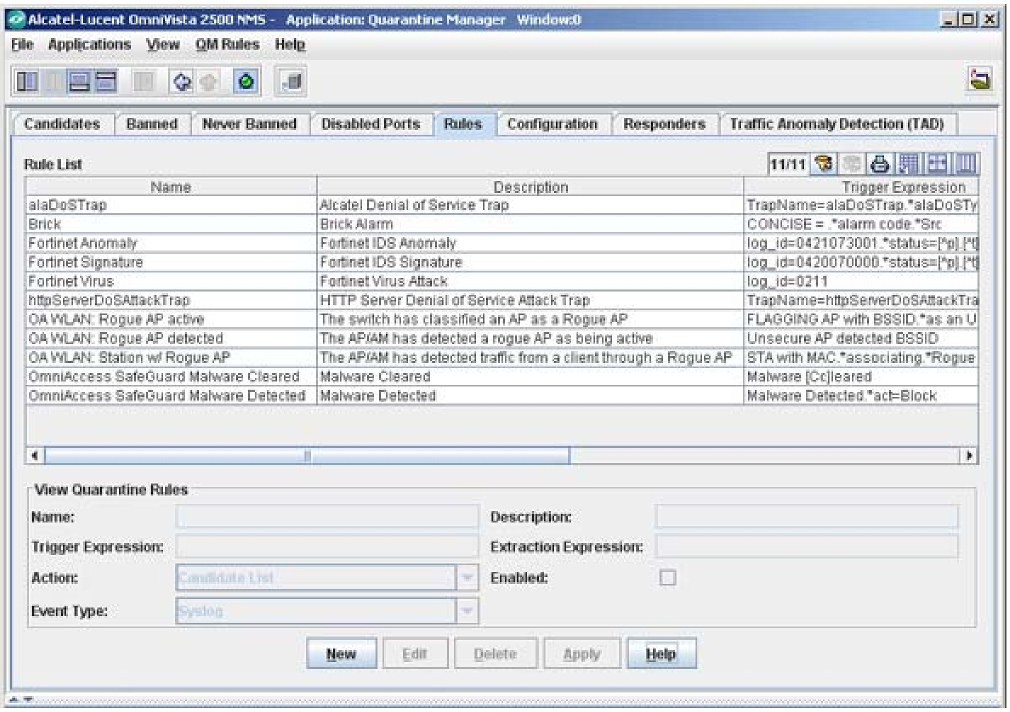
Reason - The reason a port was disabled.

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).

Rules Tab



Rule List 11/11

Name	Description	Trigger Expression
alaDoSTrap	Alcatel Denial of Service Trap	TrapName=alaDoSTrap.*alaDoSTy
Brick	Brick Alarm	CONCISE = .*alarm code.*Src
Fortinet Anomaly	Fortinet IDS Anomaly	log_id=0421073001.*status=[^p].[^t]
Fortinet Signature	Fortinet IDS Signature	log_id=0420070000.*status=[^p].[^t]
Fortinet Virus	Fortinet Virus Attack	log_id=0211
httpServerDoSAttackTrap	HTTP Server Denial of Service Attack Trap	TrapName=httpServerDoSAttackTra
OA WLAN: Rogue AP active	The switch has classified an AP as a Rogue AP	FLAGGING AP with BSSID.*as an U
OA WLAN: Rogue AP detected	The AP/AM has detected a rogue AP as being active	Unsecure AP detected BSSID
OA WLAN: Station w/ Rogue AP	The AP/AM has detected traffic from a client through a Rogue AP	STA with MAC.*associating.*Rogue
OmniAccess SafeGuard Malware Cleared	Malware Cleared	Malware [Cc]leared
OmniAccess SafeGuard Malware Detected	Malware Detected	Malware Detected.*act=Block

View Quarantine Rules

Name:

Description:

Trigger Expression:

Extraction Expression:

Action: Candidate List

Enabled: □

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 eleven (11) 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 pre-configured, 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 DOS trap (AlaDosTrap). The rule triggers an action in response to a Teardrop, Ping of Death, or Port Scan attack. You can use Regular Expressions to create rules for additional AOS DOS traps.
- **Brick -** Triggers an action on a Brick Anomaly Event.
- **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".
- **HTTP Server DOS Attack Trap -** Triggers an action when a "Denial of Service" Trap is received from an HTTP Server.
- **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."
- **OmniAccess SafeGuard Malware Cleared -** Triggers and action when SafeGuard clears malware.
- **OmniAccess SafeGuard Malware Detected -** Triggers and action when SafeGuard detects malware.

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 mis-configured 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

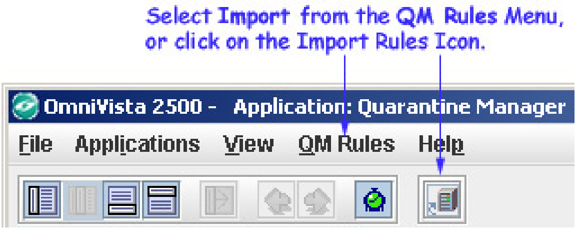
To delete a rule, select the rule (use the **SHIFT** or **CTRL** keys to select multiple rules), click the **Delete** button, and then click the **Apply** button.

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.

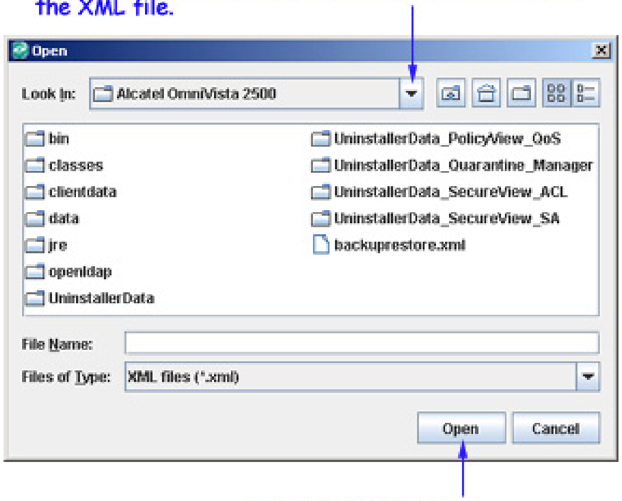
1. Save the .xml file on your machine.

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


Select Import from the QM Rules Menu,
or click on the Import Rules Icon.
OmniVista 2500 - Application: Quarantine Manager
File
Applications
View
QM Rules
Help

An Import window will open in the OmniVista directory.

Use the Look In pulldown menu to browse and locate the XML file.


Open
bin
classes
clientdata
data
jre
openldap
UninstallerData
UninstallerData_PolicyView_QoS
UninstallerData_Quarantine_Manager
UninstallerData_SecureView_ACL
UninstallerData_SecureView_SA
backuprestore.xml
Open
Cancel

Look In: Alcatel OmniVista 2500

File Name:

Files of Type: XML files (*.xml)

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. See “Regular Expressions Overview” on page 18 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. See “Regular Expressions Overview” on page 18 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 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}\.[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 of 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 expression 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 it 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.

AOS DOS Trap Configuration

In addition to the Built-In Rule for AOS DOS Traps (0, 2, 6), you can configure a Rule for other AOS DOS traps. For example, the built-in rule for AOS DOS Traps is:

TrapName=alaDoSTrap.*alaDoSType=[0|2|6]
This triggers a response on AOS DOS Trap type 0, 2, and 6.

To trigger on types 0, 2, 6, 9, 10, 11, 12 and 13, you would enter:
TrapName=alaDoSTrap.*alaDoSType=([0|2|6|9]|1[0123])

The ( ) form a group
Inside the group are basically two parts separated by a vertical bar | which means either or
so we have
(A | B)
The first part (A) is
[0|2|6|9]
The square brackets [ ] mean match a single character from the list. The vertical bar | means or.
So this expressions says either a 0 or 2 or 6 or 9.

The second part (B) is
1[0123]
which means a 1 followed by either a 0 or a 1 or a 2 or a 3
That expression could have been written as
1[0-3]

The dash - is a special character which is used to express a range.

Note that we could **not** have written the expression as alaDoSType=[0-13] to match all 13 types. This expression says a 0 through 1 or a 3. so it would match:
alaDoSType=0
alaDoSType=1
alaDoSType=3

Quarantine Manager Configuration Tab

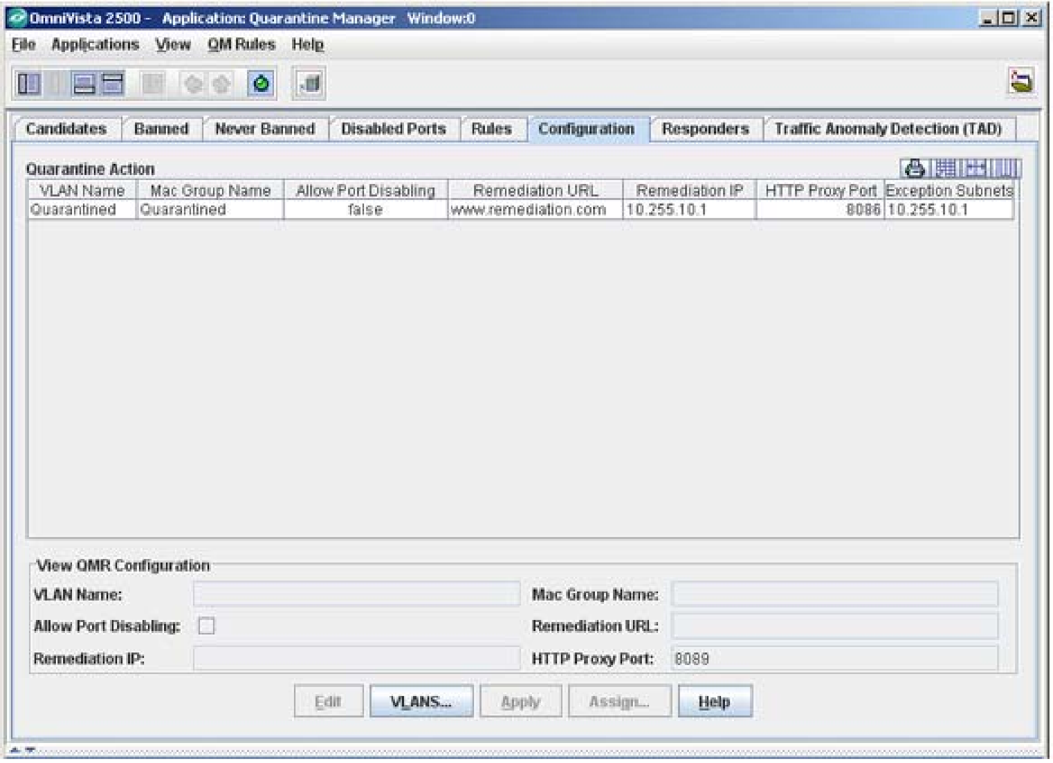
The Configuration tab is used to configure the Quarantine VLAN, Quarantine MAC Group, and the optional Quarantine Manager Remediation (QMR) feature. By default, the name of the Quarantine VLAN is "Quarantined". However, you can change the name as desired. The VLAN is created using the OmniVista **VLANs** 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.

ACLs include ACL rules 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.

When devices are banned, either through a Quarantine Manager rule or by the Network Administrator, they are added to the Quarantined VLAN and/or Quarantined MAC group. These devices no longer route traffic to any other devices in the network (although you can create a logical "Quarantine" subnet to limit Quarantine Manager actions to a specific set of switches on the network.). The devices remain in the Banned list until removed by the Network Administrator.

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

Configuration Tab


OmniVista 2500 - Application: Quarantine Manager Window:0
File Applications View QM Rules Help
Candidates
Banned
Never Banned
Disabled Ports
Rules
Configuration
Responders
Traffic Anomaly Detection (TAD)
Edit
VLANS...
Apply
Assign...
Help

Quarantine Action

VLAN Name	Mac Group Name	Allow Port Disabling	Remediation URL	Remediation IP	HTTP Proxy Port	Exception Subnets
Quarantined	Quarantined	false	www.remediation.com	10.255.10.1	8086	10.255.10.1

View QMR Configuration

VLAN Name:

Mac Group Name:

Allow Port Disabling: □

Remediation URL:

Remediation IP:

HTTP Proxy Port: 8089

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 the Quarantine VLAN based on the MAC Rule.

Quarantined Manager Remediation (QMR)

Quarantine Manager Remediation (QMR) is a switch-based application that interacts with Quarantine Manager to restrict network access of quarantined clients and provide a remediation path for these clients to regain their network access. A Network Administrator can set up a Remediation Server that will work with Quarantine Manager to notify the user when a device is placed into the Banned List. The feature can also be configured to utilize programs/patches to debug the device and restore network access.

When Quarantine Manager quarantines a client, the client MAC address is added to the MAC address group on the LDAP server. QMR pulls the MAC addresses from this group to populate the "Quarantined" MAC address group on the switch. At this point, network access for these clients is restricted to communication with the designated Remediation Server, and exception subnet if configured (and essential protocols such as ARP, DHCP, and DNS), until the client's quarantined status is corrected

When a client has corrected its quarantined state, Quarantine Manager updates the MAC address group on the LDAP server to remove the MAC address of the client. QMR will then restore network access to that client the next time QMR checks the LDAP MAC address group.

> **Note:** Configuring QMR and QoS inner VLAN or inner 802.1p policies is mutually exclusive. QMR overlays the inner VLAN tag, thus creating a conflict with related QoS policies. This is also true with QMR and VLAN Stacking services.

Quarantine Manager Setup

Before configuring Quarantine Manager, you must perform the following steps:

- Create the Quarantine VLAN
- Create the Quarantine MAC Group
- Create the Quarantine MAC Group ACL Rule

Creating the Quarantine VLAN

Create the Quarantined VLAN containing the switches you want to monitor with Quarantine Manager.

1. Click the **VLANs...** button at the bottom of the window to open the VLAN application and the VLAN wizard.

2. 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.

Creating the Quarantine MAC Group

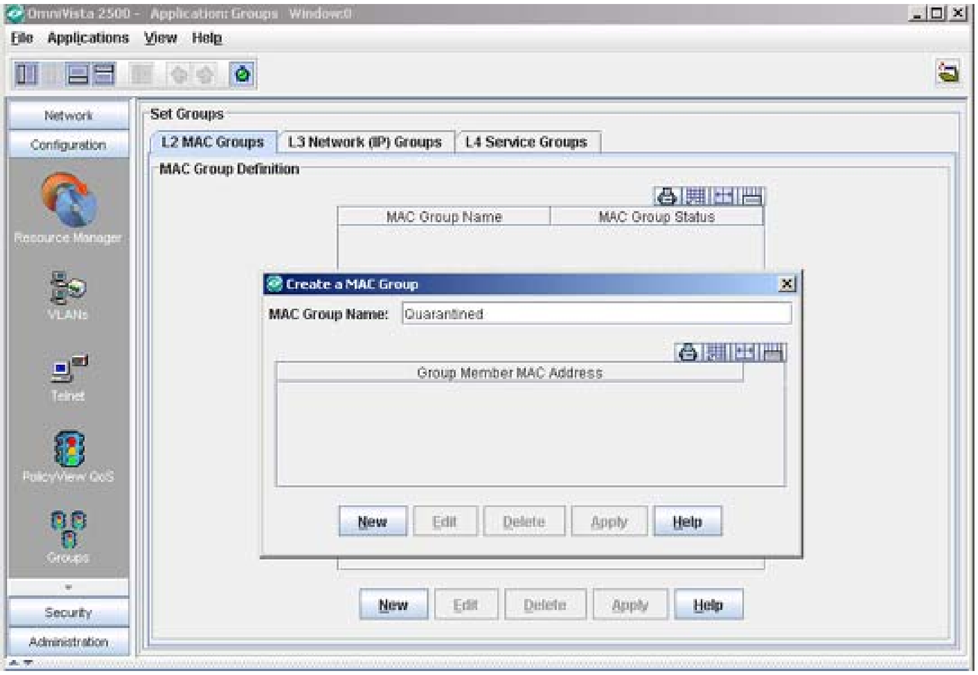
To configure Quarantine Manager to use SecureView ACL, you must first create a Layer 2 Quarantined MAC Group using the **Groups** application. After creating this MAC group, you create an ACL rule using the **SecureView ACLs** application, which drops traffic if it finds a matching MAC address. Open the **Groups** application and create the Quarantine MAC group. The Quarantined MAC group you create must have the same name as the Quarantined MAC group in the Configuration tab. If you create the MAC group with a different name, or later change the MAC group name, Quarantine Manager will not function (and an error message may not be issued).

