

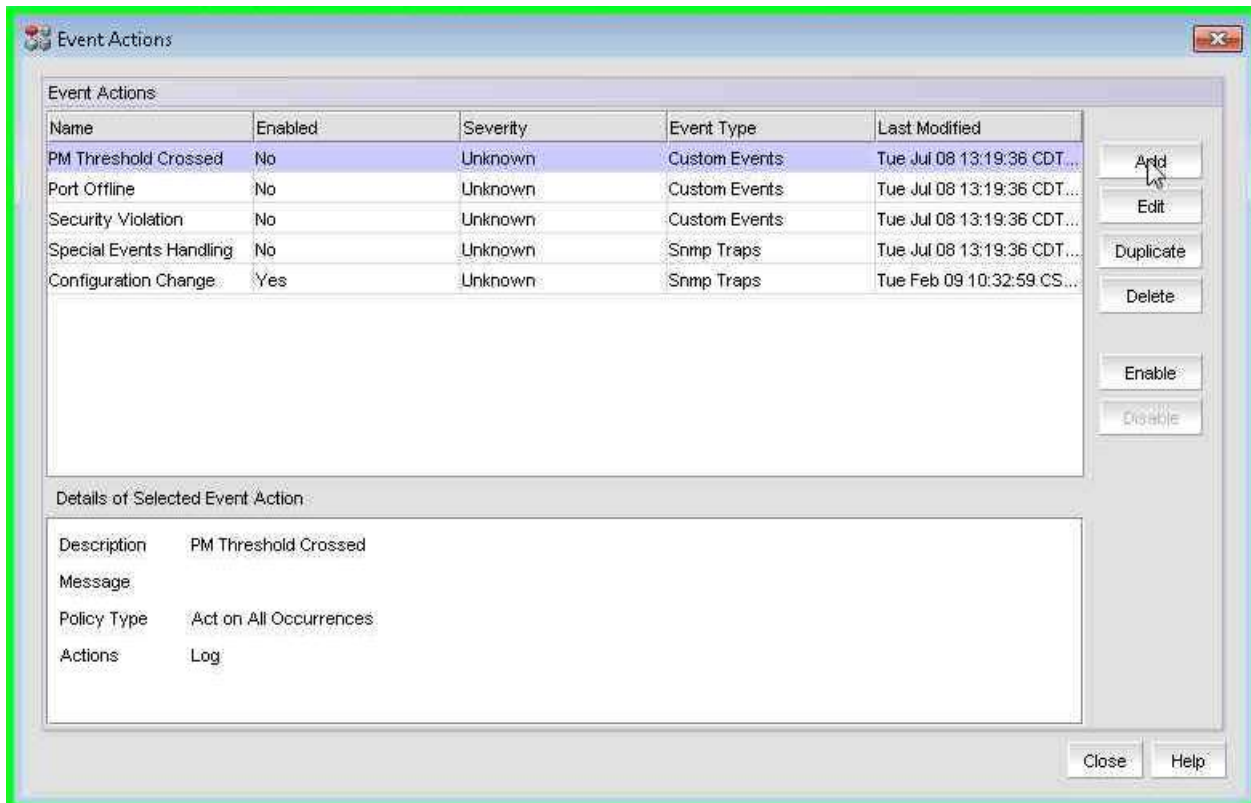
Creating an Event Action Item and Report

An event action item is used to detect when an event occurs and perform some action on it. In this example, we are going to collect SNMP traps for a user logging in to a monitored device and making changes to the startup configuration (write mem). Then we will create a report to gather these actions in one place.

First we need to create the event action:

In BNA -> IP Tab: Open Monitor -> Event Processing -> Event Actions

Click Add



Name the Event, give a description, and click next.

The screenshot shows a configuration window with the following elements:

- Steps:** A vertical pane on the left containing a single step labeled "1. Identification".
- Identification:** The main content area with the following fields:
 - Name:** A text box containing "Config File Changes".
 - Description:** A text box containing "Notifies of config file changes".
 - Enabled:** A checkbox that is checked.
- Buttons:** Located at the bottom of the window, including "Help", "Cancel", "Previous", "Next", and "Finish". A mouse cursor is pointing at the "Next" button.

