MG-SOFT Corporation

Net Inspector 2015 Client

REFERENCE MANUAL

(Document Version: 10.6)

Document published on October 16, 2015

TABLE OF CONTENTS

1 INTRODUCTION

This reference manual describes the graphical user interface (GUI) and commands available in the Net Inspector Java Client application. Net Inspector Client connects to the Net Inspector Server and provides a GUI for monitoring the status of managed objects and viewing and managing alarms on managed objects.

All program commands in this manual are written in bold and italic letters. If two or more commands are combined together, individual commands are separated by the "/" character. For example:

Tools / Client Preferences – which means: click the "Tools" entry in the menu bar and select the "Client Preferences" command from the "Tools" menu.

The term "click" in this manual means a single click with the left mouse button, while the term "right-click" is used for a single click with the right mouse button.

All hyperlinks in text are colored blue, e.g., Client Preferences dialog box. Clicking a hyperlink opens the page, which the hyperlink points to.

The content of this manual is listed in the Table of Contents.

Note: Not all commands and dialog boxes described in this manual can be accessed by all users. Which commands and dialog boxes will be available to a particular user, depends on the access rights that are assigned to this user. For more information on this, please see the About Users, Access Rights and User Views section of this manual.

2 ABOUT USERS, ACCESS RIGHTS AND USER VIEWS

Each Net Inspector user account has certain access-rights assigned. User accounts have also one or more user views assigned. User views differ in respect to what objects they include (display). The table below shows the user account types, corresponding access rights and user views:

Account type	Access rights	User View (Typical)
Administrator	unlimited	unlimited (includes all objects)
Operator	limited to managing alarms	limited to a part of the network
Guest	limited to monitoring (viewing) alarms	limited to a part of the network

User accounts are created and managed in the Server Settings dialog box, Users panel.

User views are managed in the Server Settings dialog box, User Views panel.

3 NET INSPECTOR CLIENT MAIN WINDOW

The Net Inspector Java Client main window consists of the typical graphical user interface components, like the title bar, menu bar, toolbar, one or more windows and the status bar. The following windows form the Net Inspector Client main window:

- **Maps**
- **Explorer**
- **Map Overview**
- **Events**
- **Event Details**

The above listed windows are arranged side-by-side in the main window. Windows can be resized by dragging their borders. All windows listed above, except the Maps window, which is always displayed, can be displayed or hidden by using the View menu commands or the corresponding toolbar buttons.

3.1 Maps Window

Net Inspector uses the concept of maps, which are containers that can hold:

1. objects (managed objects, action objects, system objects)
2. other maps (submaps)
3. graphic elements (e.g., lines, rectangles, bitmaps, etc.)

An “object” can be:

- a **managed object** (e.g., an object representing a physical device on the network)
- an **action object** (e.g., an object representing e-mail sending functionality in Net Inspector)
- a **system object** (e.g., an object representing Net Inspector’s event storage subsystem)

As maps can contain other maps (i.e., submaps), they can be stacked in layers. Due to this fact, the terms “map”, “submap” and “(sub)map” are used as synonyms in this document.

“Graphic elements” (e.g., lines, connections, circles, rectangles, bitmap images, artistic text, etc.) are added to maps by users to enhance the visual appearance of maps (e.g., to visually connect or group icons, set bitmap wallpapers, etc).

The Maps window displays the contents of maps, i.e., objects, submaps and graphic elements. Objects and submaps can be displayed either by means of icons (Graphics view), where every icon represents one object or submap, or by means of a table (Details view), where each row represents one object or a submap. Graphic elements, however, are shown only in the Graphics view.

3.1.1 Purpose

The Maps window is used for viewing the status and basic information about active alarms associated with the objects and submaps, as well as for moving, arranging and deleting icons representing objects and submaps and for manipulating graphic elements on the maps. Besides, the Maps window is used also for viewing charts.

3.1.2 Opening

Maps window is always open (provided that connection between Net Inspector Client and Server is established).

3.1.3 Description

Tabs

The Maps window contains one or more tabs. When the user opens a user view for the first time, only one tab is displayed in the Maps window. This tab carries the name of the currently active user view and displays the contents of the root map of the given user view.

To create a new tab in the Maps window, select a map in the Explorer window or a submap icon in the Maps window and choose the ***Open*** pop-up command or double-click the submap icon. This will create a new tab in the Maps window and display the contents of the selected submap in it. The newly created tab will carry the name of the map whose contents it displays. Only one tab can be created for each map. Besides, new tabs can be created also by opening charts. To remove an existing tab from the Maps window, right-click its tab symbol at the top of the Maps window and select the ***Close*** pop-up command. To close all tabs, right-click any tab symbol at the top of the Maps window and select the ***Close All*** pop-up command.

Net Inspector automatically saves the information about open tabs in the Maps window for every user and user view and restores the tabs (except the chart tabs) next time the user opens the user view.

Map Views

The Maps window can display objects and submaps either as icons (Graphics view) or by means of a table (Details view). You can switch between both views by selecting the ***Graphics*** and ***Details*** entries in the toolbar drop-down list.

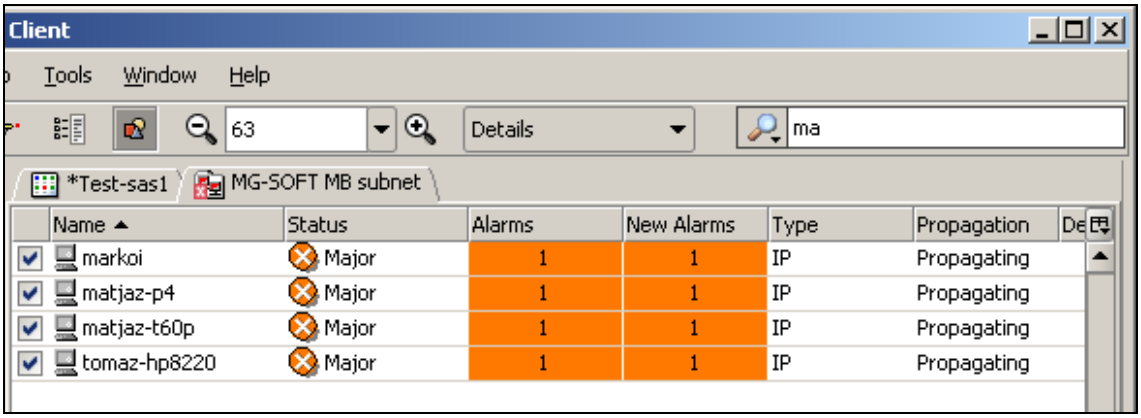
1. Details View

The Details view displays the contents of a map by means of a table, where each table row represents one object (managed, action or system object) or submap.

Filter Bar (drop-down list)
The Filter Bar is displayed on the right side of the toolbar above the Maps window. It lets you enter text that functions as a filter, i.e., it displays only those objects in the currently active tab of the Maps window (Details view) that contain the entered text in selected columns. To specify which columns will be taken into account, click the filter

symbol  and select desired columns from the drop-down menu that appears (columns are described in details below). Then, enter the text in to the accompanying input line, which will serve as the filter criterion.

For example, if the ***Name*** and ***Status*** columns are selected in the Filter Bar drop-down list and you enter the string "ma" into the ***Filter Bar*** drop-down list, the active tab of the Maps window (Details view) will display only those rows (objects) that contain the string "ma" in the ***Name*** and ***Status*** columns (e.g., **Ma**jor [Status], **ma**rko [Name], to**ma**z [Name], etc. – see the picture below).



Example: Filtering objects in the Maps window, Details view

The Details view provides information in the following columns (you can display or hide each column by clicking its name in the column selector  displayed above the vertical scrollbar of the Maps window):

Monitoring State (checkbox)
A check mark in this checkbox indicates that the corresponding object is enabled. For a managed object, this means that the device it represents is being monitored by Net Inspector. For an action object, this means that the action functionality it represents (e.g., sending e-mails to particular recipients) is enabled and its operation is being monitored by Net Inspector. For a system object, this means that the Net Inspector subsystem it represents (e.g., event storage subsystem) is enabled and its functioning is being monitored by Net Inspector. This checkbox is always unchecked for maps.

Name
Displays the symbol and name of the object or map.

Status
Displays the status of the object (e.g., "Normal"). In case of a map, this field displays the most critical status of the object(s) included in the given map and all its submaps (if propagation is not disabled).

Alarms
Displays the total number of active alarms on the object or the total number of active alarms on objects in the map (in case of a map). This field also reflects the color of the most severe active alarm that currently exists on the object, according to the alarm severity colors configured in the User Preferences dialog box (Colors panel). In case of a map, this field reflects the color of the most severe alarm that exists on the objects within the given map and all its submaps (if propagation is not disabled).

New Alarms
Displays the number of new alarms on the object or the number of new alarms on all objects in the map (in case of a map). “New” alarms are active alarms, which are not acknowledged. The New Alarms field also reflects the color of the most severe new alarm that currently exists on the object, according to the alarm severity colors configured in the User Preferences dialog box (Colors panel). In case of a map, this field reflects the color of the most severe new alarm that exists on the objects within the given map and all its submaps (if propagation is not disabled).

State
Displays a graphic symbol (circle) whose color indicates the current operability state of the SNMP agent on the managed object (this property is shown only for the managed objects). The following operability states and colors are used:

operability state:	color of the graphic symbol:
Disabled	grey
Enabled	green
Unavailable	red
Testing	blue

Type
Displays the type of the object (e.g., “IP”, etc.) or the “Submap” for maps.

Propagation
Displays whether the status and alarms associated with the object or map are propagated upward to its parent map(s) or not.

Description
Displays and lets you edit a short description of the object. For managed objects, Net Inspector discovery operation sets this value to the value of the sysDescr.0 object instance returned by the SNMP agent on the managed object.

Object ID
Displays the unique identification code of the object within the Net Inspector system. This identification code consists of two integers separated by a dot (e.g., “1.2”). The first integer is the Net Inspector configuration number, while the second integer uniquely identifies the object within the given configuration.

Node ID
Displays the identification number that has been assigned to the object by the user (according to the user’s classification system).

Class
The class of the object, which can be one of the following:
- Workstation
- Server
- Printer
- Switch
- Router
- Gateway
- Equipment
- Multiplexer
- Transport
- Database

- Firewall
- Transmitter
- Any
- Action (used for action objects)
- System (used for system objects)

Tags
Displays tags (user descriptions) annotated to the managed object. Objects can be searched by the value of their tags.

Location
Displays the physical location of the managed object. Net Inspector discovery operation sets this value to the value of the sysLocation.0 object instance returned by the SNMP agent.

Vendor
Displays the managed object vendor name. Net Inspector discovery operation sets this value to the name of the enterprise responsible for the OID namespace returned by the sysObjectID.0 object instance. The enterprise names displayed are taken from the list of private numbers as registered with IANA and stored on the Net Inspector Server (//Engine/data/nienterprise.txt).

OS
The operating system running on the managed object.

URL
The URL (uniform resource locator) address that provides additional information about the managed object. By default, this is the URL of the performance statistics page of the managed object.

OS
The operating system running on the managed object.

URL
The URL (uniform resource locator) address that provides additional information about the managed object. By default, this is the URL of the performance statistics page of the managed object.

Coordinate X
The geographic coordinate X of the managed object.

Coordinate Y
The geographic coordinate Y of the managed object.

Coordinate Z
The geographic coordinate Z of the managed object.

Address
The host name or the fully qualified domain name of the managed object. If none of these exist, it displays the IP address of the managed object.

IP address
The IP address of the managed object.

Polling Profile
The poling profile assigned to the managed object.

SNMP Access Profile
The SNMP access profile assigned to the managed object.

Entity ID
The entity ID of the managed object – entity.

Entity Address
The address of the managed object - entity.

Entity SNMP Access Profile
The name of the SNMP access profile used for directly accessing the managed object - entity.

NetFlow Source
Indicates whether the managed object is a NetFlow/sFlow source or not.

New Device
Indicates whether the managed object (device) is new or not. New managed objects are those that have been added to the system by the Auto configuration and network discovery features.

2. Graphics View

Icons

The Graphics view displays the contents of a map by means of icons that represent managed objects, action objects, system objects, and submaps. In addition, the Graphics view displays also graphic elements.

Types of Objects

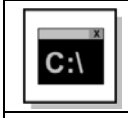
This section describes the built-in object types. In addition, new object types can be defined in the Server Settings dialog box, Object Types panel.

a) The following icons are used to represent **managed objects** (devices):

	IP (generic IP device)
	IP switch
	IP router
	IP server
	IP database

	IP firewall
	IP equipment
	IP transmitter
	IP printer

b) The following icons are used to represent different **types of <u>action objects</u>** (actions that are performed on events):

	MAIL (mail object)
	CMD (command object)
	SMS (SMS object)

The action objects represent actions (e.g., e-mail sending, SMS sending, command execution) that are carried out by Net Inspector when events are triggered in order to notify users of events or to fix a detected network problem in an automated fashion. Action objects can be placed onto maps and monitored in the same way as managed objects. Although being primarily used for notifying users about alarms associated with managed objects, action objects themselves trigger alarms when they fail to perform the designated action (e.g., send an e–mail). Furthermore, the status of the action object changes if any critical fault occurs while performing the action operation.

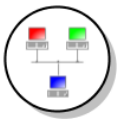
c) The following icons are used to represent different **types of <u>system objects</u>** (Net Inspector subsystems):

	SYS_CONFIG (configuration object)
	SYS_SNMP_NOTIF (SNMP notification object)
	SYS_EVENT (event object)

	SYS_PERF_MNG (performance manager object)

The system objects represent different parts of Net Inspector system. System objects can be placed onto maps and monitored in the same way as managed objects. System objects trigger alarms when there are problems with the Net Inspector subsystems they represent. Furthermore, the status of system objects changes if any critical faults associated with the corresponding subsystems occur. This principle lets you monitor the health of the network and the management system in the same manner.

d) The following icon is used to represent a **map** (submap):

	Map (submap)

e) The **cloud** symbol is used to represent an unknown device (e.g., hub, unmanaged switch, etc.) or a part of the network. Cloud symbols are added to the workspace by the Net Inspector discovery module or manually by using the Graphics Toolbar.

	Cloud (unknown device or part of the network)

Status of Objects

The background color of an object icon indicates the **status** of that object (device, action functionality, Net Inspector subsystem). The following table shows the default object status colors, object statuses and their meanings (statuses are ordered from least to most critical):

Default Icon Background Color	**Object Status**	**Meaning** (M=managed object, A=action object, S=system object)	
 (blue)	unmanaged	M	Device is not being managed (polling is disabled).
		A	Action operation (e.g., e-mail sending) is disabled.
		S	Net Inspector subsystem (e.g. configuration module 3) is disabled.
 (light blue)	indeterminate	M	Device is being managed (polling is enabled) but information about device reachability is currently unavailable (e.g., immediately after enabling polling or after losing connection with the polling engine).
		A	Not applicable.
		S	Not applicable.

 (green)	normal	M	Device is being managed (polling is enabled) and it is responding to Net Inspector queries.
		A	Action operation (e.g., e-mail sending) is enabled and it functions normally (no critical faults exist).
		S	Net Inspector subsystem (e.g. event storage subsystem) is enabled and performs its function successfully (no critical faults exist).
 (orange)	major	M	Device is being managed (polling is enabled), but it is not responding to Net Inspector SNMP queries.
		A	Not applicable.
		S	Not applicable.
 (red)	critical	M	Device is being managed (polling is enabled), but it is not responding to Net Inspector queries.
		A	Action operation (e.g., e-mail sending) is enabled, but it fails to perform its function due to at least one critical fault.
		S	Net Inspector subsystem (e.g. event storage subsystem) is enabled, but it fails to perform its function due to at least one critical fault.

By default, the background of the map icon reflects the color of the most critical status that can be found among the objects in the given map and all its submaps. The map propagation options can be configured in the Propagation view of the (sub)map Properties window.

Note: Object status colors can be configured in the User Preferences dialog box, Colors panel.

Indication and Propagation of Alarms in the Maps window

Alarm Balloons

Small graphic symbols called “alarm balloons” () dynamically appear and disappear above the icons that represent managed objects, action objects, system objects and (sub)maps (if objects are not disabled). An alarm balloon appears above an object icon when at least one new alarm (i.e., active alarm that is not acknowledged) exists on that object, and disappears when all alarms associated with the object are acknowledged or cleared. Similarly, an alarm balloon appears above the submap icon is displayed if at least one new alarm exists on the objects within that submap or any of its submaps (if alarm propagation is not disabled), and such alarm balloon disappears when all alarms on those objects are acknowledged or cleared.

The alarm balloon above the object icon displays the number of new alarms that currently exist on that object. The alarm balloon above the submap icon displays the number of new alarms that currently exist on the objects within that submap.

Note: The alarm numbers are propagated only one hierarchical level higher, while alarm severity colors are propagated up to the top-level submap(s) of the user view.

An alarm balloon automatically changes its color to match the color of the most severe new alarm that currently exists on the object. In case of a submap, the alarm balloon reflects the color of the most severe new alarm that exists on the objects within the given map branch (i.e., in the given map and its submaps).

Alarm severity level colors can be configured in the User Preferences dialog box. The alarm severity levels and their default colors - and thus also the default colors of alarm balloons are:

The alarm severity levels, their symbols and default colors (listed from least to most severe)

Indicating Total Number of Active Alarms

Besides the alarm balloons, which display the number and severity of new alarms (i.e., active alarm that are not acknowledged), small rectangles (2) in the lower-right section of object and submap icons indicate the total number (and severity level) of active alarms on the given object and on the objects within the given submap, respectively.

As alarm balloons, rectangles that indicate the total number of active alarms also dynamically appear and disappear (when objects are enabled). A rectangle symbol appears in the lower-right section of the object icon when at least one active alarm exists on that object, and disappears when no more active alarms exist on that object (i.e., when all alarms are cleared). Similarly, a rectangle appears on the submap icon if at least one active alarm exists on the objects within that submap or any of its submaps (if alarm propagation is not disabled), and such alarm balloon disappears when no more active alarms exist on those objects.

The alarm rectangle on the object icon displays the total number of active alarms that currently exist on that object. The alarm rectangle on the submap icon displays the total number of active alarms that currently exist on the objects within that submap.

Note: The alarm numbers are propagated only one hierarchical level higher, while alarm severity colors are propagated up to the top-level submap(s) of the user view.

The alarm rectangle on the object icon automatically changes its color to match the color of the most severe alarm that currently exists on that object. The alarm rectangle on the submap icon reflects the color of the most severe alarm that exists on the objects within the given submap and all its submaps. The picture above displays the alarm severity levels and their default colors.

Example:

	*Let us suppose that 2 active alarms concurrently exist on the managed object. The severity levels of these alarms are Major and Critical. The 'critical' alarm has been acknowledged by the network operator, while the 'major' alarm has not been acknowledged yet. In such case, the alarm balloon will indicate the number 1 (as there is one non-acknowledged alarm associated with the object) and reflect the color assigned to the Major severity level (i.e., orange, by default, as shown in the picture on the left). The alarm rectangle, on the other hand, will show the total number of active alarms (2) and reflect the color of the critical alarm (i.e., red, by default). Note also that the icon background in the picture on the left reflects the red color, indicating that the status of this managed object is Critical (according to the default color settings).*

Graphics Toolbar

The Graphics toolbar is used for adding **graphic elements** (lines, connections, rectangles, ellipses, images, etc.) and text to the Maps window. In addition, it is used for setting the properties of graphic elements (color, line width, etc.), and for arranging icons and graphic elements in the Maps window (snap to grid). Furthermore, the Graphics toolbar is used for saving the layout of maps, for locking and unlocking maps for editing and for toggling displaying some information in the Maps window (connection labels, tooltips, etc.). Graphic elements are shown only in the Graphics view.

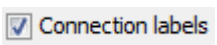
Only users with administrator access rights are authorized to add and remove graphic elements to and from maps, as well as set their properties and reposition object and submap icons on the maps.

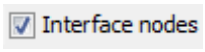
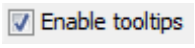
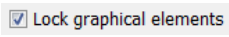
To display or hide the Graphics toolbar, use the ***View / Graphics*** command.

The Graphics toolbar contains the following buttons:

	Saves the current map layout. This button is disabled if no modifications were made to the given map.
	Discards all modifications and reverts the map layout to its last saved state.
	**Locks or unlocks the map for editing** (enables or disables the map Edit mode). The map contents can be changed only if the map is unlocked for editing (Edit mode is enabled). If the Edit mode is disabled, this button is in the locked state (), and all other buttons in the Graphics toolbar are disabled. This means that no items can be added to the currently selected map (tab) in the Maps window, and the existing graphic elements and icons in the Maps window cannot be edited, repositioned or deleted. Only users with administrator access rights can unlock a map for editing.
	Selection tool. When this button is selected, the mouse cursor is represented with the normal arrow symbol and can be used for selecting objects on the map (left-click or left-click and drag) or displaying the context menus (right-click).

	Hand tool. When this button is selected, the mouse cursor cursor is represented with hand symbol. It is used for easier navigation (panning) within the map – graphics view. Click and hold down the left mouse button and drag the map to pan it and display the map portion you want to view (unless the entire map is already displayed).
	Connection tool. It lets you add a connection line between two icons in the Maps window an optionally name the connection endpoints. To add a connection line, select this button and click the first and the second device icon that you want to connect. A connection line will appear, connecting the two icons and the Interfaces dialog box will be displayed to let you select the network interfaces used on both ends of the connection (if this information is available). If you select a network interface on one or both connected devices, a network interface status node (e.g.: ) appears at the corresponding end of the connection line by default (if interface nodes are not disabled). The interface node represents the current status of the network interface used for the given connection. In addition, the description of the selected interface automatically appears as a label on the corresponding end of the connection line by default (if connection labels are not disabled). A connection line can have 3 labels: left, right and center label, used for, e.g., naming the connection and its endpoint interfaces. To edit labels or select endpoint interfaces, double-click the connection line with the selection tool () to open the Connection Labels dialog box and specify labels and interfaces in it. *Example of a connection line with **labels** and **interface status nodes**:*  To delete a connection line, select it with the selection tool and press the *Delete* button on the keyboard. To add a breakpoint to the connection line, select the line at the desired point and drag the mouse pointer in any direction while holding down the mouse button.
	Lets you add a line to the Maps window. To add a line, first click this button, then click within the Maps window and hold down the mouse button while dragging the mouse pointer across the Maps window. Release the mouse button at the point where you want the line to end.
	Lets you add a rectangle to the Maps window. To add a rectangle, first click this button, then click within the Maps window and hold down the mouse button while dragging the mouse pointer across the Maps window. Release the mouse button when the size of the rectangle matches your preferences.
	Lets you add an ellipse to the Maps window. To add an ellipse, first click this button, then click within the Maps window and hold down the mouse button while dragging the mouse pointer across the Maps window. Release the mouse button when the size of the ellipse (circle) matches your preferences.