> **Note:** If after creating the Quarantined MAC group you modify the name (either using the Groups application, CLI, or WebView), you must also modify the Quarantined MAC group name in the Configuration tab and poll the switch for the change to take effect.

Follow the steps below to create a Layer 2 Quarantined MAC Group

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.



MAC Group Name: Quarantined

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.

Creating the Quarantine MAC Group ACL Rule

After creating this MAC group, you create a Quarantined MAC Group ACL Rule using the **SecureView ACLs** application, which drops traffic if it finds a matching MAC address. 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.

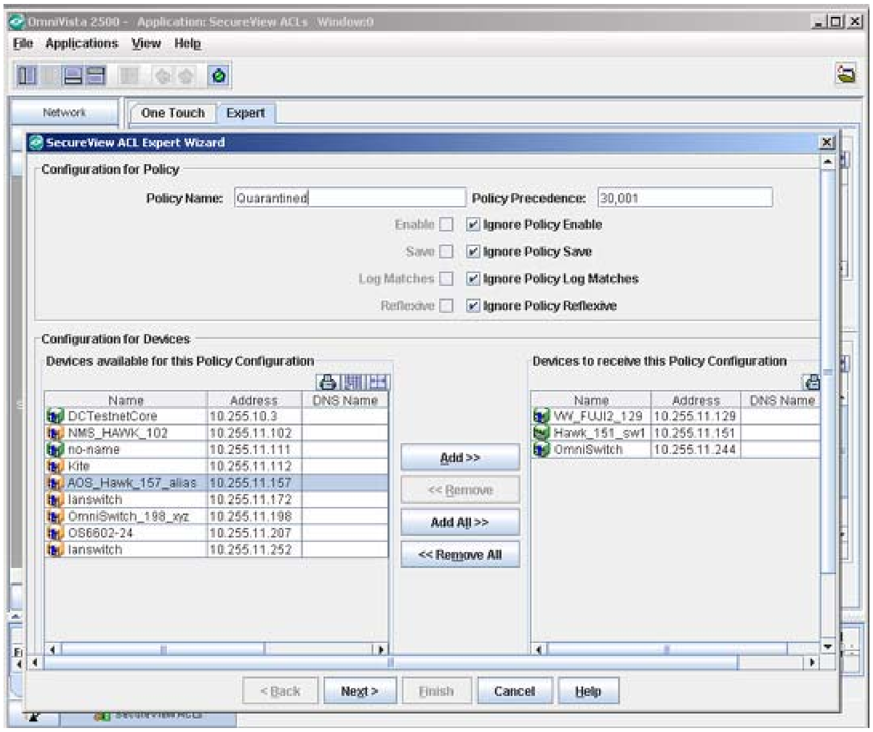
> **Note:** Quarantine Manager does not support ACLs on XOS devices.

Follow the steps below to create a Quarantined MAC Group ACL Rule to drop traffic from a Quarantined MAC address.

> **Note:** OS6250 and OS6250-M devices have a limitation where “non IP conditions (no L3, L4 conditions) only apply to non IP packets. This requires you to create an additional L3 ACL condition for these devices so L3 traffic will be included in Quarantine process. If you are creating an ACL Rule for a 6250 device, go to "Creating a Quarantined MAC Group Rule for OS6250 Devices" on page 26.

1. Start the **SecureView ACLs** application and click the **Expert** tab.

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



OmniVista 2500 - Application: SecureView ACLs Window:0
File Applications View Help
Network
One Touch
Expert
SecureView ACL Expert Wizard

Configuration for Policy

Policy Name: Quarantined

Policy Precedence: 30,001

Enable □ ☑ Ignore Policy Enable

Save □ ☑ Ignore Policy Save

Log Matches □ ☑ Ignore Policy Log Matches

Reflexive □ ☑ Ignore Policy Reflexive

Configuration for Devices

Devices available for this Policy Configuration

Name	Address	DNS Name
DCTestnetCore	10.255.10.3	
NMS_HAWK_102	10.255.11.102	
no-name	10.255.11.111	
Kite	10.255.11.112	
AOS_Hawk_157_alias	10.255.11.157	
lanswitch	10.255.11.172	
OmniSwitch_198_xyz	10.255.11.198	
OS6602-24	10.255.11.207	
lanswitch	10.255.11.252	

Devices to receive this Policy Configuration

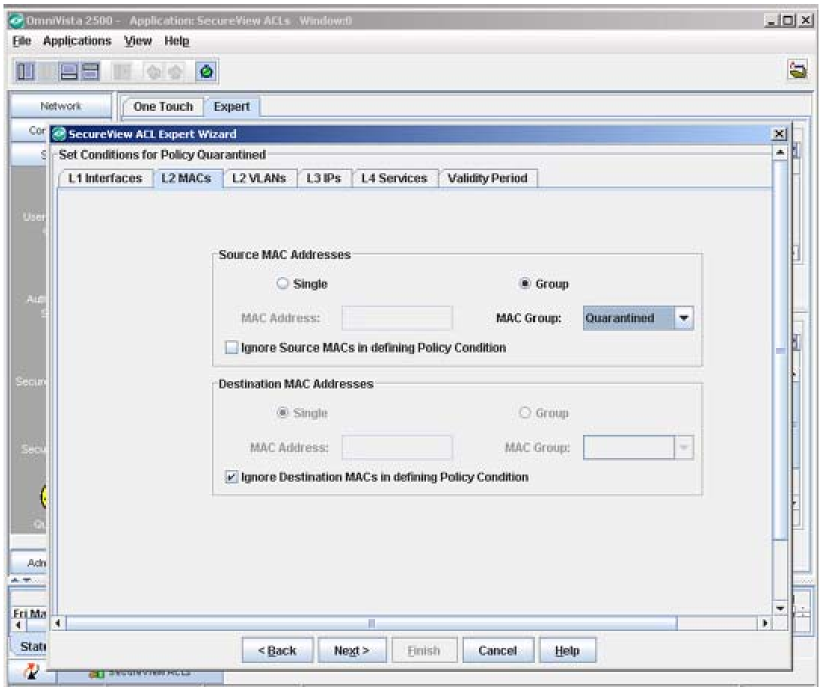
Name	Address	DNS Name
VV_FUJI2_129	10.255.11.129	
Hawk_151_sw1	10.255.11.151	
OmniSwitch	10.255.11.244	

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

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

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

6. Click the **L2 MACs** tab.



OmniVista 2500 - Application: SecureView ACLs Window:0
File Applications View Help
Network
One Touch
Expert
SecureView ACL Expert Wizard
L1 Interfaces
L2 MACs
L2 VLANs
L3 IPs
L4 Services
Validity Period

Set Conditions for Policy Quarantined

Source MAC Addresses

○ Single ● Group

MAC Address:

MAC Group: Quarantined

□ Ignore Source MACs in defining Policy Condition

Destination MAC Addresses

● Single ○ Group

MAC Address:

MAC Group:

☑ Ignore Destination MACs in defining Policy Condition

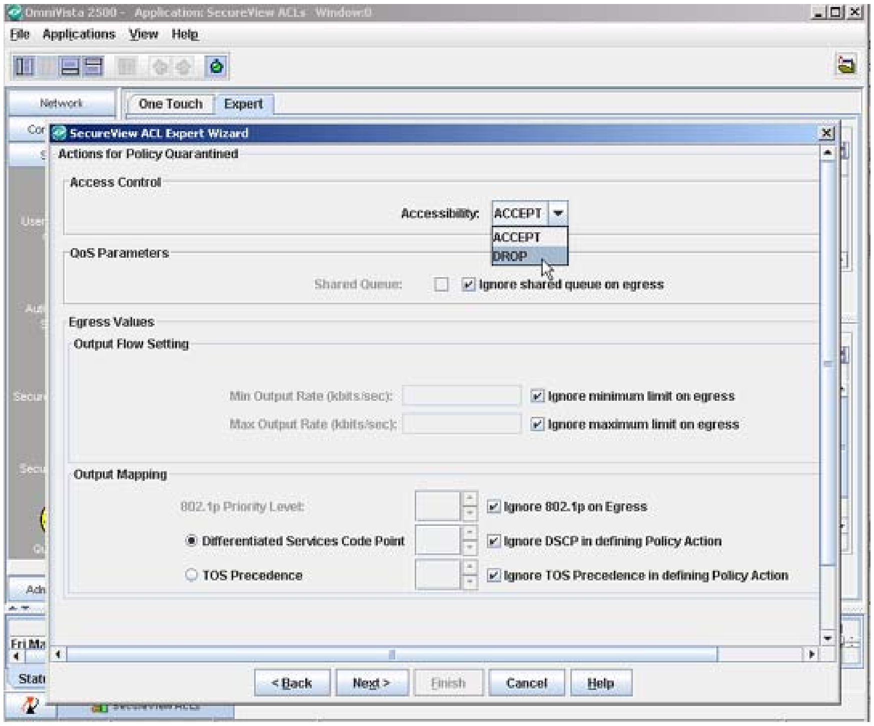
7. In the Source MAC Addresses panel, uncheck the **Ignore Source MACs in defining Policy Condition** checkbox. This will enable the other controls in this section.

8. Click the **Group** radio button.

9. In the **MAC Group** drop-down list select the Quarantined MAC group.

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

> **Note:** If you selected a switch in Step 4 that does not support the MAC group, an error will be displayed. You must go back and remove the switch from the selection list.


OmniVista 2500 - Application: SecureView ACLs Window:0
File
Applications
View
Help
Network
One Touch
Expert
SecureView ACL Expert Wizard
< Back
Next >
Finish
Cancel
Help

Actions for Policy Quarantined

Access Control

Accessibility: ACCEPT
ACCEPT
DROP

QoS Parameters

Shared Queue: ☐ ☑ Ignore shared queue on egress

Egress Values

Output Flow Setting

Min Output Rate (kbits/sec): ☑ Ignore minimum limit on egress

Max Output Rate (kbits/sec): ☑ Ignore maximum limit on egress

Output Mapping

802.1p Priority Level: ☑ Ignore 802.1p on Egress

● Differentiated Services Code Point ☑ Ignore DSCP in defining Policy Action

○ TOS Precedence ☑ Ignore TOS Precedence in defining Policy Action

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

12. Click the **Next** button.

13. 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.

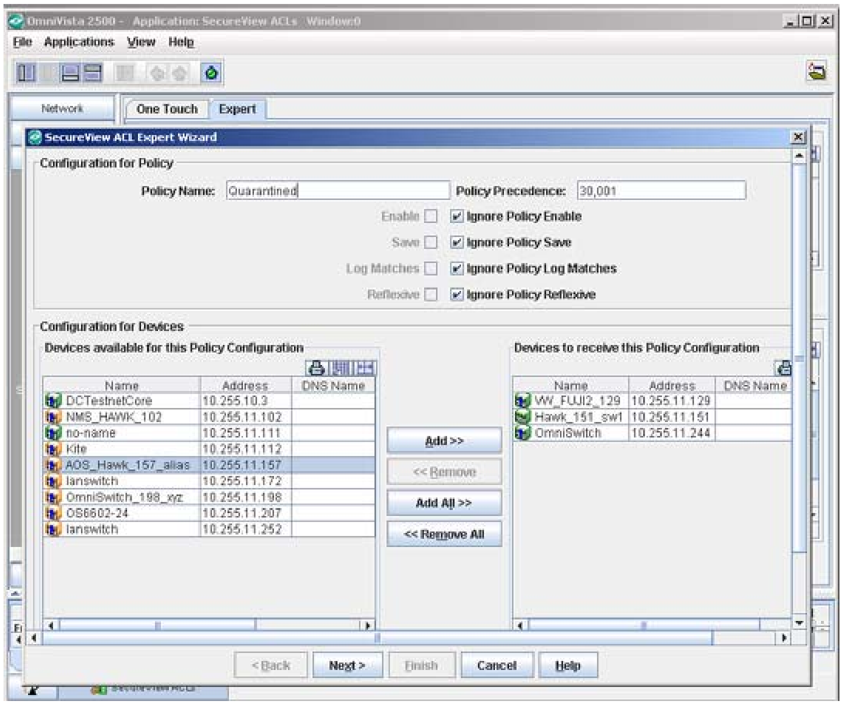
14. Click the **Notify** button to allow the switches to re-cache their policies.

Creating a Quarantined MAC Group Rule for OS6250 Devices

OS6250 and OS6250-M devices have a limitation where “non IP" rules (no L3, L4 conditions) only apply to "non IP" packets. This requires an additional L3 ACL Rule for these devices so that L3 traffic will be included in Quarantine process.

1. Start the **SecureView ACLs** application and click the **Expert** tab.

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


OmniVista 2500 - Application: SecureView ACLs Window:0
File Applications View Help
Network
One Touch
Expert
SecureView ACL Expert Wizard
Add >>
<< Remove
Add All >>
<< Remove All
< Back
Next >
Finish
Cancel
Help

Configuration for Policy

Policy Name: Quarantined

Policy Precedence: 30,001

Enable □ ☑ Ignore Policy Enable

Save □ ☑ Ignore Policy Save

Log Matches □ ☑ Ignore Policy Log Matches

Reflexive □ ☑ Ignore Policy Reflexive

Configuration for Devices

Devices available for this Policy Configuration

Name	Address	DNS Name
DCTestnetCore	10.255.10.3	
NMS_HAWK_102	10.255.11.102	
no-name	10.255.11.111	
Kite	10.255.11.112	
AOS_Hawk_157_alias	10.255.11.157	
lanswitch	10.255.11.172	
OmniSwitch_198_xyz	10.255.11.198	
OS6602-24	10.255.11.207	
lanswitch	10.255.11.252	

Devices to receive this Policy Configuration

Name	Address	DNS Name
VW_FUJI2_129	10.255.11.129	
Hawk_151_sw1	10.255.11.151	
OmniSwitch	10.255.11.244	

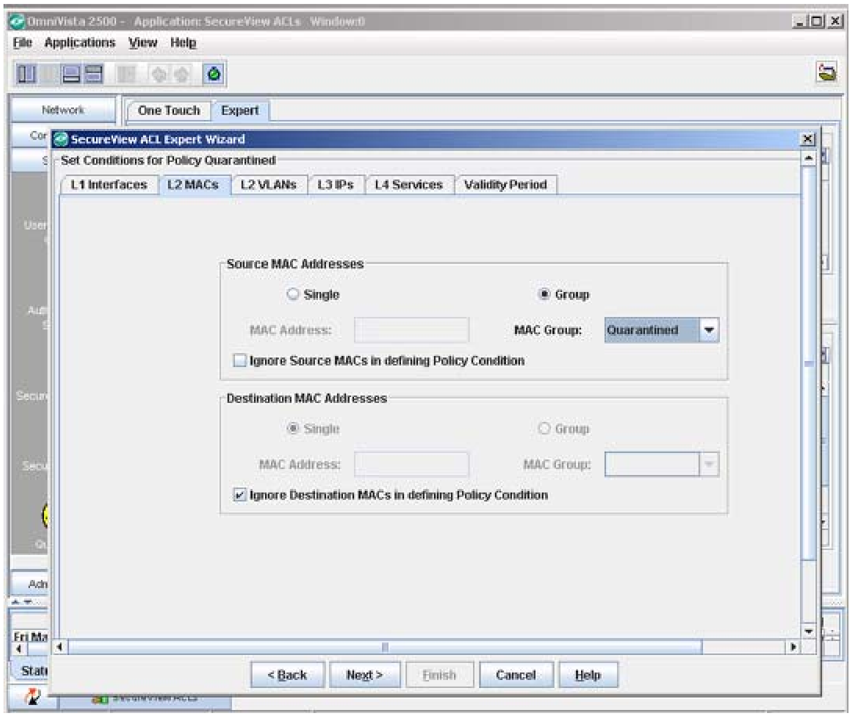
3. In the **Policy Name** field, enter a policy name such as "Quarantined".

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

> **Note:** Be sure you are only adding 6250 Devices.