Select the events to act upon. For this example, we are selection traps from the following:

- Foundry-SN-Notification-MIB
 - snTrapRunningConfigChanged
 - snTrapStartupConfigChanged
 - snTrapUserLogin

Click Next.

The screenshot shows a configuration wizard interface with the following components:

- Steps:** A sidebar on the left with two steps: "1. Identification" and "2. Events". "2. Events" is currently selected.
- Events:** The main area is titled "Events". It has a "Show" dropdown menu set to "Traps" and a "Filter" button. There are two radio buttons: "MIB Information" (selected) and "MIB Alias".
- Available Traps:** A list of traps with icons and names:
 - snTrapL4TcpAttackRateExceedThres (Warning icon)
 - snTrapL4ConnectionRateExceedMax (Error icon)
 - snTrapL4ConnectionRateExceedThre (Warning icon)
 - snTrapRunningConfigChanged [1.3.6.1.4.1.1991.0.75] (Info icon)
 - snTrapStartupConfigChanged [1.3.6.1.4.1.1991.0.75] (Info icon)
 - snTrapUserLogin [1.3.6.1.4.1.1991.0.75] (Info icon)
 - snTrapUserLogout [1.3.6.1.4.1.1991.0.75] (Info icon)
 - snTrapPortSecurityViolation [1.3.6.1.4.1.1991.0.75] (Warning icon)
- Selected Traps:** A list of selected traps under the "FOUNDRY-SN-NOTIFICATION-MIB" folder:
 - snTrapRunningConfigChanged [1.3.6.1.4.1.1991.0.75]
 - snTrapStartupConfigChanged [1.3.6.1.4.1.1991.0.75]
 - snTrapUserLogin [1.3.6.1.4.1.1991.0.75]
- Trap Details:** An empty text box.
- Configure varbind filters:** A checkbox that is currently unchecked.
- Available Varbinds:** A list containing "snAgGblTrapMessage".
- Selected Varbinds:** An empty table with columns "Name", "Operation", and "Value".

At the bottom of the window, there are buttons for "Help", "Cancel", "Previous", "Next", and "Finish". The "Next" button is highlighted with a mouse cursor.

Select the Sources and Click Next.

Steps

1. Identification
2. Events
3. Sources

Sources

Provide the IP Address / Node WWN / Name of the source

IP Address:

Multiple entries need to be separated by ";"

Select from the available list of sources

Use Ifindex in Source Matching

Trap Variable (Ifindex):

Available IP Sources

Group / Product	Name
Products	
Edge-Switch [192.168.Edge-Switch	
CME-RTR.lab.local [10.:CME-RTR.lab.loc	
LAB-7250 [10.20.10.27:LAB-7250	
3.3.3.3 [3.3.3.3]	3.3.3.3
Lab-6610 [10.254.0.1]	Lab-6610
Lab-7450 [10.254.0.2]	Lab-7450
Product Groups	
IP Subnets	

Selected Sources

- SAN Products
- IP Products
 - Products
 - Lab-6450 [10.10.10.22]

Help Cancel Previous Next Finish

We are using the defaults to take an action. Click Next.

Steps

1. Identification
2. Events
3. Sources
4. Policy

Policy

Take actions for the selected events when they occur.

Take actions for the selected events based on below criteria

Frequency-bound (act as count reached the count specified)

Time-bound (act at the end of the duration specified)

If occur: times within Minutes

Reset:

Minutes

Message

Severity:

