

# CA APM SNMP Alert Action to CA Nimsoft Monitor Alarm Integration



The integration enables CA Nimsoft Monitor to process SNMP trap notifications from CA Application Performance Management (APM) using SNMP Alert Actions. SNMP trap notifications are received and processed by the Nimsoft Monitor snmptd probe acting as a SNMP manager; the snmptd probe CA APM profile provides the rules for converting CA APM SNMP enterprise specific trap notifications to Nimsoft alarms. This document provided the information for implementing this integration.

**Table of Contents:**

Configuring CA Nimsoft Monitor snmptd .....	2
Configuring CA APM SNMP Alert Actions.....	3
Configuring CA Nimsoft Monitor snmptd Profile.....	8

## Configuring CA Nimsoft Monitor snmptd

The snmp probe, Nimsoft SNMP-TRAP Daemon v3.01 or higher must be deployed on the Nimsoft Monitor primary hub robot or any Nimsoft Monitor robot.

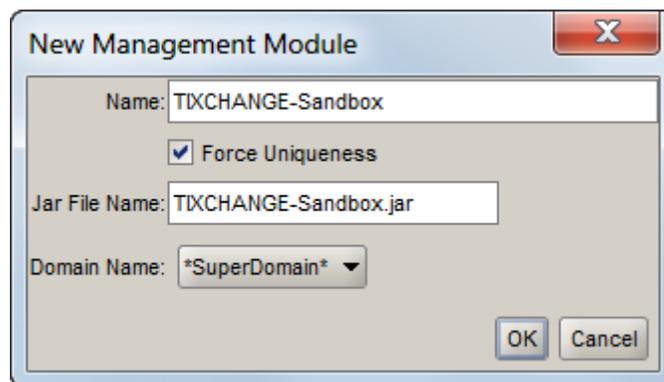
1. If the snmp probe v3.01 or higher is not already deployed on a robot, download the latest version 3.01 or higher of the snmp probe to the archive if necessary, and then deploy the probe to designated robot acting as the SNMP manager/trap daemon.
2. Save the attached `_snmptd.zip` probe archive to a computer running Nimsoft Monitor Infrastructure Manager, then import it to your archive by right-clicking in the Archive pane of the Infrastructure Manager window, then select Import, then navigate to the saved `_snmptd.zip`, and then click Open to import the zip file snmptd probe configuration to the archive.
3. Drag and drop the `_snmptd` probe package in the archive to the robot running the default v3.01+ snmptd probe. This will overwrite the default snmptd probe configuration.
4. Locate and select the snmptd probe in the Probe list pane for the selected robot of the Infrastructure Manager, and then right-click and select Configure...
5. From the snmpd probe GUI expand the V1 Traps folder, confirm that the CA APM subfolder is listed, and then click OK or Cancel to close the window.
6. Right-click the snmptd probe in the Probe list pane for the selected robot, and then click Restart to restart the probe.
7. Note: For more information about snmptd probe requirements and see the *CA Nimsoft Monitor snmptd Guide, v3.0 series*.

## Configuring CA APM SNMP Alert Actions

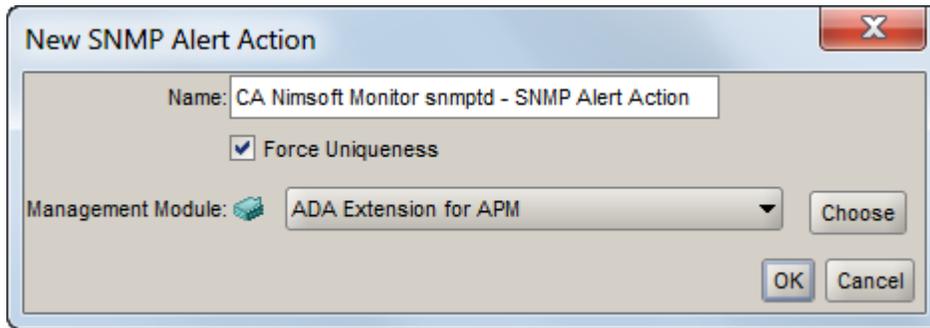
Use the CA Introscope Workstation 9.0 or higher Management Module Editor to edit an existing management module or create a new management module for the designated application to configure its actions and alerts.