5. Click the **Next** button to create the L2 Condition.

6. Click the **L2 MACs** tab.



Set Conditions for Policy Quarantined

Source MAC Addresses

○ Single ● Group

MAC Address:

MAC Group: Quarantined

□ Ignore Source MACs in defining Policy Condition

Destination MAC Addresses

● Single ○ Group

MAC Address:

MAC Group:

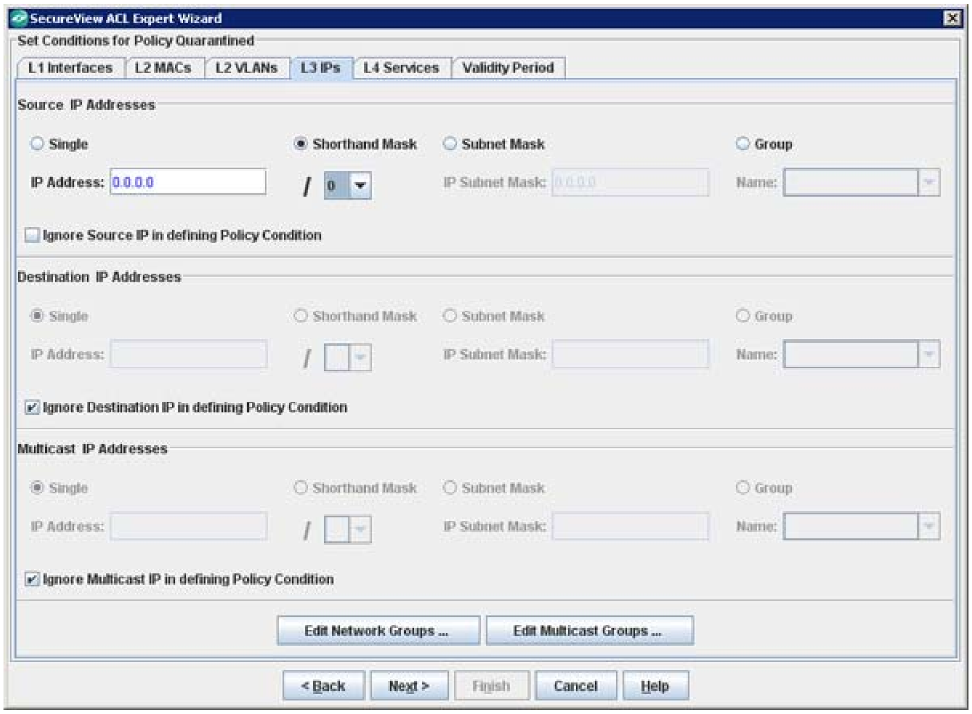
☑ Ignore Destination MACs in defining Policy Condition

7. 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.

8. Click the **Group** radio button.

9. In the **MAC Group** drop-down list select the Quarantined MAC group.

10. Click on the **L3 IPs** tab.



SecureView ACL Expert Wizard

Set Conditions for Policy Quarantined

Source IP Addresses

○ Single ● Shorthand Mask ○ Subnet Mask ○ Group

IP Address: 0.0.0.0 / 0 IP Subnet Mask: 0.0.0.0 Name:

□ Ignore Source IP in defining Policy Condition

Destination IP Addresses

● Single ○ Shorthand Mask ○ Subnet Mask ○ Group

IP Address: / IP Subnet Mask: Name:

☑ Ignore Destination IP in defining Policy Condition

Multicast IP Addresses

● Single ○ Shorthand Mask ○ Subnet Mask ○ Group

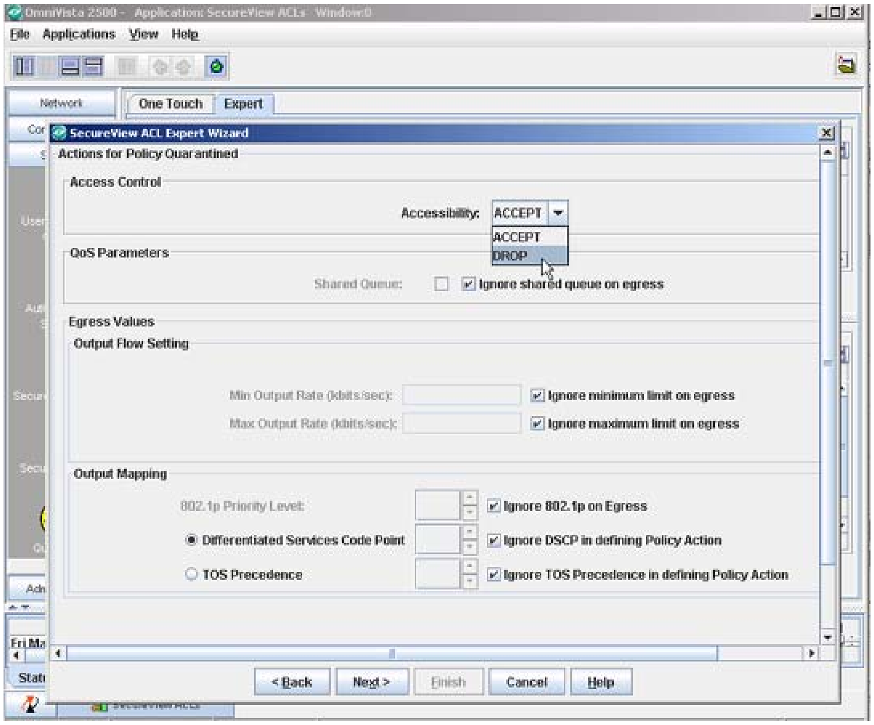
IP Address: / IP Subnet Mask: Name:

☑ Ignore Multicast IP in defining Policy Condition

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

12. Enter an IP address of "0.0.0.0", and select the **Shorthand Mask** radio button and select "0" from the drop-down menu.

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


OmniVista 2500 - Application: SecureView ACLs Window:0
File Applications View Help
Network
One Touch
Expert
SecureView ACL Expert Wizard
< Back
Next >
Finish
Cancel
Help

Actions for Policy Quarantined

Access Control

Accessibility: ACCEPT
ACCEPT
DROP

QoS Parameters

Shared Queue: □ ☑ Ignore shared queue on egress

Egress Values

Output Flow Setting

Min Output Rate (kbits/sec): ☑ Ignore minimum limit on egress

Max Output Rate (kbits/sec): ☑ Ignore maximum limit on egress

Output Mapping

802.1p Priority Level: ☑ Ignore 802.1p on Egress

● Differentiated Services Code Point ☑ Ignore DSCP in defining Policy Action

○ TOS Precedence ☑ Ignore TOS Precedence in defining Policy Action

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

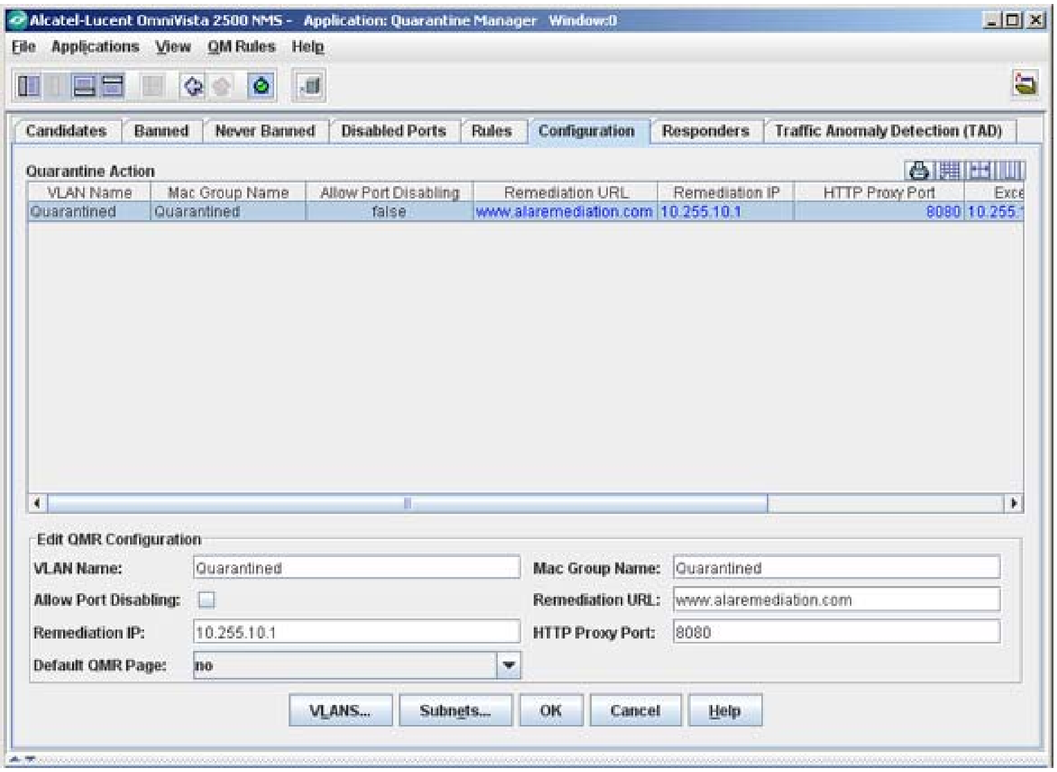
15. Click the **Next** button.

16. 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.

17. Click the **Notify** button to allow the switches to re-cache their policies.

Configuring Quarantine Manager

After completing the Quarantine Manager Setup, click on the VLAN name in the Quarantine Action table, and then click the **Edit** button. The Edit Quarantine Manager Panel is activated, as shown below. Follow the steps below to configure Quarantine Manager.



Quarantine Action

VLAN Name	Mac Group Name	Allow Port Disabling	Remediation URL	Remediation IP	HTTP Proxy Port	Exce
Quarantined	Quarantined	false	www.alaremediation.com	10.255.10.1	8080	10.255.1

Edit QMR Configuration

VLAN Name: Quarantined

Mac Group Name: Quarantined

Allow Port Disabling: □

Remediation URL: www.alaremediation.com

Remediation IP: 10.255.10.1

HTTP Proxy Port: 8080

Default QMR Page: no

1. If necessary, edit the **VLAN Name** to match the name of the VLAN you created when setting up Quarantine Manager.

2. If necessary, add or edit the **MAC Group Name** to match the name of the MAC group you when setting up Quarantine Manager.

3. Enable/Disable the **Allow Port Disabling** feature. You can enable or disable a port rather than create a VLAN or ACL rule. 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. Right-click on 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 at the bottom of the window. 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.

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

4. If there is a firewall/proxy configured for the network, enter the **HTTP Proxy Port** used by the network (e.g., 8080).

> **Note:** If you are configuring a Remediation Server, go to "Configuring a Remediation Server" on page 31. Otherwise, continue to Step 5.

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

6. Assign the configuration to switches in the network.

Configuring a Remediation Server (Optional)

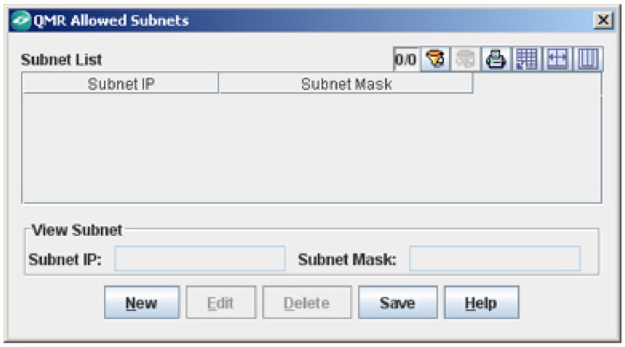
If you are configuring a Remediation Server, complete the Remediation Server fields as described below.

1. Complete the Remediation Server fields as described below.

- **Remediation URL -** Enter the URL of the Remediation Server in the field (e.g., http://alaremediation.com). If the Remediation Server is running on a port other than the default port for the browser (e.g., 8080), the port needs to be included in the Remediation URL (e.g., (http://alaremediation.com:9090).
- **Remediation IP -** Enter the IP Address of the Remediation Server in the field. You must add the Remediation Server IP address to the "QMR Allowed Subnets
- **Default QMR Page -** Select **Yes** to automatically present the Default Quarantine Manager Remediation Web Page to the user if a Remediation Server is not configured. The page to notify the client of its quarantined state. Select **No** if you do not want to display this page.

2. Click on the **Subnets** button to create a "QMR Allowed Subnets" Group. This is a reserved QoS network group that includes the Remediation Server and any subnets to which a quarantined client is allowed access. You must add the Remediation Server IP address/subnet mask to the "QMR Allowed Subnets" Group, so that a quarantined client can communicate with the Remediation Server. You can optionally add additional subnets to which quarantined devices will have access.

QMR Allowed Subnets



3. Click the **Save** button on the QMR Allowed Subnets window, then click the **Apply** button to write the changes to the server.

4. Assign the configuration to switches in the network.

> **Note:** Switches discovered after the 'Quarantined' VLAN is created cannot be added via the VLANs application. 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.

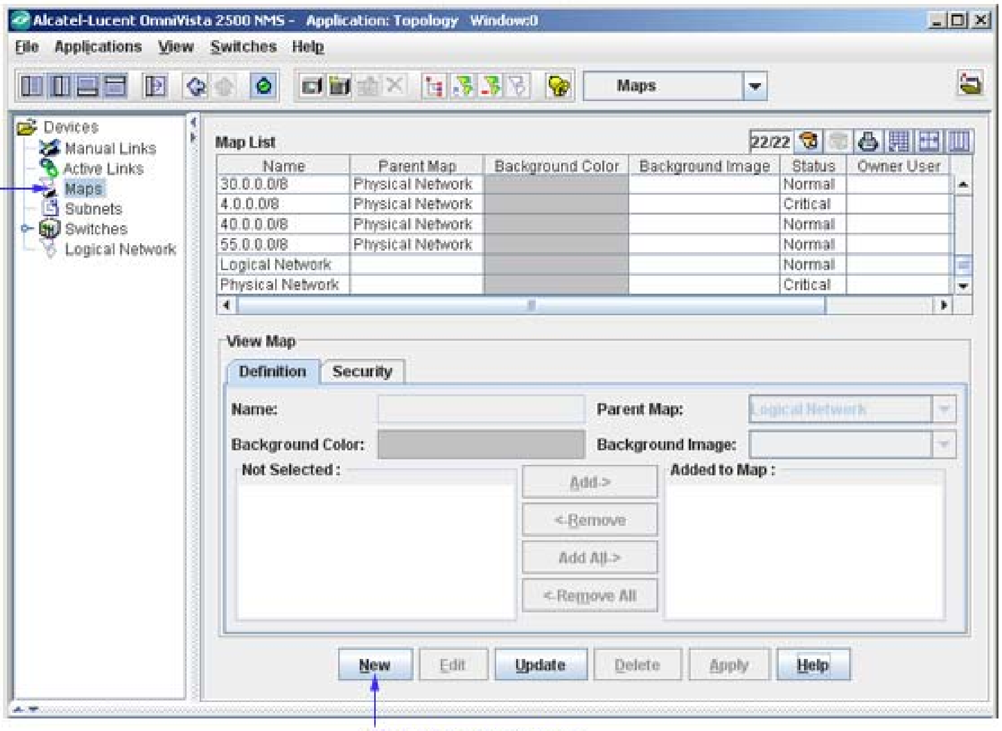
Creating Quarantine Subnets (Optional)

If a device is banned either by the Network Administrator if Quarantine Manager, 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). In this case, 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 switch's Quarantine subnet(s). For example, if a switch in "Quarantine Subnet 1" is connected to an offending device, Quarantine Manager will apply the ban only to the switches in the "Quarantine Subnet 1".

To create "Quarantine" subnet(s) you use the Maps feature within the **Topology** application to create a Logical network called "Quarantine". You then create Quarantine subnets by creating subnetworks under the Quarantine network. Follow the steps below to create "Quarantine" subnet(s).