Help Cancel Previous Next Finish

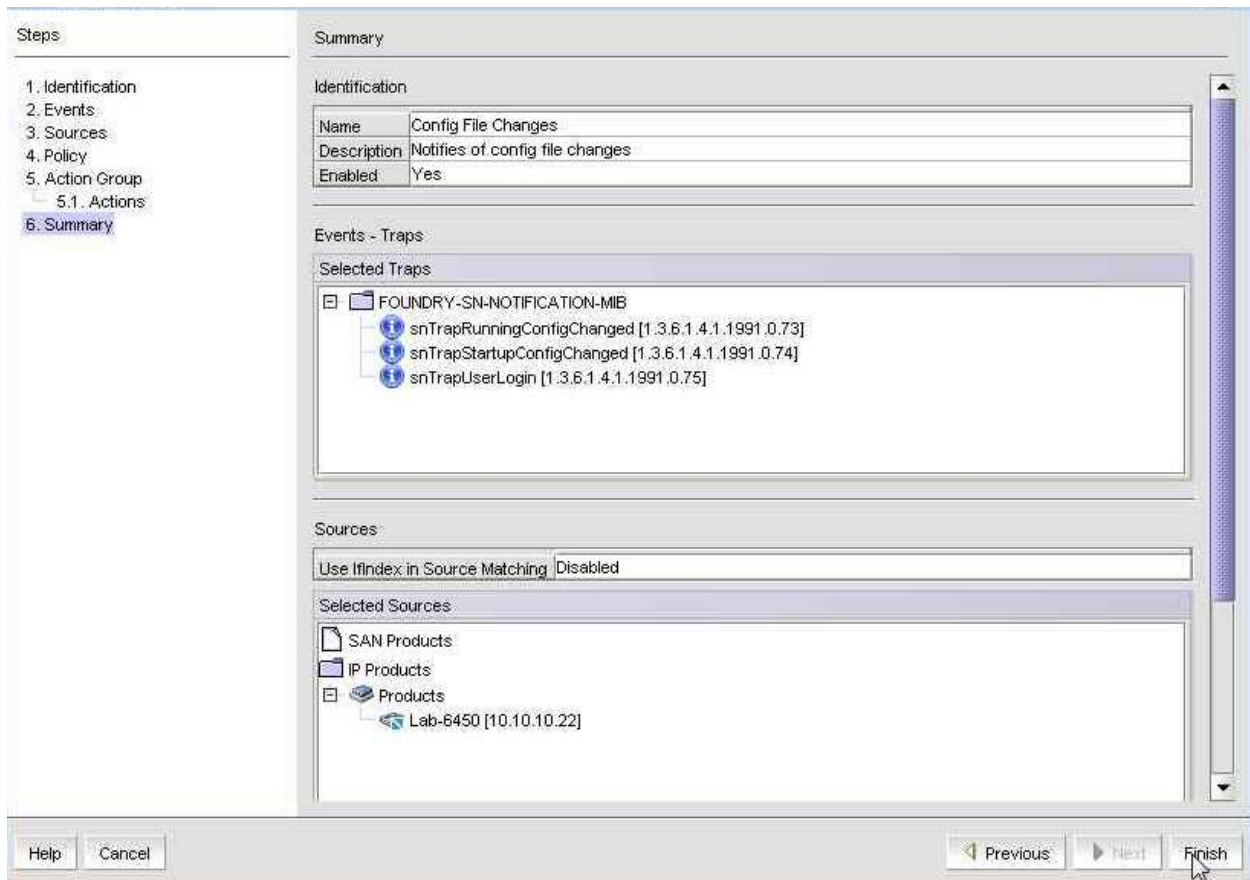
Here we can select what we want to happen when an event action happens. We are going to log the event. Click Next.

The screenshot shows a configuration window titled "Action Group - Actions". On the left, a "Steps" pane lists the following items: 1. Identification, 2. Events, 3. Sources, 4. Policy, 5. Action Group, and 5.1. Actions (which is highlighted). The main configuration area includes the following options:

- Apply as Logging Policy
 - Log Drop
- Auto Acknowledge
- Notes: [Empty text box]
- Enable Troubleshooting (IP only)
 - In case of maintenance, events can be suppressed (up to 168 hours (7 days))
 - Time: [0] (0-168 Hours) [0] (0-50 Minutes)
- Alert by E-mail
- Run Configuration Policy [Target: Event Sender]
- Launch a Script [Empty text box]
 - Send Event parameters as argument (Level, Source Name, Source Address, Type and Description)
- Broadcast to Client [Configure]
- Mark as Special Events
- Tech Support**
 - Collect support save (only for event sender)
- Deployment**
 - Deploy CLI Configuration [Configure] [Previous] [Next] [Finish]

At the bottom of the window, there are four buttons: "Help", "Cancel", "Previous", and "Next". The "Next" button is highlighted with a mouse cursor.

This is a Summary for the event action. Click Finish.