	Lets you add a new or edit an existing text in the Maps window. To add a text, first click this button, then click within the Maps window at the point where the text should start. This opens the Text Editor dialog box. Enter the text into the Text Editor dialog box, adjust the font type and size to meet your preferences, and click the ***OK*** button to close the dialog and display the entered text in the Maps window. To edit an existing text, click this button and then click the text to be edited in the Maps window to open the text in the Text Editor dialog box, where you can edit it. **Note:** If you select a special font type (e.g., a Cyrillic font) that is not available on other computers running Net Inspector Client, the added text might not be visible when connecting to Net Inspector Server from other computers.
	Lets you add an image to the Maps window. To add an image, first click this button, then click within the Maps window to select a point for the upper left corner of the image. This opens the Select Image dialog box that lets you choose a bitmap image file (JPG, BMP or PNG format) to be inserted. Note that the image file must be stored on the computer running Net Inspector Server (in the “Engine” folder or its subfolders).
	Shows or hides the gridline that can be used for evenly aligning icons and graphic elements on the map.
	Enables or disables arranging object icons and graphic elements in the currently active tab of the Maps window onto a gridline.
	Brings the selected graphic element to the foreground layer (i.e., in front of all overlapping graphic elements).
	Sends the selected graphic element to the background layer (i.e., behind all overlapping graphic elements).
	Lets you set the line (border) color of the selected graphic element.
	Lets you set the fill color of the selected graphic element.
	Lets you set the line (border) width of the selected graphic element.
	Lets you add a cloud symbol to the Maps window. To add a cloud symbol, first click this button, then click the target location within the Maps window.
	Check this checkbox to display connection labels in the current map in the Maps window (Graphics view). Uncheck this checkbox to hide the connection labels.
	Click the **A-** symbol to decrease the font size of connection labels. Click the **A+** symbol to increase the font size of connection labels.

	Check this checkbox to enable displaying the network **interface status nodes** (e.g.:) at connection line endpoints in the current map in the Maps window (Graphics view) and to enable dynamic visualization of link traffic. Interface status nodes are displayed for devices that support the standard SNMP MIB-II Interfaces table and for which the connection endpoint interfaces are known). The interface node represents the current status of the network interface used for the connection. The interface status can be either **up** ( ), **down** ( ) **disabled** ( ), or **not present** ( ). The interface status nodes are not shown if the corresponding SNMP agent or entire managed object is down.
	Check this checkbox to enable displaying device performance tooltips in the current map in the Maps window (Graphics view). If this option is enabled, the current device performance information (interface, CPU, memory, storage utilization - whichever available) and active alarms are displayed in a tooltip when you hover the mouse cursor over a managed object icon (without clicking it). Click the titlebar of the tooltip to pin the tooltip window to the desktop and move it to the desired position on the screen (e.g., to monitor device performance parameters and alarms in it).
	Check this checkbox to lock the position of existing graphic elements and text on the map, while allowing adding, repositioning and deleting managed objects, action objects, system objects, submaps and links. This option is useful, for example, if you want to reposition icons on the map and do not want to move also the background image or other graphic elements (lines, rectangles, ellipses,..) and text.

Graphic elements (i.e., lines, rectangles, ellipses, images) and object icons can be **resized** by dragging the element handles (small grey rectangles) that are displayed along the edges of the graphic element or the icon when it is selected. To move a graphic element or an icon, select it and drag it to the desired position.

3.1.4 Maps Window Pop-Up Menu

The Maps window pop-up (context) menu can be displayed by right-clicking an object represented either by an icon (Graphics view) or a row (Details View) or by right-clicking inside a tab in the Maps window. This menu contains a list of commands specific to that object or tab.

This section describes the pop-up menu available in regular tabs in the Maps window. For description of the pop-up menu displayed in chart tabs, please refer to the Chart Tab Pop-up Menu section. The pop-up menu in a regular tab in the Maps window contains the following commands (some of them may be available only to users with administrator access rights):

- ***Properties***
  If a managed object is selected, this command opens the Properties window, which lets you view and configure properties of the selected managed object. If a system object is selected, this command opens the corresponding system object Properties window. If an action object is selected, this command opens the corresponding action object Properties window. If a (sub)map is selected, this command opens the

(sub)map Properties window, which lets you view and configure the map propagation settings.

- ***Show Performance Statistics***

> **Note:** This command is disabled in the Net Inspector LITE edition.

If a managed object is selected, this command opens the Performance Statistics window displaying the performance statistics of the selected managed object provided that this object is being polled by a Performance Manager polling engine. (PM polling engine can be set in the device's Properties dialog box, General view). This command is available only for managed objects, i.e., objects representing network devices.

- ***Show NetFlow Statistics***

> **Note:** This command is disabled in the Net Inspector LITE edition.

On a managed object that is set as a NetFlow source, this command displays the Performance Manager NetFlow page for the given NetFlow/sFlow source (e.g. a router). The NetFlow page contains the TopN NetFlow/sFlow traffic reports for the given NetFlow source (for all network interfaces on this source). By expanding and clicking the individual subentries in the Top N reports, more detailed statistics for the selected item (e.g., conversation, application, protocol etc.) is shown. This command is available only for managed objects that are set as the NetFlow sources in Net Inspector (indicated by a "NF" sign on the object icon).

- ***Enable***
  Enables selected objects (i.e., starts polling managed objects, activates the action operations for action objects). If a submap is selected, this enables all action and managed objects included in the selected submap and its submaps. This command has no effect on system objects.

- ***Disable***
  Disables selected objects (i.e., stops polling managed objects, deactivates the action operation for action objects). In case of a submap, this command disables all action and managed objects included in the selected submap and its submaps. This command has no effect on system objects.

- ***Alarms (cascading menu)***

  - ***Active Alarms***
    Creates a new tab in the Events window and displays all active alarms associated with the selected objects in it. For the description of alarms and related commands, please refer to the Events Window section of this manual.

  - ***Acknowledge New Alarms***
    Acknowledges all new alarms associated with the selected objects. New alarms are active alarms that are not acknowledged.

  - ***Find Events***
    Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the selected objects.

  - ***History***
    Creates a new tab in the Events window and displays a history of alarms associated with the selected objects in it.

- ***Tools (cascading menu)***
  - ***Ping***
    Opens the Ping and SNMP Console dialog box(es) and starts “pinging” the selected managed object(s).
  - ***MIB Browser***
    Opens the MIB Browser window. If a managed object is selected, this command automatically contacts the selected managed object by means of the SNMP GetNext request.
  - ***Change Profile***
    Opens the Change Profile dialog box, which lets you assign a different poling profile and SNMP access profile to the selected managed object(s).
  - ***Change Polling Engine***
    Opens the Change Polling Engine dialog box, which lets you assign a different poling engine to the selected managed object(s).
  - ***Resolve Device Address***
    Forces resolving the device name to IP address at user request. This is useful in environments using dynamic IP addresses in order to manually refresh the device IP address in Net Inspector (e.g., after it has been changed by a DHCP server). Note that this function is executed automatically anytime a managed object monitoring is enabled. This command is available only for managed objects, i.e., objects representing network devices.
  - ***Manage Tools***
    Opens the Client Preferences dialog box, Tools panel, which lets you manage user-defined commands (actions).
  - ***NetFlow Source***
    Sets the selected managed object as a NetFlow source device in Net Inspector, i.e., a device that sends NetFlow v5 or v9 packets or sFlow v5 packets to Net Inspector polling engine (this must be first configured on the given device (e.g., a router) using the vendor-specific commands). Net Inspector WorkGroup and Enterprise Editions incorporate a software NetFlow/sFlow collector and analyzer module that receive NetFlow packets from source devices and provide NetFlow traffic statistics in the Performance Manager Home Page window, NetFlow page.
- ***New Device***
  Toggles displaying the “New” label for the selected managed object. Managed objects that have been added to the system by the Auto configuration and network discovery features are automatically marked with the “New” label displayed in the upper-left corner of the managed object icon (Graphics view).
- ***Copy (Ctrl+C)***
  Copies the selection to the clipboard.
- ***Cut (Ctrl+X)***
  Removes the selection and puts it on the clipboard. This command is available only when the map is in the edit mode.
- ***Paste (Ctrl+V)***
  Places the clipboard contents on the selected map. This command is available only when the map is in the edit mode.

- **Duplicate**
  Duplicates the selected managed and action object(s). This command actually adds new objects to the configuration. New object(s) that are created with this command have the same properties as the source object(s) they have been created from, except the object ID value and the name of the object. The latter is composed of the name of the source (original) object and the "`_Copy`" suffix. If an object with such name already exists, an index number is added to the suffix (e.g.: `_Copy1`, `_Copy2`, …). This command is available only to users with Administrator user privileges.
- ***Delete (Del)***
  Deletes selected objects from the map. This command is available only when the map is in the edit mode.
- ***Remove from Configuration***
  Removes selected objects from the system (configuration). This command is available only to users with Administrator user privileges.
- ***Add (cascading menu)***
  - ***New Submap***
    Creates a new submap in the current map. This command is available only when the map is in the edit mode.
  - ***New Object***
    Opens the New Object dialog box that lets you add a new object of a certain type to the selected map in two steps. This method actually enables adding new objects to the system. New objects appear also in the Device Panel dialog box. This command is available only when the map is in the edit mode.
  - ***Import from CSV File***
    Lets you select the CSV file from disk and opens the Import from CSV File dialog box that allows you to view and edit the list of managed objects (devices) to be imported, and finally, import new objects and add them to the currently active map in the Maps window. Importing devices is one of the methods of adding new objects to the system. Imported objects appear also in the Device Panel dialog box.
- ***Export***
  Opens the **Export Submap** dialog box, which lets you export the table displayed in the currently active tab of the Maps window (Details view) to an HTML or a CSV (comma-separated value) file format. The Export Submap dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information in columns that are currently displayed in the given tab of the Maps window will be exported. This command is available only in the Details view.
- ***Save as Default Layout***
  Users with administrator access rights are authorized to use this command to save the current layout of the Maps window - Details view as a default layout. Default layout stores the information about the display status (displayed/hidden), order and width of the columns displayed in the currently active tab of the Maps window, Details view. Once the default layout is defined (saved), it automatically applies to all maps (tabs) you open in the Maps window (Details view). The default layout is also automatically applied to all users when they connect to Net Inspector Server for the first time (until they modify their layout). Therefore, this command is typically

used by administrators when configuring the system (i.e., when defining default layouts of Net Inspector Client main windows etc.). This command is available only in the Details view.

- ***Load Default Layout***
  Loads and applies the default layout in the current tab of the Maps window - Details view. Default layout stores the information about the display status (displayed/hidden), order and width of the columns. This command is available only in the Details view.

3.1.5 Device Performance Tooltips

To enable displaying the current device performance data in tooltips on the currently active map in the Maps window, check the *Enable tooltips* checkbox in the Graphics toolbar. Then, hover the mouse cursor over a device icon on the map (Graphics view), to display the tooltip for the given device.

The tooltip displays the last retrieved device performance information (interface, CPU, memory, storage utilization rates – if this information is available via SNMP) and active alarms in a pop-up tooltip. Tooltip disappears automatically when you move the mouse cursor away from the device icon.

Click the titlebar of the tooltip to pin the tooltip window to the desktop and move it to the desired position on the screen (e.g., to monitor device performance parameters and alarms in it). The contents of the pinned tooltip window are automatically refreshed when new information is available. You can horizontally resize the pinned tooltip window to match your preferences. To close the pinned tooltip window, click the *Close (X)* button in the upper right section of the tooltip window.

Device performance tooltips display the following information about the device (the data is taken from the respective device Properties window):

Titlebar with pin symbol ( )
Click the titlebar to transform the tooltip into a window and pin it to the desktop. You can move and horizontally resize the pinned tooltip window. The content of the pinned tooltip window is automatically refreshed when new information is available.

Name
Name of the managed object (device).

Object ID
The unique Object ID of the managed object.

Address
The IP address or the host name of the managed object.

Type and class
Displays the type and class of the managed object.

Interfaces (section)

Name
The name and the current status of the network interface, as retrieved from the SNMP agent on the managed object. The interface status can be either **up** ( ), **down** ( ) **disabled** ( ), or **not present** ( ).

IP address
The IP address assigned to the network interface (if any).

Status
The interface status. Possible values are: **`up`**, **`down`**, **`disabled`** , or **`not present`**.

In Utilization
The last retrieved inbound utilization rate of the interface.

Out Utilization
The last retrieved outbound utilization rate of the interface.

CPU (section)

Number of cores
Total number of CPU cores.

Usage
The last retrieved average CPU usage in %.

Storage (section)

Name
The name of the storage unit (including disk units and memory).

Type
Type of the storage unit (disk, physical memory, virtual memory).

Used size
The last retrieved storage unit used capacity in %.

Free size
The last retrieved storage unit free capacity in %.

Active alarms (section)
Displays the list of active alarms if present on the given object, as follows:

Severity
Displays the alarm severity level.

Date/Time
Displays the date and time of triggering the alarm.

Comment
Displays the comment added to the alarm by a user.

Message
Displays a short description of the alarm (e.g. “Device is down”).

Ack. Date/Time
Displays the date and time of acknowledging or unacknowledging the alarm (whichever was last).

Message ID
Displays the event/alarm message identifier number (e.g. “10002”).

Source Info
Displays information about the source of the problem. For example, in case of a threshold alarm, it explains what threshold has been crossed (e.g., Physical memory).

Add. Info/Threshold
Displays additional information about the problem. For example, in case of a threshold crossed alarm, it provides the actual value of the parameter (e.g., 95%).

If SNMP agent on the managed object does not provide information for some section (Interfaces, CPU, Storage), the respective section is not shown in the tooltip.

3.1.6 New Object Dialog Box

To open the New Object dialog box, select the ***Add / New Object*** pop-up command in the Maps window.

The New Object dialog box lets you create a new object of a certain type and add it to the selected map in the Maps window in two simple steps. In the first step, you need to select the type of the object to be added. This can be an IP managed object or an action object. In the second step, you need to specify the object properties (e.g., name, description, etc.), as well as select the (sub)map and configuration to which you want to add the object.

This dialog box lets you add a new object to the system in a wizard-like fashion and has two screens: the Select object type screen and the Object properties screen.

1. The **Select object type** screen provides the following controls:

Select object type (list)
Displays and lets you select the type and class of the object to be added. This can be an IP managed object (e.g., IP server, IP router,…) or an action object (MAIL, SMS, CMD). Select the desired type of the object and click the ***Next*** button to proceed to the next screen.

Next (button)
Lets you proceed to the next screen, i.e., the **Object properties** screen.

Cancel (button)
Discards all changes and closes the dialog box.

2. The **Object properties** screen provides the following controls:

Name (input line)
Lets you enter the name for the new object.

Address (input line)
Lets you enter the IP address or the host name for the IP managed object. This input line is disabled for other objects.

Description (input line)
Lets you enter a short description of the object.

Vendor (input line)
Lets you enter the vendor of the object.

Class (drop down list)
Lets you choose the class of the object.

Submap (drop down list)
Displays the name of the (sub)map to which the new object will be added. By default, this drop-down list displays the name of the currently active (sub)map in the Maps window. To add the object to another (sub)map, click the ***Browse*** button next to his input line and select the (sub)map from the Browse dialog that appears.

Browse (button)
Opens the Browse dialog box that lets you select the (sub)map to which you want to add the new object. To create a new (sub)map, select a map in the expandable map tree and click the ***Create New Map*** button. This will create a new (sub)map directly below the selected (sub)map in the Browse dialog box. To select a (sub)map, expand the hierarchical map tree, choose the desired (sub)map and click the ***OK*** button. The name of the selected (sub)map will be displayed in the ***Submap*** drop down list.

Configuration (drop down list)
Displays the configuration to which the object will be added, i.e., the name of the `[configX]` section in the Net Inspector Server initialization file. If more than one configuration (`[configX]` section) is present, you can select the desired configuration from this drop-down list.

Polling Engine (drop down list)
Lets you choose the polling engine that will poll the given managed object.

Back (button)
Lets you return to the previous screen, i.e., the **Select object type** screen.

Finish (button)
Closes the New Object dialog box and adds the new object to the selected map and configuration. New object appears also in the Device Panel dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

3.1.7 Connection Labels Dialog Box

To open the Connection Labels dialog box, double-click a connection line with the selection tool ( ) in the Maps window, Graphics view when map editing is enabled.

The Connection Labels dialog box lets you add, edit and delete connection line labels and select the connection endpoint interfaces.

A connection line can have 3 labels: left, right and center label. They are used, for example, for naming the connection and its endpoint interfaces.

The dialog provides the following controls:

Left label (input line)
Lets you specify the left label for the connection (e.g., interface address or name) displayed on left hand side (or upper section in vertical lines) of the connection line.

Position (drop-down list)
Lets you select the position of the left label relative to the connection line (left, right, center).

Auto rotation enabled (left) (checkbox)
If this checkbox is checked, the label text is automatically rotated/aligned with the connection line if you reposition any of the two objects the line is connecting.

Center label (input line)
Lets you specify the center label for the connection (e.g., a link name) displayed in the central section of the connection line.

Position (drop-down list)
Lets you select the position of the label relative to the connection line (left, right, center).

Auto rotation enabled (left) (checkbox)
If this checkbox is checked, the label text is automatically rotated/aligned with the connection line if you reposition any of the two objects the line is connecting.

Right label (input line)
Lets you specify the right label for the connection (e.g., a link name) displayed on right hand side (or lower section in vertical lines) of the connection line.

Position (drop-down list)
Lets you select the position of the label relative to the connection line (left, right, center).

Auto rotation enabled (left) (checkbox)
If this checkbox is checked, the label text is automatically rotated/aligned with the connection line if you reposition any of the two objects the line is connecting.

Interfaces (frame)
Lets you select the network interfaces used on both ends of the connection (e.g., interface name). This information is used for presenting the interface status nodes (e.g.: ) at connection line endpoints. Interface status nodes are displayed for devices that support the standard SNMP MIB-II Interfaces group of objects and for which the connection endpoint interfaces are selected.

Source (drop-down list)
Specifies the name of the source endpoint device and lets you select the network interface on that device used for establishing the given connection.

Target (drop-down list)
Specifies the name of the target endpoint device and lets you select the network interface on that device used for establishing the given connection.

OK
Applies the changes and closes the Connection Labels dialog box.

Cancel
Discards all changes and closes the Connection Labels dialog box.

3.1.8 Find Objects Dialog Box

To open the Find Objects dialog box, select the ***Edit / Find Objects*** command.

The Find Objects dialog box lets you search for those objects in the given user view that match the user-specified search condition. The result of a search operation is displayed in a separate “Search” tab in the Maps window, where found objects are listed using the details view. Search condition can be specified by using the following controls in the Find Objects dialog box:

Search by (drop-down list)
Lets you select the property (type of the condition) by which the objects will be searched (e.g., Name, Description, Status, IP address, etc). A detailed description of object properties can be found in the Map window details view section of this manual. Managed objects can be searched also by the names of the assigned polling and SNMP access profiles.

Operator (drop-down list)
Lets you select the operator, e.g., “is”, “is not”, “contains”, “is greater or equal”, “is smaller or equal”, etc. Available operators depend on type of the condition selected in the ***Search by*** drop-down list.

Value (input line)
Lets you enter the condition value. Valid values depend on the type of the condition selected in the ***Search by*** drop-down list.

Search within results (checkbox)
Enables you to search only within the scope of the existing results (i.e., a list of objects returned by a previously performed **Find Objects** operation) and thus refine the search. This option is enabled only if an existing “Search” tab in the Maps window is currently active.

OK
Searches the entire user view for the matching object(s) and displays results in a new “Search” tab in the Maps window.

Cancel
Discards all changes and closes the Find Objects dialog box.

Search Tab Pop-up Menu

By performing the **Find Objects** operation, a new Search tab in the Maps window is created, displaying the search results, i.e., objects that match the search condition.

Found objects are listed using the details view. Besides the columns displayed in the Maps window details view, an additional “Submap” column can be displayed in the Search tab. The Submap column displays the name of the (sub)map containing the found object.

By right-clicking inside the Search tab a pop-up menu appears, which contains the same commands as the regular Maps window pop-menu and the following command:

- ***Open Containing Submap***
  Displays the submap that contains the given object in a regular tab in the Maps window and selects the object.

3.1.9 Change Profile Dialog Box

To open the Change Profile dialog box, select one or more objects in the Maps window and use the ***Tools / Change Profile*** pop-up command.

The Change Profile dialog box lets you assign a different poling profile and SNMP access profile to the managed object(s) selected in the Maps window. These profiles must already exist in the Server Settings dialog box, Profiles panel. The dialog provides the following controls:

Polling profile (checkbox and drop-down list)
The drop-down list lets you select among the existing polling profiles. The chosen profile will be assigned to the selected managed objects. Uncheck the **Poling Profile** checkbox if you don’t want to change the polling profile for selected objects.

SNMP access profile (checkbox and drop-down list)
The drop-down list lets you select among the existing SNMP access profiles. The chosen profile will be assigned to the selected managed objects. Uncheck the **SNMP access profile** checkbox if you don’t want to change the SNMP access profile for selected objects.

OK
Applies the changes and closes the dialog box.

Cancel
Discards all changes and closes the dialog box.

