



TRAP MANAGER USER GUIDE

The Trap Manager User Guide gives you the thorough instructions on how to use OiDVIEW Trap Manager. This user guide is an in-depth look in the basics of Trap Manager covered in our **online tutorial**.

Additional support

Please visit our **customer support page** to request additional information, including technical questions and software questions, or product support.

Customer Support

If you have any questions about your account or service, you may contact our sales department at sales@oidview.com or +1 (617) 475-5209.

All inquiries are reviewed and responded to within 24 hours, and within 2-4 hours if you have a priority support contract.

Trap Manager™ by **OiDVIEW**

Phone | +1 617 475 5209
www.oidview.com
260 Franklin Street, 11th Floor
Boston, MA 02110

Copyright © 2013 OiDVIEW. All Rights Reserved.

No part of this publication may be reproduced without the written permission of OiDVIEW, Bytesphere LLC, its suppliers, or affiliate companies. TRADEMARK ATTRIBUTIONS OiDVIEW PRO, OiDVIEW ENTERPRISE, TRAP MANAGER, MIBACQUIRE, JAGUAR, and JAGUARSX are registered trademarks or trademarks of OiDVIEW and Bytesphere LLC and/or its affiliates in the US and/or other countries.

Contents

Introduction to Trap Manager 1

- What is Trap Manager?
- Why use Trap Manager?
- Supported for a range of platforms
- Killer Features

Licensing + Maintenance2

Installation 3

The legal stuff.....4

Overview 5

- How does Trap Manager work?
- Trap Viewer

The Basics 6

- What is a trap filter?
- What is a notification profile?
- Running Trap Manager
- System tray icon

How to...

Acknowledge, clear, and delete alarms.....9

Set up trap forwarding10

Set up trap logging11

Load a new filter file.....12

Customization

Adding a filter.....16

Modifying a filter.....16

Filter properties16

Trap conditions.....17

Condition operations17

Adding a condition.....17

Modifying a condition.....17

Condition properties.....18

Condition types.....18

Notifier profiles.....19

Notification types19

Creating a profile.....20

Assigning a profile to a trap filter..... 20

Introduction to Trap Manager

What is Trap Manager?

Trap Manager is a highly customizable fault management system capable of receiving SNMP Traps, Notifications, and Informs, and also handles (both forwarding and receiving) SNMPv3 secure traps. It alerts on a very large number of fault metrics out of the box (currently over 11,000 at time of writing). When the filter mechanism is enabled, each alarm is assigned a severity and any number of actions can be performed when an alarm is triggered. It is easily integrated with other monitoring and alerting systems.

Why use Trap Manager?

Trap Manager will instantly give you a more detailed view of what is occurring in your IT environment. Once your devices are configured to send SNMP Traps, within minutes you will be alerted of any possible problems, automatically in the console or by using notification profile alerts. You will save your business time and money and Trap Manager should pay for itself very quickly.

Trap Manager is also an incredibly powerful noise reduction system, and can be placed in front of your primary NOC systems in order to filter out excessing noise and useless alarms and then it will forward on the important stuff to your primary and/or secondary EMS, NMS, FCAPS, etc.

Supported for a range of platforms

Trap Manager comes as a client-server application on both Windows, Linux, and OSX. It is released in stand-alone server and fault-tolerant server configurations.

Killer Features

Some of our killer features include (but definitely are not limited to)...

De-Dupe Mechanism - TMS deduplication technology is completely customizable on any property in the Trap and enables the system to withstand the heaviest of trap storms, and allows absolute control over grouping and how discrete events are processed.

Trap Filter Technology - TMS Filtering is the key recognition engine of the system and allows lightning fast matching of events without having to compile or load mibs. Filters can be created, modified and customized to handle any number of different properties and behaviors.

Forwarding - TMS forwarding can happen on the Global, Filter, or on the Notifier Level. Traps can be forwarded to multiple destinations, using either an IP address or hostname.

IP Spoofing - If TMS is forwarding traps, you have the option of making the Trap appear it is from the original sender rather than the Trap Manager machine itself. For some NMS, this is critical.