**Note:** It is recommended to use an existing management module with alerts that have already been defined by a CA APM administrator.

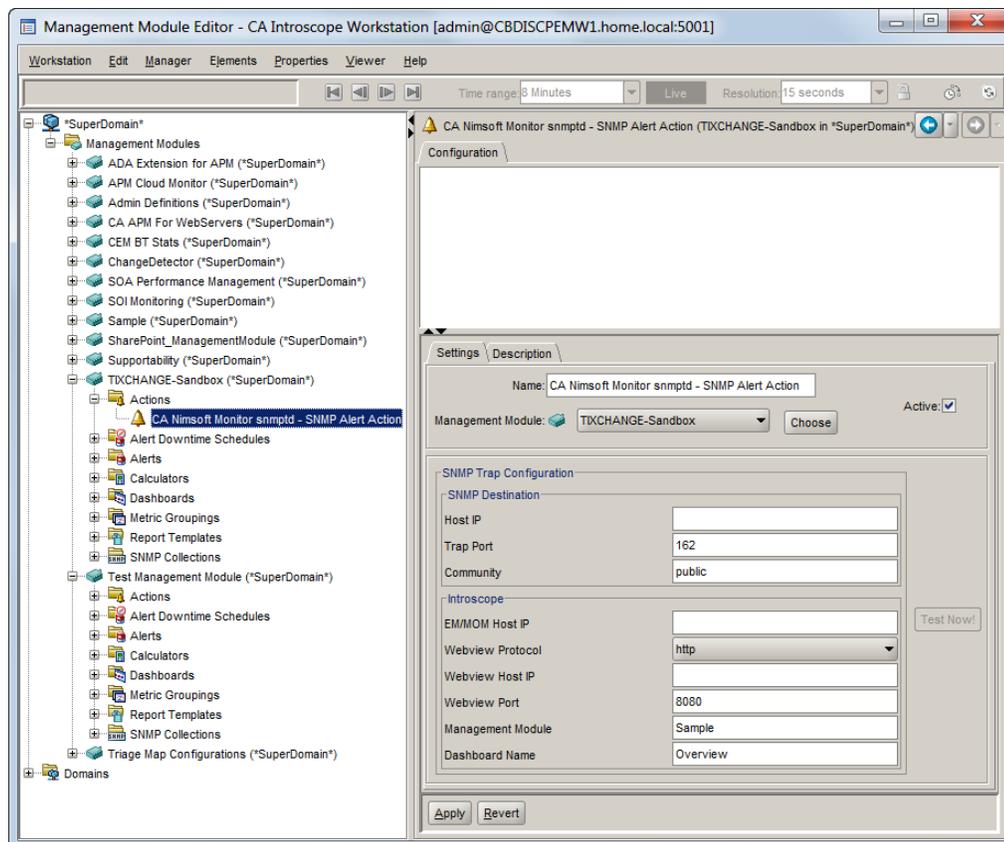
1. Launch CA Introscope Workstation, then enter the User name and Password of an administrator user, and then click OK to connect to the Introscope Enterprise Manager.
2. Select New Management Module Editor from the Workstation menu.
3. If you want to create a new management module rather than use an existing management module for the designated application:
  - a. Select New Management Module from the Elements menu, then type a name for the new management module in the Name box, then type the Jar File Name for the associated, Java archive and then click OK.