3.1.10 Import from CSV File Dialog Box

To open the Import from CSV File dialog box, select the ***Add / Import from CSV File*** pop-up command in the Maps window, and in the Import dialog box that appears, select a desired CSV text file from disk. The CSV file should contain the following data about devices to be imported (one line per device):

Device IP address, device name, polling profile, SNMP profile, PM polling engine

Allowed data separator characters: , ; |

Import rules:
1) Only one attribute for each device may be used, which must be IPv4 or IPv6 address
2) If more than 5 attributes are present for each device, only the first 5 will be used

3) All the missing attributes will be replaced with the default values

The Import from CSV File dialog box lets you view and edit the list of managed objects (devices) contained in the selected CSV file, and finally import new objects and add them to the currently active map in the Maps window.

The Import from CSV File dialog box contains the following controls:

Devices (list)
Displays the list of devices to be imported. For each device the following information is displayed is separate columns:

IP address
The IPv4 or IPv6 address of the managed object (device). This attribute must be present.

Name
The name of the managed object (device). If this attribute is absent, the IP address attribute is used as the name.

Polling profile
The name of the polling profile that will be used for polling the managed object (device). If this attribute is absent in the CSV file, the “default” polling profile is used.

SNMP profile
The name of the SNMP access profile that will be used for polling the managed object via SNMP. If this attribute is absent in the CSV file, the “default” SNMP profile is used.

Polling engine
The name of the polling engine that will be used for polling the managed object. If this attribute is absent in the CSV file, the “Built-in” polling engine is used.

Add (button)
Adds a new managed object (new line) to the Devices list. Enter the IP address and the name properties of the managed object and optionally edit its other attributes.

Remove (button)
Deletes the selected managed object from the Devices list.

Open File (button)
Displays the Import dialog box that lest you select an additional CSV text file for import.

Modify Selected (button)
Opens the Settings dialog box that lets you select the polling profile, SNMP profile, and the polling engine for multiple selected objects.

Poll imported devices (checkbox)
If this checkbox is checked, Net Inspector will start immediately monitoring the newly imported devices.

Import (button)
Imports the managed objects (devices) into Net Inspector and adds their icons to the currently displayed map in the Maps window. Imported objects appear also in the Device Panel dialog box.

Close (button)
Discards all changes and closes the dialog box.

3.1.11 Adding Objects to Maps

Net Inspector can automatically add discovered devices to the workspace (i.e., selected user view) and to the Device Panel dialog box (i.e., to selected configuration), depending on the discovery operation settings.

Furthermore, users with administrator access rights are authorized to manually add objects, which are registered with the system, to maps (as well as configure their settings and remove them from maps). Objects can be placed onto maps from the Device Panel dialog box or from the Discovery dialog box.

Additionally, users with administrator access rights can manually create new objects of certain types and add them to the currently active map in the Maps window by using the Maps window ***Add / New Object*** pop-up command. This method allows adding new objects to the system.

Next, users with administrator access rights can import managed objects from a CSV (comma separated value) file by using the Maps window ***Add / Import from CSV File*** pop-up command.

Finally, new objects can be added to the system also by selecting one or more existing managed object(s) and choosing the ***Edit / Duplicate*** command. Newly added objects appear also in the Device Panel dialog box.

3.1.12 Viewing Alarms for Selected Objects

To view all active alarms on selected objects, select one or more object in the Map window, and use the ***Alarms / Active Alarms*** pop-up command. This operation creates a new tab in the Events window and displays all active alarms associated with the selected objects in it. For the description of alarms and related commands, please refer to the Events Window section of this manual.

3.2 Explorer Window

3.2.1 Purpose

The Explorer window is used for exploring and switching between user views assigned to the user, as well as for creating new user views. It is also used for viewing and modifying the hierarchical map structure of user views and for displaying the contents of submaps in the Maps window. Moreover, the Explorer window is used for configuring and monitoring the object status and alarm propagation.

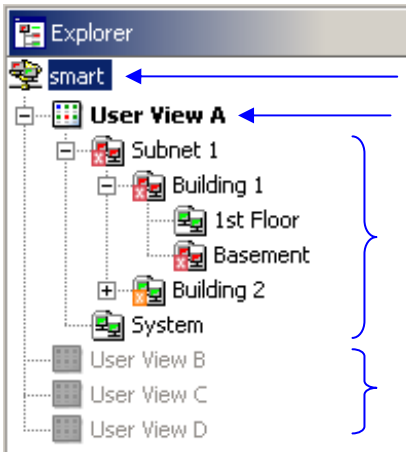
3.2.2 Opening

To display or hide the Explorer window, use the ***View / Explorer*** toggle command or the  ***Explorer*** toolbar button.

3.2.3 Description

The Explorer window graphically displays the Net Inspector workspace structure, i.e., all user views assigned to the user and hierarchical tree-like structures of maps and submaps within the active user view. The workspace is a conceptual environment that allows users to group objects into maps and to structure such maps in a hierarchical manner within user views. Double-clicking a map icon in the Explorer window, creates a new tab in the Maps window and displays the map contents in it. Double-clicking a user view icon in the Explorer window, activates the double-clicked user view and displays its top-level maps in the Explorer window. To view the entire structure of maps and submaps, select the active user view icon in the Explorer window and choose the ***Expand*** pop-up command.

Example of the Explorer window contents:



Net Inspector Server name
active user view

hierarchical map structure within the user view

inactive user views

Explorer Window in Design Mode

Net Inspector Client offers two modes of operation: normal and design mode. In normal mode, only one user view can be active (open) at a time. In design mode, on the other hand, users can have more than one user view open at the same time and copy objects between active user views.

In design mode, you can open any inactive user view by selecting its icon in the Explorer window and choosing the ***Open*** pop-up command. This will activate the selected user view without deactivating other active user views.

For more information about the design mode, please see the Net Inspector Client Design Mode section.

Object Status and Alarm Propagation

The colors of map icons in the Explorer window dynamically change to indicate the current status of objects and alarms on objects within those maps and their submaps. By default, the most critical object status and active alarm is propagated upward the hierarchical map branch for all objects and submaps. The Propagation view of the relevant submap Properties window lets you enable or disable the propagation for individual objects included in that map.

A map icon in the Map Explorer window reflects different colors to indicate the current status of objects included in the map and its submaps (if propagation is not disabled). Colors reflected by map icons can be can be configured in the User Preferences dialog box. By default, map icons reflect the following colors:

 - the map contains no managed, action or system objects

 - the status of all objects in the given map and its submaps is “unmanaged”

 - the most critical object status in the given map and its submaps is “indeterminate” (this is an intermediate status, e.g., displayed immediately after enabling device polling)

 - the most critical object status in the given map and its submaps is “normal” (note that such maps may contain also unmanaged objects)

 - the most critical status of the objects in the given map and its submaps is “major” (status of at least one object in the given map branch is “major”)

 - the most critical status of the objects in the given map and its submaps is “critical” (status of at least one object in the given map branch is “critical”)

Note: Map icons always reflect the most critical status, for example, if a map contains objects whose statuses are “normal” and “critical”, the map will reflect the color assigned to the “critical” status (i.e., red (by default)).

Furthermore, a map icon also indicates the most critical new alarm (i.e., active alarm that is not acknowledged) that exists on the objects within the given map and its submaps. This is achieved by displaying the alarm severity level symbol on top of the map icon, for example:


Severity level of the most critical new alarm on the objects within this map and its submaps is "Warning"


Severity level of the most critical new alarm on the objects within this map and its submaps is "Major"


Severity level of the most critical new alarm on the objects within this map and its submaps is "Critical"

3.2.4 Pop-Up Menu

The Explorer window pop-up menu can be displayed by right-clicking an icon that represents the Net Inspector Server (root icon), user view, or a (sub)map, or by right-clicking the white area inside the Explorer window. This menu contains commands specific to the selected object or commands specific to the Explorer window (when nothing is selected). Furthermore, some of the commands in this pop-up menu are available only in the design mode.

The Explorer window pop-up menu contains the following commands (depending on the selection and on the mode of operation, as described below):

- ***Disconnect***
  Disconnects Net Inspector Client from the Server and closes all windows in the Client main window. If the workspace has been modified and not saved yet, the Save Maps dialog box appears, which lets you save the layout of modified user views or cancel the modifications. This command is available only when the root (Net Inspector Server) icon is selected or when nothing is selected in the Explorer window.
- ***Open***
  This command is available only when a user view or a submap icon is selected in the Explorer window. When a submap or the active user view icon is selected, this command creates a new tab in the Maps window and displays the contents of the selected submap or the selected user view's top-level objects in it. If an inactive user view icon is selected (such user views are represented with grayed-out icons), this command opens (activates) the selected user view.
- ***Close***
  Closes (deactivates) the selected user view. This command is available only in the design mode.
- ***Properties***
  Opens the (Sub)map Properties Window of the selected (sub)map or user view. This command is available only when a (sub)map or a user view icon is selected in the Explorer window.
- ***Enable***
  Enables all action and managed objects in the given map branch (i.e., the selected map and its submaps). This command is available only when a (sub)map or an active user view icon is selected in the Explorer window.
- ***Disable***
  Disables all action and managed objects in the given map branch (i.e., the selected map and its submaps). This command is available only when a (sub)map or an active user view icon is selected in the Explorer window.

- ***Rename***
  Lets you rename the selected map or user view. After renaming the map or user view, press the ***Enter*** key to apply the changes. This command is available only when a (sub)map or an active user view icon is selected in the Explorer window.
- ***Users***
  Opens the Edit User View dialog box that lists all users in the system and lets you assign the user view to users. This command is available only when a user view icon is selected in the Explorer window.
- ***Expand***
  Expands the hierarchical map structure below the selected (sub)map or active user view.
- ***Collapse***
  Collapses the hierarchical map structure below the selected (sub)map or active user view.
- ***Cut (Ctrl+X)***
  Removes the selected map and its submaps (if any) and puts it on the clipboard. This command is available only when a (sub)map icon is selected in the Explorer window.
- ***Copy (Ctrl+C)***
  Copies the selected map and its submaps (if any) to the clipboard. This command is available only when a (sub)map icon is selected in the Explorer window.
- ***Paste (Ctrl+V)***
  Inserts the clipboard contents onto the selected map. This command is available only when a (sub)map icon is selected in the Explorer window.
- ***Delete (Del)***
  Deletes the selected map and its submaps (if any). This command is available only when a (sub)map icon is selected in the Explorer window.
- ***New Submap***
  Creates a new (sub)map below the selected map or active user view. This command is available only when a (sub)map or an active user view icon is selected in the Explorer window.
- ***New User View***
  Opens the New User View dialog box that lets you create a new user view. This command is available only when the root icon (Net Inspector Server) is selected or when nothing is selected in the Explorer window.

3.3 Map Overview Window

3.3.1 Purpose

The Map Overview window is a floating window that displays a graphical overview of the content of the map currently selected in the Maps window - Graphics view and indicates what portion of the map is displayed in the Maps window. This principle enables better orientation and easier map navigation.

3.3.2 Opening

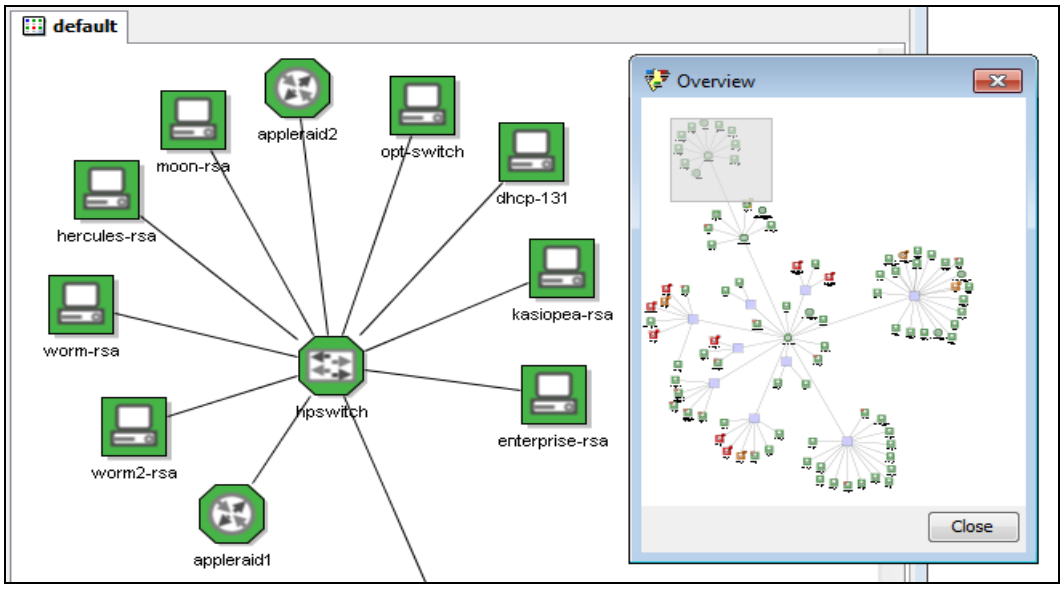
To display or hide the Map Overview window, use the ***View / Map Overview*** toggle command.

The Map Overview window is a floating window that can be resized and repositioned independently of the Net Inspector Client main window.

3.3.3 Description

The Map Overview window graphically displays the entire content of the map that is currently displayed in the Maps window – Graphics view. If the Map Overview window is resized, its content is also automatically resized (reduced or enlarged) to fit the window. The Map Overview window contains a shaded rectangle (current view), which indicates what portion of the map is currently displayed in the active tab of the Maps window. This is particularly useful if the Maps window Zoom-in feature is used to display only a portion of the entire map. By clicking and dragging the shaded rectangle in the Map Overview window, the user can quickly display other parts the map in the Maps window. Similarly, by clicking a portion in the Map Overview window that is not covered by the shaded rectangle, the rectangle moves to the clicked position and the corresponding portion of the map is shown in the currently active tab of the Maps window. By using the Zoom-in and Zoom-out feature in the Maps window, the shaded rectangle is automatically reduced or enlarged to indicate what portion of the map is currently shown in the Maps window.

Example: Viewing the part of a map marked by the shaded rectangle in the Map Overview window



3.4 Events Window

3.4.1 Purpose

It is used for viewing and finding alarms and events and for managing alarms.

3.4.2 Opening

The Events window can be opened by selecting the ***View / Events*** command or by clicking the  ***Events*** toolbar button.

3.4.3 Description

The Events window is used for viewing alarms and events and for managing alarms. Managing alarms includes acknowledging, manually clearing, as well as unacknowledging and manually unclearing alarms.

Additionally, the Events window lets you view filtered active alarms in separate tabs, as well as search for alarms and events that match the user-specified conditions and display search results in separate tabs of the Events window.

Events, Alarms and Active Alarms

Net Inspector alarming system is based on events. Net Inspector Server triggers (and optionally logs) all events that are essential for the monitoring of managed objects. Net Inspector Server triggers **events** when it receives SNMP notification messages sent by the managed objects and when it detects network problems or changes in important parameters of managed objects functioning while polling the objects (e.g., managed object is not responding, SNMP agent on the managed object is not responding, CPU load on the managed object is high, etc.). Events are triggered also if problems occur within particular Net Inspector subsystems (e.g., the configuration module triggers an event if Net Inspector Server cannot connect to the configuration database, etc.) and if Net Inspector fails to perform the designated action (e.g., send an e–mail) for some reason. Events trigger, change and clear alarms.

Alarms are messages that indicate faults or conditions that could lead to faults on managed, action and system objects. An alarm can be **active** or **cleared**. When an event triggers an alarm, the alarm becomes and remains active until the event that clears this alarm is triggered. Typically, for every event that triggers an alarm, there is also one that clears it (e.g., event that is triggered when a managed object is not responding to queries, triggers (activates) the “Device is down” alarm; while the event that is triggered when the object starts responding again, clears (deactivates) the “Device is down” alarm).

In addition to events, which are triggered automatically as a result of important or abnormal occurrences detected on the managed objects or within the Net Inspector system itself, there are also events that are triggered when users manage alarms, i.e., acknowledge/unacknowledge or manually clear/unclear alarms. These events change the **state of alarms**, e.g., from active to manually cleared, from new to acknowledged, etc. New alarms are active alarms, which are not acknowledged. Alarm acknowledging plays a confirming role, i.e., by acknowledging alarms, users declare that they are aware of them.

Note: Not all alarms can be manually cleared. Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared, as this could cause malfunctioning of the fault management application itself.

Severity Levels of Alarms

Every alarm and event in Net Inspector has a particular severity level. A severity level indicates the severity (difficulty) of the condition on the object. To provide a better overview of alarms and events, each severity level is assigned a different symbol and color. User Preferences dialog box (Colors panel) lets you set the colors of alarm (and event) severity levels according to your preferences.

The following picture shows alarm severity levels (listed from least to most severe), their symbols and default colors:

The severity level of an active alarm can be **Informational**, **Warning, Minor, Major**, or **Critical**. When an alarm is cleared, its state changes from **active** to **cleared**, however, the severity level of a cleared alarm does not change. By default, cleared alarms have green background color.

By default, cleared alarms automatically disappear from the Events window (with the exception of manually cleared alarms). Users can search for cleared alarms and display them in a separate tab of the Events window by using the Find Events dialog box (***Event / Find Events***). The Find Events dialog box also lets you find and display events, which trigger, modify and clear alarms (events are otherwise not displayed).

Tabs in Events Window

The Events window can contain one or more tabs. By default, the Events window contains only the **`Active Alarms`** tab, which displays all active alarms that exist on the objects included in the currently displayed user view. Additional tabs can be added to the Events window as described below. By default, cleared alarms automatically disappear from the list of alarms displayed in the `Active Alarms` tab in the Events window. Furthermore, by default, alarms that have been manually cleared by users remain listed in the `Active Alarms` tab. This behavior can be customized for each tab by means of the Table Options toggle commands.

Users can **add new tabs** to the Events window in several ways:

- By searching for alarms or events using the Find Events dialog box (***Event / Find***), which displays the search results in a new search tab ( ). Alarm lists in the search tabs are static, meaning that they do not change over time, as opposed to the dynamic alarm lists displayed in the Active Alarms tab, alarm history tabs, and in filter tabs. Furthermore, alarms displayed in the search tabs cannot be managed (acknowledged, unacknowledged, manually cleared, manually uncleared).

- By creating a filter in the Create Filter dialog box (***Event / Create Filter***), which displays filtered alarms in a new display filter tab ( ). A filtered list of alarms is dynamic, meaning that newly triggered alarms that match the filter conditions are automatically added to the list, and cleared alarms automatically disappear from the list (by default).
- By selecting one or more objects in the Maps window and choosing the ***Alarms / Active Alarms*** pop-up command. This command creates a new display filter tab in the Events window and displays a list of all active alarms on the selected objects in it. The list of alarms is dynamic, meaning that newly triggered alarms on the selected objects are automatically added to the list, and cleared alarms automatically disappear from the list (by default).
- By selecting one or more objects in the Maps window and choosing the ***Alarms / History*** pop-up command. This command creates a new history tab ( ) in the Events window, displaying a list of all alarms (active and cleared) that exist in the Net Inspector database for the selected object(s). The newly triggered alarms on the selected objects are automatically added to the list, while cleared alarms do not disappear from the list.
- By loading a filter using the ***Events / Load Filter*** command and selecting a filter either from the "My filters" repository (which contains all previously saved display and search filters), from the "Action filters" repository (which contains all action filters available in the Manage Action Filters dialog box) or from a file (filters that have been previously saved to files). When loading an action filter, a new action filter tab ( ) appears in the Events window, displaying all events that match the action filter conditions (useful for testing action filters).
- By importing a filter from a file using the ***Events / Import Filter from File*** command and selecting a filter file from disk on the computer running Net Inspector Client (only filters that have been previously saved to a file by using the ***Events / Export Filter to File*** command can be imported).

To **remove** an existing tab from the Events window, right-click its tab symbol at the bottom of the Events window and select the ***Close '[tab name]'*** pop-up command.

Net Inspector lets you save currently open display and action filter tabs with the ***Event / Save Filters Layout*** command. This command ensures that the existing display and action filter tabs are automatically restored next time the user opens the same user view.

Information about Alarms and Events

The left border of the Events window displays the number of alarms/events by their severity levels and the total number of alarms or events in the currently selected tab. Place the mouse pointer over alarm symbol, to see its description in a tooltip.

The right border of the Events window displays a toolbar with the following buttons:

Event Details – shows or hides the Event Details sub-window of the Events window.

Find Events – opens the Find Events dialog box, which lets you search for alarms and events.

Beep – enables or disables emitting audible signals (system default beep) upon triggering alarms.

Load Filter – opens the Load Filter dialog box, which lets you select a previously saved display or search filter and apply it to the currently active tab of the Events window. The Load Filter dialog box lets you select the filter either from the "My filters" repository (which contains all previously saved display and search filters), from the "Action filters" repository (which contains all action filters available in the Manage Action Filters dialog box) or from a file (filters that have been previously saved to files).

Save Filter – lets you save the display or search filter that is applied in the currently selected tab of the Events window for later use. The filter will be saved to the "My filters" repository, which is stored on the Net Inspector Server computer. This way, the same user can later load the filter. This button is disabled if no filter of search tab is selected in the Events window.

The central part of the Events window displays the contents of the currently selected tab. Every alarm or event in the Events window is displayed in a separate row. Details about the alarms/events are displayed in the following columns (you can display or hide individual columns by clicking their names in the column selector displayed on top of the vertical scrollbar of the Events window):

Cleared (checkbox)
By checking or unchecking this checkbox you can **manually clear** an active alarm or **manually unclear** an alarm, which has been previously manually cleared (this makes the alarm active again). The alarm is active when the Cleared checkbox is not checked. Events cannot be managed.

> **Note:** Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.

Acknowledged (checkbox)
By checking or unchecking this checkbox you can **acknowledge** or **unacknowledge** an alarm. If this checkbox is checked, the alarm is acknowledged. By acknowledging an alarm the user declares that he/she is aware of it. Events cannot be managed.

Severity
Displays the symbol and description of the alarm or event severity level.

Date/Time
Displays the date and time of triggering the alarm or event. The date and time format depends on the ***Date/Time format*** parameter setting in the User Preferences dialog box.

Source
Displays the name of the object (as shown on the map), which has triggered the alarm/event.

Comment
Displays the comment added to the alarm by a user. Each comment is automatically prefixed with the username of the user that has added the comment and the IP address of the Net Inspector Client from which the comment has been added.