ODBC Support - TMS can send traps to an ODBC datasource (e.g. MySQL, SQL Server)

Licensing + Maintenance

Licensing

Like all of OiDVIEW's Network Monitoring and IT Management products, Trap Manager is designed to be scalable and affordable.

The base package of Trap Manager comes enabled with 100 IP licenses and Notifier by default. This means it will accept alarms from up to 100 hosts and you can send Notification messages based on those alarms. Other packages include increased number of Hosts, Trap Forwarding, Trap Filter technology, De-Duplication technology, ODBC support, and IP Spoofing capability.

The Enterprise (Unlimited) Trap Manager package comes with an unlimited IP license pack, allowing any number of hosts to send traps to a single TMS host, and has all features included. There is also a Telco package which supports a Fault Tolerant configuraton.

To purchase a Trap Manager license or package, please **visit our sales page**.

To inquire about licensing, please **send us an email on our contact page**, our team will be in touch in 24 hours. Or for more immediate assistance, please contact us by phone at +1 (617) 475 5209.

Maintenance

Each Trap Manager license purchase includes one (1) year of maintenance FREE with purchase. Maintenance is an essential part of keeping your Trap Manager console running smoothly and up-to-date with the latest technologies and features. Your maintenance plan provides rapid technical support, account support, updates, version releases, feature additions and more. Maintenance renewal is on an annual basis, with the options to buy ahead of time for incremental savings. For more information or to renew your maintenance plan, please **visit us online**.



Installation

Trap Manager is easy to download and install online. To install and start the product:

1. **Click here to go our download page** and download to your computer
2. Install the product
3. Click the 'Activate' button
4. Your licenses should have been activated upon payment or receipt of a PO from your company. Enter in your email address* and order number* from your paid quote or invoice to launch the program. If you are trialing the program, don't forget to register to receive your FREE key!

*If you are a paid customer and do not know your order number, please contact us at +1 (617) 474 5209 or send us an email at sales@oidview.com with "Order Number Request" as your subject heading.

Best Practices

Please make sure that all firewalls and/or anti-virus packages have been configured with the appropriate permissions allowing the TMS executables (trap_manager.exe, trap_console.exe, trap_tray.exe, oidview.exe), and the specific ports (80, 161, 162, 25 - if using email, etc.) to operate freely. Most commonly any problems with operating the TMS product are related firewalls and anti-virus products. Windows Firewall, McAfee, Symantec, Trend-Micro, among others, all need to be either shut off or configured in order for the Trap Manager Service to run correctly and effectively.

Please make sure WMI (Windows Management Instrumentation) Service is running, this allows the Trap Console and/or OiDVIEW to start/stop the Trap Manager service on Windows.

Port Conflicts

If another Trap Receiver, is running on the same machine and listening on UDP port 162 (e.g. Microsoft's SNMP Trap Service or any other 3rd party tool), the TMS will not be able to start up and listen on the default port.

The OiDVIEW TMS installer is smart enough to detect the Microsoft SNMP Trap Service, and if it is running, will attempt to stop the service so the OiDVIEW TMS can start up. Upon startup the TMS will attempt to shutdown and set the Microsoft SNMP Trap Service to "Manual" start up mode. There are other 3rd party tools that may need to be shutdown and/or set to manual or disabled. User intervention is required for any of these other 3rd party tools.

The legal stuff

For more information about Trap Manager and OiDVIEW Network Monitoring and IT Management products, please visit our website at www.oidview.com or contact us at:

OiDVIEW

260 Franklin Street, 11th Floor
Boston, MA 02110

+1 617 475 5209

OiDVIEW (also known as Bytesphere LLC) is the creator of Trap Manager and OiDVIEW products. Bytesphere software is a registered trademark and all other product names mentioned herein are the trademarks of Bytesphere LLC for its proprietary computer software. No material describing such software may be produced or distributed without the express written permission of the owners of the trademark and license rights in the software and the copyrights in the published materials.

This software and documentation are provided with restricted rights. Use, duplication, or disclosure is subject to restrictions as set forth by the Government in subdivision (c) (1) (ii) of The Rights in Technical Data and Computer Software clause at 52.227-7013. Contractor/manufacturer is 260 Franklin Street, 11th Floor, Boston, MA 02110 USA.

