

# Chapter 19



## Event Manager

### 19.1 Overview

The NetVigil Event Manager Console displays messages (traps, logs, windows events) forwarded from the Message Handler (described in Chapter 7, “Message Handler for Traps & Logs”), as well as threshold violations. It provides features for acknowledging, suppressing and deleting events using a web interface. Events can be suppressed until a particular date and time, or until the state changes. The screen refreshes automatically every few minutes (this interval can be changed on the `Manage -> Prefs` page).

**NOTE:** *The Event Manager window accessed by clicking on the “Event Manager” hyperlink on the main NetVigil Status screen.*

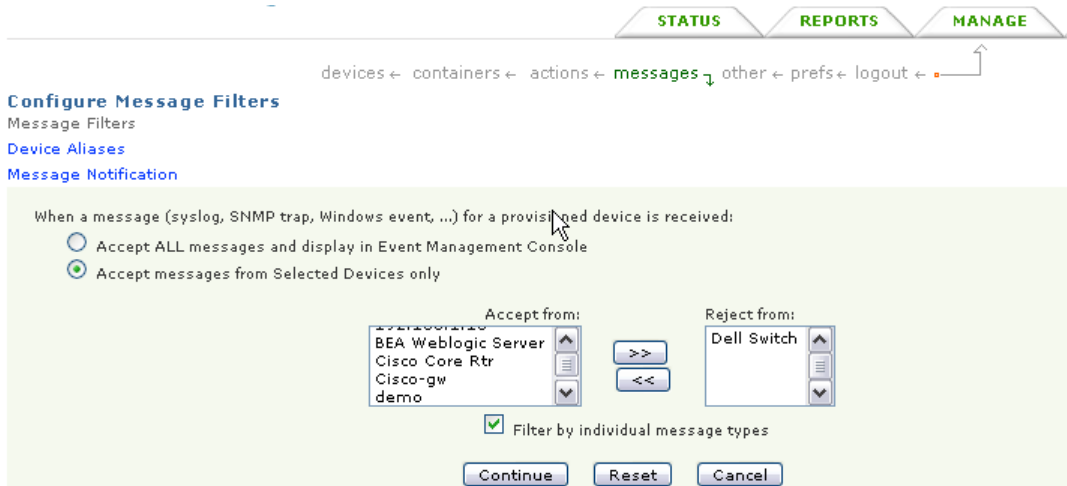
### 19.2 Managing Messages on the DGE

You can trigger actions & notifications when an incoming log or trap message matches a particular rule, and whether it should be displayed on the Event Manager console. Once messages are displayed on the Event Console, they can be annotated, acknowledged or suppressed.

The following message related changes are managed by going to `Manage-> Messages` when logged in as an end user.

## 19.2.1 Event Filters

You can either accept all messages that are forwarded by the Message Handler and display them on the Event Manager Console, or else select the devices and the message types to be accepted from each device. Messages that do not match the specified filter are not displayed on the Event Manager and cannot trigger any notifications.



### ❑ To create an Event Filter:

1. Click on manage -> Messages
2. To accept all messages and display them, click on the radio button "Accept All messages"
3. To select a list of devices to accept messages, click on the alternate radio button and select devices

- You can also select which types of messages to accept by clicking on the “filter by individual message types” checkbox and then selecting the message type for each device from the list.

**Configure Message Filters**

Please select the types of events you would like to accept for each device

192.168.1.10 (192.168.1.10)	<input checked="" type="radio"/> all types of message(s) <input type="radio"/> select individual message types	(file/syslog) SSH: Break-In Attempt as ROOT (file/syslog) SSH: Invalid Password For ROOT (file/syslog) SSH: Invalid Password Specified (socket/ism) ISM: Used For Testing
BEA Weblogic Server (192.168.1.160)	<input checked="" type="radio"/> all types of message(s) <input type="radio"/> select individual message types	(file/syslog) SSH: Break-In Attempt as ROOT (file/syslog) SSH: Invalid Password For ROOT (file/syslog) SSH: Invalid Password Specified (socket/ism) ISM: Used For Testing
Cisco Core Rtr (r00.dl1s01.inetaddr.net)	<input checked="" type="radio"/> all types of message(s) <input type="radio"/> select individual message types	(file/syslog) SSH: Break-In Attempt as ROOT (file/syslog) SSH: Invalid Password For ROOT (file/syslog) SSH: Invalid Password Specified (socket/ism) ISM: Used For Testing