Source Info
Displays additional information about the problem. For example, in case of a threshold event/alarm, it explains what threshold has been crossed (e.g., Physical memory).

Source Type
Displays the type of the object, which has triggered the alarm/event (e.g., “IP”).

Message
Displays a short description of the alarm or event (e.g. “Missing ATM connection data on remote CBx”).

Cause
Displays the cause of the alarm or event (e.g. “Line Card Problem”)

Ack. Date/Time
Displays the date and time of acknowledging or unacknowledging the alarm (whichever was last).

Ack/Cleared Info
Displays the username and IP address of the user who has acknowledged or cleared the alarm (whichever was last).

Cleared Date/Time
Displays the date and time of manually clearing or unclearing the alarm (whichever was last).

Event Type
Displays the type of the event/alarm (e.g. “Quality Of Service”, “Communication”, itd.)

Message ID
Displays the event/alarm message identifier number (e.g. “10002”).

Note 1: To sort alarms or events displayed in the Events window by a column, click the relevant column heading.

Note 2: To change the position of a column in the Events window, click the column heading and drag it to the desired position left or right from its current position.

Note 3: To enable or disable coloring rows with the colors assigned to alarm severity levels, check or uncheck the ***Use Colors*** option in the Events window column selector  .

Note 4: To view the details about the alarms or events, open the **Event Details** window by clicking the  button.

3.4.4 Pop-Up Menu

The Events window pop-up menu contains the following commands (some of them are not available in all tabs of the Events window):

- ***Go To Source***
  Selects the object in the Maps window, which is has triggered the selected alarm or event.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you annotate the selected alarms with a comment. Comments are displayed in the Comment column in the Events window.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of them. Acknowledged alarms are not shown in the alarm balloons. Events cannot be acknowledged/unacknowledged.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared. Events cannot be manually cleared/uncleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the currently active tab of the Events window.
- ***Find Events***
  Opens the Find Events dialog box, which lets you search for alarms and events. This command is available only in the Active Alarms tab in the Events window.
- ***Modify Filter***
  This command is used for modifying (e.g., refining) the conditions of an existing filter, i.e., either a display filter or a search filter. This command is available only if a find or filter tab is selected in the Events window. It opens the Find Events dialog box or the Create Filter dialog box (depending on which dialog box has been used initially) and lets you modify the existing filter.
- ***Save Filter***
  Lets you save the search or display filter that is applied in the currently selected tab of the Events window for later use. The filter will be saved to the “My filters” repository, which is stored on the Net Inspector Server computer. This way, the same user can later load the filter. This command is available only if a filter of find tab is selected in the Events window.
- ***Save Filters Layout***
  Lets you save all currently displayed display and action filter tabs in the Events window. This command ensures that the existing display and action filter tabs are automatically restored next time the user opens the same user view. This command is available only if a filter of find tab is selected in the Events window.

- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms or events displayed in the currently active tab of the Events window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Export Filter to File***
  Opens the **Export Filter** dialog box, which lets you save the filter that is applied in the currently selected tab of the Events window to a file stored on Net Inspector Client computer. This command is enabled only if a filter tab is selected in the Events window.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms or events.
- ***Save as Default Layout***
  Users with administrator access rights are authorized to use this command to save the layout of the currently active tab in the Events window as the default layout. Default layout stores the information about the display status (displayed/hidden), order and width of the columns displayed. Once the default layout is defined (saved), it automatically applies to all tabs you create in the Events window. The default layout is also automatically applied to all users when they connect to Net Inspector Server for the first time (until they modify their layout in the Events window). Therefore, this command is typically used by administrators when configuring the system (i.e., when defining default layouts of Net Inspector Client main windows etc.).
- ***Load Default Layout***
  Loads and applies the default layout in the current tab of the Events window. Default layout stores the information about the display status (displayed/hidden), order and width of the columns available in this window.
- ***Create Trap to Alarm Rule***
  Opens the New Trap-To-Alarm dialog box (first screen) and automatically inserts filter conditions that match the SNMP notification attributes of the selected alarm. This way, you can quickly create a trap-to-alarm rule from a received specific SNMP notification, that is, from a "Specific SNMP notification" alarm. This command is enabled only if you select an alarm that is based on a received enterprise specific SNMP Trap or Inform message (such alarms have "Specific SNMP notification" alarm message and "Warning" severity level).
- ***Table Options (cascading menu)***

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared automatically by Net Inspector remain listed in the current view (otherwise, they automatically disappear from the current list of alarms).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms).

3.4.5 Event Details Sub-Window

Purpose

Is a sub-window of the Events window used for viewing detailed information about the event or alarm selected in the Events window.

Opening

The  **Event Details** button in the Events window displays or hides the Event Details sub-window.

Description

The General Event Info Section

Select an alarm or event in the Events window and expand the **`General Event Info`** section in the Event Details sub-window to view alarm/event details. The following details are displayed under the **`General Event Info`** section:

Severity
Displays the symbol and description of the alarm or event severity level.

Date/Time
Displays the date and time of triggering the alarm or event. The date and time format depends on the ***Date/Time format*** parameter setting in the User Preferences dialog box.

Source
Displays the name of the object (as shown on the map), which has triggered the alarm/event. Subordinated to this item, the location of the source object is displayed, i.e., the full path to the containing map.

Comment
Displays the alarm comment added by a user. Each comment is automatically prefixed with the username of the user that has added the comment and the IP address of the Net Inspector Client from which the comment has been added.

Source Type
Displays the type of the object, which has triggered the alarm/event (e.g., “IP”).

Source Info
Displays additional information about the problem. For example, in case of a threshold event/alarm, it explains what threshold has been crossed (e.g., Physical memory).

Message
Displays a short description of the alarm/event (e.g. “Missing ATM connection data on remote CBx”).

Cause
Displays the cause of the alarm/event (e.g. “Line Card Problem”).

Event Type
Displays the type of the event/alarm (e.g. “Quality Of Service”, “Communication”, etc.).

Threshold
This property is shown only for threshold alarms/events and displays the crossed threshold value (e.g., “90.0026“).

(Un)acknowledged
Displays the date and time of (un)acknowledging the alarm and the username and IP address of the user who has acknowledged or unacknowledged the alarm (whichever was last).

Manually (un)cleared
Displays the date and time of manually (un)clearing the alarm and the username and IP address of the user who has manually cleared or uncleared the alarm (whichever was last).

The SNMP Notification Section

If the event/alarm has been generated from an SNMP Trap or Inform notification message, which is not included in the built-in notification-to-event mapping table (e.g., a generic SNMP Trap), the **`SNMP Notification: <name of notification>`** expandable section is displayed in the Event Details sub-window (besides the **`General Event Info`** section). This section provides details of the original SNMP Trap or Inform notification. Expand this section to view the following notification details:

Time stamp
Displays the time stamp value of the received SNMP notification. This value should correspond to the Trap sender’s sysUpTime.0 OID value at the time of sending the notification.

Message type
Displays the type of received SNMP notification message: Trap or Inform.

Protocol version
Displays the SNMP protocol version of the notification.

Transport
Displays the transport protocol used to convey the notification message.

Agent address, port
Displays the IP address of the agent that has sent the SNMP notification and the port from which the notification has been sent.

Manager address, port
Displays the IP address of the manager (Net Inspector Server) that has received the SNMP notification and the port on which the notification has been received.

Community
Displays the community name included in the SNMP notification message (except for SNMPv3 notifications).

SNMPv1 agent address (only for SNMPv1 Traps)
Displays the address of the agent associated with the received SNMPv1 Trap notification.

Enterprise (only for SNMPv1 Traps)
Displays the OID of the enterprise associated with the received SNMPv1 Trap notification.

Security parameters (only for SNMPv3 notifications)

Security user name
The name of the SNMPv3 USM user on behalf of which the notification was sent.

Security engine ID
The SNMP engine ID value used for the notification reception.

Context name
The name of the context in which the management information conveyed in SNMPv3 notification is accessed.

Context engine ID
The context engine ID value used for the notification reception.

Authentication protocol
The SNMPv3 USM authentication protocol (HMAC-MD5 or HMAC-SHA) used for authenticating the notification.

Privacy protocol
The SNMPv3 privacy protocol (CBC-DES or CFB-AES-128) used for encrypting the notification.

Bindings
Displays the variable bindings included into the received SNMP notification message.

3.4.6 Filtering and Finding Alarms and Events

The procedure of finding alarms and events is described in the Find Events dialog box section. The procedure of creating a filter for displaying only those alarms that match the filter conditions is described in the Create Filter dialog box section.

4 (SUB)MAP PROPERTIES WINDOW

4.1 Purpose

The Submap Properties window lets you view and configure the map name, icon and map propagation settings.

4.2 Opening

To open the Submap Properties window, select a (sub)map or an active user view icon in the Explorer window and choose the ***Properties*** pop-up command. Alternatively, select a (sub)map icon (Graphics view) or row (Details view) in the Maps window and choose the ***Properties*** pop-up command.

4.3 Description

The Submap Properties window provides the following controls:

Apply (button)
Applies all modifications.

Cancel (button)
Rejects all modifications.

Category (drop-down list)

- **General**
  Displays and lets you edit the name and icon of the selected map.

- **Propagation**
  Displays the Propagation view that lets you configure propagation settings for the selected map.

Status bar
Is at the bottom of the Submap Properties window and displays the name of the (sub)map and the propagated status of managed objects (if propagation is not disabled).

General View

The General view lets you view and set the name and icon for the selected map. It provides the following controls:

Name (input line)
Displays and lets you edit the name of the map.

Icon (drop-down list)
Displays the name of the icon used for representing the given map. By default, the Submap icon is used. To use a different icon for the given (sub)map, select it from the Icon drop-down list. The Icon drop-down list contains all icons currently available on Net Inspector Server computer, in the //Engine/workspace/icon folder. To add a new icon, copy two files of different sizes (16x16 pixels for the Details view and NxN pixels for the Graphics view) to the Net Inspector Server computer, in the //Engine/workspace/icon folder and restart Net Inspector Server. Both icon files must be saved in PNG file format and need to have the same name prefix, with the "_large" suffix for the larger icon file (e.g., "name.png" and "name_large.png").

Propagation View

The Propagation view lets you view and configure propagation settings for the selected map. It provides the following controls:

Map (input line)
Displays the name of the map for which the propagation settings are displayed.

Children (list)
Displays all objects and submaps on the selected map and lets you configure whether their status and alarms should be propagated up to the parent map or not. The Children list contains the following columns:

Name
Displays the name of the managed object or the submap.

Propagation
Displays the propagation state of the object or the submap ("propagating" or "not propagating").

Propagate (button)
Enables the alarm and status propagation for the object or submap selected in the Children list.

Don't Propagate (button)
Disables the alarm and status propagation for the object or submap selected in the Children list.

5 PROPERTIES WINDOW

5.1 Purpose

The Properties window is used for viewing various information about the selected managed object, like the general information about the managed object, alarms associated with the object, and settings used for polling the managed object. This window displays also the information collected through SNMP polling, i.e., the status and utilization of all network interfaces on the managed object and the system resources utilization (CPU load, memory usage, storage capacity utilization) for managed objects that provide this information via SNMP, as well as the information about the monitored network services. In other editions of Net Inspector (which incorporate the full-featured Performance Manager functionality), the corresponding interface, device performance statistics and monitored network services are displayed in the Performance Statistics window instead. Some of the properties, like the managed object name, address, description, etc. can also be configured in this window. Furthermore, the Properties window is used also for assigning SNMP and polling profiles to managed objects.

For more information about the (sub)map Properties window see the (Sub)map Properties Window section. For more information about the Properties windows of action and system objects, see the Action Object Properties Windows and the System Object Properties Windows section, respectively.

5.2 Opening

The Properties window can be opened by double-clicking the managed object icon in the Maps window or by right-clicking the managed object and selecting the ***Properties*** pop-up command.

5.3 Description

The Properties window contains several views, displaying different categories of parameters (e.g., General, Settings, System, …). Users can switch between views, by selecting the corresponding entries from the category drop-down list displayed in upper section of the Properties window. Note that some of the entries displayed in the category drop-down list are **static** (i.e., always displayed), while others are **dynamic**, i.e., they are displayed only if the managed object provides information from the respective category. If polling is performed by a Performance Manager polling engine (e.g., when using MG-SOFT Net Inspector WorkGroup, Enterprise or Carrier Edition), more comprehensive interface, device performance and services statistics are displayed also in the Performance Statistics window.

The following entries (and views) in the Properties window are static:

- General (object name, address, description, polling engine, list of active alarms, etc.)
- System (object type, class, location, vendor, OS, etc.)
- Settings (assigned polling and SNMP profiles, resynchronization configuration)
- Services (monitored TCP and UDP services) – present in LITE Edition only

If the managed object supports SNMP protocol, the following dynamic entries may appear in the category drop-down list of the Properties window (depending on the MIB modules supported by the SNMP agent on the given device and the polling profile assigned to the corresponding managed object):

- Interfaces (information about system network interfaces)
- Resources (information about the system resources)
- Storage (information about the system storage units)

General View

The General view contains the following controls:

Name (input line)
Displays and lets you edit the name of the managed object. By default, this is the host name of the managed object.

Type (input line)
Displays the type of the managed object (e.g., IP).

Address (input line)
Displays and lets you edit the IPv4 or IPv6 address or the host name of the managed object. This input line also provides a tooltip that displays the IP address of the managed object as well as the ***Copy IP Address*** pop-up command, which can be used for copying the IP address of the managed object to the clipboard.

Description (input line)
Displays and lets you edit a short description of the managed object. Net Inspector discovery operation enters the value of the sysDescr.0 object instance returned by the SNMP agent into this input line.

Polling engine (drop-down list)
Displays and lets you lets you select the polling engine used for polling the given device. This is especially useful if there are multiple Performance Manager polling engines deployed in your network. If you select a Performance Manager polling engine in this drop-down list, additional performance statistics about the given device will be available via the ***Show Performance Statistics*** command. If the **`Built-in engine`** option is selected, then the given device is polled by Net Inspector Server and no performance history data is available for it.

> **Note:** This drop-down list is enabled only when using Net Inspector Workgroup, Enterprise or Carrier Edition, which include the Performance Management functionalities.

NetFlow source (checkbox)
Sets the selected managed object as a NetFlow source device, i.e., a device that sends NetFlow v5 or v9 packets or sFlow v5 packets to Net Inspector (this must be first configured on the given device, e.g., a router, using the vendor-specific commands). Net Inspector WorkGroup and Enterprise Editions incorporate a NetFlow/sFlow collector and analyzer software module that receives NetFlow and sFlow packets from source devices and provide NetFlow/sFlow traffic statistics in the

Performance Manager Home Page window, NetFlow page. This option is disabled if the given device is polled by Net Inspector Server (`Built-in engine`).

Active alarms (frame)
Displays the object alarm summary (the total number of active alarms and number of active alarms broken down by severity levels) and a list of active alarms on the given object (same as in the Events window).

Pop-Up Menu
To display the pop menu, right-click one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Acknowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the list.
- ***Find Events***
  Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the given object.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms.

- ***Table Options*** (cascading menu)

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared (by Net Inspector) remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

System View

The System view contains the following controls:

Type (input line)
Displays the type of the managed object (e.g., IP).

Class (input line)
Displays the class of the managed object, which can be one of the following:

- Workstation
- Server
- Printer
- Switch
- Router
- Gateway
- Equipment
- Multiplexer
- Transport
- Database
- Firewall
- Transmitter
- Any

Tags (input line) and **Edit (button)**
Displays and lets you add a tag (user description) to the managed object. Objects can be searched by the value of their tags. To add or edit a tag, click the ***Edit*** button and enter a new tag into the dialog box that appears.

Location (input line)
The physical location of the managed object. Net Inspector discovery operation sets this value to the value of the sysLocation.0 object instance returned by the SNMP agent.

Vendor (input line)
The vendor of the managed object. Net Inspector discovery operation sets this value to the name of the enterprise responsible for the OID returned by the sysObjectID.0 object instance. The enterprise names displayed are taken from the list of private numbers as registered with IANA and stored on the Net Inspector Server (//Engine/data/nienterprise.txt).

OS (input line)
The operating system running on the managed object.

URL (input line) and **Open (button)**
The URL (uniform resource locator) address that provides additional information about the managed object. By default, this is the URL of the performance statistics page of the device.
To open the URL with the application associated with the specified protocol or URL, click the ***Open*** button next to this input line.

Icon (input line)
The name of the icon used for representing the managed object (as configured in the Server Settings dialog box, Object Types panel). To change the icon for a particular object only, enter the name of the icon file into this input line and click the ***Apply*** button. Icon files are stored on the Net Inspector Server computer in the //Engine/workspace/icon folder. Icons need to be saved in PNG image file format and two files of different sizes (16x16 pixels and NxN pixels (e.g., 32x32)) need to be present for every icon. Both icon files need to have the same name prefix, with the "_large" suffix for the larger icon file (e.g., "name.png" and "name_large.png").

Geographic coordinates (frame)
The geographic coordinates that specify the physical location of the managed object. The geographic coordinates are compatible with the Google™ Maps coordinates.

X (input line)
Specifies the geographic coordinate projected on the X-axis.

Y (input line)
Specifies the geographic coordinate projected on the Y-axis.

Z (input line)
Specifies the geographic coordinate projected on the Z-axis.

Settings View

The Settings view contains the following controls:

Polling profile (drop-down list)
This drop-down list displays the name of the polling profile assigned to the managed object. A polling profile contains a set of parameters for polling managed objects via ICMP and SNMP protocols. To assign a different polling profile to the managed object, select its name from the **Polling profile** drop-down list. Polling profiles are managed in the Server Settings dialog box, Profiles panel.

SNMP access profile (drop-down list)
This drop-down list displays the name of the SNMP access profile assigned to the managed object. An SNMP access profile contains a set of parameters for accessing SNMP agents on managed objects. To assign a different SNMP access profile to the

managed object, select its name from the drop-down list. SNMP access profiles are managed in the Server Settings dialog box, Profiles panel.

Manages Profiles (button)
Opens the Server Settings dialog box, Profiles panel.

Resynchronization (frame)
The settings in this frame control how the event resynchronization is performed (**Command**) with the given object and how Net Inspector monitors whether the events are synchronized or not for the given object (e.g., a third-party device). These settings are used for synchronizing the events with arbitrary third-party SNMP agents that support event resynchronization.

Command (input line)
Specifies the command that triggers the resynchronization of events with a third-party SNMP agent. The syntax of this command is as follows:

a) `SNMPSET <oid> <syntax> <value>`

or

b) `CMD <command>`

Add a) SNMP Set request is sent to the given SNMP agent, where:

`<oid>` is the OID to be set with the SNMP Set request

`<syntax>` is the SNMP syntax of the OID to be set, i.e., it can be one of the following:

```
integer
counter
gauge
counter64
timeticks
octet
opaque
ipaddress
oid
```

`<value>` is the value to be set.

Add b) Command is executed (on Net Inspector Server computer), where:

`<command>` is the command (including optional switches and parameters) to be executed to trigger event resynchronization with the given SNMP agent (managed object).

Enterprise OID (input line)
Specifies the enterprise OID associated with the SNMP notification (i.e., the value of the `Enterprise` field in SNMPv1 Trap messages or the value of the `snmpTrapEnterprise.0` variable binding in SNMPv2 and SNMPv3 Trap and Inform messages). Each SNMP notification message that reports an event on the

managed object must contain the specified enterprise OID in order for it to be accepted by Net Inspector as event.

Trap count binding (input line)
Specifies which variable binding in the variable bindings list (e.g., binding nr. 3 or 4 or 5…) of the SNMP notification message reports the current event count (i.e., the number of events on the given managed object). Net Inspector Server checks the continuity of this counter in every received SNMP notification message reporting events to determine if its list of events is synchronized with the list of events maintained internally by the managed object. If a difference in the trap count value is detected, Net Inspector executes the above configured resynchronization command.

Services View

The Services view is displayed **only in the LITE Edition** of Net Inspector. In other editions of Net Inspector, the services statistics are displayed in the Performance Statistics window.

The Services view lets you scan the well-known ports on the device for supported TCP and UDP network services. These services include HTTP, HTTPS, FTP, DNS, SMTP, IMAP, IMAPS, POP3, SSH, Telnet, NNTP, NNTPS, SIP, H.323, LDAP, LDAPS, IPP, LPD, MsSQL, MySQL and Oracle service. The Services view lets you configure which of the detected network services will be monitored on the given device. Furthermore, in this view, you can configure to monitor supported services on non-standard ports, as well as configure and monitor custom, user-defined services. Once configured, the Services view displays the status of monitored services (i.e., whether the services are accessible or not).

> **Note:** Services will be monitored only if services monitoring is enabled in the polling profile assigned to the given managed object. How frequently the information displayed in this view is updated depends on the polling interval (Poll every X seconds) set in the polling profile.

The Services view contains the following controls.

The Services list contains information about network services in the following columns:

Name
Displays the name of the service.

Status
Displays the service status, which can be one of the following:

Unmanaged	-	monitoring is disabled
Indeterminate	-	monitoring is enabled and the first query is in progress (immediately after enabling service monitoring)
Normal	-	monitoring is enabled and the service is accessible
Critical	-	monitoring is enabled and the service is not accessible

Port
Displays the port number on which the service listens to for incoming connections.

Protocol
Displays the transport protocol used by the service (TCP or UDP).

Scan (button)
Starts scanning well-known ports on the device for supported TCP and UDP services. Detected services are added to the Services list. To enable monitoring a detected service, check the checkbox in front of its name in the Services list and click the ***Apply*** button in the Properties window toolbar.
This button is disabled while the scan operation is in progress.

Add (button)
Opens the New Service dialog box, which lets you manually add a service to the Services list. This is useful, for example, if a service does not listen on the standard port, or if you want to monitor a user-defined TCP or UDP service. To enable monitoring a manually added service, check the checkbox in front of the services name in the Services list and click the ***Apply*** button in the Properties window toolbar.

Edit (button)
Opens the Edit Service dialog box, which lets you edit service properties.

Remove (button)
Removes the selected service from the list and stops monitoring the service (if monitoring was enabled).