General notice: Other product names mentioned herein are used for identification purposes only and may be trademarks of their respective companies. Windows is a registered trademark of Microsoft Corporation.



Overview

How does Trap Manager work?

Trap Manager has two main components, a listening service that runs in the background, and a viewer. On Windows operating systems, Trap Manager is integrated with the system within the Services Manager.

When SNMP traps arrive, the listener receives them, decodes and processes them according to "Trap Filter" definitions. Then, actions are executed and alerts are sent via "Notification Profiles". The Trap Manager Console allows a user to view alarms that the Trap Manager Service has received.

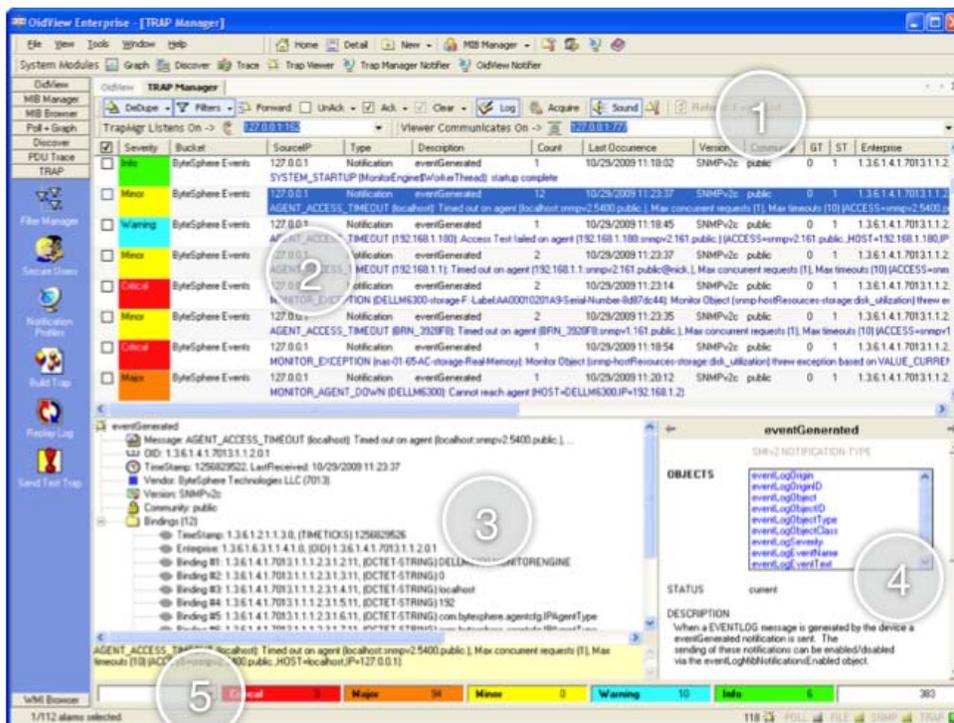
At various points in this manual, we will refer to the Trap Manager Service as TMS, and the Trap Manager Console, as TMC.

Trap Viewer

Trap Manager has a standalone console viewer on Windows.

The components of the console are:

1. Toolbar;
2. Alarm Display;
3. Trap PDU Components;
4. MIB Variable Information; and
5. Severity Bar



The Basics

What is a Trap Filter?

A Trap Filter is a set of conditions that allows Trap Manager to recognize and alert on events that come in from your network. There are over 11,000 Trap Filters that are preloaded into your with Trap Manager license - no need to spend hours putting together filters for your system like most Trap Managers require you to do!

For highly technical and or specialized needs, more filters can be added simply by compiling SNMP MIBs or manually creating them using the Trap Filter Manager.

What is a Notification Profile?

A Notification Profile is an assignment of rules for when and how you would like to be notified of an event within Trap Manager.

Once a SNMP Trap is recognized by a Trap Filter, it has the option of activating a notification sequence, which can consist of sending emails, sending SMS, executing programs, etc. These notifications are set in a Notification Profile.

Unlimited Notification Profiles can be created in the Notification Profile Manager, and each Trap Filter can be assigned the same or a different Notification Profile. The entire system can also be assigned a single Notification Profile in order to simplify configuration, if desired (e.g. if you would like to be emailed for all events).