1. Open the Topology application and click on **Maps** in the Topology Tree to bring up the Topology Maps feature.

Topology Maps



Name	Parent Map	Background Color	Background Image	Status	Owner User
30.0.0.0/8	Physical Network	▨		Normal	
4.0.0.0/8	Physical Network	▨		Critical	
40.0.0.0/8	Physical Network	▨		Normal	
55.0.0.0/8	Physical Network	▨		Normal	
Logical Network		▨		Normal	
Physical Network		▨		Critical	

Name:

Parent Map: Logical Network

Background Color:

Background Image:

Not Selected :

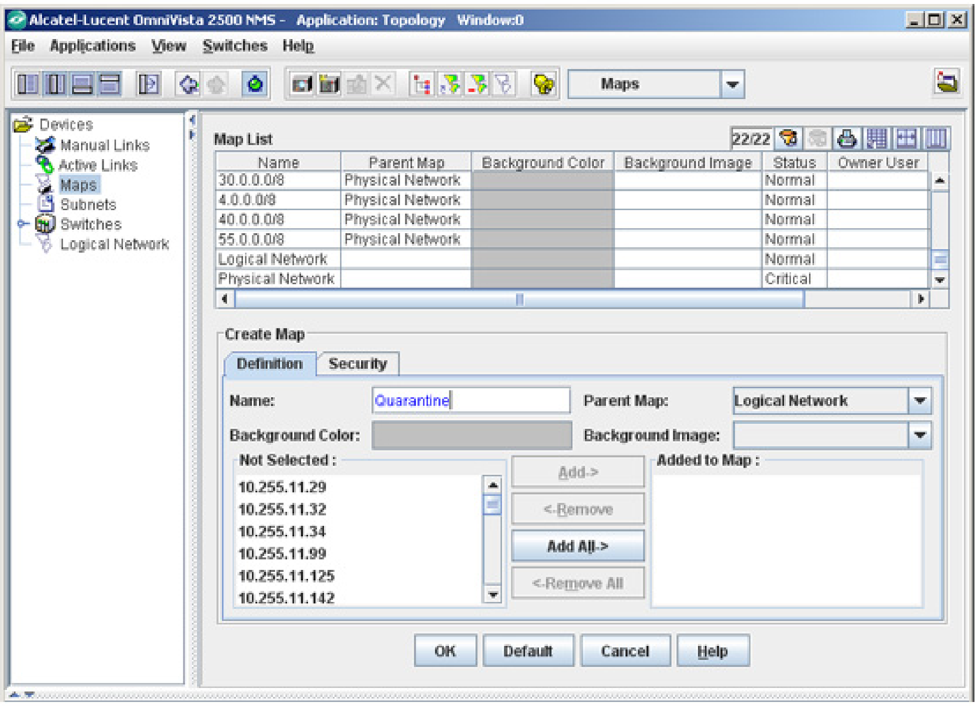
Added to Map :

Click on Maps to bring up the Topology Maps Feature.

Click New to create a "Quarantine" Subnet.

2. Click on the **New** button to create the "Quarantine" Logical network.

Creating The Quarantine Logical Network



Map List 22/22

Name	Parent Map	Background Color	Background Image	Status	Owner User
30.0.0.0/8	Physical Network			Normal	
4.0.0.0/8	Physical Network			Normal	
40.0.0.0/8	Physical Network			Normal	
55.0.0.0/8	Physical Network			Normal	
Logical Network				Normal	
Physical Network				Critical	

Create Map

Definition | Security

Name: Quarantine

Parent Map: Logical Network

Background Color:

Background Image:

Not Selected :

10.255.11.29
10.255.11.32
10.255.11.34
10.255.11.99
10.255.11.125
10.255.11.142

Added to Map :

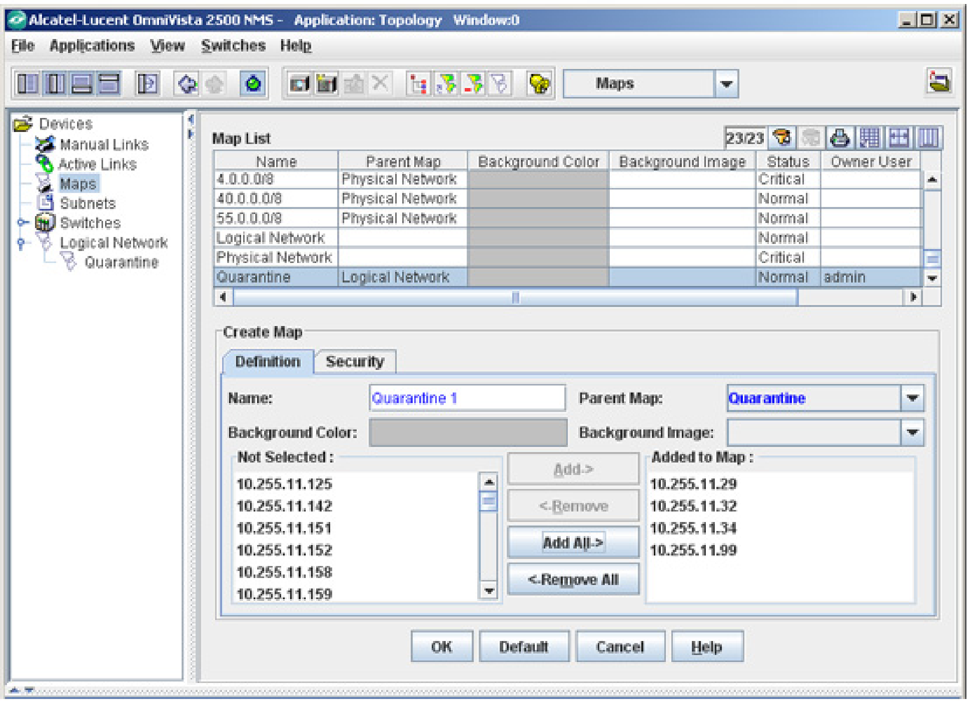
3. Enter *Quarantine* in the **Name** field. You must enter the name with a capital "Q".

4. Make sure the **Parent Map** is **Logical Network**.

5. Click **OK**, then click the **Apply** button.

6. Click the **New** button to create your Quarantine Subnet(s) under the Quarantine Network.

Creating a Quarantine Subnet



Map List 23/23

Name	Parent Map	Background Color	Background Image	Status	Owner User
4.0.0.0/8	Physical Network			Critical	
40.0.0.0/8	Physical Network			Normal	
55.0.0.0/8	Physical Network			Normal	
Logical Network				Normal	
Physical Network				Critical	
Quarantine	Logical Network			Normal	admin

Create Map

Definition | Security

Name: Quarantine 1

Parent Map: Quarantine

Background Color:

Background Image:

Not Selected :

10.255.11.125
10.255.11.142
10.255.11.151
10.255.11.152
10.255.11.158
10.255.11.159

Added to Map :

10.255.11.29
10.255.11.32
10.255.11.34
10.255.11.99

7. Enter the name of the Quarantine Subnet in the **Name** field (e.g., Quarantine 1). This can be any name. It is not case-sensitive.

8. Make sure the **Parent Map** is **Quarantine**.

9. Add the switches you want to include in the Quarantine Subnet by selecting them from the "Not Selected" column and clicking the **Add** button to move them to the "Added to Map" column.

10. Click **OK**, then click the **Apply** button.

Repeat Steps 6 through 10 to create additional Quarantine Subnets..

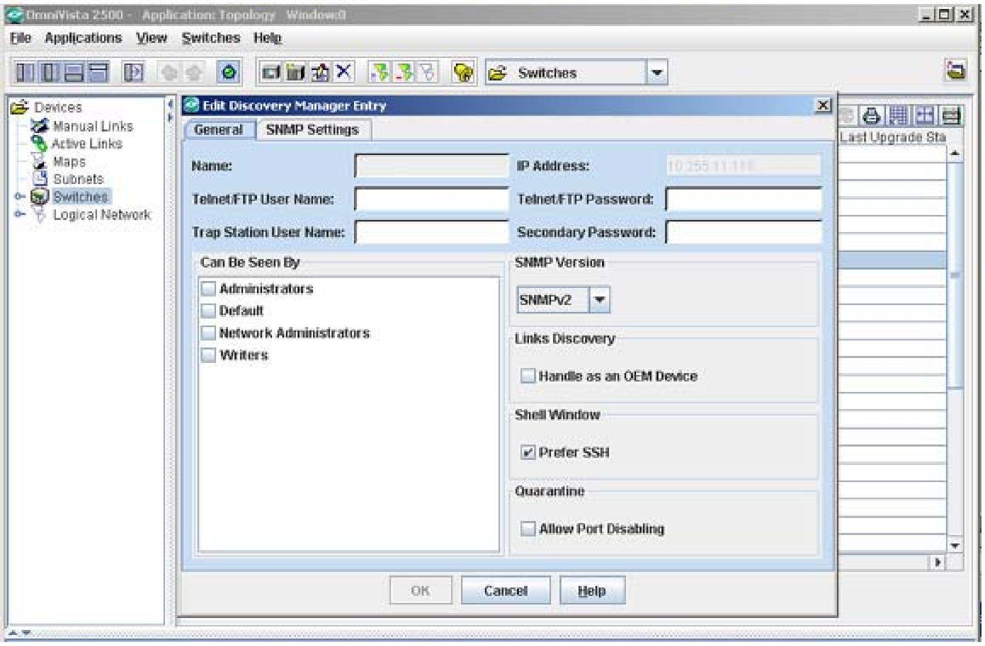
> **Note:** If Quarantine Manager is unable to determine which switch an offending host is actually connected to, it will ban on all the switches, regardless of any configured "Quarantine" Subnets.

Configuring Quarantine Manager on OmniAccess WLAN Devices

Quarantine Manager 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 OmniAcess 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.

Configuring OmniAccess for Quarantine Manager



Edit Discovery Manager Entry

Name:

IP Address: 10.255.11.118

Telnet/FTP User Name:

Telnet/FTP Password:

Trap Station User Name:

Secondary Password:

Can Be Seen By

☐ Administrators
☐ Default
☐ Network Administrators
☐ Writers

SNMP Version: SNMPv2

Links Discovery: ☐ Handle as an OEM Device

Shell Window: ☑ Prefer SSH

Quarantine: ☐ Allow Port Disabling

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.

Assigning the QMR Configuration to Switches

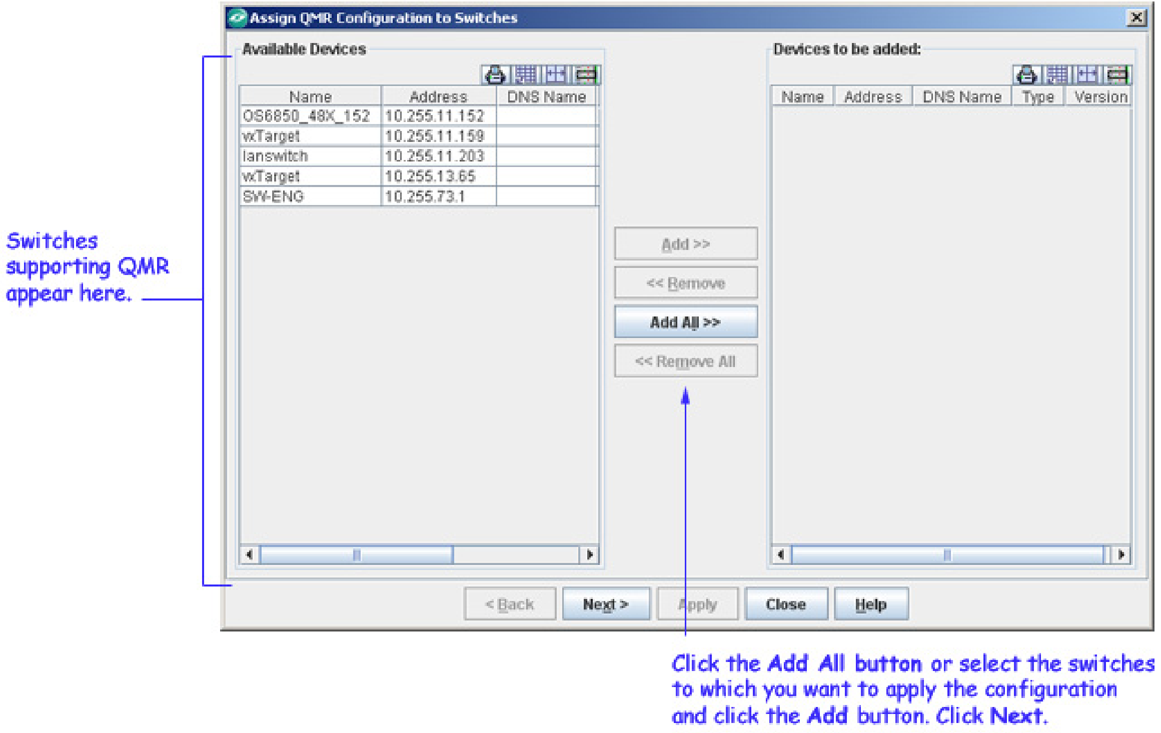
After creating a Quarantine Manager Remediation (QMR) configuration, you must assign the policy to specific switches on the network. The "Assign QMR Configuration" wizard guides you through the steps to assign policies to specific switches.

> **Note:** The "Assign Access Guardian Policy" wizard can also be used to remove Access Guardian Policies.

Adding Devices

As shown below, the switches supporting QMR in the "Available Device" area. Select the switch(es) to which you want to assign the policies and use the **Add** button to move the devices to the "Devices to be added" area. (Use the **Add** or **Remove** buttons to add or delete switches.) When you are done selecting devices, click the **Next** button.

Assign QMR Configuration Wizard - Page 1



Assign QMR Configuration to Switches

Available Devices

Name	Address	DNS Name
OS6850_48X_152	10.255.11.152	
vxTarget	10.255.11.159	
lanswitch	10.255.11.203	
vxTarget	10.255.13.65	
SW-ENG	10.255.73.1	

Devices to be added:

Name	Address	DNS Name	Type	Version

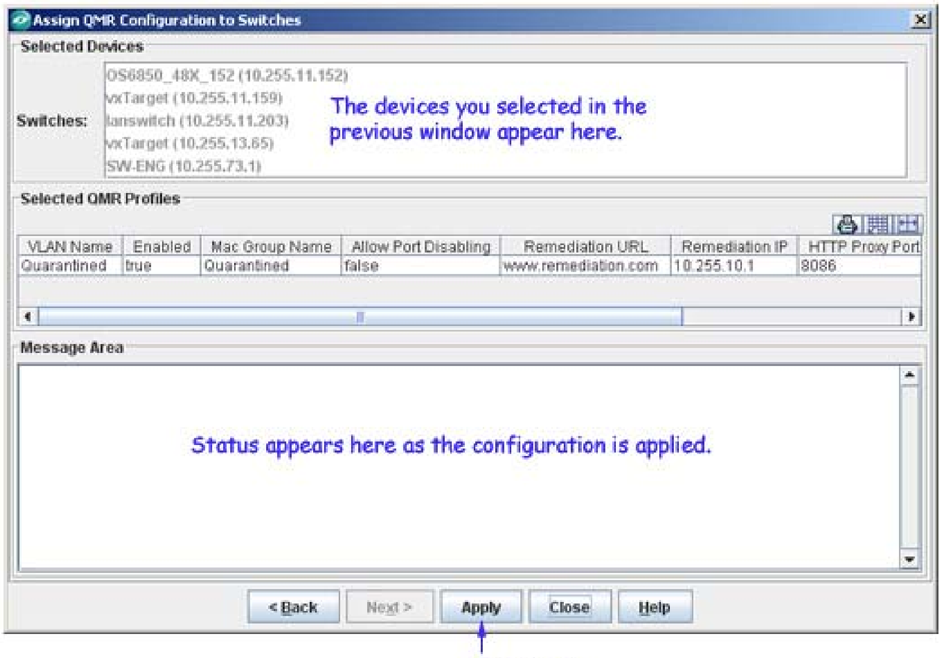
Switches supporting QMR appear here.

Click the Add All button or select the switches to which you want to apply the configuration and click the Add button. Click Next.

Applying the Configuration

After selecting the switches to which you want to apply the configuration, you must assign the configuration to those switches. As shown below, the devices you selected appear in the "Selected Devices" area. Click the **Apply** button to apply the policy. The Message Area shows the progress of the operation. When the process is complete, click the **Close** button, then click **Yes** at the exit prompt.

Assign QMR Configuration Wizard - Page 2



Assign QMR Configuration to Switches

Selected Devices

Switches:
OS6850_48X_152 (10.255.11.152)
vxTarget (10.255.11.159)
lanswitch (10.255.11.203)
vxTarget (10.255.13.65)
SW-ENG (10.255.73.1)

The devices you selected in the previous window appear here.

Selected QMR Profiles

VLAN Name	Enabled	Mac Group Name	Allow Port Disabling	Remediation URL	Remediation IP	HTTP Proxy Port
Quarantined	true	Quarantined	false	www.remediation.com	10.255.10.1	8086

Message Area

Status appears here as the configuration is applied.

Click Apply.