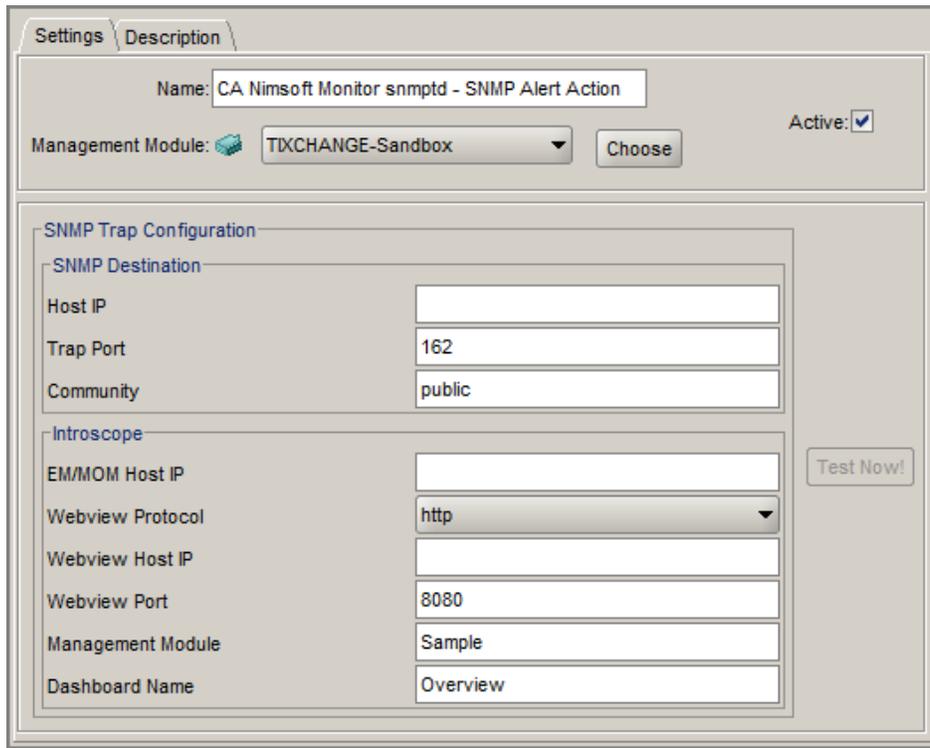


4. Select New Action ► New SNMP Alert Action from the Elements menu.
5. In the New SNMP Alert Actions window, type CA Nimsoft Monitor snmptd - SNMP Alert Action in the name box, and then click OK.



6. Expand the Management Modules folder in the Management Modules Editor, then expand the new or existing management module for the designated application, then expand the Actions folder and then select the new SNMP Alert Action, CA Nimsoft Monitor snmpd - SNMP Alert Action.





The screenshot shows the configuration window for an SNMP Alert Action. It has two tabs: 'Settings' (selected) and 'Description'. The 'Name' field is 'CA Nimsoft Monitor snmptd - SNMP Alert Action'. The 'Management Module' is set to 'TXCHANGE-Sandbox' with a 'Choose' button. The 'Active' checkbox is checked. The 'SNMP Trap Configuration' section includes:

- SNMP Destination:** Host IP (empty), Trap Port (162), Community (public).
- Introscope:** EM/MOM Host IP (empty), Webview Protocol (http), Webview Host IP (empty), Webview Port (8080), Management Module (Sample), Dashboard Name (Overview).

A 'Test Now!' button is located to the right of the Introscope section.

7. On the Settings tab type the host IP address of the server/robot running the snmptd probe in the Host IP box, then enter the EM/MOM Host IP address and Webview Host IP address in their boxes respectively, and optionally enter the Management Module name and Dashboard name, and then click Apply.
8. Expand the Alerts folder and select an existing alert or select New Alert ► New Simple Alert from Elements menu.

**Note:** It is beyond the scope of this document to provide recommendations for creating meaningful actionable alerts for an application and its management module. For more information about configuring notifications and alerts with CA Introscope Workstation, see the *CA Application Performance Management Configuration and Administration Guide*.