Running Trap Manager

Running Trap Manager and changing your preferences is easy from within your system. You can start or stop the service, perform basic administration, set up logging, forward, and load new filters.

Trap Manager has a stand-alone service (TMS) that runs as a Windows Service. TMS can be started/stopped a couple of different ways:

Windows Service Manager

The TMS can be controlled by the Windows Service Manager.

Simply go to the services section under the control panel to do this (Settings -> Control Panel -> Administrative Tools -> Services). Highlight the OiDVIEW Trap Manager service, and you can Stop, Start, Restart, and change properties of the service simply by right-clicking on the entry in the list.

The other (faster) way to do this is to run services.msc from Start -> RUN

The Basics (cont'd)

System Tray Icon

When running, the TMS displays an icon in the windows system tray (Windows XP and 2003 only). The icon changes state based on the overall status of TMS (Green, Orange, and Red). The icon can also be clicked to show status or a menu of commands.

- GREEN - everything is OK and the console is connected to the TMS
- ORANGE - the TMS is busy with maintenance or reading filter changes
- RED - the TMS is either not running or TMC cannot connect to it



TRAP MANAGER

HOW TO's

Continue reading for an in depth look at all the features of Trap Manager and how you can tap into its powerful functionality. For a basic tutorial online, check out www.oidview.com/how-to-use-trap-manager.html.

Here's a look at how to...

Acknowledge, clear, and delete alarms

Once alarms come into the Trap Manager they are displayed in the Trap Manager console window. They can be acknowledged, cleared, deleted. Acknowledging an alarm is only a simple state change, it can be used by NOC personnel to understand which alarms are being looked at, being processed by a ticketing system, etc. Clearing an alarm puts it into a state in which the TMS can (at a later time during the automatic maintenance job) delete it. Once alarms are deleted they are purged by the system. Clearing an alarm also alerts personnel that this alarm is not valid anymore.

To operate on a single or multiple selected alarms: Right click on the particular alarm(s) and choose one of the several options available. One can also click the "checkbox" column to toggle state.

<input checked="" type="checkbox"/>	Severity	Bucket	SourceIP	Type	Description
<input type="checkbox"/>	Warning	WRN-RTR	127.0.0.1	Trap	fwMoFwdSmWithSpoc Inbound MD-Forward-SM operation received with spo
<input type="checkbox"/>	Warning	WRN-RTR	127.0.0.1	Trap	externalConditionClient An external co pped out and
<input type="checkbox"/>			127.0.0.1		Exited
<input type="checkbox"/>			127.0.0.1		The applicatio er request.
<input type="checkbox"/>			127.0.0.1		Stopped
<input type="checkbox"/>			127.0.0.1		The watchdog d on user rec
<input type="checkbox"/>			127.0.0.1		Started
<input type="checkbox"/>			127.0.0.1		The watchdog Started
<input type="checkbox"/>			127.0.0.1		trap applicationStarted

- UnAcknowledge
- Acknowledge
- Clear
- Delete
- Telnet
- Ping

To operate on ALL alarms:

Check off the button from the toolbar menu at the top of the screen. This signifies the operation you wish to execute on ALL of the alarms.

Set up trap forwarding

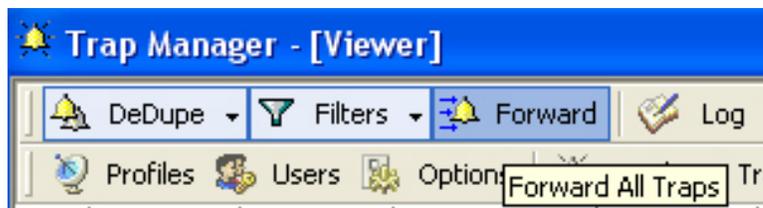
Once alarms come into the Trap Manager, they can be forwarded in a variety of ways.

To specify the hosts to forward traps to, you must set the forward IP addresses/hosts. Go to Options → Trap Manager → Forwarding → Forward IP Address or Hostname. Use a comma (“,”) to enter multiple hosts.

The following categories of forwarding options are available:

Standard Forwarding

Traps are evaluated by the event filter processor, and then forwarded on to a number of hosts specified in the configuration (see below). Traps may or may not be processed in a FIFO manner, based on deduplication rules and matched filters, etc. To turn forwarding ON/OFF, simply check/uncheck the Forward button on the toolbar.