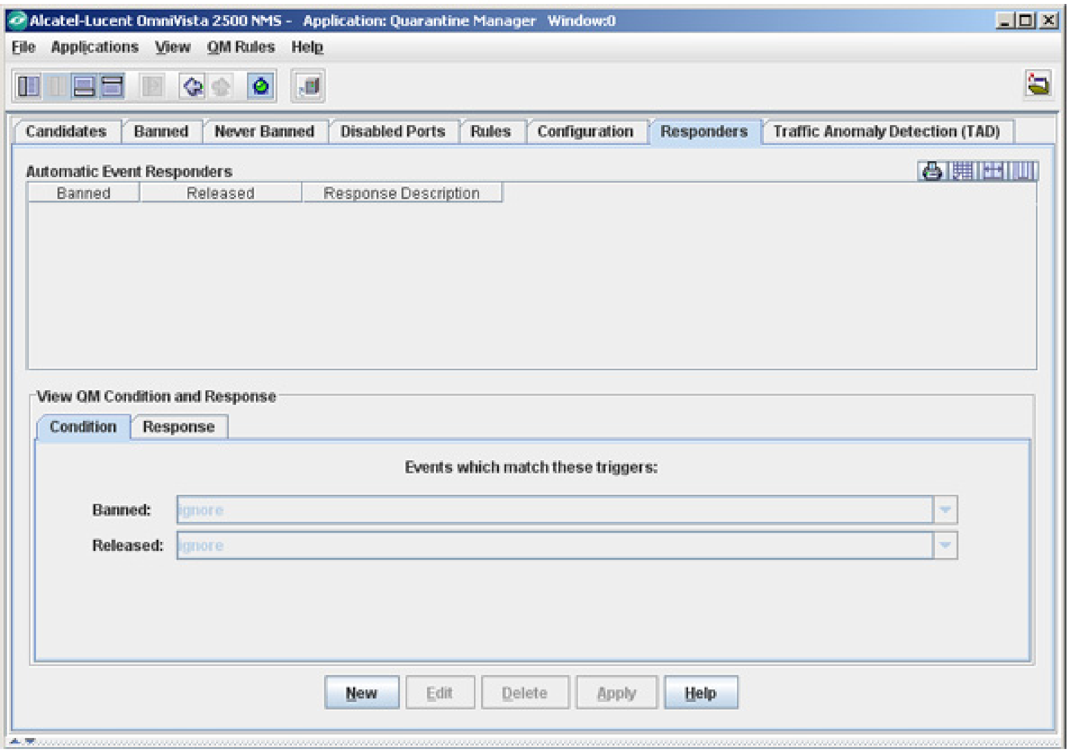
Quarantine Manager Responders Tab

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.

Responders Tab


Alcatel-Lucent OmniVista 2500 NMS - Application: Quarantine Manager Window:0
File Applications View QM Rules Help
Candidates
Banned
Never Banned
Disabled Ports
Rules
Configuration
Responders
Traffic Anomaly Detection (TAD)
Automatic Event Responders
Banned
Released
Response Description
View QM Condition and Response
Condition
Response
New
Edit
Delete
Apply
Help

Events which match these triggers:

Banned: ignore

Released: ignore

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.

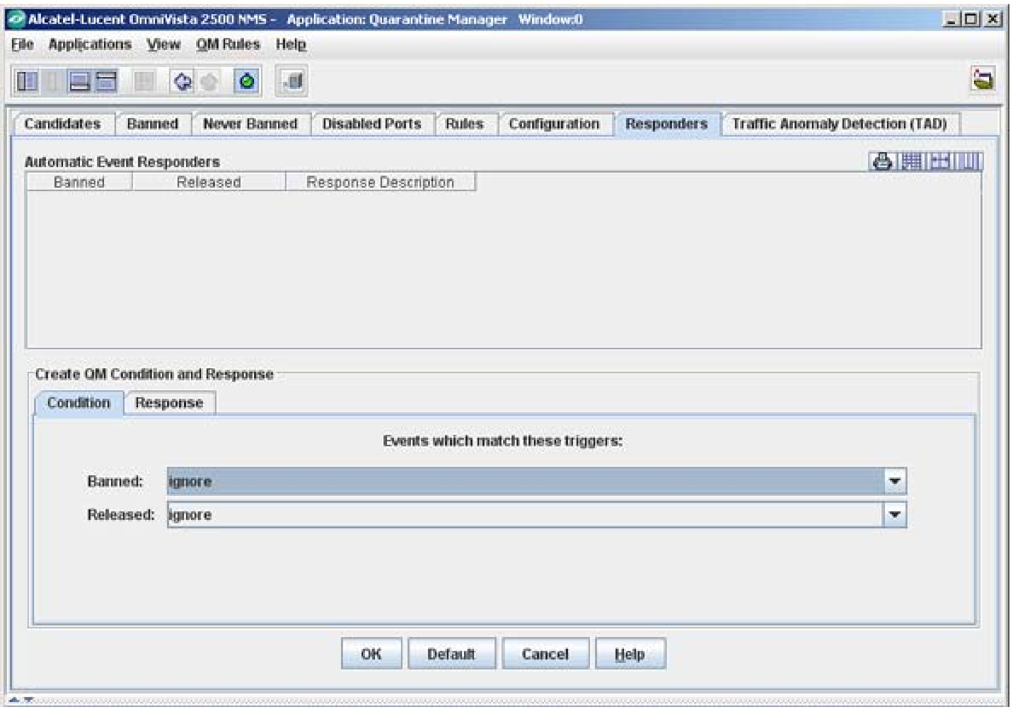
How to Configure an Event Responder

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.

Condition Tab


Alcatel-Lucent OmniVista 2500 NMS - Application: Quarantine Manager Window:0
File Applications View QM Rules Help
Candidates Banned Never Banned Disabled Ports Rules Configuration Responders Traffic Anomaly Detection (TAD)
Automatic Event Responders
Banned Released Response Description
Create QM Condition and Response
Condition Response
OK Default Cancel Help

Events which match these triggers:

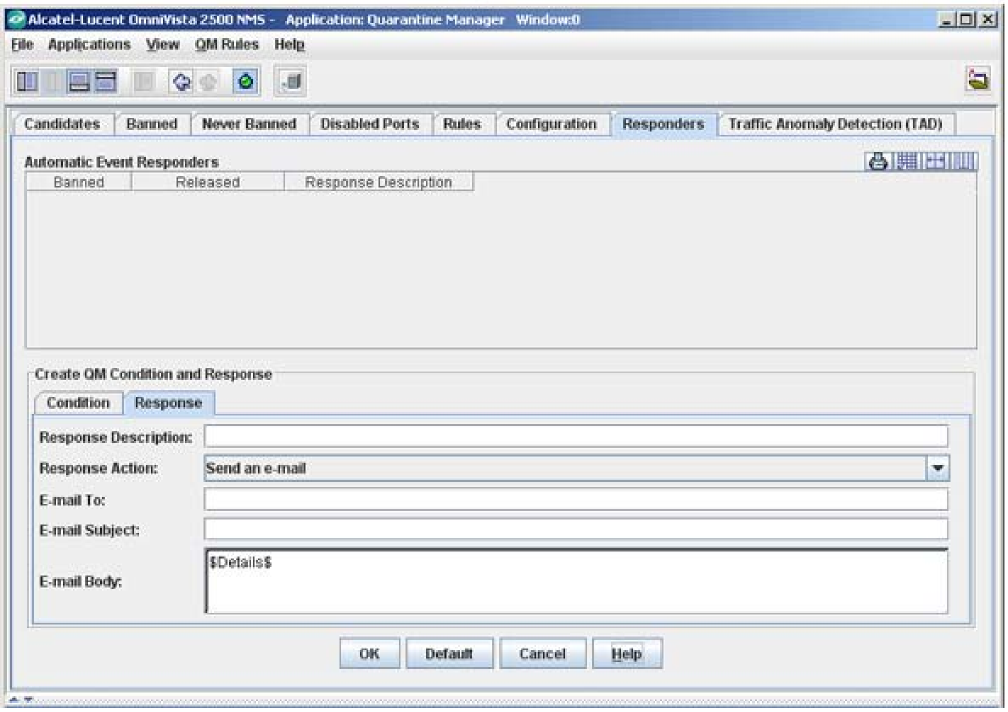
Banned: ignore

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

Response Tab


Alcatel-Lucent OmniVista 2500 NMS - Application: Quarantine Manager Window:0
File Applications View QM Rules Help
Candidates Banned Never Banned Disabled Ports Rules Configuration Responders Traffic Anomaly Detection (TAD)
Automatic Event Responders
Banned Released Response Description
Create QM Condition and Response
Condition Response
OK Default Cancel Help

Response Description:

Response Action: Send an e-mail

E-mail To:

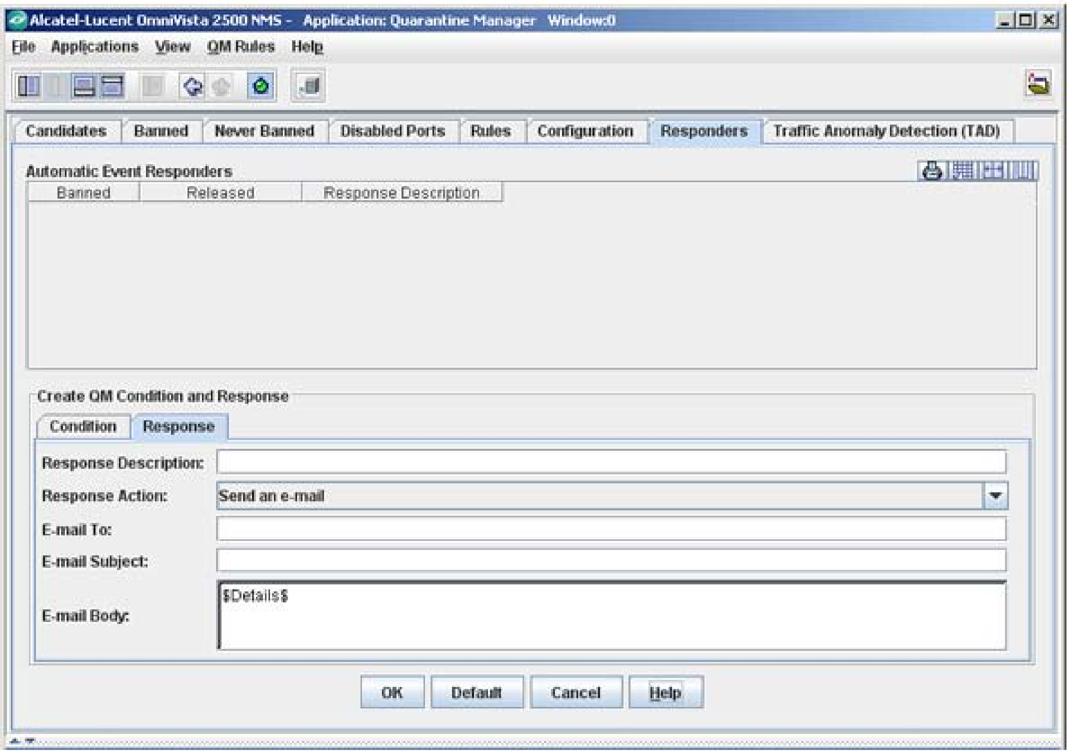
E-mail Subject:

E-mail Body: $Details$

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.

Response Tab



Response Description:

Response Action: Send an e-mail

E-mail To:

E-mail Subject:

E-mail Body: $Details$

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.)

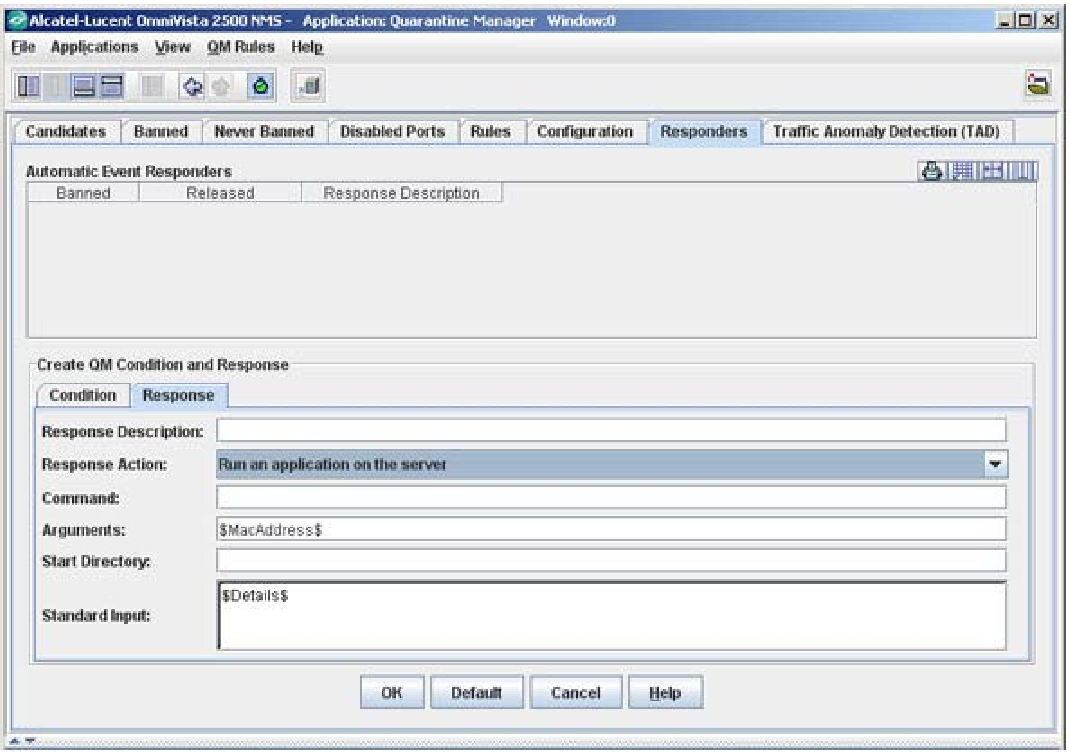
3. Enter a subject for the email that is to be sent in response.

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.


Alcatel-Lucent OmniVista 2500 NMS - Application: Quarantine Manager Window:0
File Applications View QM Rules Help
Candidates Banned Never Banned Disabled Ports Rules Configuration Responders Traffic Anomaly Detection (TAD)
Automatic Event Responders
Banned Released Response Description
Create QM Condition and Response
Condition Response
OK Default Cancel Help

Response Description:
Response Action: Run an application on the server
Command:
Arguments: $MacAddress$
Start Directory:
Standard Input: $Details$

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 0.0.0.0

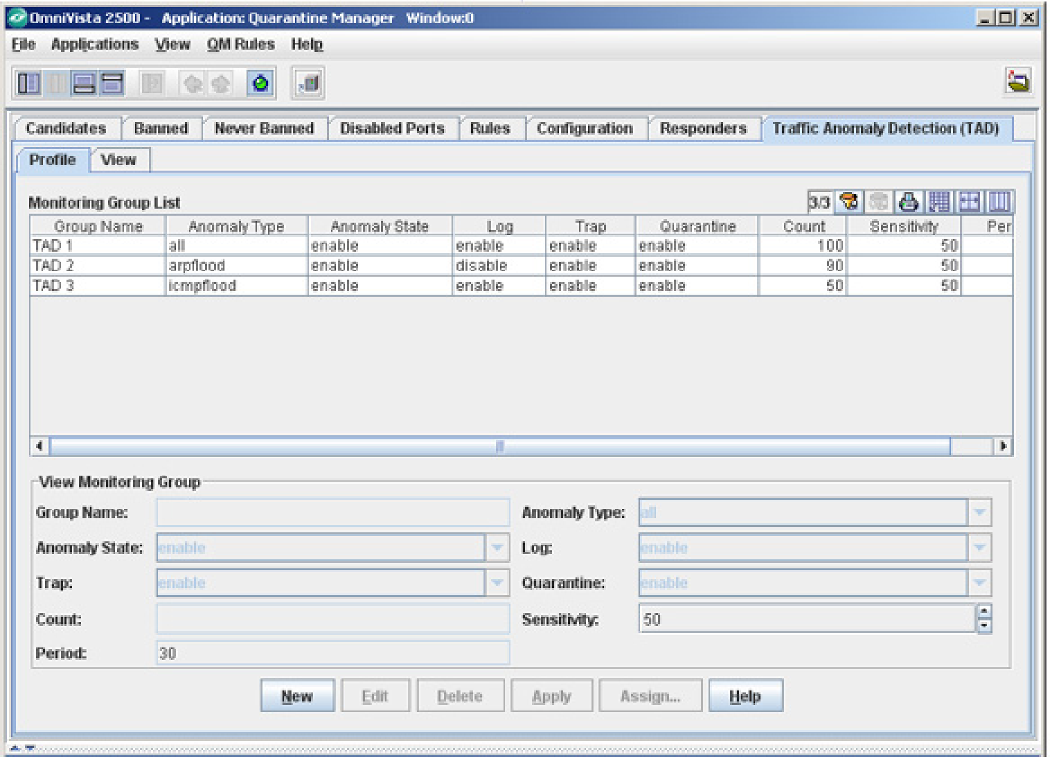
$VlanName$
The name of the vlan that the device was banned to or released from.
$MacGroupName$
The MAC group that the device was banned to or released from.
$Details$
Contains a message with the Action, Mac, IP address, Vlan, and MacGroupName.