Details (button)
Opens the Service Properties dialog box, which lets you view service properties. This dialog has the same appearance as the Edit Service dialog box, with a difference that all properties are displayed read-only here.

New/Edit Service dialog box

The New Service dialog box and Edit Service dialog box let you add a new network service and edit the properties of an existing network service.

To open the New Service dialog box, click the ***Add*** button in the Services view of the managed object Properties window. To open the Edit Service dialog box, click the ***Edit*** button in the Services view of the managed object Properties window.

The New/Edit Service dialog box provides the following controls:

Monitoring (checkbox)
If this checkbox is checked, the service monitoring is enabled.

Name
Name of the service.

Type
Service type, i.e., HTTP, HTTPS, FTP, DNS, SMTP, IMAP, IMAPS, POP3, SSH, Telnet, NNTP, NNTPS, SIP, H.323, LDAP, LDAPS, IPP, LPD, MsSQL, MySQL, or Oracle.

Port
Port number on which the service listens to.

Protocol
Transport protocol used by the service (TCP or UDP)

Username
Username for connecting to service (if supported and required).

Password
Password for connecting to service (if supported and required).

Service protocol data (frame)

ASCII / Binary (radio buttons)
Specifies whether the service data is transmitted in ASCII or binary format.

Expect on connect (input line and **button)**
Specifies the string that must be returned by the service when a TCP connection to it is established (e.g., `220` for SMTP service). Click the button next to this input line to display the Set Value dialog box, which lets you configure the expected value using an operator (none/is/contains) and value (string). If the "contains" operator is selected, you can also specify the start and end character numbers in the returned data that must contain the specified string.

Send/Response (list)
Lets you configure the send-response values for querying a custom (user-defined) service. If he binary option is selected, you need to configure the send-response values in hexadecimal notation, where individual octets are separated by a dot (e.g., 6F.70.65.6E). To add a send-response value pair to the list, click the **Add** button in the right section of the dialog box. This adds a new line to the Send/Response list and lets you edit its send-response values.

Send/Response section contains the following components:

Send message (column)
Lets you configure the value that will be sent by Net Inspector to query the custom service. The value is specified either in ASCII (plain text) or in binary (hexadecimal notation), depending on the corresponding setting above.

Expected response (column)
Lets you configure the value that must be returned by the custom service when the given message is sent to it. The value is specified either in ASCII (plain text) or in binary (hexadecimal notation), depending on the corresponding setting above.

Add (button)
Adds a new line to the Send/Response list and lets you edit its values.

Remove (button)
Removes the selected line from the Send/Response list.

OK (button)
Applies all modifications and closes the dialog box.

Cancel (button)
Discards all modifications and closes the dialog box.

Interfaces View

The Interfaces view is displayed only if the SNMP agent on the managed object returns information provided by the MIB-II interfaces group of objects.

> **Note:** How frequently the information displayed in this view is updated depends on the polling interval set in the polling profile assigned to the given managed object.

By default, the Interfaces view lists all network interfaces on the managed object and displays the following columns:

Interface
Displays the name of the interface as reported by the SNMP agent.

Status
Displays the status of the interface as reported by the SNMP agent.

In Util
Displays the inbound utilization rate of the interface (as reported by the SNMP agent).

Out Util
Displays the outbound utilization rate of the interface (as reported by the SNMP agent).

Additional information about interfaces (in additional columns) can be displayed in this view by selecting entries from the column selector  displayed above the vertical scrollbar of this view. For the meaning of these columns, please see the description of columnar objects in the ifTable (RFC1213-MIB).

Details (button)
Opens the Details dialog box, displaying detailed information about the selected interface.

Resources View

The Resources view is displayed only if the SNMP agent on the managed object supports the HOST-RESOURCES-MIB module and provides this MIB information via SNMP.

> **Note:** How frequently the information displayed in this view is updated depends on the polling interval set in the polling profile assigned to the given managed object.

The Resources view displays the following information:

Info (frame)
This frame displays information about the available memory, used memory, number of processes and users on the system, as reported by the SNMP agent. Besides, the memory usage (in %) is displayed in a linear gauge chart.

Processor (frame)
Displays the CPU load (in %) for all processors in the system (as reported by the SNMP agent).

Storage View

The Storage view is displayed only if the SNMP agent on the managed object supports the HOST-RESOURCES-MIB module and provides this MIB information via SNMP.

> **Note:** How frequently the information displayed in this view is updated depends on the polling interval set in the polling profile assigned to the given managed object.

The Storage view provides the following information and controls:

Hide removable storages (checkbox)
If this checkbox is checked, the information about removable storage units (e.g., floppy drives, optical drives, etc.) is not displayed.

Storages (frame)
Displays all data storage units on the system (e.g., disk partition, virtual memory, physical memory, etc.), capacities of these storage units and their current usage. Usage of storage units (in %) is depicted also in 3-D pie charts in the right section of the view.

Buttons

Enable - Start Polling (button)
Starts polling the object.

Disable - Stop Polling (button)
Stops polling the object.

Apply (button)
Applies all modifications.

Cancel (button)
Rejects all modifications.

Resolve Device Address (button)
Forces resolving the device name to IP address at user request. This is useful in environments with dynamic IP addresses in order to manually refresh the device IP address in Net Inspector (e.g., after it has been changed by a DHCP server). Note that this function is executed automatically anytime the monitoring of an object is (re)enabled.

Category (drop-down list)
Displays the currently selected view (e.g., General, Settings, System, …) and lets you switch between views in the Properties window. For more information on views (categories of parameters), see the Description section.

Ping (button)
Opens the Ping and Traceroute Console window and queries the managed object by means of ICMP Echo request(s). The "ping" results are displayed in the Ping and Traceroute Console window.

MIB Browser (button)
Opens the MIB Browser window and queries the managed object by means of an SNMP GetNext request. The results are displayed in the Results panel of the MIB Browser window.

Status bar

The status bar is displayed at the bottom of the Properties window and provides information about the following object properties (from left to right):

- The icon and name of the managed object,
- The node ID of the managed object,
- The object ID of the managed object,
- The current status of the managed object.

6 ACTION OBJECT PROPERTIES WINDOWS

The action objects represent specific actions that are performed by Net Inspector Server when events occur. Actions are used for notifying users of events (e.g., via e-mail) and for fixing specific network problems reported by events in an automated manner (e.g. by running a program/script that performs the appropriate operation).

Authorized users can place action objects onto maps, configure action object properties, and monitor the action object functioning in the same way as this can be done for the managed objects.

Although being primarily used for notifying users about alarms on managed objects, action objects themselves trigger alarms when they fail to perform the designated action (e.g., send an e–mail). Furthermore, the status of the action object changes if any critical fault occurs while executing the action.

Note 1: Actions are carried out on events, not on alarms. This means that for a single alarm, two or more actions can be carried out by the action objects. More specifically, if no filters are applied, the action will be executed when the event that raises a particular alarm occurs, and when the event that clears this alarm occurs. In addition, the actions are carried out also when users manage the alarm (acknowledge, unacknowledge, manually clear, manually unclear), as this also triggers events.

Note 2: It is important to note that **action objects function globally**, i.e., by default, they perform actions for all objects included in the system, irrespective of the user views. For example, if you add an action object (e.g., Mail object) to a user view, it will carry out the designated action (e.g., send e-mail) not only when events associated with the objects included in the currently active user view are triggered, but also when events on any other object registered with Net Inspector are triggered. To limit the functionality of action objects to perform actions only for a particular subgroup of objects (e.g., to objects included in the given user view), administrators should configure appropriate action filters and apply them to action objects.

Note 3: At least one action filter must be applied to each action object. If no filter is applied, the action object will fail to perform its function. Filters are configured in the Manage Action Filters dialog box and can be applied to action objects in their respective Properties windows (Filters view), as described in the following sections.

The properties of action objects can be viewed and configured in their respective Properties windows. This section describes the Properties windows of action objects.

6.1 Mail Properties Window

6.1.1 Purpose

The Mail Properties window is used for viewing and configuring parameters of the given mail object. These parameters are used by Net Inspector Server to send e-mails

through a SMTP server in order to notify users about events. The Mail Properties window also displays alarms triggered by the given mail object itself.

6.1.2 Opening

The Mail Properties window can be opened by double-clicking the mail object icon in the Maps window or by right-clicking the mail object and selecting the ***Properties*** pop-up command.

6.1.3 Description

A mail object represents a particular Net Inspector e-mail sending mechanism that connects to the specified SMTP mail server and sends e-mails containing event descriptions to specified recipients through the mail server. The mail object itself triggers events and alarms if the connection with the SMTP server is lost, or if the e-mail sending operation fails for some other reason. In addition, the status of the mail object changes if any critical problem in e-mail sending occurs.

Mail objects function globally, meaning that they send e-mails not only when events on the objects included in the currently active user view occur, but also when events on any other object registered with Net Inspector occur. By configuring and applying action filters, one can restrict the e-mail sending functionality of a mail object in various ways. For example, you can setup a filter that will allow sending e-mails only for events associated with particular objects or only for events of a particular severity level, etc. Action filters are configured in the Manage Action Filters dialog box and applied to mail object in the Filters view of the Mail Properties window.

The Mail Properties window contains several views, displaying different categories of parameters (e.g., General, Settings, Message, …). Users can switch between the views, by selecting the corresponding entries from the category drop-down list displayed in upper section of the Mail Properties window.

General View

The General view contains the following controls:

Name (input line)
Displays the name of the action object.

Type (input line)
Displays the type of the action object.

Description (input line)
Displays a short description of the action object.

Active alarms (frame)
Displays a summary and a list of active alarms associated with the object. Summary displays the total number of active alarms and the number of active alarms broken down by severity levels. The list of alarms is displayed in the same manner as in the Events window.

The Mail action object triggers the following events and alarms:

MessageID	Severity	Message
10004	Critical	Invalid address or DNS error
10040	Critical	Invalid filter
10041	Critical	Extension process is not running
10044	Major	Sending messages is temporarily disabled due to full buffer
14001	Major	Failed to send message

All alarms listed above except the last one change the status of the Mail object (the status will match the alarm severity level).

Pop-Up Menu

To display the pop menu, right-click one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the list.
- ***Find Events***
  Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the given object.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the Mail Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms.

- ***Table Options*** (cascading menu)

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared (by Net Inspector) remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

Settings View

The Settings view contains the following controls:

Sender (frame)

Name (input line)
Lets you specify the name of the e-mail sender (e.g., the name of the e-mail account holder.

E-mail (input line)
Specifies the sender's e-mail address.

Reply-to (input line)
Specifies the reply-to e-mail address.

Organization (input line)
Specifies the name of the sender's organization.

Recipients (frame)

To/Cc (field with multiple input lines)
Lets you select the ***To*** or ***Cc*** (carbon copy) option from the ***To/Cc*** drop-down button and specify the e-mail address of the recipient. Pres the ***Enter*** or ***Tab*** key to go to the next line and repeat the procedure for another e-mail recipient.

Server (frame)

Mail server (SMTP) (input line)
The name or IP address of the SMTP mail server used for sending outgoing e-mails.

Configure (button)
Opens the Server Settings dialog box that lets you view and modify the following parameters:

- **Server**
  The name or IP address of the SMTP mail server used for sending e-mails.

- **Timeout**
  The timeout value (in seconds) for connecting to the SMTP server.

- **Port**
  The TCP port on which the SMTP server listens to for incoming connections (the default SMTP port number is 25. For secure SMTP connections over SSL or TLS, the default port numbers are 465 and 587, respectively).

Authentication (frame)
Lets you configure the AUTH LOGIN SMTP server authentication parameters:

- **Use name and password (checkbox)**
  If this checkbox is checked, the AUTH LOGIN SMTP authentication mechanism is enabled and you should specify the corresponding username and password in the input lines below. You should enable this option only if the (E)SMTP server specified in the ***Server*** input line above supports the AUTH LOGIN authentication mechanism.
  - **Username**
    The username for AUTH LOGIN authentication at SMTP server.
  - **Password**
    The password for AUTH LOGIN authentication at SMTP server.
- **TLS (checkbox)**
  If this checkbox is checked, the TLS transport protocol is used for securing the communication with the (E)SMTP server. You should enable this option only if the (E)SMTP server specified in the ***Server*** input line above supports it.

> **Note:** If this option is disabled (Linux version), please refer to the TROUBLE_SHOOTING.TXT document that installs with the software for instructions on how to enable it.

Merging (frame)

Merge maximum X events within time interval of Y s
Specifies up to how many events (X) triggered within a specified interval (Y) will be included into one e-mail message. This option can be useful for reducing the number of e-mail messages sent.

Delay e-mailing active alarms (delay is between 1 and 2 merge intervals)
If this option is enabled, Net Inspector Server checks the age of every alarm-raising event and e-mails it only if it is older than the merge interval (Y) set above and if no corresponding clear event exists (meaning the alarm is still active). If the alarm-raising event is younger than the merge interval (Y), it will be e-mailed in the next merge interval. If the corresponding event that clears the alarm is triggered in the meanwhile, both raise and clear events are ignored (not e-mailed). This option is used for e-mailing alarms that are active for at least a specific amount of time (between 1 and 2 merge intervals).

Message View

The Message view contains the following controls:

Message (frame)

Subject (input line)
Lets you specify the contents of the e-mail subject section by combining arbitrary text with **reserved words**, which let you include desired information about events into the e-mail subject. All reserved words start with the "$" character. The reserved words are replaced with the actual event attributes when the e-mail is sent, e.g., the "$SEVERITY" reserved word is replaced with the severity level of the event (e.g., "Critical"). To view all available reserved words click the ***Browse*** (**…**) button next to the ***Subject*** input line to open the Reserved Words dialog box, listing available reserved words and their descriptions. To add a reserved word to the ***Subject*** input line, select it in the Reserved Words list and click the ***Insert*** button. You can also combine regular text with reserved words (e.g., "Event severity level: $SEVERITY")

Body (input area)
Lets you specify the contents of the e-mail message body section.

You can specify the contents of the e-mail body section by combining arbitrary text with **reserved words**, which let you include desired information about events into the e-mail body. To view all available reserved words click the ***Insert*** (**…**) button at the bottom of the Mail Properties dialog box to open the Reserved Words dialog box, which lists available reserved words and their descriptions. To add a reserved word to the e-mail body, select it in the Reserved Words list and click the ***Insert*** button.

Alternatively, you can load and use one of the built-in e-mail body templates by clicking the ***Load template*** button and selecting the desired template from the Select Template dialog box that appears. The Select Template dialog box consists of two panels. The upper panel displays the names of the e-mail body templates and the lower panel shows the contents of the template selected in the upper panel. Choose the desired template in the upper panel and click the ***Select*** button to add the selected template to the e-mail body and close the Select Template dialog box. The contents of the selected template appears in the Body input area of the Mail Properties dialog box. You can then use the template as it is, or edit it to adjust it to your preferences.

Send as HTML (checkbox)
Enables or disables sending e-mails in HTML format.

Load template (button)
Opens the Select Template dialog box, which lets you select e-mail body templates.

Insert (Button)
Opens the Reserved Words dialog box, which lets you add reserved words to the e-mail body.

Description of Reserved Words

a) The following reserved words are available for all events:

$SEVERITY	Event severity level (e.g., critical, major,…)
$SEVERITY_ID	Event severity ID number (2=normal, 4=informational, 8=warning, 16=minor, 32=major, 64=critical)
$SOURCE_ID	ID number of event source (e.g., 65595)
$SOURCE_NAME	Name of event source (e.g., MyServer)
$SOURCE_INFO	Additional information about the source of event (e.g., Physical Memory)
$SOURCE_TYPE	Type of source (e.g., IP)
$MESSAGE	Event message (e.g., Threshold value for storage usage exceeded)
$MESSAGE_ID	Event message ID number (e.g., 11007)
$CAUSE	Event cause (e.g., Threshold Crossed)
$CAUSE_ID	Event cause number (e.g., 549)
$EVENT_TYPE	Event type (e.g., Equipment)
$EVENT_TYPE_ID	Event type ID number (e.g., 5)
$DATE_TIME	Date and time of event (e.g., Thu 19 Oct 2006 01:50:28 PM CEST)
$THRESHOLD	Threshold value in case of a threshold event (e.g., 86.744)

b) The following “notification” reserved words are available for events generated from received SNMP Trap and Inform notifications that are not included in the built-in notification-to-event mapping table (see also the SNMP notification section of Event Details sub-window):

$NOTIFICATION	Identity (name) of SNMP notification
$TIME_STAMP	Notification’s time stamp value
$AGENT_ADDRESS	Address of notification sender
$V1AGENT_ADDRESS	SNMPv1 agent address (from SNMPv1 Trap)
$PROTOCOL	SNMP protocol version of notification
$ENTERPRISE	Enterprise associated with notification
$COMMUNITY	SNMPv1/v2c community string
$TRANSPORT	Notification’s transport protocol
$PORT	UDP port of notification receiver
$VBCOUNT	Total number of variable bindings in notification
$VB(E)	Log E bindings. E can be individual bindings from the variable bindings list (1,3,19), ranges of bindings (3-6), or both (1,3-6,19).
$VB_VALUE(N)	Log the value part of the N-th binding.
$VBALL	Log all bindings
$SEC_USER_NAME	SNMPv3 security user name
$SEC_AUTH_PROTOCOL	SNMPv3 authentication protocol
$SEC_PRIV_PROTOCOL	SNMPv3 privacy protocol
$SEC_CONTEXT	SNMPv3 context name

c) The following “for-each” loop reserved words are available:

$FOR_EACH_BEGIN	Starts the for-each loop
$FOR_EACH_END	Ends the for-each loop

Every reserved word inside the for-each loop (i.e., between the $FOR_EACH_BEGIN and $FOR_EACH_END reserved words) is expanded repeatedly for each event that is merged and sent in a message.

d) The following reserved words are available for a conditional notification block:

```
$IF_SNMP_NOTIFICATION_BEGIN    Starts the SNMP notification block
$IF_SNMP_NOTIFICATION_END      Ends the SNMP notification block
```

Any reserved word (and regular text) can be put into the conditional notification block (i.e., between the $IF_SNMP_NOTIFICATION_BEGIN and $IF_SNMP_NOTIFICATION_END reserved words). The conditional notification block is executed (i.e., the reserved words are expanded and the regular text is copied to the output) only for those events, which originate from SNMP notifications that are not included in the built-in notification-to-event mapping table. For every other event, the block is not executed and no output is generated. The notification block can also be placed inside the for-each loop.

Filters View

The Filters view contains the following controls:

Available filters (frame)

Enabled (checkbox)
If this checkbox is checked, the corresponding filter is enabled (applied), meaning that only events that match the filter conditions will be included into outgoing e-mails sent by the given mail object.

Filter (list)
Displays the names of available filters.

Manage Action Filters (button)
Opens the Manage Action Filters dialog box.

Statistics View

The Statistics view provides the following controls (all input lines are read-only):

Events processed (input line)
Displays the total number of processed events since enabling the object or last resetting the statistics.

Successful (input line)
Displays the number of successfully processed events since enabling the object or last resetting the statistics.

Last successful (input line)
Displays the date and time of the last successfully processed event (since enabling the object or last resetting the statistics).

Failed (input line)
Displays the number of unsuccessfully processed events since enabling the object or last resetting the statistics.

Last failed (input line)
Displays the date and time of the last unsuccessfully processed event (since enabling the object or last resetting the statistics).

Reset statistics (button)
Resets (clears) the statistics for the given action object. Disabling and re-enabling the object does not reset the statistics.

Buttons

Enable (button)
Activates the action operation (e-mail sending) and starts monitoring its functioning.

Disable (button)
Dectivates the action operation (e-mail sending) and stops monitoring its functioning.

Apply (button)
Applies all modifications.

Cancel (button)
Rejects all modifications.

Category (drop-down list)
Displays the currently selected view (e.g., General, Settings, …) and lets you switch between the views. For more information on views (categories of parameters), see the Description section.

Test (button)
Tries to execute the action to check if everything is configured properly.

Status bar

The status bar is displayed at the bottom of the Mail Properties window and provides information about the following object properties (from left to right):

- The icon and name of the action object,
- The object ID of the action object,
- The current status of the action object.

6.2 SMS Properties Window

6.2.1 Purpose

The SMS Properties window is used for viewing and configuring parameters of the given SMS action object. These parameters are used by Net Inspector Server to send SMS (Short Message Service) text messages through a modem in order to notify users about Net Inspector events. Such a modem device must be connected to a serial port of the PC running Net Inspector Server. The SMS Properties window also displays alarms triggered by the given SMS object.

6.2.2 Opening

The SMS Properties window can be opened by double-clicking the SMS object icon in the Maps window or by right-clicking the SMS object and selecting the ***Properties*** pop-up command.

6.2.3 Description

An SMS object represents a particular Net Inspector SMS sending mechanism, i.e., a mechanism that sends SMS messages containing event information to the specified phone numbers through a specific (GSM or regular) modem connected to a serial port of the PC running Net Inspector Server (SMS messages are relayed to the recipients by the corresponding telecommunications services provider). The SMS object itself triggers events and alarms if communication with the modem is unsuccessful, or if the SMS sending operation fails for some other reason. In addition, the status of the SMS object changes if any critical problem in SMS message sending occurs.

As other action objects, SMS objects function globally, meaning that they send SMS messages when an event on any object registered with Net Inspector occurs, not only when events on the objects included in the same user view occur. By configuring and applying action filters, one can restrict the message sending functionality of an SMS object in various ways. For example, you can setup a filter that will allow sending SMS messages only on events associated with particular objects or only on events of a particular severity level, etc. Action filters are configured in the Manage Action Filters dialog box and applied to SMS object in the Filters view of the SMS Properties window.

The SMS Properties window contains several views, displaying different categories of parameters (e.g., General, Settings, etc.). Users can switch between the views, by selecting the corresponding entries from the category drop-down list displayed in upper section of the SMS Properties window.

General View

The General view contains the following controls:

Name (input line)
Displays the name of the action object.

Type (input line)
Displays the type of the action object (SMS).

Description (input line)
Displays a short description of the action object.

Active alarms (frame)
Displays a summary and a list of active alarms associated with the object. Summary displays the total number of active alarms and the number of active alarms broken down by severity levels. The list of alarms is displayed in the same manner as in the Events window.