Management Module Editor - CA Introscope Workstation [admin@CBDISCPEMW1.home.local:5001]

Workstation Edit Manager Elements Properties Viewer Help

Time range: 8 Minutes Live Resolution: 15 seconds

**\*SuperDomain\***

- Management Modules
  - ADA Extension for APM (\*SuperDomain\*)
  - APM Cloud Monitor (\*SuperDomain\*)
  - Admin Definitions (\*SuperDomain\*)
  - CA APM For WebServers (\*SuperDomain\*)
  - CEM BT Stats (\*SuperDomain\*)
  - ChangeDetector (\*SuperDomain\*)
  - SOA Performance Management (\*SuperDomain\*)
  - SOI Monitoring (\*SuperDomain\*)
  - Sample (\*SuperDomain\*)
  - SharePoint\_ManagementModule (\*SuperDomain\*)
  - Supportability (\*SuperDomain\*)
  - TXCHANGE-Sandbox (\*SuperDomain\*)
    - Actions
      - CA Nimsoft Monitor snmpd - SNMP Alert Action
    - Alert Downtime Schedules
    - Alerts
      - Frontend RPI
    - Calculators
    - Dashboards
    - Metric Groupings
    - Report Templates
    - SNMP Collections
  - Test Management Module (\*SuperDomain\*)
    - Actions
    - Alert Downtime Schedules
    - Alerts
    - Calculators
    - Dashboards
    - Metric Groupings
    - Report Templates
    - SNMP Collections
  - Triage Map Configurations (\*SuperDomain\*)
- Domains

**Frontend RPI (TXCHANGE-Sandbox in \*SuperDomain\*)**

Configuration



\*SuperDomain\*/ITXCHANGE/Tomcat/ITXCHANGE-Web-Responses Per Interval = 0

Settings Description

Name: Frontend RPI Active:

Management Module: TXCHANGE-Sandbox Choose

Metric Grouping: Frontend RPI Choose

Resolution: 15 seconds Combination: any

Comparison Operator: Greater Than Notify by individual metric:

Trigger Alert Notification: When Severity Increases

**Danger**

Threshold: 2

Periods Over Threshold: 1 Observed periods: 1 (last 0:15)

Actions

CA Nimsoft Monitor snmpd - SNMP Alert Action

Test Add Remove

Action Delay: 0 h 0 m 0 s

**Caution**

Threshold: 1

Periods Over Threshold: 1 Observed periods: 1 (last 0:15)