Traffic Anomaly Detection Tab

Traffic Anomaly Detection (TAD) is a network monitoring feature that detects anomalies in the network traffic by monitoring the difference in the rate of ingress and egress packets on a port, matching a specific traffic pattern. TAD monitors these packets at configured intervals, counts the packets matching certain patterns, and applies anomaly detection rules configured by the user when an anomaly exceeds user-defined thresholds (e.g., log the event, send a trap, quarantine a port). There are two tabs within the TAD tab:

- The Profile Tab - is used to create, edit, and delete TAD Monitoring Groups and assign a group to a set of ports.
- The View Tab - is used to view TAD configurations and anomaly statistics for specific switches in the network.

Traffic Anomaly Detection Tab


OmniVista 2500 - Application: Quarantine Manager Window:0
File Applications View QM Rules Help
Candidates
Banned
Never Banned
Disabled Ports
Rules
Configuration
Responders
Traffic Anomaly Detection (TAD)
Profile
View
3/3

Monitoring Group List

Group Name	Anomaly Type	Anomaly State	Log	Trap	Quarantine	Count	Sensitivity	Per
TAD 1	all	enable	enable	enable	enable	100	50	
TAD 2	arpflood	enable	disable	enable	enable	90	50	
TAD 3	icmpflood	enable	enable	enable	enable	50	50	

View Monitoring Group

Group Name:		Anomaly Type:	all
Anomaly State:	enable	Log:	enable
Trap:	enable	Quarantine:	enable
Count:		Sensitivity:	50
Period:	30		

Profile Tab

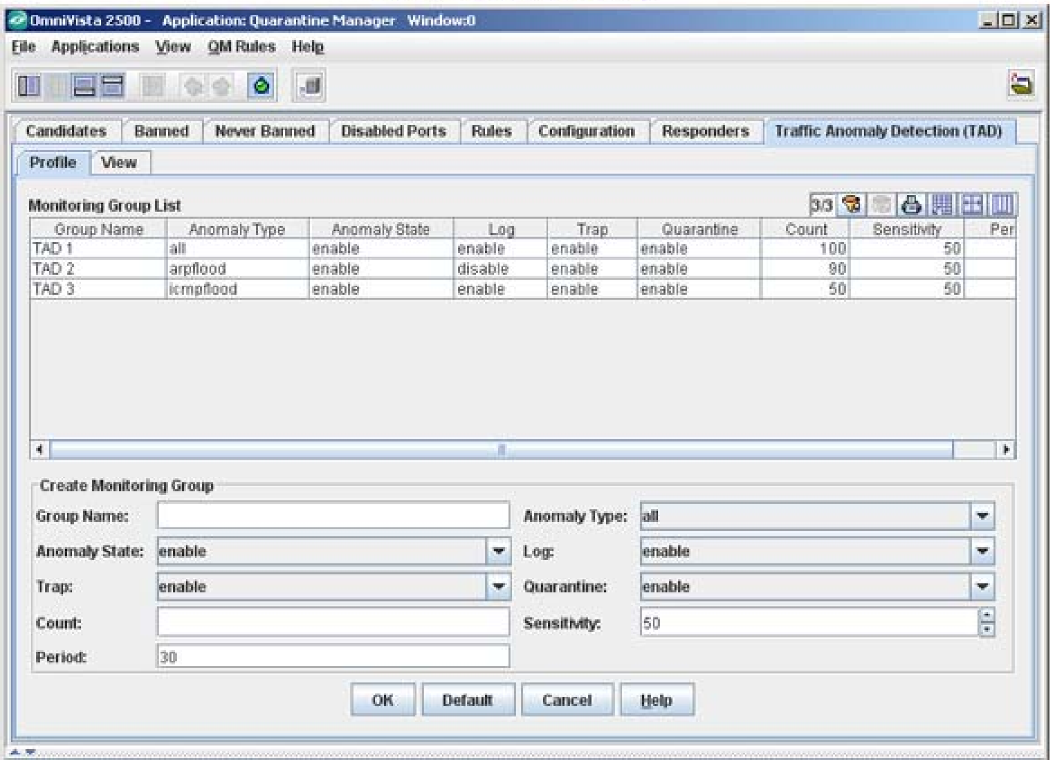
The profile tab is used to create, edit, and delete TAD Monitoring Groups. To enable TAD, you must first configure a TAD Monitoring Group.

Configuring a TAD Monitoring Group

TAD Monitoring Groups are configured using the **TAD Profile** Tab. You can create up to 32 monitoring-groups including at a time. After creating the group, you then configure the anomaly you want to detect, configure a rule to execute when the anomaly is detected, and assign a port or set of ports to the TAD Group. Follow the steps below to configure a TAD Monitoring Group.

1. Click on the **New** button to activate the Create Monitoring Group pane.

Creating a TAD Group



Monitoring Group List

Group Name	Anomaly Type	Anomaly State	Log	Trap	Quarantine	Count	Sensitivity	Per
TAD 1	all	enable	enable	enable	enable	100	50	
TAD 2	arpflood	enable	disable	enable	enable	90	50	
TAD 3	icmpflood	enable	enable	enable	enable	50	50	

Create Monitoring Group

Group Name:		Anomaly Type:	all
Anomaly State:	enable	Log:	enable
Trap:	enable	Quarantine:	enable
Count:		Sensitivity:	50
Period:	30		

2. Enter a group name (e.g., TAD 1) and specify the anomaly you want to detect (and under what conditions that anomaly is reported) by completing the fields as described below.

- **Group Name -** The name of the TAD Monitoring Group (up to 32 characters)
- **Anomaly Type -** The type of the anomaly to be enabled or disabled. Supported anomalies are described below.
  - **All** (all) - All anomaly types are monitored.
  - **ARP Address Scan** (arpaddrscan) - Occurs when a host sends a burst of ARP requests for multiple IP addresses.
  - **ARP Flood** (arpflood) - Occurs when a host receives a burst of ARP request packets.
  - **ARP Failure** (arpfailure) - Occurs when ARP queries do not elicit ARP responses.
  - **ICMP Address Scan** (icmpaddrscan) - Occurs when multiple hosts receive ICMP echo request packets at the same time.
  - **ICMP Flood** (icmpflood) - Occurs when a host receives a burst of ICMP echo request packets.

  - **ICMP Unreachable** (icmpunreachable) - Occurs when a host receives a flood of ICMP Unreachable packets.
  - **TCP Port Scan** (tcpportscan) - Occurs when a host receives a burst of TCP SYN packets for multiple TCP ports.
  - **TCP Address Scan** (tcpaddrscan) - Occurs when multiple hosts receive TCP SYN packets at the same time.
  - **SYN Flood** (synflood) - Occurs when a host receives a burst of TCP SYN packets on the same TCP port.
  - **SYN Failure** (synfailure) - Occurs when a host receives fewer SYNACKs than SYNs it sent out.
  - **SYN-ACK Scan** (synackscan) - Occurs when a host receives more SYNACKs than SYNs it sent out.
  - **Fin Scan** (finscan) - Occurs when a host receives a burst of FIN packets.
  - **Fin-Ack Diff** (finackdiff) - Occurs when a host sees more or fewer FINACK packets than it sent.
  - **Rst Count** (rstcount) - Occurs when a host receives a flood of RST packets.
- **Anomaly State -** Enables/Disabled anomaly detection.
- **Log -** Enables/Disables logging of detected anomalies. If enabled, the anomaly information will be written to a syslog if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Trap -** Enables/Disables the sending of a trap when an anomaly is detected. If enabled, a trap is sent if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Quarantine -** Enables/Disables quarantining of the port on which an anomaly is detected. If enabled, a port is quarantined if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Count -** The number of packets that must be seen during the monitoring period to trigger anomaly detection. The valid range is 1 - 100,000. Supported anomalies and the default count for each are listed below:
  - **all** - NA
  - **arpaddrscan** - 50
  - **arpflood** - 90
  - **arpfailure** - 6
  - **icmpaddrscan** -30
  - **icmpflood** -90
  - **icmpunreachable** - 20
  - **tcpportscan** - 20
  - **tcpaddrscan** - 30
  - **synflood** - 90
  - **synfailure** - 10
  - **synackcan** - 2
  - **finscan** - 6
  - **finackdiff** - 5
  - **rstcount** - 50

- **Sensitivity -** Sensitivity of anomaly detection to deviation from the expected traffic pattern. The valid range is 1 - 100. (Default = 50)
- **Period -** The time duration to observe traffic pattern, in seconds. The valid range is 5 to 3,600. (Default = 30)

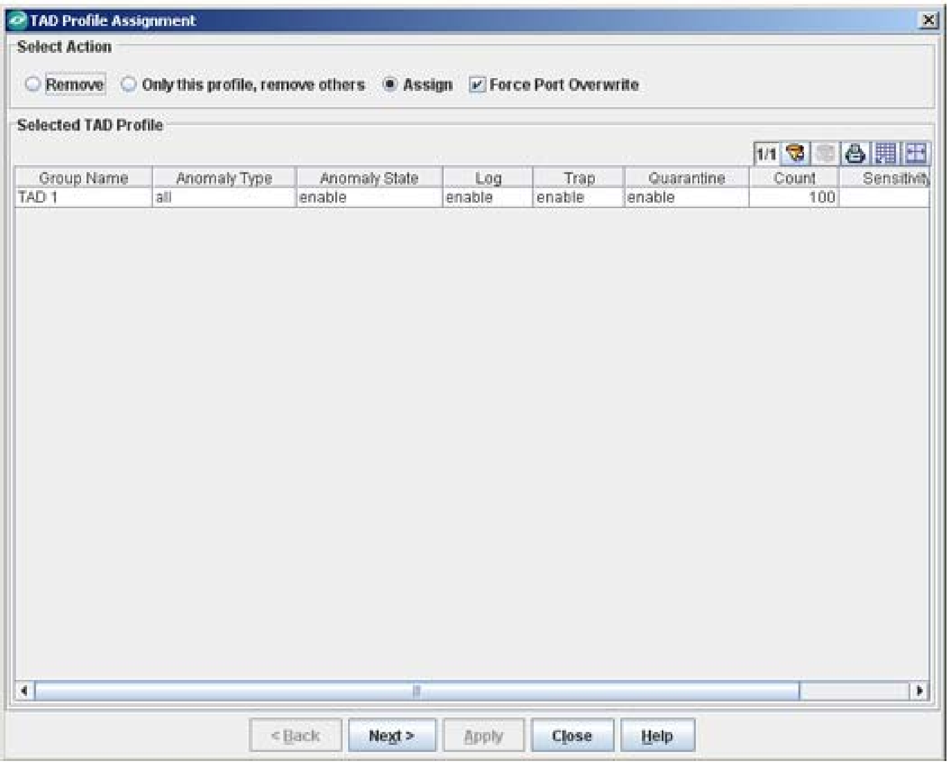
3. Click the **OK** button, then on the **Apply** button to write the configuration to the server.

4. Click on the **Assign** button to bring up the "TAD Profile Assignment" Wizard and assign a port or set of ports to the group.

Assigning Ports to the TAD Monitoring Group

After configuring the monitoring group, you must assign the ports that you want to monitor to that group. TAD applies the rules to match the specific packets when a port is in a monitoring-group. These rules exist as long as the port is a member of any monitoring-group. Follow the steps below to assign ports to the group.

TAD Profile Assignment Wizard - Page 1



TAD Profile Assignment

Select Action

○ Remove ○ Only this profile, remove others ● Assign ☑ Force Port Overwrite

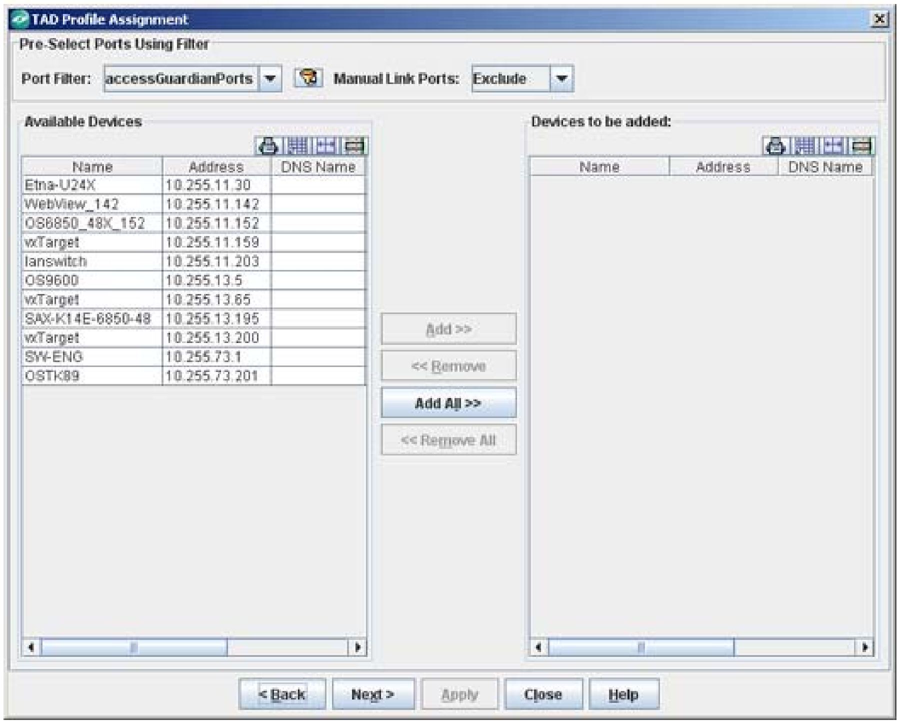
Selected TAD Profile

Group Name	Anomaly Type	Anomaly State	Log	Trap	Quarantine	Count	Sensitivity
TAD 1	all	enable	enable	enable	enable	100	

1. The first page of the wizard displays the group to which you are assigning the ports. By default, the "Action" is to "Assign" ports. Select the "Force Port Overwrite" checkbox to assign all selected ports to this TAD Group (and remove them from any previously assigned groups, if applicable). Click the **Next** button. Page 2 of the wizard appears.

> **Note:** You can also used the wizard to remove ports from a TAD Group, by selecting the "Remove" radio button; or select the "Only this profile, remove others" radio button to remove ports from any existing profiles to which they are assigned and assign them to this new profile.