Filter Forwarding

Only those traps that match certain Trap Filters are forwarded. To enable this, you must check the forwarding checkbox in the particular filter (see Trap Filters section).

Raw Forwarding

Traps are not even processed by the Event Filter Processor, they are simply forwarded out to a number of hosts in a FIFO manner. To enable RAW forwarding, go to Options → Trap Manager → Forwarding - Raw Forwarding, and check it off.

NOTE: this is a very unusual configuration should *not* be enabled under most conditions.

Set up trap logging

Once alarms come into the Trap Manager they can be logged in a variety of ways. Trap Log files are stored in the OiDVIEW/logs directory. These log files can be used by 3rd party systems and also can be replayed by the Trap Console.

- 1. Global Logging** - All traps that come into the system, are logged to the global log file. The global log file is named "trapLog.log"
- 2. Filter Based Logging** - Any traps that match a specific filter will be logged to a special file named "trapLog_{filtername}.log". To enable this, you must check the logging checkbox in the particular filter (see Trap Filters section).

Load a new filter file

At times you may decide to manually edit your filters, or you may receive a new Trap Filter File (ovEvents.xml) from Customer Support. In these events, you will need to tell the TMS to reload the filter file, in order for the new trap definitions to be read.

If you have the Trap Manager System Tray Icon, you can simply right-click and select "Reload Trap Filters"



If you do not see the system tray icon, you will have to restart (stop and start) the TMS via the Window Service Manager (please see Windows Service Manager section above).

CUSTOMIZATION

This section is an depth look into customization capabilities within Trap Manager.

Trap filters

Trap Manager recognizes alarms and can produce actionable results because of the Trap Filter definitions. To add new SNMP Trap support to Trap Manager, it is necessary to add and/or modify one or more Trap Filters.

To load the Trap Filter Manager, click on the “Filters” dropdown in the toolbar at the top of the Trap Viewer, and click “Modify Filters”.



Once the Filter Manager is loaded, a window will be displayed showing a toolbar at the top with two sections (Filters and Conditions), and a treeview showing a number of different telecommunications equipment vendors.

Click on a vendor to show customized filters for that vendor.

Filter operations

Filters can be Added, Copied, Modified, or Deleted. These operations can be achieved by clicking the appropriate button on the Filter Toolbar in the Filter Manager window.



ADD

will open up the Filter Dialog and allow you to add a new Filter to the system. One you add a Filter it must also have at least ONE Trap Filter Condition added as well.

MODIFY

will open up the Filter Dialog and allow you to change a pre-existing filter. It will only change the top level Filter information only, conditions need to be modified separately.

COPY

will copy an existing Filter, including all of its' conditions, and just give it a new name, that you will have to change using the MODIFY Filter function. The COPY Filter function is very useful especially if you need to create a number of very similar Filters that have many complex conditions.

DELETE

will delete an existing Filter, including all of its' conditions. This operation cannot be undone, be careful.

Selecting a particular filter and double-clicking on the "Bucket", "Severity", "Class Type" or "Event Type" columns will allow you to quickly edit those components of the Filter, instead of displaying the enter Filter Dialog and changing there.

FilterName	Bucket	Severity
+  ciscoShutdownNotification		Critical
+  ciulfLoopStatusNotification		Warning
-  clogMessageGenerated		<input type="text" value=""/>
-  Conditions	ConditionType	
 Condition [1]	TrapOID	Info Warning
 Condition [2]	BindingValue	Minor
 Condition [3]	BindingValue	Major Critical

Adding a filter

Click the ADD Filter button on the toolbar. The Filter dialog will appear. The FilterName must be filled out before you can click on OK to add the filter.

Modifying a filter

Select the filter in the Filter Manager. Click the MODIFY Filter button on the toolbar. The Filter dialog will appear.

Filter properties

The following properties are available for defining a top-level Filter definition.

FilterName (required*)

gives it a unique name in the system

Bucket (optional)

an alternate method of classification in the system. Special function buckets include DELETE, IGNORE, and LOGONLY.