The image shows a software configuration window titled "Summary". On the left, a "Steps" pane lists the configuration process: 1. Identification, 2. Events, 3. Sources, 4. Policy, 5. Action Group (with a sub-item "5.1. Actions"), and 6. Summary (which is currently selected). The main area is divided into three sections: "Identification", "Events - Traps", and "Sources".

Identification:

Name	Config File Changes
Description	Notifies of config file changes
Enabled	Yes

Events - Traps:

Selected Traps

- FOUNDRY-SN-NOTIFICATION-MIB
 - snTrapRunningConfigChanged [1.3.6.1.4.1.1991.0.73]
 - snTrapStartupConfigChanged [1.3.6.1.4.1.1991.0.74]
 - snTrapUserLogin [1.3.6.1.4.1.1991.0.75]

Sources:

Use Ifindex in Source Matching: Disabled

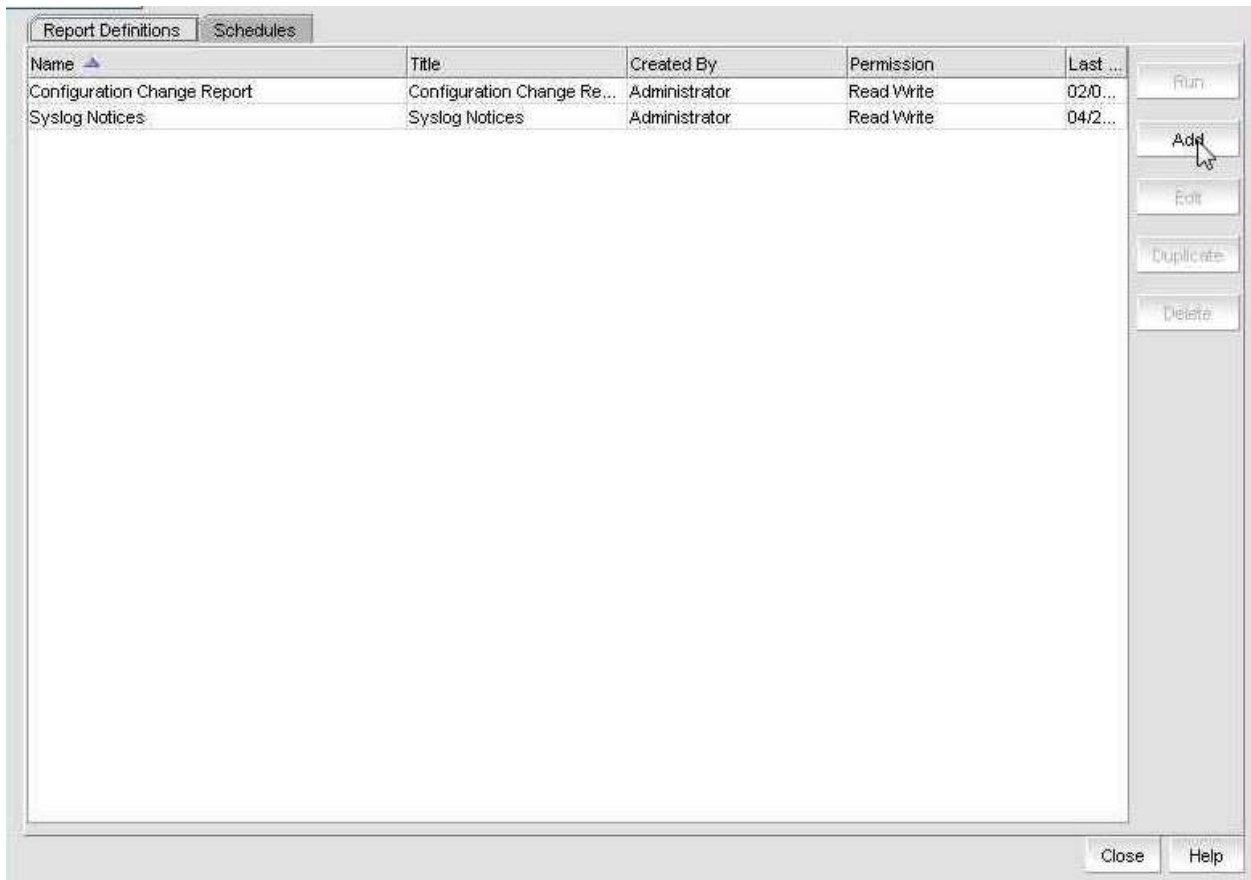
Selected Sources

- SAN Products
- IP Products
- Products
 - Lab-6450 [10.10.10.22]

At the bottom of the window, there are four buttons: "Help", "Cancel", "Previous", and "Finish". A mouse cursor is pointing at the "Finish" button.