TAD Profile Assignment Wizard - Page 2



Pre-Select Ports Using Filter

Port Filter: accessGuardianPorts   Manual Link Ports: Exclude

Available Devices

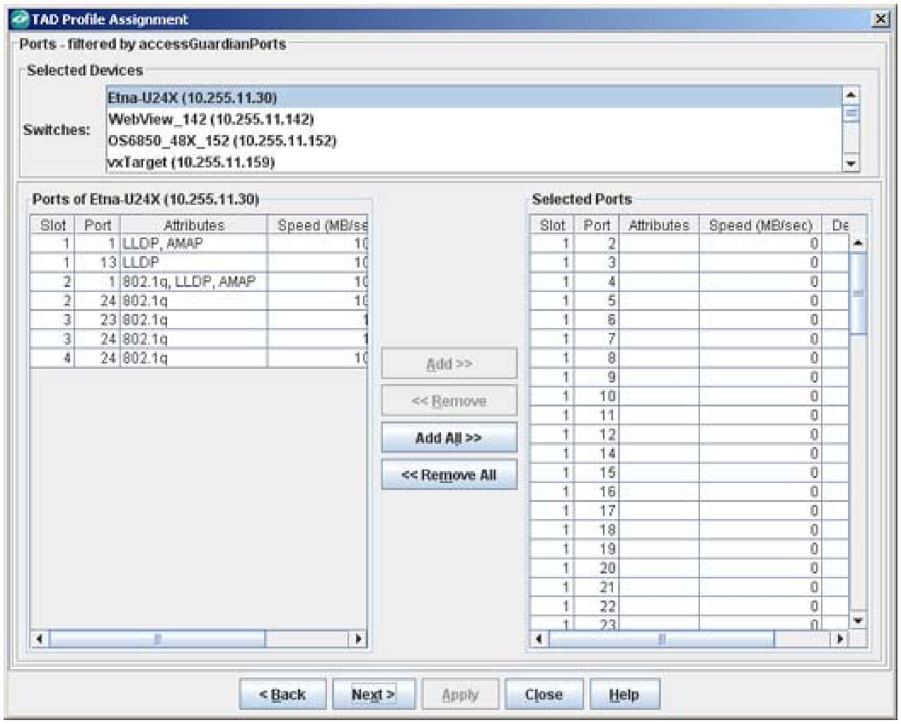
Name	Address	DNS Name
Etna-U24X	10.255.11.30	
WebView_142	10.255.11.142	
OS6850_48X_152	10.255.11.152	
vxTarget	10.255.11.159	
lanswitch	10.255.11.203	
OS9600	10.255.13.5	
vxTarget	10.255.13.65	
SAX-K14E-6850-48	10.255.13.195	
vxTarget	10.255.13.200	
SW-ENG	10.255.73.1	
OSTK89	10.255.73.201	

Devices to be added:

Name	Address	DNS Name

2. The devices that support TAD appear in the "Available Devices" area. Select the switches that you want to monitor and use the **Add** button to move them to the "Devices to be added" area. Click the **Next** button. Page 3 of the wizard appears.

TAD Profile Assignment Wizard - Page 3



Ports - filtered by accessGuardianPorts

Selected Devices

Switches:
Etna-U24X (10.255.11.30)
WebView_142 (10.255.11.142)
OS6850_48X_152 (10.255.11.152)
vxTarget (10.255.11.159)

Ports of Etna-U24X (10.255.11.30)

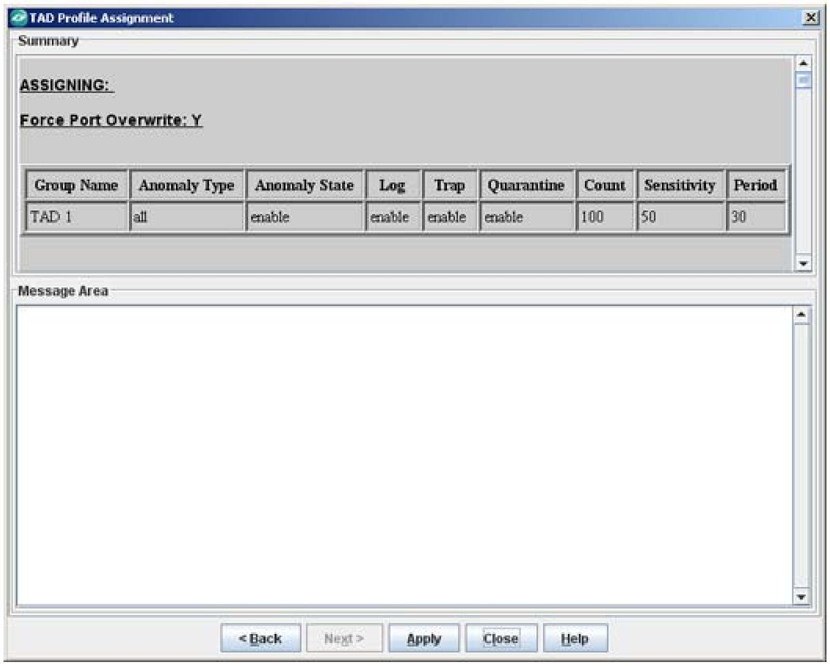
Slot	Port	Attributes	Speed (MB/se
1	1	LLDP, AMAP	10
1	13	LLDP	10
2	1	802.1q, LLDP, AMAP	10
2	24	802.1q	10
3	23	802.1q	1
3	24	802.1q	1
4	24	802.1q	10

Selected Ports

Slot	Port	Attributes	Speed (MB/sec)	De
1	2		0	
1	3		0	
1	4		0	
1	5		0	
1	6		0	
1	7		0	
1	8		0	
1	9		0	
1	10		0	
1	11		0	
1	12		0	
1	14		0	
1	15		0	
1	16		0	
1	17		0	
1	18		0	
1	19		0	
1	20		0	
1	21		0	
1	22		0	
1	23		0	

3. Select a device in the "Selected Devices" area, select the ports that you want to monitor and use the **Add** button to move them to the "Selected Ports" area. Page 4 of the wizard appears.

TAD Profile Assignment Wizard - Page 4



ASSIGNING:

Force Port Overwrite: Y

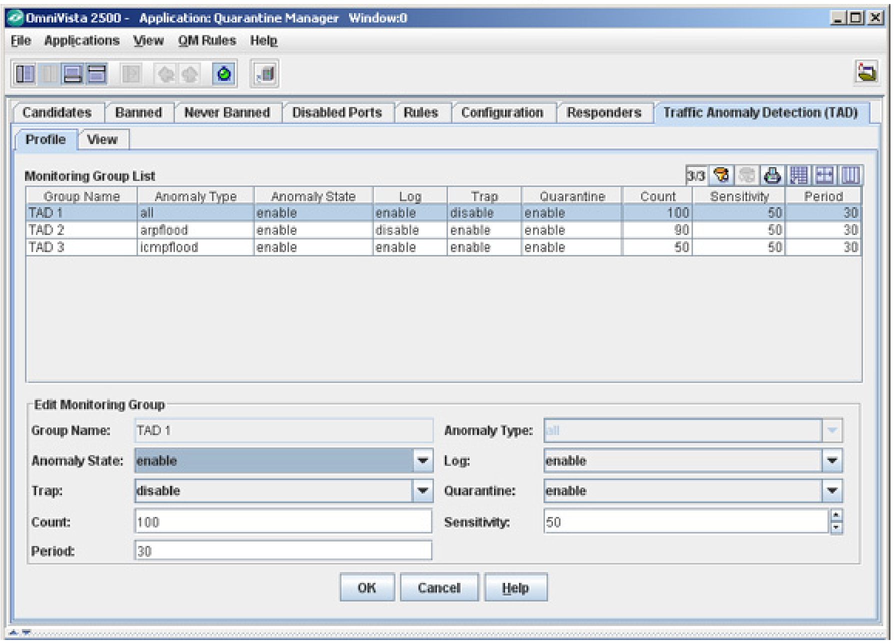
Group Name	Anomaly Type	Anomaly State	Log	Trap	Quarantine	Count	Sensitivity	Period
TAD 1	all	enable	enable	enable	enable	100	50	30

4. The final page of the wizard displays the TAD to which you are assigning the ports. Click the Apply button to assign the ports. The progress of the operation is displayed in the Message Area.

Editing a TAD Monitoring Group

To edit an existing TAD Monitoring Group, select the group in the Monitoring Group List Table and click on the **Edit** button. The Edit Monitoring Group Pane is activated.

Editing a TAD Group


OmniVista 2500 - Application: Quarantine Manager Window:0
File Applications View QM Rules Help
Candidates
Banned
Never Banned
Disabled Ports
Rules
Configuration
Responders
Traffic Anomaly Detection (TAD)
Profile
View
3/3
OK
Cancel
Help

Monitoring Group List

Group Name	Anomaly Type	Anomaly State	Log	Trap	Quarantine	Count	Sensitivity	Period
TAD 1	all	enable	enable	disable	enable	100	50	30
TAD 2	arpflood	enable	disable	enable	enable	90	50	30
TAD 3	icmpflood	enable	enable	enable	enable	50	50	30

Edit Monitoring Group

Group Name:	TAD 1	Anomaly Type:	all
Anomaly State:	enable	Log:	enable
Trap:	disable	Quarantine:	enable
Count:	100	Sensitivity:	50
Period:	30		

1. Make any edits to the configuration fields, as described below.

- **Group Name -** The name of the TAD Monitoring Group (up to 32 characters)
- **Anomaly Type -** The type of the anomaly to be enabled or disabled. Supported anomalies are described below.
    - **All** (all) - All anomaly types are monitored.
    - **ARP Address Scan** (arpaddrscan) - Occurs when a host sends a burst of ARP requests for multiple IP addresses.
    - **ARP Flood** (arpflood) - Occurs when a host receives a burst of ARP request packets.
    - **ARP Failure** (arpfailure) - Occurs when ARP queries do not elicit ARP responses.
    - **ICMP Address Scan** (icmpaddrscan) - Occurs when multiple hosts receive ICMP echo request packets at the same time.
    - **ICMP Flood** (icmpflood) - Occurs when a host receives a burst of ICMP echo request packets.
    - **ICMP Unreachable** (icmpunreachable) - Occurs when a host receives a flood of ICMP Unreachable packets.
    - **TCP Port Scan** (tcpportscan) - Occurs when a host receives a burst of TCP SYN packets for multiple TCP ports.
    - **TCP Address Scan** (tcpaddrscan) - Occurs when multiple hosts receive TCP SYN packets at the same time.
    - **SYN Flood** (synflood) - Occurs when a host receives a burst of TCP SYN packets on the same TCP port.
    - **SYN Failure** (synfailure) - Occurs when a host receives fewer SYNACKs than SYNs it sent out.
    - **SYN-ACK Scan** (synackscan) - Occurs when a host receives more SYNACKs than SYNs it sent out.
    - **Fin Scan** (finscan) - Occurs when a host receives a burst of FIN packets.
    - **Fin-Ack Diff** (finackdiff) - Occurs when a host sees more or fewer FINACK packets than it sent.
    - **Rst Count** (rstcount) - Occurs when a host receives a flood of RST packets.
- **Anomaly State -** Enables/Disabled anomaly detection.
- **Log -** Enables/Disables logging of detected anomalies. If enabled, the anomaly information will be written to a syslog if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Trap -** Enables/Disables the sending of a trap when an anomaly is detected. If enabled, a trap is sent if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Quarantine -** Enables/Disables quarantining of the port on which an anomaly is detected. If enabled, a port is quarantined if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Count -** The number of packets that must be seen during the monitoring period to trigger anomaly detection. The valid range is 1 - 100,000. Supported anomalies and the default count for each are listed below:
    - **all** - NA

  - **arpaddrscan** - 50
  - **arpflood** - 90
  - **arpfailure** - 6
  - **icmpaddrscan** -30
  - **icmpflood** -90
  - **icmpunreachable** - 20
  - **tcpportscan** - 20
  - **tcpaddrscan** - 30
  - **synflood** - 90
  - **synfailure** - 10
  - **synackcan** - 2
  - **finscan** - 6
  - **finackdiff** - 5
  - **rstcount** - 50
- **Sensitivity -** Sensitivity of anomaly detection to deviation from the expected traffic pattern. The valid range is 1 - 100. (Default = 50)
- **Period -** The time duration to observe traffic pattern, in seconds. The valid range is 5 to 3,600. (Default = 30)

2. Click the **OK** button, then on the **Apply** button to write the configuration to the server.

3. Click on the **Assign** button to bring up the "TAD Profile Assignment" Wizard and assign a port or set of ports to the edited group.

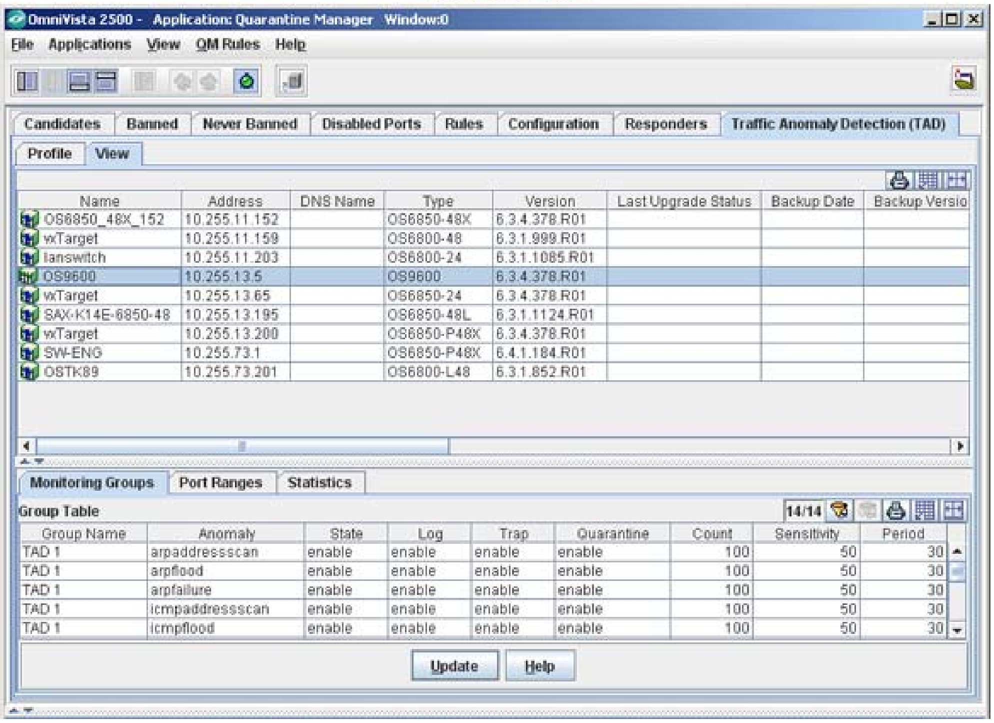
Deleting a TAD Monitoring Group

To delete a TAD Monitoring Group, select the group in the Monitoring Group List. Click the **Delete** button, then click the **Apply** button.

View Tab

The View Tab is used to view TAD configurations and anomaly statistics for specific switches in the network. There are three tabs within the View Tab: Monitoring Groups, Port Ranges, and Statistics

TAD View Tab



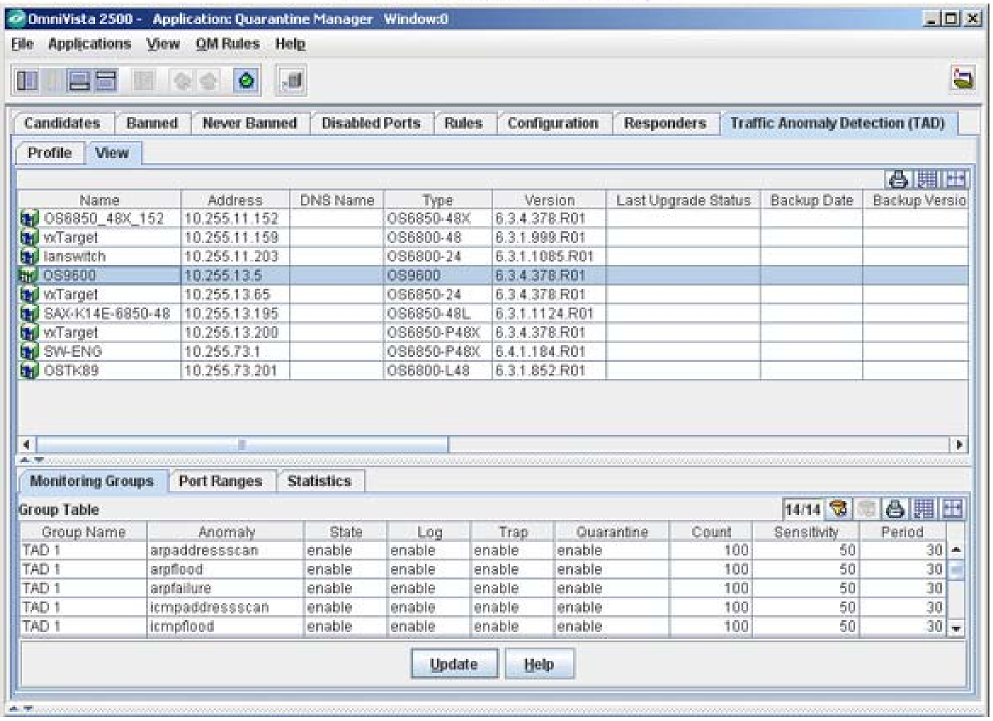
Name	Address	DNS Name	Type	Version	Last Upgrade Status	Backup Date	Backup Versio
OS6850_48X_152	10.255.11.152		OS6850-48X	6.3.4.378.R01			
wxTarget	10.255.11.159		OS6800-48	6.3.1.999.R01			
lanswitch	10.255.11.203		OS6800-24	6.3.1.1085.R01			
OS9600	10.255.13.5		OS9600	6.3.4.378.R01			
wxTarget	10.255.13.65		OS6850-24	6.3.4.378.R01			
SAX-K14E-6850-48	10.255.13.195		OS6850-48L	6.3.1.1124.R01			
wxTarget	10.255.13.200		OS6850-P48X	6.3.4.378.R01			
SW-ENG	10.255.73.1		OS6850-P48X	6.4.1.184.R01			
OSTK89	10.255.73.201		OS6800-L48	6.3.1.852.R01			

Group Name	Anomaly	State	Log	Trap	Quarantine	Count	Sensitivity	Period
TAD 1	arpaddressscan	enable	enable	enable	enable	100	50	30
TAD 1	arpflood	enable	enable	enable	enable	100	50	30
TAD 1	arpfailure	enable	enable	enable	enable	100	50	30
TAD 1	icmpaddressscan	enable	enable	enable	enable	100	50	30
TAD 1	icmpflood	enable	enable	enable	enable	100	50	30

Monitoring Groups

The Monitoring Groups tab displays configuration information for all TAD Groups configured for a switch on the network. Select the switch you want to monitor from the list of available switches above to display the configuration information for that switch.