Severity

assign a severity to this filtered event

Format Text

the message seen in the Trap Viewer display. This property can use parameters like \$1 for varbind 1 and \$aR for address. A full set of parameters and commands are available in the "OidView\profiles\traps\variables.txt file.

Time Filter

only process this filter during the specified time period

Notifier

assign a Notifier Profile to trigger if this filter is matched

Processing Order

the group in which this will be processed; some filters can be given priority over others and be processed at the top, while others can be given lowest priority and be processed at the bottom

Notifier Trigger Threshold

only trigger after X events (0 is disabled)

JaguarSX Integration

choose an Event and Class Type to assign for processing by the Jaguar Event Engine

AutoStatus

automatically change the status of this event (i.e. to acknowledged, cleared, deleted), after X minutes

Forward Traps

forward any traps that match this Filter up to 4 hosts. Forwarded traps can also be transformed by adding varbinds and/or converting to generic traps

Log Traps

log any traps that match this Filter to a special log file

Negate

match anything that does NOT match this Filter (includes filter conditions as well). BE CAREFUL using this feature

Continue

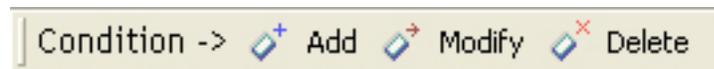
if this filter is matched, continue processing other filters for matches as well. The default is to stop when the first match is found.

Trap conditions

Trap Filters will not work unless there is at least ONE condition assigned to it. A condition tells the system what type of heuristics to apply during the matching algorithm. Trap Conditions are the true workhorses of the system.

Condition Operations

Conditions can be Added, Modified, or Deleted. These operations can be achieved by clicking the appropriate button on the Condition Toolbar in the Filter Manager screen.



ADD

a condition will open up the Condition Dialog. You must have the Filter definition OPEN in the treeview and be selecting the Conditions folder or one of the existing conditions.

MODIFY

a condition will open up the Condition Dialog. You must have the particular condition selected.

DELETE

a condition will delete the condition from the filter. *BE CAREFUL* as you cannot undo this function.

Adding a condition

Click on the ADD condition button. The Add Condition dialog will appear. Specify the appropriate condition properties and click Add Condition to save the Condition.

Modifying a condition

Click on the MODIFY condition button. The Modify Condition dialog will appear. Specify the appropriate condition properties and click Modify Condition to save the Condition.

Condition properties

The following condition properties can be used to define a condition: Condition Type, Value, Time, Binding Index, Binding Type, CLEAR, SEVERITY.

Condition types

The following types of conditions can be created to define a filter.

Source Address - Specify the IP address that the Trap must have come from

Source Port - Specify the source (UDP) port that the Trap must have arrived on

BindingOID - Specify a particular OID in the Trap Varbinds

BindingOIDValueMatch - Specify a particular OID and Value in the Trap Varbinds

BindingValue - Specify a specific value that must be found in the Trap Varbinds

Community - Specify the SNMP Community string that the Trap must contain

TrapOID - Specify the TRAP / Enterprise OID that was in the SNMP Trap

Trap Name - Specify the MIB variable name of the TRAP / Enterprise OID from the Trap (only works with OIDVIEW in debug mode when MIBs are loaded)

SNMP Version - The SNMP Version of the trap

SNMP Agent Address - The SNMP Agent Address in the Trap (SNMPv1 only)

Generic Type - The Generic Type of the Trap

Specific Type - The Specific Type of the Trap

ArrivalTime - Specify an arrival time in order to activate this condition

Varbind Exclusion - exclude a particular varbind from trap deduplication parameters

Clear Filter - clears the most recent trap with this Filter name from the same host

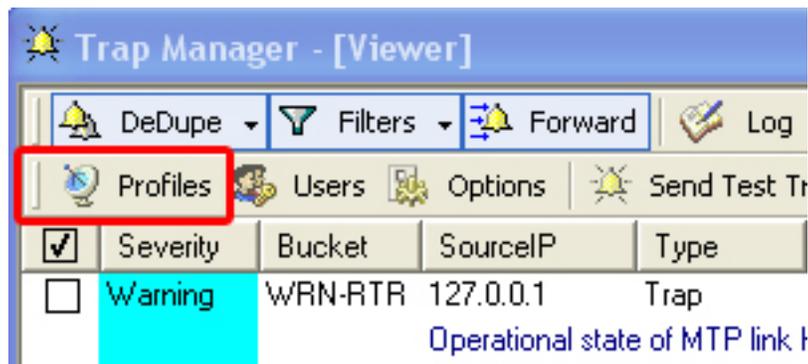
Match IP Group - matches a group of IP addresses