## 19.2.2 Notifications

You can trigger notifications for incoming messages and traps by assigning action profiles to them. You can select whether to trigger an action profile for all devices, for selected devices or no devices.

### Configure Message Notification

[Message Filters](#)

[Device Aliases](#)

Message Notification

When a message (syslog, SNMP trap, Windows event, ...) for a provisioned device is received:

Apply  To

### Assign Action Profile

Action: Test Action

Select the message types to which you would like to assign this action profile.

DEVICE
BEA Weblogic Server (192.168.1.160)
<ul style="list-style-type: none"><li>(file/syslog) SSH: Break-In Attempt as ROOT</li><li>(file/syslog) SSH: Invalid Password For ROOT</li><li>(file/syslog) SSH: Invalid Password Specified</li><li>(socket/ism) ISM: Used For Testing</li><li>(trap/162) Generic SNMP authenticationFailure Event</li></ul>
Cisco-gw (192.168.1.254)
<ul style="list-style-type: none"><li>(file/syslog) SSH: Break-In Attempt as ROOT</li><li>(file/syslog) SSH: Invalid Password For ROOT</li><li>(file/syslog) SSH: Invalid Password Specified</li><li>(socket/ism) ISM: Used For Testing</li><li>(trap/162) Generic SNMP authenticationFailure Event</li></ul>

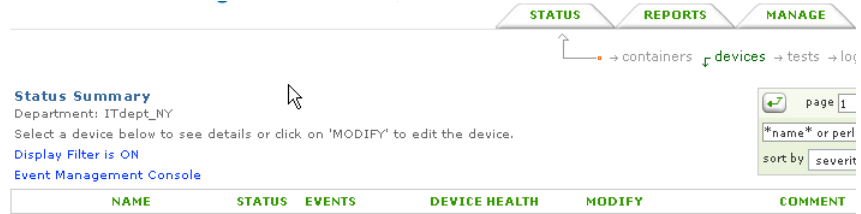
**NOTE:** *you can only trigger notifications for messages which have been accepted by the Event Filter already.*

## 19.2.3 Device Aliases

Since devices can be multi-homed (live on multiple IP addresses), you can setup aliases for these devices so that any incoming messages from these devices are treated to be the same. You can load existing aliases and save any changes you make to the device aliases from this page.

## 19.3 Using the Event Manager Console

The Event Manager (EM) console can be accessed by clicking on the “Event Manager” hyperlink on the Status Summary page. You need a modern browser which supports frames in order to use the Event Manager.



### Filtering Display Results

You can filter the displayed events by the type, the device name or the severity. The two types of events that are displayed on the Event manager are:

- log messages, traps, windows events that have been processed by the Message Handler
- threshold violations (that are caused from the polling done by the various NetVigil monitors)

You can enter a simple regular expression to search for all devices matching a name (e.g. gw-\* will display messages for all devices whose name begins with “gw-”)

## The EM Console

Each event displayed on the EM Console is assigned a unique Event ID automatically by the system. By default, the events are sorted in reverse time order (newest events at the top), but you can click on the header to change the sort order.