The SMS action object triggers the following events and alarms:

MessageID	Severity	Message
10040	Critical	Invalid filter
10041	Critical	Extension process is not running
10042	Critical	Invalid settings
10043	Critical	Modem timeout
10044	Major	Sending messages is temporarily disabled due to full buffer
14001	Critical	Failed to send message

All alarms listed above change the status of the SMS object (the status will match the alarm severity level).

Pop-Up Menu
To display the pop menu, right-click one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).

- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the list.
- ***Find Events***
  Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the given object.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the SMS Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms.
- ***Table Options*** (cascading menu)

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared (by Net Inspector) remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

Settings View

The Settings view contains the following controls:

Recipient number (input line)

Displays and lets you enter the phone number of the SMS message recipient. The phone number must include the international country code, the area code or mobile network code (without the leading zero), and the actual mobile phone number. Do **not** prefix the number with the international direct-dial prefix (which is 00 in most countries (011 in North America) and sometimes substituted with the plus (+) sign).

For example, to send SMS messages to the mobile phone number (041) 222-222 in Slovenia, you should enter the following into the Recipient number input line:

```
38641222222
```

…where the "386" is the international country code for Slovenia, "41" is the mobile network code, and the "222222" is the mobile phone number.

Message (frame and input area)

Lets you specify the contents of the SMS messages. You can specify the contents of the SMS message by combining regular text with **reserved words**, which allow you to include desired details of events into SMS messages. All reserved words start with the "$" character. The reserved words are replaced with the actual event attributes when the SMS message is sent, e.g., the "$SEVERITY" reserved word is replaced with the event severity level description (e.g., "Critical"). To view all reserved words, click the ***Insert reserved words*** button at the bottom of this frame to open the Reserved Words dialog box, which lists all available reserved words and their descriptions. To add a reserved word to the Message input area, select it in the Reserved Words list and click the ***Insert*** button.

By default, the Message input area contains a pre-configured expression, which can be freely edited.

Send method (frame)

The radio buttons below let you select the desired message sending method, as follows:

Through GSM modem (radio button)
Sends SMS messages through a GSM modem (e.g., a GSM modem built into a GSM mobile phone) connected to a serial port of the PC running Net Inspector Server. The GSM modem must be correctly pre-configured for sending SMS messages to the desired SMS center.

Direct link to SMS center (UCP) (radio button)
Connect directly to the specified SMS center via a modem and sends SMS messages by using the Universal Computer Protocol (UCP).

SMS center number (input line)
The telephone number of the SMS center that will receive SMS messages via the UCP protocol and relay them to the recipients.

Sender number (input line)
Optional telephone number of the SMS message sender.

Direct link to SMS center (TAP) (radio button)
Connect directly to the specified SMS center via a modem and sends SMS messages by using the Telocator Alphanumeric Protocol (TAP).

SMS center number (input line)
The telephone number of the SMS center that will receive SMS messages via the TAP protocol and relay them to the recipients.

Sender number (input line)
Optional telephone number of the SMS message sender.

Modem settings (frame)

Serial port (input line)
Specifies the serial port to which the mobile phone is connected.

Port settings (button)
Opens the Port Settings dialog box that lets you set communication parameters for the given serial port, as described below.

Port Settings dialog box:

Baud rate (drop-down list)
Lets you select the desired baud rate (speed in bits per second) for communication with the modem. If unsure, check with the device manufacturer for the best baud rate for your specific device. Some devices can only communicate at a particular speed, for example at 19200 bps.

Data bits (drop-down list)
Lets you select the number of data bits used for each character that is transmitted and received, e.g., 8.

Parity (drop-down list)
Lets you select the parity setting, which controls the communication error checking, e.g., none.

Stop bits (drop-down list)
Lets you select the stop bits setting, e.g., 1.

OK (button)
Applies all modifications and closes the dialog box.

Cancel (button)
Discards all modifications and closes the dialog box.

Filters View

The Filters view contains the following controls:

Available filters (frame)

Enabled (checkbox)
If this checkbox is checked, the corresponding filter is enabled (applied), meaning that only alarms that match the filter conditions will be included into outgoing e-mails sent by the given mail object.

Filter (list)
Displays the names of available filters.

Manage Action Filters (button)
Opens the Manage Action Filters dialog box.

Statistics View

The Statistics view provides the following controls (all input lines are read-only):

Events processed (input line)
Displays the total number of processed events since enabling the object or last resetting the statistics.

Successful (input line)
Displays the number of successfully processed events since enabling the object or last resetting the statistics.

Last successful (input line)
Displays the date and time of the last successfully processed event (since enabling the object or last resetting the statistics).

Failed (input line)
Displays the number of unsuccessfully processed events since enabling the object or last resetting the statistics.

Last failed (input line)
Displays the date and time of the last unsuccessfully processed event (since enabling the object or last resetting the statistics).

Reset statistics (button)
Resets (clears) the statistics for the given action object. Disabling and re-enabling the object does not reset the statistics.

Buttons

Enable (button)
Activates the action operation (SMS sending) and starts monitoring its functioning.

Disable (button)
Dectivates the action operation (SMS sending) and stops monitoring its functioning.

Apply (button)
Applies all modifications.

Cancel (button)
Rejects all modifications.

Category (drop-down list)
Displays the currently selected view (e.g., General, Settings, …) and lets you switch between the views. For more information on views (categories of parameters), see the Description section.

Test (button)
Tries to execute the action to check if everything is configured properly.

Status bar

The status bar is displayed at the bottom of the SMS Properties window and provides information about the following object properties (from left to right):

- The icon and name of the action object,
- The object ID of the action object,
- The current status of the action object.

6.3 Command Properties Window

6.3.1 Purpose

The Command Properties window is used for viewing and configuring parameters of the given command object. These parameters are used by Net Inspector Server to launch a command when events occur. The Command Properties window also displays alarms triggered by the given command object itself.

6.3.2 Opening

The Command Properties window can be opened by double-clicking the command object icon in the Maps window or by right-clicking the command object and selecting the ***Properties*** pop-up command.

6.3.3 Description

A command object represents a Net Inspector mechanism that runs a specific command, program or script and optionally passes desired event attributes as command line arguments to it. The command object itself triggers events and alarms if the command execution fails for some reason. In addition, the status of the command object changes if any critical faults in command execution process occur.

As other action objects, Command objects function globally, meaning that they run commands not only when events on the objects included in the currently active user view occur, but also when events on any other object registered with Net Inspector occur. By configuring and applying action filters, one can restrict the command execution functionality of a command object in various ways. For example, you can setup a filter that will allow running commands only for events associated with particular objects or only for events of a particular severity level, etc. Action filters are configured in the Manage Action Filters dialog box and applied in the Filters view of the Command Properties window.

The Command Properties window contains several views, displaying different categories of parameters (e.g., General, Settings,…). Users can switch between the views, by selecting the corresponding entries from the category drop-down list displayed in upper section of the Command Properties window.

General View

The General view contains the following controls:

Name (input line)
Displays the name of the action object.

Type (input line)
Displays the type of the action object.

Description (input line)
Displays a short description of the action object.

Active alarms (frame)
Displays the object alarm summary (the total number of active alarms and number of active alarms broken down by severity levels) and a list of active alarms on the given object (same as in the Events window).

The Command action object triggers the following events and alarms:

MessageID	Severity	Message
10040	Critical	Invalid filter
10044	Major	Sending messages is temporarily disabled due to full buffer
10045	Critical	Failed to run process
10050	Critical	Invalid command line

All alarms listed above change the status of the Mail object (the status will match the alarm severity level).

Pop-Up Menu
To display the pop menu, select one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons. Events cannot be acknowledged/unacknowledged.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared. Events cannot be manually cleared/uncleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the currently active tab of the Events window.
- ***Find Events***
  Opens the Find Events dialog box, which lets you search for alarms and events.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the

operating system's standard "Save As" dialog box. Note that only information provided by the columns which are displayed will be exported.

- ***Select All (Ctrl+A)***
  Selects all displayed alarms.
- ***Table Options*** (cascading menu)

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared automatically by Net Inspector remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

Settings View

The Settings view contains the following controls:

Command (frame)

Execute (input line)
Lets you specify the system command or the full path to the program or script (e.g., //Engine/bin/sendtrap.sh) that will be executed by Net Inspector Server when an event is triggered. You can use the ***Browse*** (**…**) button next to this input line to select the executable file from the disk. Note that the file must be stored on the computer running Net Inspector Server (in the "Engine" folder or its subfolders).

Arguments (input line)
Lets you specify program switches and parameters to be appended to the command specified above. To enable passing desired details about Net Inspector events to the invoked program, use the **reserved words**. All reserved words start with the "$" character. The reserved words are replaced with the event attributes when the command is executed, e.g., the "$SEVERITY" reserved word is replaced with the severity level of the event (e.g., "Critical"). To view all available reserved words click the ***Insert*** (**…**) button next to the ***Arguments*** input line to open the Reserved Words dialog box, listing available reserved words and their descriptions. To add a reserved word to the ***Arguments*** input line, select it in the Reserved Words list and click the ***Insert*** button. You can also combine regular text with the reserved words (e.g., "-s $SEVERITY").

Insert (Button)
Opens the Reserved Words dialog box, which lets you add reserved words to the ***Arguments*** input line.

Terminate command after X seconds (checkbox and input line)
If this checkbox is checked you can specify how long each command (process) started by this action object can run, before it will be forcedly terminated by Net Inspector Server (if it is still running). This option lets you terminate the processes, which do not end by themselves after they have performed the designated action.

Filters View

The Filters view contains the following controls:

Available filters (frame)

Enabled (checkbox)
If this checkbox is checked, the corresponding filter is enabled (applied), meaning that only events that match the conditions of the selected filter will trigger the command specified in the Settings view of the given command object.

Filter (list)
Displays the names of available filters.

Manage Action Filters (button)
Opens the Manage Action Filters dialog box.

Statistics View

The Statistics view provides the following controls (all input lines are read-only):

Events processed (input line)
Displays the total number of processed events since enabling the object or last resetting the statistics.

Successful (input line)
Displays the number of successfully processed events since enabling the object or last resetting the statistics.

Last successful (input line)
Displays the date and time of the last successfully processed event (since enabling the object or last resetting the statistics).

Failed (input line)
Displays the number of unsuccessfully processed events since enabling the object or last resetting the statistics.

Last failed (input line)
Displays the date and time of the last unsuccessfully processed event (since enabling the object or last resetting the statistics).

Reset statistics (button)
Resets (clears) the statistics for the given action object. Disabling and re-enabling the object does not reset the statistics.

Buttons

Enable (button)
Activates the command execution operation and starts monitoring its functioning.

Disable (button)
Dectivates the command execution operation and stops monitoring its functioning.

Apply (button)
Applies all modifications.

Cancel (button)
Rejects all modifications.

Category (drop-down list)
Displays the currently selected view (e.g., General, Settings, …) and lets you switch between the views. For more information on views (categories of parameters), see the Description section.

Test (button)
Tries to execute the action to check if everything is configured properly.

Status bar

The status bar is displayed at the bottom of the Command Properties window and provides information about the following object properties (from left to right):

- The icon and name of the action object,
- The object ID of the action object,
- The current status of the action object.

7 SYSTEM OBJECT PROPERTIES WINDOWS

The system objects represent different parts of Net Inspector system. System objects can be placed onto maps and monitored in the same way as managed objects. A system object triggers alarms when there is a problem with the Net Inspector subsystem it represents. Furthermore, the status of a system objects changes if any critical faults occur in the subsystems it represents. This principle lets you monitor the health of the system in the way that is consistent with the way of monitoring the network devices.

It is recommend that administrators add system objects to user view(s) that are assigned to administrators and group the system objects in a separate map (e.g., “System”) within those user view(s).

This section describes the Properties windows of system objects.

7.1 Event Properties Window

7.1.1 Purpose

The Event Properties window is used for viewing the configuration settings of the Net Inspector event storage subsystem and alarms associated with it.

7.1.2 Opening

The Event Properties window can be opened by double-clicking the event system object icon in the Maps window or by right-clicking the event object and selecting the ***Properties*** pop-up command.

7.1.3 Description

The event object represents Net Inspector event storage subsystem (module). This object triggers alarms when there are problems with the Net Inspector event storage module (e.g., if it cannot access the event storage database, etc.). Furthermore, the status of the event object changes if any critical faults associated with the event storage subsystem occur.

The Event Properties window contains two views that display different categories of parameters (i.e., General and Settings view). Users can switch between the views, by selecting the corresponding entries from the category drop-down list displayed in upper section of the Event Properties window.

General View

The General view contains the following controls:

Name (input line)
Displays the name of the system object.

Type (input line)
Displays the type of the system object.

Description (input line)
Displays a short description of the system object.

Active alarms (frame)
Displays a summary and a list of active alarms associated with the object. Summary displays the total number of active alarms and the number of active alarms broken down by severity levels. The list of alarms is displayed in the same manner as in the Events window.

The Event system object triggers the following events and alarms:

MessageID	Severity	Message
10210	Critical	Failed to connect to event storage database
10211	Critical	Failed to initialize event storage database
10212	Critical	Failed to access event storage database
10215	Critical	Failed to connect to event storage database for event queries
10216	Critical	Failed to initialize event storage database for event queries
10217	Critical	Failed to access event storage database for event queries
10220	Critical	Failed to connect to event storage database for event maintenance
10221	Critical	Failed to initialize event storage database for event maintenance
10222	Critical	Failed to access event storage database for event maintenance

Pop-Up Menu
To display the pop menu, right-click one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the list.

- ***Find Events***
  Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the given object.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms.
- ***Table Options*** (cascading menu)

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared (by Net Inspector) remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

Settings View

The Settings view provides the following read-only information (acquired from the `[event]` section of the Net Inspector Server initialization file):

DB type (input line)
The type of the event database used (Solid or ODBC).

DSN (input line)
The data source name of the ODBC database or the parameters (protocol, IP address and port) for accessing the Solid database (e.g., TCP 192.168.187.122 1320).

User (input line)
The username used for accessing the database.

Write (input line)
Controls what events are stored in the event database (alarms and events or only alarms).

Catalog (input line)
The catalog name for accessing the Solid database.

Execute maintenance (checkbox)
If this checkbox is checked, the database maintenance is enabled. Its operation depends on the option selected below.

- **When the number of events exceeds X (radio button and input line)**
  If this radio button is selected, the maintenance operation is executed when the total number of events/alarms in the database exceeds the configured value (X). For example, if X=10000 and the actual number of events/alarms in the database is 11500, the maintenance operation will delete the 1500 oldest events/alarms from the database.
- **When events are older than X days and Y hours (radio button and input lines)**
  If this radio button is selected, the maintenance operation is executed when the age of events/alarms in the database exceeds the configured value (X days and Y hours). All events/alarms older than X days and Y hours will be deleted from the database.

Status bar

The status bar is displayed at the bottom of the Properties window and provides information about the following object properties (from left to right):

- The icon and name of the system object,
- The object ID of the system object,
- The current status of the system object.

7.2 Configuration Properties Window

7.2.1 Purpose

The Configuration Properties window is used for viewing the settings of a particular Net Inspector configuration object and alarms associated with it.

7.2.2 Opening

The Configuration Properties window can be opened by double-clicking the configuration system object icon in the Maps window or by right-clicking the configuration object and selecting the ***Properties*** pop-up command.

7.2.3 Description

The configuration object represents a particular Net Inspector configuration (i.e., a `[configX]` section present in Net Inspector Server initialization file). Depending on the configuration of the system, more than one configuration object may exist in Net Inspector. A configuration object triggers alarms when there are problems with the corresponding Net Inspector configuration module (e.g., if it cannot connect to the configuration database, etc.). Furthermore, the status of a configuration object changes if any critical faults occur in the given configuration subsystem (module).

The Configuration Properties window contains two views that display different categories of parameters (i.e., General and Settings view). Users can switch between

the views, by selecting the corresponding entries from the category drop-down list displayed in upper section of the Configuration Properties window.

General View

The General view contains the following controls:

Name (input line)
Displays the name of the system object.

Type (input line)
Displays the type of the system object.

Description (input line)
Displays a short description of the system object.

Active alarms (frame)
Displays a summary and a list of active alarms associated with the object. Summary displays the total number of active alarms and the number of active alarms broken down by severity levels. The list of alarms is displayed in the same manner as in the Events window.

The Configuration system object triggers the following events and alarms:

MessageID	Severity	Message
10201	Critical	Failed to load configuration database
10202	Critical	Failed to connect to configuration database
10203	Critical	Failed to read from configuration database

Pop-Up Menu
To display the pop menu, right-click one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.

- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the list.
- ***Find Events***
  Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the given object.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms.
- ***Table Options*** (cascading menu)

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared (by Net Inspector) remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

Settings View

The Settings view provides information acquired from the corresponding `[config]` section of the Net Inspector Server initialization file. Each configuration section in the initialization file (e.g., `[config]`, `[config1]`, `[config2]`) is represented with one configuration object in Net Inspector, each carrying the name of the configuration section it represents.

The Settings view displays the following information in read-only mode:

Type (input line)
Specifies the type of the configuration database. Valid values are:

- **Configuration file** – the configuration information is stored in a text file

File (input line)
The path to the configuration file.

Status bar

The status bar is displayed at the bottom of the Properties window and provides information about the following object properties (from left to right):

- The icon and name of the system object,
- The object ID of the system object,
- The current status of the system object.

7.3 SNMP Notification Properties Window

7.3.1 Purpose

The SNMP Notification Properties window is used for viewing the configuration settings of the Net Inspector SNMP notification receiving subsystem and alarms associated with it.

7.3.2 Opening

The Mail Properties window can be opened by double-clicking the SNMP notification system object icon in the Maps window or by right-clicking the SNMP notification object and selecting the ***Properties*** pop-up command.

7.3.3 Description

The SNMP notification object represents Net Inspector SNMP notification receiving subsystem. This object triggers alarms when there are problems with the Net Inspector notification receiving module (e.g., if it cannot be initialized, etc.). Furthermore, the status of the SNMP notification object changes if any critical faults occur in the SNMP notification receiving subsystem.

The SNMP Notification Properties window contains two views that display different categories of parameters (i.e., General and Settings view). Users can switch between views, by selecting the corresponding entries from the category drop-down list displayed in upper section of the SNMP Notification Properties window.

General View

The General view contains the following controls:

Name (input line)
Displays the name of the system object.

Type (input line)
Displays the type of the system object.

Description (input line)
Displays a short description of the system object.

Active alarms (frame)
Displays a summary and a list of active alarms associated with the object. Summary displays the total number of active alarms and the number of active alarms broken down by severity levels. The list of alarms is displayed in the same manner as in the Events window.

The SNMP Notification system object triggers the following events and alarms:

MessageID	Severity	Message
10230	Critical	Failed to initialize SNMP sub-system to register SNMP notifications
10231	Major	Failed to register port for SNMP notifications
10232	Critical	Receiving SNMP notifications is temporarily disabled due to full buffer

Pop-Up Menu

To display the pop menu, right-click one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the list.
- ***Find Events***
  Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the given object.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms.
- ***Table Options*** (cascading menu)

  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared (by Net Inspector) remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

Settings View

The Settings view provides the following read-only information (acquired from the `[snmp notifications]` section of the Net Inspector Server initialization file):

Assign SNMP notifications to managed objects (checkbox)
Enables or disables assigning received SNMP Trap and Inform notification messages to corresponding managed objects. If this checkbox is checked, Net Inspector checks the address from which the SNMP notification has been sent and tries to assign the received SNMP notification to the managed object with the same address. If the managed object with the matching address exists in the Net inspector system, its name is displayed in the “Source” field of the alarm or event that has been created from the notification. If the managed object with the matching address does not exist in Net inspector, the SNMP notification is discarded and no event or alarm is created.

Ignore SNMP notifications from unknown sources (checkbox)
If this checkbox is checked, Net Inspector ignores the received SNMP notification messages that could not be assigned to managed objects because no matching objects exists in the system. Currently, all such SNMP notifications are discarded.

Filter notifications through SNMP profile (checkbox)
If this checkbox is checked, Net Inspector checks if the community name in the received SNMP notification message matches the Trap community name specified in the SNMP profile that is assigned to the source managed object. If the community names match, the SNMP notification is converted to alarm and assigned to the managed object. Otherwise, the SNMP notification is discarded. If this checkbox is not checked, Net Inspector does not check the community name of received SNMP notification messages.

Registered ports (list)

Port
Displays the port number on which Net inspector Server listens to for incoming SNMP notification messages.

Transport
Displays the transport protocol (e.g., IPv4/UDP) for each port.

Status
Displays the current status of each port (e.g., Ready).

Status bar

The status bar is displayed at the bottom of the Properties window and provides information about the following object properties (from left to right):

- The icon and name of the system object,
- The object ID of the system object,
- The current status of the system object.

7.4 Performance Manager Properties Window

7.4.1 Purpose

The Performance Manager Properties Window is used for monitoring and managing alarms associated with the Performance Manager subsystem (e.g., polling engines).

7.4.2 Opening

The Performance Manager Properties window can be opened by double-clicking the Performance Manager system object icon in the Maps window or by right-clicking the Performance Manager object and selecting the ***Properties*** pop-up command.

7.4.3 Description

The Performance manager object represents Performance Manager subsystem. This object triggers alarms if it cannot connect to configured polling engines. Furthermore, the status of the Performance Manager object changes to critical if any critical faults occur in the Performance Manager subsystem.

The Performance Manager polling engines can be configured in the Manage Polling Engines dialog box that can be opened by clicking the ***Manage Polling Engines*** button in this window.

General View

The General view contains the following controls:

Name (input line)
Displays the name of the system object.

Type (input line)
Displays the type of the system object.

Description (input line)
Displays a short description of the system object.

Manage Polling Engines (button)
Opens the Manage Polling Engines dialog box, where you can add, edit, or remove polling engines.

Active alarms (frame)
Displays a summary and a list of active alarms associated with the object. Summary displays the total number of active alarms and the number of active alarms broken down by severity levels. The list of alarms is displayed in the same manner as in the Events Window.