To create the report, go to: Reports -> Event Custom Reports.

Click Add to create a new report.



We will not select any products for the report, so go to the Filters Tab. Here we will select the Event Action we just created to match for reporting.

The screenshot shows a software configuration window with the following elements:

- Product** tab selected.
- Filter** sub-tab selected.
- Description**: A dropdown menu set to "=" followed by an empty text input field.
- Addresses**: A dropdown menu set to "=" followed by an empty text input field.
- Acknowledged**: An unchecked checkbox.
- Available Severity**: A list box containing "Alert", "Critical", "Debug", "Emergency", "Error", "Info", "Notice", and "Unknown".
- Selected Severity**: An empty list box.
- Available Event Category**: A list box containing "Link Incident Event", "Management Server Event", "Product Audit Event", "Product Event", "Product Status Event", "Security Event", and "Unknown".
- Selected Event Category**: An empty list box.
- Available Event Actions**: A list box containing "Configuration Change", "PM Threshold Crossed", "Port Offline", "Security Violation", and "Special Events Handling".
- Selected Event Actions**: A list box with "Config File Changes" selected.
- Run** button at the bottom left.
- OK**, **Cancel**, and **Help** buttons at the bottom right.

Select the period of time to report. We are selecting the last 24 hours.

The screenshot shows a software interface with a tabbed menu at the top containing 'Product', 'Filter', 'Time Settings', 'Result Settings', and 'Identification'. The 'Time Settings' tab is active. Under this tab, there are two radio button options: 'Relative Time' (which is selected) and 'Absolute Time'. Below 'Relative Time', there is a 'Select' label followed by a dropdown menu currently displaying 'Last 24 Hours'. Below 'Absolute Time', there are four date and time pickers: 'Start Date' (February 09, 2016), 'End Date' (February 09, 2016), 'Start Time' (1:00 AM), and 'End Time' (1:00 AM).

Select the items you would like to see on the report. We are selecting the following:

- First Event Server Time
- Description
- Product Address
- Source Name
- Source Address
- Category
- Count

The screenshot shows a software interface for configuring a report. At the top, there are tabs for 'Product', 'Filter', 'Time Settings', 'Result Settings', and 'Identification'. Below these tabs are three main columns: 'Available Columns', 'Selected Columns', and 'Sort By Columns'. The 'Available Columns' list includes: Acknowledged, Acknowledged By, Audit, Category, Contributor, Count, Event Action Name, Fabric Name, First Event Server Time, Group By Count, Last Event Server Time, Module Name, Node VWMN, OID, Operational Status, Port, Port Name, Severity, Source Address, Source Name, and Virtual Fabric ID. The 'Selected Columns' list includes: Description, Event Type, First Event Product Time, Last Event Product Time, Message ID, Notes, Origin, and Product Address. The 'Product Address' item in the 'Selected Columns' list is highlighted with a blue background. There are also navigation arrows between the columns.

Give the Report a name and title, then click OK.

The screenshot shows a software configuration window with the following elements:

- Product:** Filter, Time Settings, Result Settings, Identification (selected)
- Name:** Config File Changes Report
- Title:** Config File Changes Report
- Sharing:**
 - Do not share this definition
 - Share this Definition (Read Only Share)
- Available Roles:** (Empty list box)
- Selected Roles:** (Empty list box)
- Available Users:** (Empty list box)
- Selected Users:** (Empty list box)
- Navigation:** Two sets of arrow buttons (right and left) between the Available and Selected list boxes.
- Buttons:** Run, OK, Cancel, Help

On the Schedule Tab, you can schedule the report to run and be sent to you at a given time. You can also manually run the report.