5/11/05 12:39:52 PM EDT

**:: Netvigil Event Manager** [close window](#)

page 1 of 10 [→](#)

State <input type="checkbox"/>	Event ID	Device Name Address	Timestamp Source	Message Text
<input type="checkbox"/>	731	lab4 192.168.1.154	5/11/05 12:34 PM winevt/log	(System/DhcpServer) The DHCP/BINL service has determined that it is not authorized to service clients on this network for the Windows domain: lab.hq.fidelia.com.
<input type="checkbox"/>	730	Oracle Server 192.168.1.160	5/11/05 12:28 PM winevt/log	(System/DCOM) DCOM was unable to communicate with the computer 192.168.1.59 using any of the configured
<input type="checkbox"/>	729	Oracle Server 192.168.1.160	5/11/05 12:20 PM winevt/log	(System/DCOM) DCOM was unable to communicate with the computer 192.168.1.60 using any of the configured
<input type="checkbox"/>	728	Oracle Server 192.168.1.160	5/11/05 12:09 PM winevt/log	(System/DCOM) DCOM was unable to communicate with the computer 192.168.1.60 using any of the configured
<input type="checkbox"/>	727	Oracle Server 192.168.1.160	5/11/05 12:07 PM winevt/log	(System/DCOM) DCOM was unable to communicate with the computer 192.168.1.10 using any of the configured
<input type="checkbox"/>	726	Oracle Server 192.168.1.160	5/11/05 11:59 AM winevt/log	(System/DCOM) DCOM was unable to communicate with the computer 192.168.1.254 using any of the configured
<input type="checkbox"/>	725	Oracle Server 192.168.1.160	5/11/05 11:58 AM winevt/log	(System/DCOM) DCOM was unable to communicate with the computer 192.168.1.10 using any of the configured
<input type="checkbox"/>	724	lab4 192.168.1.154	5/11/05 11:56 AM winevt/log	(System/NETLOGON) Registration of the DNS record '2aaf4f71-0037-4526-a7b8-cadd62d46338._msdcs.lab.hq.fidelia.com. 600 IN CNAME lab4-win2k.lab.hq.fidelia.com.' failed with the following error:
<input type="checkbox"/>	723	Oracle Server 192.168.1.160	5/11/05 11:55 AM winevt/log	(System/DCOM) DCOM was unable to communicate with the computer 192.168.1.57 using any of the configured

**filter search results by:** event type:  :messages  :thres violations device name:  severity:  Ok

All  [close window](#)

The following columns (fields) are displayed on the Event Manager:

Field	Description
State	This shows the severity of the event, and acknowledged events are shown with a special icon.
Event ID	A unique number assigned to each event. Clicking on this field will bring up the acknowledge window
Device Name	The device name and IP address
Timestamp	The timestamp of the event
Source	The event source. Note that the message handler can have multiple input sources (such as traps, logs, windows events). All threshold violations show the source "internal/dge"
Message	The event text. This can be on several lines.

**NOTE:** *You can control the number of messages to display on each page by setting it in Manage->Prefs*

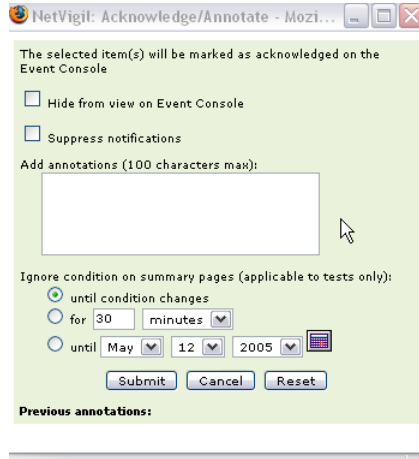
### 19.3.1 Acknowledge / Suppress Events

Clicking on an event ID or a checkbox for an event and clicking on "Ack/Suppress" at the bottom brings up the annotation window.

You can hide the event from the Event Console and also suppress notifications until one of the following conditions are met:

- The severity changes (only for threshold violations)
- For a specified period of time
- Until a specific date and time

When a threshold violation is acknowledged, the state of the device also changes on the Status Summary screen. The acknowledged test is no longer used to calculate the overall device severity as long as the test is in a suppressed state.



**NOTE:** *You can also suppress a threshold violation test without using the Event Manager by “updating” a test and setting the suppress radio button on this page.*