Pop-Up Menu

To display the pop menu, right-click one or more alarms in the list of active alarms. The pop-up menu contains the following commands:

- ***Details***
  Opens the Event Details window, which displays details of the selected alarm. This window display the same information as the Event Details sub-window.
- ***Add Comment***
  Opens the Add Comment dialog box that lets you enter or edit comment for the selected alarms. Comments are displayed in the Comment column.
- ***Akcnowledge***
  Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons.
- ***Unacknowledge***
  Unacknowledges the selected alarms (reverses the Acknowledge operation).
- ***Manually Clear***
  Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared.
- ***Manually Unclear***
  Unclears the selected alarms (reverses the Manually Clear operation).
- ***Remove Cleared Alarms***
  Removes all cleared alarms from the list.
- ***Find Events***
  Opens the Find Events dialog box and automatically inserts appropriate search conditions for finding events or alarms associated with the given object.
- ***Export***
  Opens the **Export Events** dialog box, which lets you export alarms currently displayed in the General view of the Properties window to a HTML or CSV (comma-separated value) file format. The Export Events dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information provided by the columns which are currently displayed will be exported.
- ***Select All (Ctrl+A)***
  Selects all displayed alarms.
- ***Table Options*** (cascading menu)
  - **Keep Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are cleared (by Net Inspector) remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).
  - **Keep Manually Cleared Alarms** (toggle menu option)
    If this option is checked, alarms that are manually cleared by the user remain listed in the current view (otherwise, they automatically disappear from the current list of alarms when cleared).

Status bar

The status bar is displayed at the bottom of the Performance Manager Properties window and provides information about the following object properties (from left to right):

- The icon and name of the system object,
- The object ID of the system object,
- The current status of the system object.

8 SERVER SETTINGS DIALOG BOX

Purpose

The Server Settings dialog box is used for configuring the server-specific settings, e.g., the users that can connect to the Net Inspector Server, the user views that they have access to, SNMP and polling profiles, trap to alarm rules, and other server-related settings.

Opening

To open this dialog box, select the ***Tools / Server Settings*** command.

> **Note:** Only users with administrator access rights are authorized to open this dialog box to view and change the server settings.

Description

The left section of the Server Settings dialog box contains a navigation tree with several entries. Depending on the entry selected in the navigation tree, different panel and buttons are displayed in the right section of the Server Settings dialog box. In addition, the following button is displayed at the bottom of the Server Settings dialog box:

Close (button)
Closes the dialog box.

8.1 User Views Panel

Purpose

The User Views panel is used for creating user views and for assigning user views to Net Inspector users.

Description

A user view is a particular view of objects registered with the Net Inspector system. User views differ in respect to what objects they display and how those objects are grouped and hierarchically structured. A user view can display either all managed, action and system objects registered with Net Inspector (e.g., an administrator user view), or any subgroup of those objects (e.g., user views assigned to users with limited access rights). An object can be displayed (included) in more than one user view. A user view displays only those alarms, which are associated with the objects included in that user view. See also section About Users, Access Rights and User Views.

Normally, at least one user view is assigned to each Net Inspector user. If only one user view is assigned to the user, this user view is automatically activated and displayed when the user logs on to Net Inspector Server (i.e., the Client main window displays only those objects that are included in the given user view). If more than one

user view is assigned to the user, the user can select the desired user view upon logging on to Net Inspector Server. When a connection between Net Inspector Server and Client is established, users can switch between the user views that are assigned to them.

For more information on creating user views in the design mode, please see the Net Inspector Client Design Mode section.

The complete procedure of creating a user view and assigning it to a user includes the following steps:

1. Creating a new user view in the Server Settings dialog box, User Views panel,
2. Assigning a user view to one or more users in the User Views panel,
3. Switching into the new user view, e.g., by using the User Views panel (a new, empty workspace is displayed),
4. Adding objects to the new user view from the Device Panel dialog box and organizing those objects into maps and submaps in the Maps and Explorer windows.

The User Views panel includes the following controls:

User Views (list)
Displays the list of existing user views.

Add (button)
Opens the New User view dialog box, which lets you create a new user view and assigned it to users.

Edit (button)
Opens the Edit User view dialog box.

Remove (button)
Deletes the selected user view.

Open (button)
Activates (switches into) the selected user view.

8.1.1 New User view dialog box

The New User View dialog box lets you create a new user view and assign it to existing Net Inspector users.

To open this dialog box, click the ***Add*** button in the User Views panel.

This dialog box provides the following controls:

Name (input line)
Lets you enter a name for the new user view.

Users (list)
Lists all existing users in Net Inspector system by displaying their user names, access rights, user groups and descriptions. If the checkbox in front of a user is checked, the user is allowed to access (open) the given user view (in other words, the user view is assigned to the user). You can control which users are allowed to access the user view by checking and unchecking the checkboxes displayed in front of users.

Assign All (button)
Grants access to the given user view to all users (assigns the user view to all users).

Unassign All (button)
Denies access to the given user view to all users.

Full propagation (checkbox)
Enables propagating the number of alarms from all the subordinated maps up to the root of the given user view (otherwise, the number of alarms is propagated only one hierarchical level higher). If enabled, this setting can reduce the application performance.

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

Pop-up Menu

To display the pop-up menu, select a user view in the User Views list and right-click it. This pop-up menu contains the following commands:

- **Assign**
  Entitles selected users to access the given user view (assigns the user view to users).
- **Unassign**
  Debars selected users from accessing the given user view ("unassigns" the user view from users).

8.1.2 Edit User View Dialog Box

The Edit User dialog boxes is used for viewing and controlling which users are allowed to access the given user view. The dialog box lists all existing users with checkboxes in front of them. Check the checkbox to add (assign) the user view to the user.

To open this dialog box, select an existing user view and click the ***Edit*** button in the User Views panel.

Name (input line)
Displays the name of the user view and lets you change it.

Users (list)
Lists all existing users in Net Inspector system by displaying their user names, access rights, user groups and descriptions. If the checkbox in front of a user is checked, the user is allowed to access (open) the given user view (in other words, the user view is assigned to the user). You can control which users are allowed to access the user view by checking and unchecking the checkboxes displayed in front of users.

Assign All (button)
Grants access to the given user view to all users (assigns the user view to all users).

Unassign All (button)
Denies access to the given user view to all users.

Full propagation (checkbox)
Enables propagating the number of alarms from all the subordinated maps up to the root of the given user view (otherwise, the number of alarms is propagated only one hierarchical level higher). If enabled, this setting can adversely affect the application performance.

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

Pop-up Menu

To display the pop-up menu, select a user view in the User Views list and right-click it. This pop-up menu contains the following commands:

- **Assign**
  Entitles selected users to access the given user view (assigns the user view to users).
- **Unassign**
  Debars selected users from accessing the given user view ("unassigns" the user view from users).

8.2 Users Panel

Purpose

The Users Panel is used for creating and managing user accounts for Net Inspector users.

Description

The Users Panel provides a graphical user interface for managing Net Inspector user accounts, i.e., creating, editing and deleting user accounts and their properties (usernames, passwords, access rights, user groups, descriptions). Once you create a new user account, you need to assign one or more user views to it in the User Views Panel

This panel provides the following controls:

User Accounts List

Displays the list of existing Net Inspector user accounts. It contains the following columns:

User
Displays the username of the user account.

Access
Displays the user account access rights (i.e., administrator, operator or guest).

Group
Displays the name of the user group the user account is a member of.

Description
Displays a short description of the user account.

Buttons

Add User
Opens the New User dialog box, which lets you create a new user account.

Remove User
Deletes the selected user account.

Edit User
Opens the Edit User dialog box, which lets you edit the attributes of the selected user account.

Change Password
Opens the Change Password dialog box that lets you change the password for the selected user account.

Pop-up Menu

To display the pop-up menu, select an account in the list of user accounts and right-click it. Pop-up menu contains the following commands:

- ***Change Description***
  Lets you change the textual description for selected user accounts.
- ***Change Group***
  Lets you change the name of the user group for selected user accounts.
- ***Change Access***
  Lets you change the access rights (i.e., administrator, operator or guest) for selected user accounts.

8.2.1 New User Dialog Box

The New User dialog box is used for creating a new user account. To open this dialog box, click the ***Add User*** button in the Users panel of the Server Settings dialog box.

This dialog box provides the following controls:

Username (input line)
Lets you enter/edit the name for the user account.

Encryption (drop-down list)
Lets you select the password encryption method (i.e., MD5 or None (i.e., plain text)).

Password (input line)
Lets you enter the password for the user account.

Retype (input line)
Lets you confirm the password by re-entering it.

User must change password at login (checkbox)
If this checkbox is checked, the user will be prompted to change his/her password the next time he/she logs on to Net Inspector Server.

Group (input line)
Lets you enter/edit the user group the given user account belongs to.

Access (radio buttons)
Lets you select the access rights for the given user (administrator, operator, guest).
Description (input line)
Lets you enter/edit the user account description.

OK (button)
Applies the changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

8.2.2 Edit User Dialog Box

The Edit User dialog box is used for editing an existing user account. To open this dialog box, select an item in the list of user accounts in the Users panel of the Server Settings dialog box and click the ***Edit User*** button.

This dialog box provides the following controls:

Username (input line)
Displays the name for the user account.

Encryption (drop-down list)
Displays the password encryption method (i.e., MD5 or None).

User must change password at login (checkbox)
Lets you check or uncheck the checkbox. If the checkbox is checked, the user will be prompted to change his/her password the next time he/she logs on to Net Inspector Server.

Group (input line)
Lets you enter/edit the user group the given user account belongs to.

Access (radio buttons)
Lets you select the access rights for the given user (administrator, operator, guest).

Description (input line)
Lets you enter/edit the user account description.

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

8.2.3 Change Password Dialog Box

This dialog box is used for changing the user account password.

To open this dialog box, select an item in the list of user accounts in the Users panel of the Server Settings dialog box and click the ***Change Password*** button. Only users with administrator access rights are able to do this.

Alternatively, to change your own password, open this dialog box by selecting the ***Tools / Change Password*** command. Any user can do this.

The Change Password dialog box provides the following controls:

Username (input line)
Displays the name for the user account.

Encryption (drop-down list)
Displays the current password encryption method and lets you change it (i.e., MD5 or None, i.e., plain text).

Old password (input line)
Lets you enter the old password. This input line is shown only to users with operator and guest access rights when changing their own passwords. Users with administrator

access rights can change the password of any user account without providing the old password.

New password (input line)
Lets you enter a new user account password.

Retype password (input line)
Lets you confirm the new password by re-entering it.

User must change password at login (checkbox)
Lets you check or uncheck the checkbox. If the checkbox is checked, the user will be prompted to change his/her password the next time he/she logs on to Net Inspector Server. This checkbox is not available if you open this dialog box by selecting the ***Tools / Change Password*** command.

Change (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

8.3 Profiles Panel

Purpose

The Profiles Panel is used for viewing and managing SNMP and polling profiles for monitoring managed objects.

Description

The **SNMP access profiles** contain parameters for accessing SNMP agents on managed objects (e.g., community names etc.) and for receiving SNMP Trap and Inform notification messages sent by those SNMP agents.

The **polling profiles** contain parameters for polling managed objects by means of ICMP and SNMP protocols (e.g., polling intervals, alarm thresholds, etc.).

Once a new SNMP access or polling profile is created, it can be manually assigned to managed objects in the managed object's Properties window. Profiles are assigned to managed objects also automatically by the discovery operation.

The Profiles Panel contains two tabs: the **Polling** tab and the **SNMP** tab.

8.3.1 Polling Tab

The Polling tab is used for managing polling profiles. It provides the following controls:

Polling (list)
Displays a list of existing polling profiles.

Add (button)
Opens the New Polling Profile dialog box, which lets you create and configure a new polling profile.

Edit (button)
Opens the Edit Polling Profile dialog box, which lets you view and modify the properties of the selected polling profile.

Remove (button)
Deletes the selected polling profile.

> **Note:** Polling profiles that are currently in use (i.e., assigned to one or more managed objects) cannot be deleted.

Show usage (button)
Opens a new tab in the Maps window (Details view) that displays all managed objects that have the selected polling profile assigned.

Export
Opens the Export Profile dialog box that lets you export the selected polling profile(s) to XML file(s) on disk.

Import
Opens the Import Profile dialog box that lets you import a polling profile from an XML file on disk.

New/Edit Polling Profile Dialog Box

The New Polling Profile and Edit Polling Profile dialog boxes provide the following controls:

Profile (frame)

Name (input line)
The name of the polling profile.

General (frame)

Check every (input line)
Specifies the interval in seconds for checking the managed object status and SNMP agent state (i.e., ICMP Echo and SNMP Ping polling).

Poll every (input line)
Specifies the interval for monitoring parameters that are collected through SNMP (like information about the interfaces, resources, storages, etc.) and the interval for monitoring network services (non-SNMP).

Resync Interval (2 input lines)
Specifies the interval in hours and minutes for automatic alarm resynchronization (if both input lines contain 0 (zero), the automatic alarm resynchronization is disabled).

Timeout (input line)
Specifies the timeout value in seconds. This value determines how long Net Inspector Server will wait for a response to each SNMP and ICMP Echo request it sends to the managed object, before generating a timeout interrupt signal.

Retries (input line)
Specifies the number of times the SNMP and ICMP Echo request will be retransmitted after the first timeout occurs.

Monitors (frame)

ICMP (checkbox)
If this checkbox is checked, the ICMP (ping) polling is enabled.

Services (checkbox)
If this checkbox is checked, the monitoring of network services is enabled. If monitoring of network services is enabled in Net Inspector WorkGroup and better editions, each managed object is automatically scanned for the supported network services and detected services are automatically monitored. In the LITE Edition of Net Inspector, you need to manually configure which network services will be monitored on each managed object in the Services view of the device Properties window.

SNMP (checkbox)
If this checkbox is checked, the SNMP polling is enabled. The checkboxes below determine what parameters besides the basic system information will be monitored via SNMP (e.g., network interfaces, resources, etc.). If any custom (user configured) polling group is configured and applied, it will appear in this list.

Override ping OID (checkbox, input line and drop-down list)
If this checkbox is checked, the default “SNMP Ping” parameters can be overridden. “SNMP Ping” operation is used to monitor the status (availability) of the SNMP agent on the managed device. By default, this is achieved by periodically querying it with SNMP GetNext requests containing the `0.0` OID (this mechanism retrieves the value of the first accessible OID that lexicographically follows the OID of `0.0`). If you would like some other OID to be queried or use the SNMP Get operation instead, check the **Override ping OID** checkbox and enter the desired OID into the ***OID*** input line and select the SNMP operation (GetNext or Get) to be used for retrieving this OID from the ***Operation*** drop-down list.

Network interfaces (checkbox and input line)
If this checkbox is checked, the network interfaces on the managed object will be monitored via SNMP. In the accompanying ***Poll every*** input line enter the polling interval (in seconds) for monitoring network interface statistics. Furthermore, you can set the threshold values for triggering and clearing alarms associated with interfaces.

If Net Inspector Server is used for polling, the collected information will be displayed in the Interfaces view of the managed object’s Properties window. If Performance Manager polling engine is polling the device, the collected information will be displayed in the Interfaces frame in the Device Statistics window.

Interface status (checkbox)
If this checkbox is checked, Net Inspector monitors the status network interfaces on the given managed object and triggers alarm if any of the interfaces goes down without being administratively disabled. The alarm is automatically cleared when the interface comes up again.

In utilization (checkbox and two input lines)
If this checkbox is checked, you can enter the interface inbound utilization threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the interface inbound utilization rate exceeds the configured value for triggering the alarm (first input line) and clear the alarm when the same utilization rate falls below the clear alarm threshold value (second input line).

Out utilization (checkbox and two input lines)
If this checkbox is checked, you can enter the interface outbound utilization threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the interface outbound utilization rate exceeds the configured value for triggering the alarm (first input line) and clear the alarm when the same utilization rate falls below the clear alarm threshold value (second input line).

In error rate (checkbox and two input lines)
If this checkbox is checked, you can enter the interface inbound error rate threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the interface inbound error rate exceeds the configured value for triggering the alarm (first input line) and clear the alarm when the error rate falls below the clear alarm threshold value (second input line).

Out error rate (checkbox and two input lines)
If this checkbox is checked, you can enter the interface outbound error rate threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the interface outbound error rate exceeds the configured value for triggering the alarm (first input line) and clear the alarm when the error rate falls below the clear alarm threshold value (second input line).

Host Resources (checkbox and input line)
If this checkbox is checked, the utilization of device system resources, like the memory usage, CPU load, etc., will be monitored via SNMP. In the accompanying ***Poll every*** input line enter the polling interval (in seconds) for monitoring host resources statistics. Furthermore, you can set the threshold values for triggering and clearing alarms associated with the system resource utilization.

If Net Inspector Server is used for polling, the collected information will be displayed in the Resources view of the managed object's Properties window. If Performance Manager polling engine is polling the device, the collected information will be displayed in the Memory and Processor Info frame and in the in the Storage Info frame in the Device Statistics window.

Memory usage (checkbox and two input lines)
If this checkbox is checked, you can enter the device memory usage threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the device memory usage exceeds the configured value for raising the alarm (first input line) and clear the alarm when the memory usage falls below the clear alarm threshold value (second input line).

CPU load (checkbox and two input lines)
If this checkbox is checked, you can enter the device CPU load threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the device CPU load exceeds the configured value for raising the alarm (first input line) and clear the alarm when the CPU load falls below the clear alarm threshold value (second input line).

Storage usage (checkbox and two input lines)
If this checkbox is checked, you can enter the device data storage unit usage threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the device storage usage exceeds the configured value for raising the alarm (first input line) and clear the alarm when the storage usage falls below the clear alarm threshold value (second input line).

Processes (checkbox and input line)
If this checkbox is checked, the processes running on devices supporting the HOST-RESOURCES-MIB module will be monitored via SNMP. The process information, i.e., process name, running status, process memory usage and process CPU usage, will be displayed only for the selected processes. Into the accompanying ***Poll every*** input line enter the polling interval (in seconds) for monitoring processes. Furthermore, you can set the threshold values for triggering and clearing alarms associated with the process status and resources consumption.

Collected information will be displayed in the **Processes** frame in the Device Statistics window.

Process status (checkbox)
If this checkbox is checked, Net Inspector monitors the status of processes on the given managed object and triggers alarm if any of the processes stop running. The alarm is automatically cleared when the process is running again.

Process CPU (checkbox and two input lines)
If this checkbox is checked, you can enter the processes CPU load threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the processes CPU load exceeds the configured value for raising the alarm (first input line) and clear the alarm when the CPU load falls below the clear alarm threshold value (second input line)

Process memory
If this checkbox is checked, you can enter the processes memory usage threshold values (in MB) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the processes memory usage exceeds the configured value for raising the alarm (first input line) and clear the alarm when the memory usage falls below the clear alarm threshold value (second input line).

IP SLA (checkbox and input line)

Note: This option is available only in the WorkGroup and Enterprise Edition of MG-SOFT Net Inspector application.

If this checkbox is checked, the IP SLA statistics related will be monitored on Cisco devices that are properly configured and provide this information via SNMP. Into the accompanying ***Poll every*** input line enter the polling interval (in seconds) for monitoring IP SLA statistics. Furthermore, you can set the threshold values for triggering and clearing alarms associated with the Cisco IP SLA metrics.

Collected information will be displayed in the **IP SLA** page in the Device Statistics window.

For more information on configuring IP SLA operations on Cisco devices, please consult the Cisco documentation

(e.g.: http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.html)

RTT measurement status (checkbox)
If this checkbox is checked, Net Inspector monitors the round trip time measurement status for all enabled IP SLA services on the given managed objects and triggers an alarm, if any enabled service is down. The alarm is automatically cleared when the service is up again.

Echo round trip time (checkbox and two input lines)
If this checkbox is checked, the ICMP echo round trip time threshold is enabled.
Enter the echo round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the echo round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

Path echo round trip time (checkbox and two input lines)
If this checkbox is checked, the full path echo round trip time threshold is enabled.
Enter the full path echo round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the full path echo round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

TCP connect round trip time (checkbox and two input lines)
If this checkbox is checked, the IP SLA TCP connect round trip time threshold is enabled.
Enter the TCP connect round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the TCP connect round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

HTTP round trip time (checkbox and two input lines)
If this checkbox is checked, the IP SLA HTTP round trip time threshold is enabled.
Enter the HTTP round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the HTTP round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

DNS round trip time (checkbox and two input lines)
If this checkbox is checked, the IP SLA DNS round trip time threshold is enabled.
Enter the DNS round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the DNS round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

DLSW round trip time (checkbox and two input lines)
If this checkbox is checked, the IP SLA DLSW (Data Link Switching Plus) round trip time threshold is enabled.
Enter the DLSW round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the DLSW round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

DHCP round trip time (checkbox and two input lines)
If this checkbox is checked, the IP SLA DHCP round trip time threshold is enabled.
Enter the DHCP round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the DHCP round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

FTP round trip time (checkbox and two input lines)
If this checkbox is checked, the IP SLA FTP round trip time threshold is enabled.
Enter the FTP round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the FTP round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

Jitter round trip time (checkbox and two input lines)
If this checkbox is checked, the IP SLA VoIP Jitter round trip time threshold is enabled.
Enter the Jitter round trip time threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the Jitter round trip time exceeds the configured value for raising the alarm (first input line) and clear the alarm when the round trip time falls below the clear alarm threshold value (second input line).

Cisco Jitter SD (checkbox and two input lines)
If this checkbox is checked, the VoIP source-to-destination jitter threshold is enabled.
Enter the source-to-destination jitter threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the source-to-destination jitter (as measured by the IP SLAs) exceeds the configured value for raising the alarm (first input line) and clear the alarm when the source-to-destination jitter falls below the clear alarm threshold value (second input line).

Cisco Jitter DS (checkbox and two input lines)
If this checkbox is checked, the VoIP destination-to-source jitter threshold is enabled.
Enter the destination-to-source jitter threshold values (in ms) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the destination-to-source jitter (as measured by the IP SLAs) exceeds the configured value for raising the alarm (first input line) and clear the alarm when the destination-to-source jitter falls below the clear alarm threshold value (second input line).