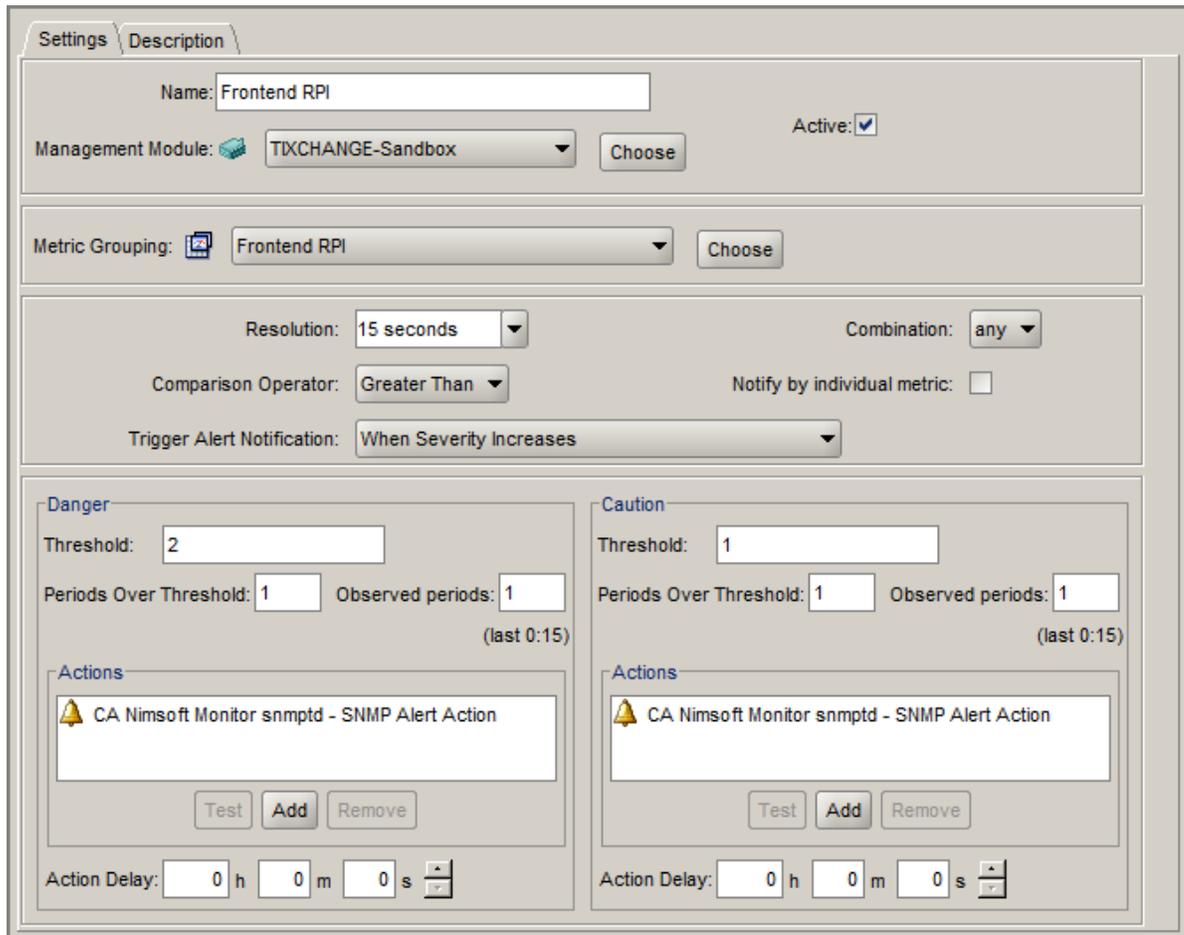
Actions

CA Nimsoft Monitor snmpd - SNMP Alert Action

Test Add Remove

Action Delay: 0 h 0 m 0 s

Apply Revert