TAD View Monitoring Groups



Name	Address	DNS Name	Type	Version	Last Upgrade Status	Backup Date	Backup Versio
OS6850_48X_152	10.255.11.152		OS6850-48X	6.3.4.378.R01			
wxTarget	10.255.11.159		OS6800-48	6.3.1.999.R01			
lanswitch	10.255.11.203		OS6800-24	6.3.1.1085.R01			
OS9600	10.255.13.5		OS9600	6.3.4.378.R01			
wxTarget	10.255.13.65		OS6850-24	6.3.4.378.R01			
SAX-K14E-6850-48	10.255.13.195		OS6850-48L	6.3.1.1124.R01			
wxTarget	10.255.13.200		OS6850-P48X	6.3.4.378.R01			
SW-ENG	10.255.73.1		OS6850-P48X	6.4.1.184.R01			
OSTK89	10.255.73.201		OS6800-L48	6.3.1.852.R01			

Group Name	Anomaly	State	Log	Trap	Quarantine	Count	Sensitivity	Period
TAD 1	arpaddressscan	enable	enable	enable	enable	100	50	30
TAD 1	arpflood	enable	enable	enable	enable	100	50	30
TAD 1	arpfailure	enable	enable	enable	enable	100	50	30
TAD 1	icmpaddressscan	enable	enable	enable	enable	100	50	30
TAD 1	icmpflood	enable	enable	enable	enable	100	50	30

Monitoring Groups Information

- **Group Name -** The name of the TAD Monitoring Group (up to 32 characters)
- **Anomaly Type -** The type of the anomaly to be enabled or disabled. Supported anomalies are described below.

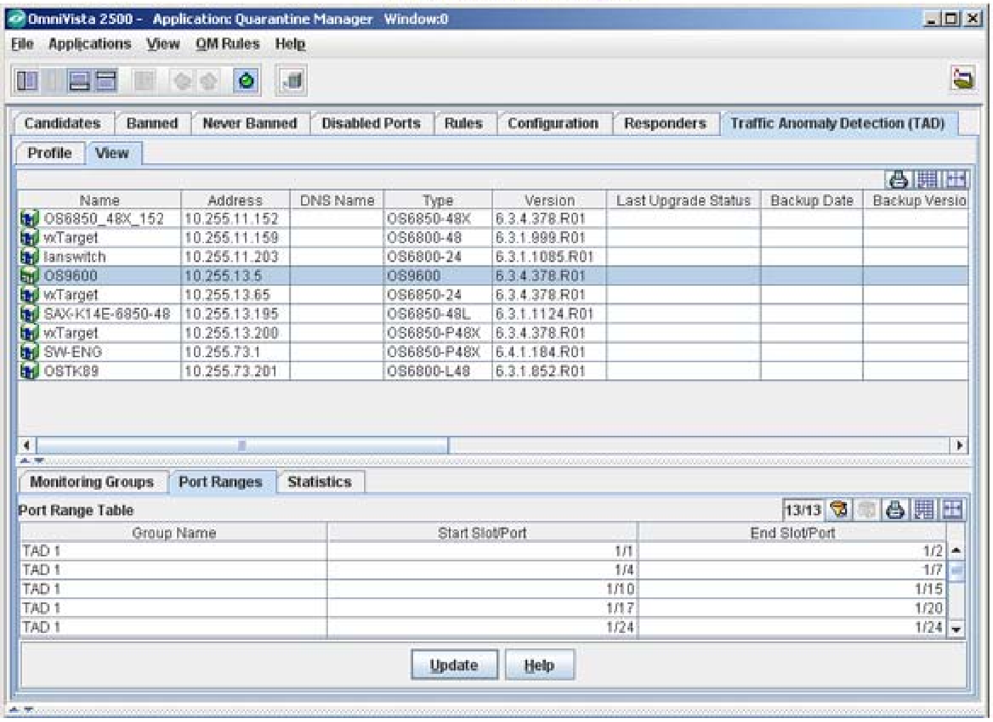
- **State -** Anomaly detection administrative status (Enabled/Disabled).
- **Log -** Anomaly detection logging state (Enabled/Disabled). (Default = Disabled)
- **Trap -** Anomaly detection trap state (Enabled/Disabled). (Default = Disabled)
- **Quarantine -** Anomaly detection quarantine state (Enabled/Disabled). (Default = Disabled)
- **Count -** Configured Count parameter. This is the number of packets that must be seen during the monitoring period to trigger anomaly detection. The valid range is 1 - 100,000.

- **Sensitivity -** Configured Sensitivity parameter. This is the anomaly detection to deviation from the expected traffic pattern. The valid range is 1 - 100. (Default = 50)
- **Period -** Configured monitoring time period. The time duration to observe traffic pattern, in seconds. The valid range is 5 to 3,600. (Default = 30)

Port Ranges

The Port Ranges tab displays switches port or ports being monitored by a TAD Monitoring Group. Select a switch from the list of available switches above to display the TAD Group port range information for that switch.

TAD View Port Ranges



Name	Address	DNS Name	Type	Version	Last Upgrade Status	Backup Date	Backup Versio
OS6850_48X_152	10.255.11.152		OS6850-48X	6.3.4.378.R01			
wTarget	10.255.11.159		OS6800-48	6.3.1.999.R01			
lanswitch	10.255.11.203		OS6800-24	6.3.1.1085.R01			
OS9600	10.255.13.5		OS9600	6.3.4.378.R01			
wTarget	10.255.13.65		OS6850-24	6.3.4.378.R01			
SAX-K14E-6850-48	10.255.13.195		OS6850-48L	6.3.1.1124.R01			
wTarget	10.255.13.200		OS6850-P48X	6.3.4.378.R01			
SW-ENG	10.255.73.1		OS6850-P48X	6.4.1.184.R01			
OSTK89	10.255.73.201		OS6800-L48	6.3.1.852.R01			

Port Range Table

Group Name	Start Slot/Port	End Slot/Port
TAD 1	1/1	1/2
TAD 1	1/4	1/7
TAD 1	1/10	1/15
TAD 1	1/17	1/20
TAD 1	1/24	1/24

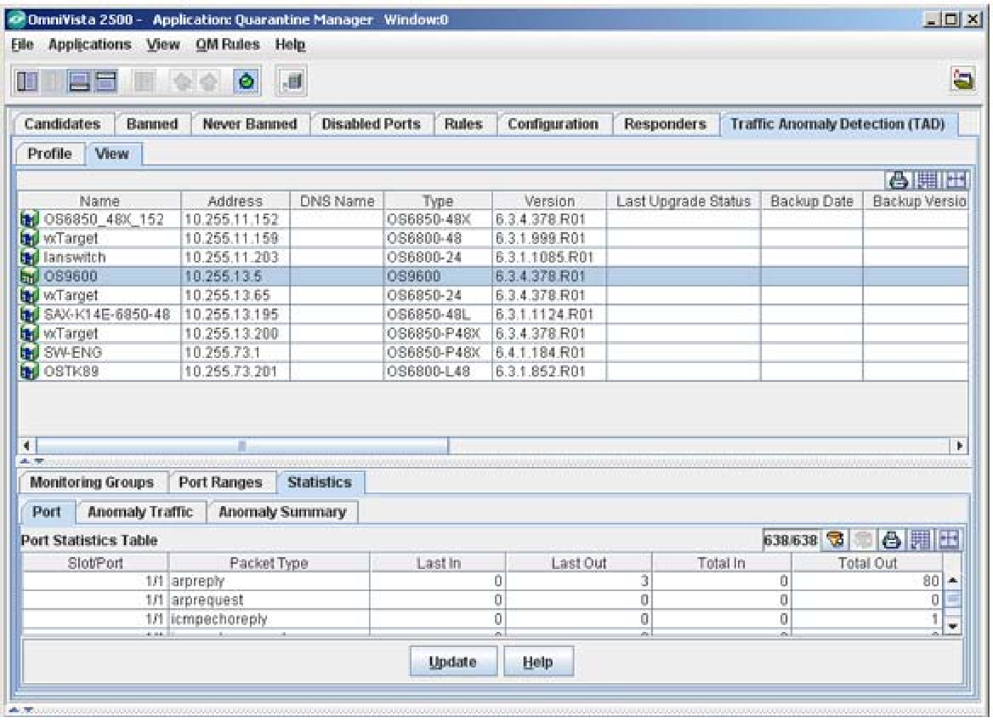
Port Ranges Information

- **Group Name -** The name of the TAD Monitoring Group for the port(s).
- **Start Slot/Port -** The first slot/port number in the range of ports being monitored.
- **End Slot/Port -** The last slot/port number in the range of ports being monitored.

Statistics

The Statistics tab is used to view traffic anomaly information for ports being monitored by a TAD Monitoring Group. Select a switch from the list of available switches above to display the monitoring information for that switch. The information is displayed in the following tabs: Port, Anomaly Traffic, Anomaly Summary.

TAD View Port Statistics



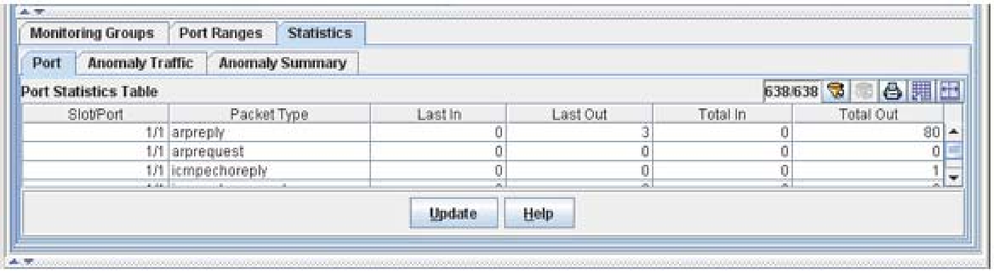
Name	Address	DNS Name	Type	Version	Last Upgrade Status	Backup Date	Backup Versio
OS6850_48X_152	10.255.11.152		OS6850-48X	6.3.4.378.R01			
wxTarget	10.255.11.158		OS6800-48	6.3.1.999.R01			
lanswitch	10.255.11.203		OS6800-24	6.3.1.1085.R01			
OS9600	10.255.13.5		OS9600	6.3.4.378.R01			
wxTarget	10.255.13.65		OS6850-24	6.3.4.378.R01			
SAX-K14E-6850-48	10.255.13.195		OS6850-48L	6.3.1.1124.R01			
wxTarget	10.255.13.200		OS6850-P48X	6.3.4.378.R01			
SW-ENG	10.255.73.1		OS6850-P48X	6.4.1.184.R01			
OSTK89	10.255.73.201		OS6800-L48	6.3.1.852.R01			

Slot/Port	Packet Type	Last In	Last Out	Total In	Total Out
1/1	arpreply	0	3	0	80
1/1	arprequest	0	0	0	0
1/1	icmpechoreply	0	0	0	1

Port Statistics

The Port tab displays anomaly pattern counts on ports belonging to TAD Monitoring Groups.

TAD View Port Statistics



Slot/Port	Packet Type	Last In	Last Out	Total In	Total Out
1/1	arpreply	0	3	0	80
1/1	arprequest	0	0	0	0
1/1	icmpechoreply	0	0	0	1

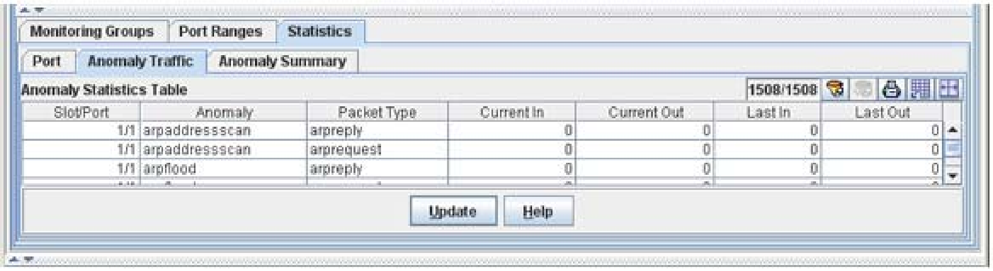
- **Slot/Port -** The slot/port being monitored.
- **Packet Type -** The type of packet being monitored.

- **Last In -** The number of incoming anomaly packets observed during the last 5 seconds.
- **Last Out -** The number of outgoing anomaly packets observed during the last 5 seconds.
- **Total In -** The total number of incoming anomaly packets observed since monitoring was enabled.
- **Total Out -** The total number of outgoing anomaly packets observed since monitoring was enabled.

Anomaly Traffic Statistics

The Anomaly Traffic Statistics tab displays anomaly specific traffic statistics

TAD View Anomaly Traffic Statistics



Anomaly Statistics Table 1508/1508

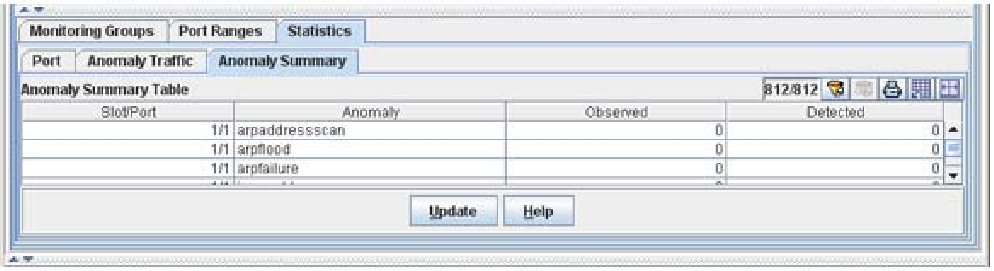
Slot/Port	Anomaly	Packet Type	Current In	Current Out	Last In	Last Out
1/1	arpaddressscan	arpreply	0	0	0	0
1/1	arpaddressscan	arprequest	0	0	0	0
1/1	arpflood	arpreply	0	0	0	0

- **Slot/Port -** The slot/port being monitored.
- **Anomaly -** The type of anomaly being monitored.
- **Packet Type -** The type of packet being monitored.
- **Current In -** The number of incoming packets during the current monitoring period.
- **Current Out -** The number of outgoing packets during the current monitoring period.
- **Last In -** The number of incoming packets during the last monitoring period.
- **Last Out -** The number of outgoing packets during the last monitoring period.

Anomaly Summary Statistics

The Anomaly Summary Statistics tab displays the anomaly check summary.

TAD View Anomaly Summary Statistics



Anomaly Summary Table 812/812

Slot/Port	Anomaly	Observed	Detected
1/1	arpaddressscan	0	0
1/1	arpflood	0	0
1/1	arpfailure	0	0

- Slot/Port - Slot number for the module and physical port number on that module.
- Anomaly - The type of anomaly.
- Observed - The number of times an anomaly was observed on this port since monitoring was enabled.
- Detected - The number of times an anomaly was detected on this port since monitoring was enabled (the number of times the anomaly exceeded monitoring limits (Count/Period/Sen.