No Match IP Group - do not match a group of IP addresses

Notifier profiles

Notifier Profiles define a set of alerting rules to use when certain conditions are met (i.e. a filter is matched or a severity is matched). Up to 5 different notification types can be set up per notification profile (including but not limited to, email, SMS, sending an SNMP Trap). An unlimited number of profiles can be created.

To show the Notifier Profile Manager, click the “Profiles” button on the Trap Viewer toolbar. The Profile manager will appear:



Notification types

EMAIL - Send an email address to one or more recipients

EXECUTE PROGRAM - run a program or script

NTEVENT LOG - Create a log event in the NT EVENT log

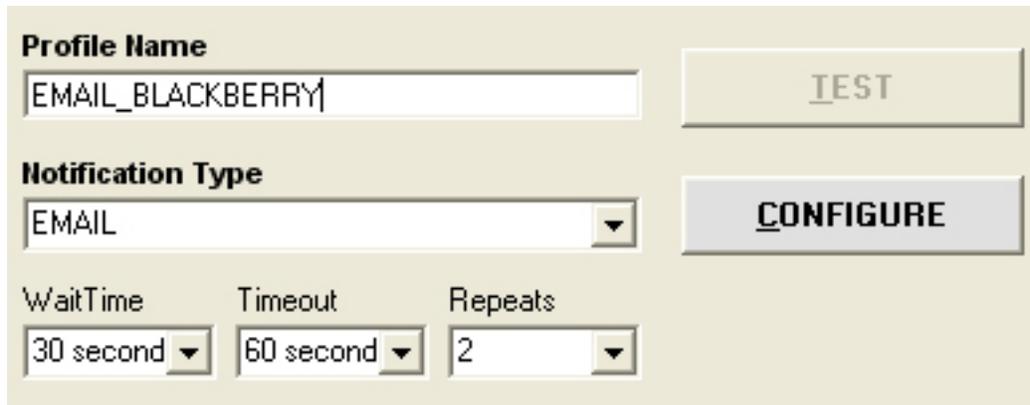
PAGER MESSAGE - Send a message to a beeper through the SNPP protocol

SMS MESSAGE - Send an SMS message through the SMPP protocol

SNMP TRAP - Send an SNMP TRAP to a receiving host

Creating a profile

To create a new Notification Profile, type the name of the new profile in the Profile Name field. Then, select a Notification Type from the dropdown.



The screenshot shows a configuration window for a Notification Profile. It has a light beige background. At the top left, the label "Profile Name" is in bold. Below it is a text input field containing "EMAIL_BLACKBERRY". To the right of this field is a button labeled "TEST". Below the "Profile Name" section is the "Notification Type" section, with a dropdown menu currently showing "EMAIL". To the right of this dropdown is a button labeled "CONFIGURE". At the bottom of the form, there are three dropdown menus: "WaitTime" set to "30 second", "Timeout" set to "60 second", and "Repeats" set to "2".

If it's an EMAIL notification type and you haven't set up your EMAIL settings yet (i.e. SMTP server, login name and password), click the CONFIGURE button and setup and test those parameters.

Once you have configured your Notification parameters for the specific Notification Type (i.e. with EMAIL you will need to enter an Email address, subject, message, etc.), click the APPLY button and the bottom of the screen. This will create the Notification profile and enable the TEST button next to the profile name field. You can now click "TEST" to test the profile.

NOTE: To include the fully translated trap filter text into the Notification (if using Filters), specify the \$FT symbol (for filter text).

Assigning a profile to a trap filter

Bring up the Trap Filter Manager and MODIFY the filter. Click the "Notification Profile" checkbox, and choose the profile from the dropdown. Click OK to save the filter and then click SAVE FILTERS to send the filter change to the server.