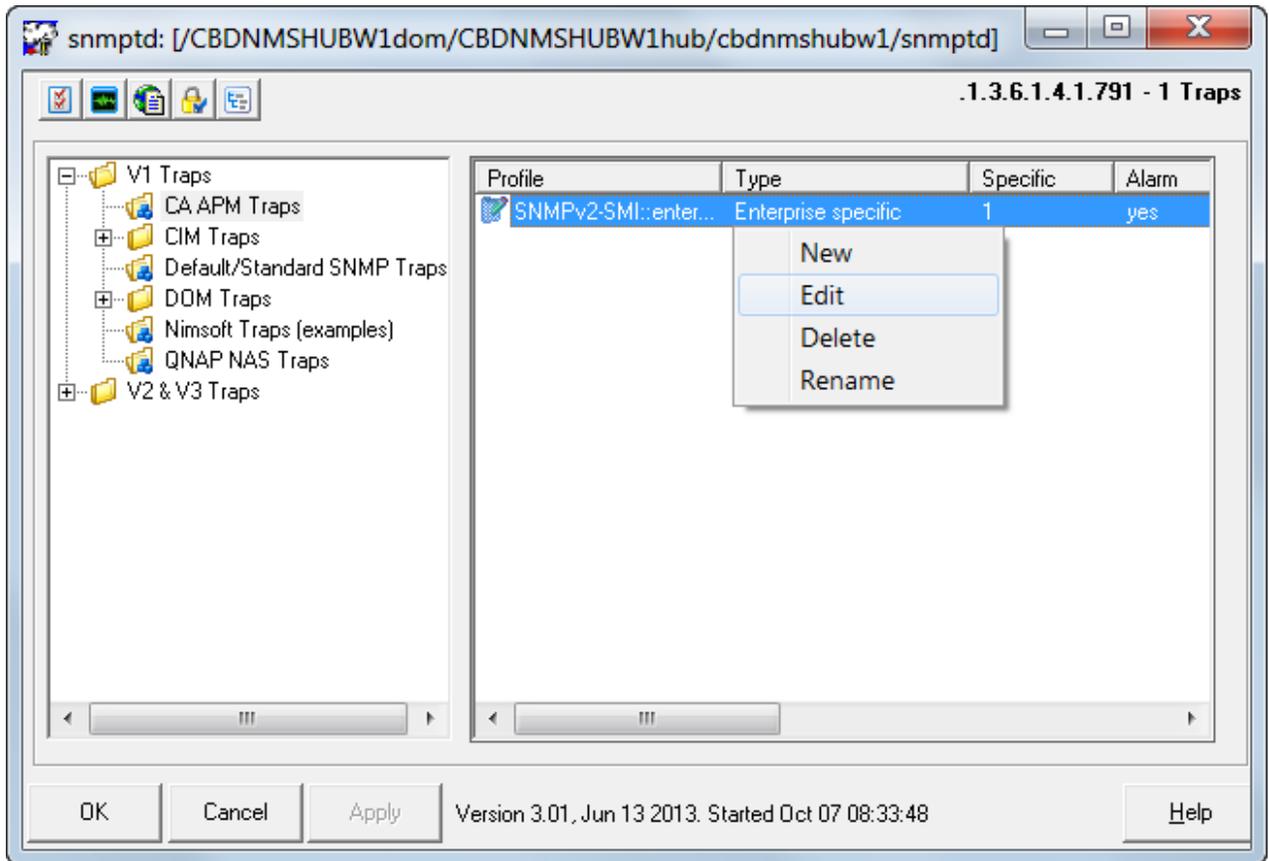
The screenshot shows the configuration page for an alert named 'Frontend RPI'. The interface is divided into several sections:

- General Settings:** Name: Frontend RPI, Management Module: TIXCHANGE-Sandbox, Active:
- Metric Grouping:** Frontend RPI
- Alert Configuration:** Resolution: 15 seconds, Comparison Operator: Greater Than, Combination: any, Trigger Alert Notification: When Severity Increases
- Danger Section:** Threshold: 2, Periods Over Threshold: 1, Observed periods: 1 (last 0:15). Action: CA Nimsoft Monitor snmptd - SNMP Alert Action.
- Caution Section:** Threshold: 1, Periods Over Threshold: 1, Observed periods: 1 (last 0:15). Action: CA Nimsoft Monitor snmptd - SNMP Alert Action.
- Action Delay:** 0 h 0 m 0 s

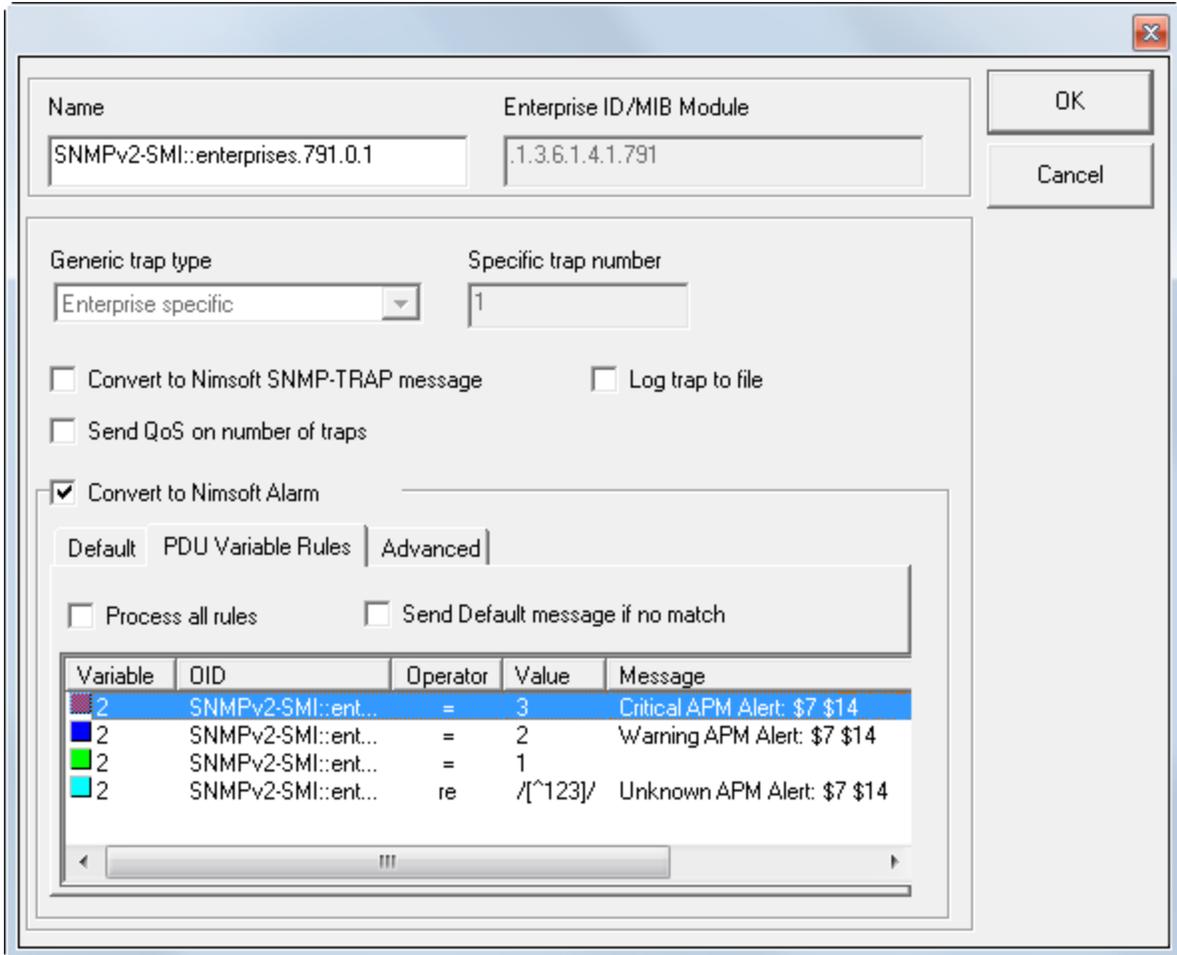
9. For new alerts select the appropriate metric grouping and resolution, and then enter the Danger and Caution threshold values.
10. For Trigger Alert Notification, select When Severity Increases, then click Add in the Danger and Caution Actions group select/choose CA Nimsoft Monitor snmptd - SNMP Alert Action then click Choose, and then click Apply to save the changes to the alert.
11. Repeat steps 9 thru 10 for all alerts in the management module as required.

## Configuring CA Nimsoft Monitor snmpd Profile

The SNMPv2-SMI::enterprises.791.0.1 profile for the snmpd probe can be edited and configured as required using Infrastructure Manager and the snmpd probe GUI.



Administrators can edit the PDU Variable Rules and edit the Severity and message Text as required.



Name: SNMPv2-SMI::enterprises.791.0.1  
Enterprise ID/MIB Module: .1.3.6.1.4.1.791

Generic trap type: Enterprise specific  
Specific trap number: 1

Convert to Nimsoft SNMP-TRAP message     Log trap to file  
 Send QoS on number of traps  
 Convert to Nimsoft Alarm

Default    PDU Variable Rules    Advanced

Process all rules     Send Default message if no match

Variable	OID	Operator	Value	Message
2	SNMPv2-SMI::ent...	=	3	Critical APM Alert: \$7 \$14
2	SNMPv2-SMI::ent...	=	2	Warning APM Alert: \$7 \$14
2	SNMPv2-SMI::ent...	=	1	Unknown APM Alert: \$7 \$14
2	SNMPv2-SMI::ent...	re	/[^123]/	Unknown APM Alert: \$7 \$14