Cisco packet loss SD (checkbox and two input lines)
If this checkbox is checked, the VoIP source-to-destination packet loss threshold is enabled. This applies to one-way packet loss from source to destination router.
Enter the source-to-destination packet loss threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the source-to-destination packet loss (as measured by the IP SLAs) exceeds the configured value for raising the alarm (first input line) and clear the alarm when the source-to-destination packet loss falls below the clear alarm threshold value (second input line).

Cisco packet loss DS (checkbox and two input lines)
If this checkbox is checked, the VoIP destination-to-source packet loss threshold is enabled. This applies to one-way packet loss from destination to source router.
Enter the destination-to-source packet loss threshold values (in %) into the accompanying input lines. This way, Net Inspector will trigger an alarm when the destination-to-source packet loss (as measured by the IP SLAs) exceeds the configured value for raising the alarm (first input line) and clear the alarm when the destination-to-source packet loss falls below the clear alarm threshold value (second input line).

Cisco MOS (checkbox and two input lines)
If this checkbox is checked, the mean opinion score (MOS) threshold is enabled.
The estimated mean opinion score (MOS) is a numerical indication of the perceived quality of sound after compression and transmission. Cisco routers with enabled VoIP UDP jitter IP SLAs will calculate and express the estimated MOS value as a number in the range of 1 to 5, where 1 is the lowest audio quality, and 5 is the highest quality. A MOS value of zero indicates that MOS data is not available.

Enter the MOS threshold values into the accompanying input lines. This way, Net Inspector will trigger an alarm when the MOS (as measured by the IP SLAs) falls bellow the trigger alarm threshold value (first input line) and clear the alarm when it raises again above the clear alarm threshold value (second input line).

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

8.3.2 SNMP Tab

The SNMP tab is used for managing SNMP access profiles. It provides the following controls:

SNMP (list)
Displays a list of the existing SNMP access profiles.

Add (button)
Opens the New SNMP Access Profile dialog box, which lets you create and configure a new SNMP access profile.

Edit (button)
Opens the Edit SNMP Access Profile dialog box, which lets you view and modify parameters of the selected SNMP access profile.

Remove (button)
Deletes the selected SNMP access profile.

> **Note:** SNMP profiles that are currently in use (i.e., assigned to one or more managed objects) cannot be deleted.

Show usage (button)
Opens a new tab in the Maps window (Details view) that displays all managed objects that have the selected SNMP access profile assigned.

Export
Opens the Export Profile dialog box that lets you export the selected SNMP access profile(s) to an .xml file on disk.

Import
Opens the Import Profile dialog box that lets you import an SNMP access profile from an .xml file on disk.

New/Edit SNMP Access Profile dialog box

The New SNMP Access profile and Edit SNMP Access Profile dialog boxes provide the following controls:

Profile (frame)

Name (input line)
The name of the SNMP access profile.

Port (input line)
The UDP port on which SNMP agents on managed objects listen to for incoming SNMP requests.

SNMP version (frame and radio buttons)
The version of SNMP protocol used for querying SNMP agents on managed objects and for receiving SNMP Trap and Inform notification messages sent by those SNMP agents.

Settings (frame)
The SNMPv1 and SNMPv2c community name settings. This frame is disabled if SNMPv3 protocol is selected in the SNMP version frame.

Read community (input line)
The SNMP community name to be used with all SNMPv1 or SNMPv2c queries sent by Net Inspector.

Write community (input line)
The SNMP community name to be included into SNMPv1 or SNMPv2c Set requests sent by Net Inspector.

Trap community (input line)
The community name included in SNMPv1 Trap or SNMPv2c Trap or Inform messages sent by the SNMP agents on managed devices.

SNMPv3 Settings (frame)
The SNMPv3 security settings. This frame is disabled if SNMPv1 or SNMPv2c protocol is selected in the SNMP version frame.

Security user name (input line)
The name of the SNMPv3 USM user to be used for exchanging all SNMPv3 messages between Net Inspector and managed objects (including SNMPv3 Trap and Inform messages sent by the managed objects).

Context name (input line)
The name of the context in which the management information conveyed in SNMPv3 messages is accessed.

Authentication protocol (drop-down list) and **Change Password/Key (button)**
The drop-down list lets you select the SNMPv3 authentication protocol (HMAC-MD5 or HMAC-SHA) to be used for authenticating SNMPv3 messages sent on behalf of the given SNMPv3 user. The **Change Password/Key** button opens the Authentication Password or Key dialog box that lets you enter the authentication protocol password or key.

Privacy protocol (drop-down list) and **Change Password/Key (button)**
The drop-down list lets you select the SNMPv3 privacy protocol (CBC-DES or CFB-AES-128) to be used for encrypting SNMPv3 messages sent on behalf of the given SNMPv3 user. The **Change Password/Key** button opens the Privacy Password or Key dialog box that lets you enter the privacy protocol password or key.

Do not localize authentication and privacy keys (checkbox)
If this checkbox is checked, the software uses non-localized authentication and privacy keys.

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

Authentication Password or Key/Privacy Password or Key dialog box

The Authentication Password or Key and the Privacy Password or Key dialog boxes have the same appearance. The provide the following controls:

Enter password (radio button)
If this option is selected, you can specify the authentication or privacy security key by entering the password into the accompanying input lines. Net Inspector will compute the security key for the SNMPv3 authentication or privacy protocol from the given password according to the algorithm defined in the *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol* document (RFC 3414).

Password (input line)
Lets you enter the authentication or privacy password.

Retype (input line)
Lets you confirm the password by re-entering it.

Show typing (checkbox)
If this checkbox is checked, the entered password characters are displayed in the **Password** and **Retype** input lines instead of masking the passwords with bullet characters.

Enter key in hex notation directly (radio button)
If this option is selected, you can specify the authentication or privacy security key directly by entering it into the accompanying input lines in hexadecimal notation. In this case, the software does not employ the USM password-to-key algorithm. Instead, if the **Do not localize authentication or privacy keys** checkbox in the SNMPv3 Settings frame is not (!) checked, Net Inspector applies only the security key localization

algorithm to the entered security key and then uses the localized security key for communicating with the SNMPv3 agents. If that checkbox is checked, Net Inspector uses the security key exactly as it was entered.

Clear Key (button)
Clears all input lines for specifying the security key.

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

8.4 Action Filters Panel

Purpose

It is used for viewing and managing action filters. Action filters can be applied to action objects to restrict their functionality so that only events that match the filter conditions will carry out the given action.

Description

Users with administrator access rights can use Action Filters panel to create, edit and remove action filters. Once the action filter is created, it can be applied to action objects in the Filters view of the action objects' Properties window.

Action filters contain one or more filter conditions, which match the filter conditions available in the Create Filter dialog box.

The Manage Action Filters panel includes the following controls:

Filter (list)
Lists the names of existing action filters.

Add (button)
Opens the New Filter dialog box, which lets you create and configure a new action filter.

Edit (button)
Opens the Edit Filter dialog box, which lets you modify the selected action filter.

Remove (button)
Deletes the selected action filter. Note that filters that are currently in use by action objects cannot be deleted.

8.4.1 New/Edit Filter dialog box

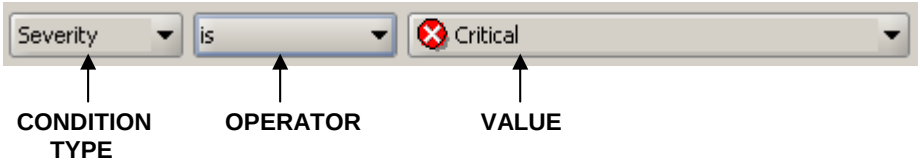
The New Filter dialog box contains and Edit Filter dialog box contain a toolbar that lets you create filter conditions and add them to the filter one-by-one, while the central section of the dialog box (Conditions panel) displays the entire filter consisting of filter conditions and relations between them. The Conditions panel displays a filter in form of a hierarchical tree, where filter conditions are connected with logical operators (AND, OR).

Action filter conditions can be specified by using the following controls in the New/Edit Filter dialog box:

Name (input line)

Specifies the name of the action filter.

New condition (toolbar)



This toolbar lets you create a filter condition by selecting the condition type, operator and value from the corresponding drop-down lists. Once the condition is configured, you can add it to the filter by clicking the ***Add*** button in the right section of the dialog box. Added conditions appear in the Conditions panel below the New condition toolbar.

Condition type (drop-down list)
Specifies the type of the condition. You can select among the following types of conditions:

- **Severity**
  Specifies the severity level of the event. If this condition type is selected, you can choose the event severity level from the ***Value*** drop-down list (e.g. "Critical", "Major", etc.).
- **Source**
  Uniquely identifies the object, which has triggered the event. This condition type lets you search for objects by their object IDs (note that different objects can have the same name, however, all objects have unique object IDs). If this type of condition is selected, click the (**…**) ***Browse*** button next to the ***Value*** field to open the **Select Source** dialog box. The **Select Source** dialog box displays two panels; the left panel contains the expandable map tree, while the panel on the right displays all objects included in the map that is selected in the left panel. The left panel also displays some properties of the listed objects, including their object IDs. To select a **Source** object (and thus its ID), click the relevant map in the left panel, choose the object on the right panel and click the ***Select*** button.
- **Source name**
  Specifies the name of the object (as displayed on the workspace), which has triggered the event. If this condition type is selected, you can enter the name of the object into the ***Value*** input line. Note, however, that two or more objects can have the same name. Use the **Source** condition type to uniquely specify the source in such case.
- **Source info**
  Specifies additional information about the problem, which has triggered the event (as displayed in the ***Source Info*** column in the Events window). If this condition type is selected, you can enter additional information about the object into the ***Value*** input line (e.g., "Processor:#1").
- **Source type**
  Specifies the type of the object, which has triggered the event. If this condition type is selected, you can choose the type of the object from the ***Value*** drop-down list (e.g. "IP", etc.).
- **Message**
  A short description of the event. If this condition type and the operator "is" or "is not" is selected, you can choose a message from the list of all messages in the ***Value*** drop-down list (e.g. "Device is down"). If this condition type and the operator

"contains" is selected, you can enter a text string (e.g., "Dev") into the ***Value*** input line to find all events whose message field contains the specified character(s).

- **Cause**
  Specifies the cause of the event. If this condition type is selected, you can choose a cause from the ***Value*** drop-down list (e.g. "Lan Error").
- **Type**
  Specifies the type of the event. If this condition type is selected, you can choose an event type from the ***Value*** drop-down list (e.g. "Communication").
- **Event State**
  Specifies the event state. If this condition type is selected, you can choose an event state from the ***Value*** drop-down list (e.g., "Acknowledged").
- **(Un)Acknowledge time**
  Specifies the (Un)Acknowledge time. If this condition type is selected, you can enter the (Un)Acknowledge time in the ***Value*** input line (e.g., May 31, 2011 9:23:50 AM)
- **(Un)Clear time**
  Specifies the (Un)Clear time. If this condition type is selected, you can enter the (Un)Clear time in the ***Value*** input line (e.g., May 31, 2011 9:23:50 AM)
- **Event State info**
  Specifies the Event state info. If this condition type is selected, you can enter the event state info in the ***Value*** input line (e.g., "Auto").

Operator

Lets you select the operator, e.g., "is", "is not", "contains", "is greater or equal", "is smaller or equal", etc. Available operators depend on type of the condition selected.

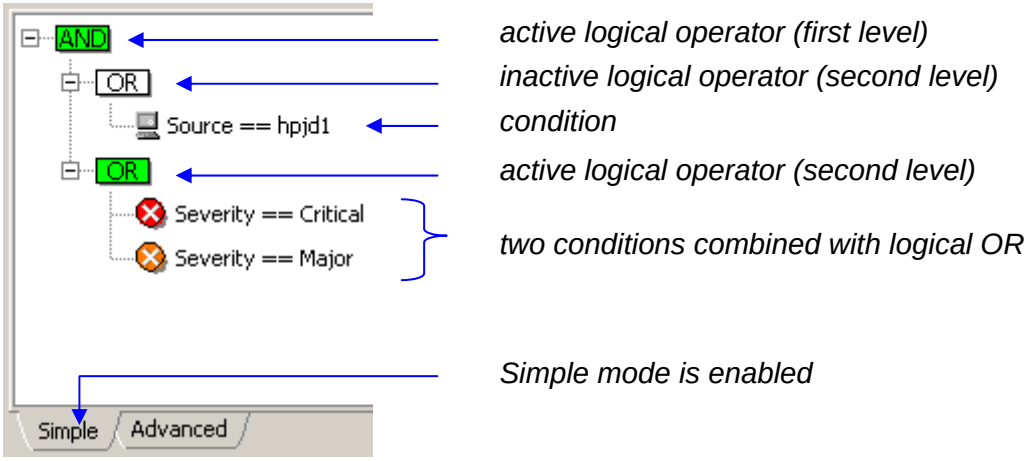
Value

Lets you enter or select the condition value. Available (and valid) values depend on the type of the condition selected.

Conditions (panel):

The **Conditions panel** displays and lets you re-configure existing filter conditions, and logical operators connecting them.

Example of the Conditions panel contents:



Expression equivalent to the filter displayed above would be:

Source=hpjd1 AND (Severity=Critical OR Severity=Major)

Meaning: Let through all events triggered by 'hpdj' object, whose severity levels are either Critical or Major

Simple and Advanced Mode

Conditions panel contains two tabs providing two modes of operation: Simple and Advanced.

The **Simple mode**, which is enabled by default, lets you create filters in a straightforward manner: you only add filter conditions to the Conditions panel and the program automatically groups conditions of the same type and connects them with logical OR operator, while conditions of a different type are connected with logical AND operator. For example, if you add two conditions of the same type (e.g., "severity=critical" and "severity=major"), they will be combined with the logical OR operator, meaning that the filter will let trough events that satisfy either one or the other condition (i.e., it will let trough all 'critical' events and all 'major' events). If you, on the other hand, add two conditions of different types (e.g., "severity=critical" and "message=device is down"), they are connected with the logical AND operator, meaning that the filter will let trough only those events that satisfy both conditions at the same time.

The Simple mode does not let you manipulate logical operators, it only lets you configure and add filter conditions to the filter. This mode also does not allow combining different types of filter conditions with the logical OR operator.

The **Advanced mode**, which can be enabled by clicking the Advanced tab in the Conditions panel, lets you create much more complex filters than the Simple mode, as it imposes no restrictions on grouping filter conditions or using logical operators.

In advanced mode, you can double-click any logical operator in the hierarchical filter tree and change it from AND to OR, or vice-versa. Furthermore, you can add new logical operators to the selected filter subtree by clicking the ***AND*** or ***OR*** buttons located in the right hand-side of the dialog box and then add new conditions as child items to those operators. This way, you can create complex filters that comprise more than two hierarchical levels, which the Simple mode of operation is restricted to.

Switching Between Modes

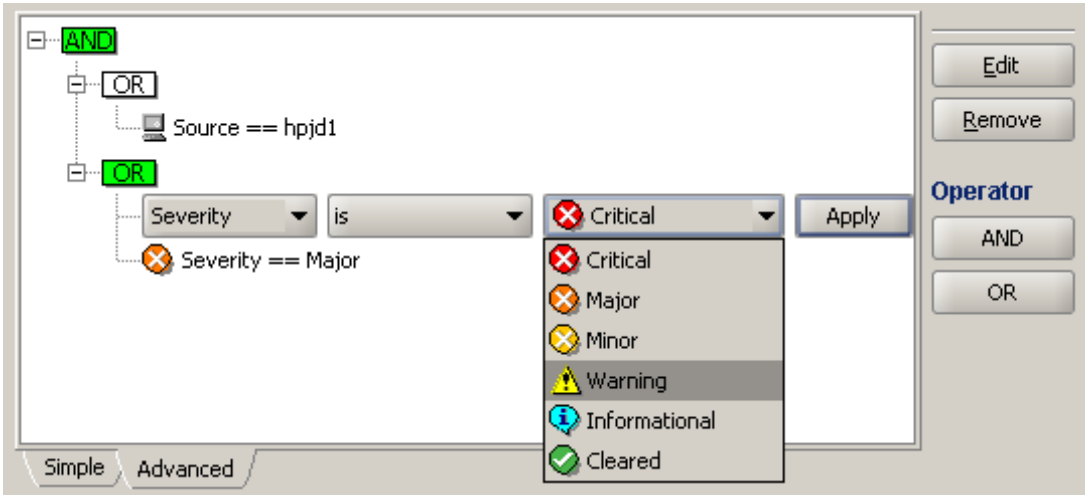
To select desired mode of operation, click the corresponding tab (Simple, Advanced) in the Conditions panel.

You can switch to another mode even while you are already creating a filter, and then continue creating it in another mode; however, with some restrictions. While you can always switch from Simple to Advanced mode, you cannot switch from Advanced to Simple mode if the filter you are currently creating does not match the simple filter scheme (max. two levels of logical operators: AND operator on the first level, OR operator(s) on the second level, conditions of the same type are grouped together under the same OR operator on the second level). In such case, you need to edit the filter to match the simple filter scheme or delete it.

Editing Conditions

To edit an existing condition, simply double-click it in the Conditions panel or select it and click the ***Edit*** button in the right section of the dialog box.

Example: Editing a filter condition (Advanced mode):



The selected condition will be displayed in editable form (see the picture above), where you can select new items from the drop-down lists or edit the value in the ***Value*** input line. For description of available condition types, operators and values, kindly refer to the New condition toolbar description. Click the ***Apply*** button in the Conditions panel to apply the changes after you finish editing the condition.

Note: The Simple mode does not lets you change the condition type when editing a condition in the Conditions panel.

To edit an existing logical operator (Advanced mode only), simply double-click it in the Conditions panel or select it and click the ***Edit*** button on the right hand-side of the dialog box. This displays the drop-down list from which you can select another logical operator.

Note: In the Conditions panel, green logical operators are active, while the white operators are inactive (see the picture above). Only active operators are in effect. A logical operator is active if it has at least two (directly or indirectly) subordinated conditions in the hierarchical filter tree.

Buttons:

- **Add**
  Adds the condition from the New condition toolbar to the Conditions panel. In Advanced mode the condition is added to the selected branch in the filter tree.
- **Edit**
  Lets you edit the selected condition or operator. Operators can be modified only in Advanced mode.
- **Remove**
  Removes the selected condition or operator (and all its subordinated objects) from the Conditions panel.

Operators

- **AND**
  Adds the logical AND operator to the selected filter branch. This button is enabled only in Advanced mode.
- **OR**
  Adds the logical OR operator to the selected filter branch. This button is enabled only in Advanced mode.

- **Import**
  Opens the Import dialog box, which lets you select a previously saved filter and import it into the New/Edit Filter dialog box (Conditions panel). The Import dialog box lets you select the filter either from the “My filters” repository (which contains all previously saved display and search filters), from the “Action filters” repository (which contains all action filters available in the Action Filter Panel) or from a file (filters that have been saved to a file in previous versions of Net Inspector).

- **OK**
  Applies all changes and closes the dialog box. The name of the filter is added to the Filter list in the Manage Action Filters dialog box (when creating a new filter).

- **Cancel**
  Discards all changes and closes the dialog box.

8.5 Polling Engines Panel

Purpose

The Polling Engines panel is used for viewing, adding, editing and removing Performance Manager polling engines.

Description

The Manage Polling Engines panel displays a list of existing Performance Manager polling engines and lets you add and configure additional polling engines for use with Net Inspector (Performance Manager polling engines must first be installed and configured on remote computers).

This view provides the following controls:

Polling engines (list)
Displays a list of existing Performance Manager polling engines (including their IP address), their status and the number of managed objects assigned to each polling engine.

Add (button)
Opens the New Polling Engine dialog box, which lets you add a new polling engine to the list. The added polling engine must first be installed on the remote computer. After adding a new polling engine to the system, you can assign it to one or more managed objects by selecting the objects in the Maps window and choosing the Tools/Change Performance Manager Polling Engine pop-up command.

Edit (button)
Opens the Edit Polling Engine dialog box, in which you can edit the settings of the selected polling engine.

Remove (button)
With this button, you can remove existing polling engines. After you have clicked the ***Remove*** button, a confirmation window appears and asks you if you really want to remove the selected polling engine.

New/Edit Polling Engine dialog box

The New Polling Engine and Edit Polling Engine dialog boxes have the same appearance and provide the following controls:

IP Address (input line)
The IP address of the computer running the polling engine you want to add/edit.

Name (input line)
The name (label) of the polling engine.

NetFlow Ports (frame)
Lets you add, edit and remove NetFlow / sFlow reception ports.

Ports (list)
Displays a list of configured UDP ports on which Net Inspector listens for incoming NetFlow and sFlow packets.

Add (button)
Adds a new line to the Ports list and lets you enter the port number into it.

Add default (button)
Adds the default NetFlow/sFlow port (9991) to the Ports list.

Remove (button)
Removes the selected port from the Ports list.

8.6 Trap to Alarm Rules Panel

Purpose

It is used for managing rules that control how enterprise specific SNMP Trap and SNMP Inform notifications sent by network devices map to Net Inspector alarms.

Opening

To open the Trap-To-Alarm Rules panel, select the ***Tools / Server Settings*** command and click on the ***Trap to Alarm Rules*** entry in the navigation tree.

Alternatively, you can create a trap-to-alarm rule by right-clicking an alarm that is based on a received enterprise specific SNMP Trap or Inform message in the Events window (such alarms have “Specific SNMP notification” alarm message and severity level of “Warning”), and selecting the ***Create Trap-To-Alarm Rule*** from the pop-up menu.

Description

Users with administrator access rights can use Trap-To-Alarm Rules panel to create, edit and remove rules that control how enterprise specific SNMP Trap and SNMP Inform notifications sent by network devices map to Net Inspector alarms. While the software automatically maps the “generic” SNMP notifications (coldStart, warmStart, linkDown, linkUp, etc.) to Net Inspector (ITU X.733) alarms, the rules for mapping enterprise specific SNMP notifications can be configured manually. This allows you to configure the alarm attributes (alarm message, severity level, alarm source information, etc.) to be displayed by Net Inspector when it receives a particular type of enterprise specific SNMP notification.

Note: If no trap-to-alarm mapping rules are configured, Net Inspector displays the same alarm message and severity level for all alarms based on received enterprise specific SNMP notifications, regardless of the type of notification and importance of the condition reported by the notification. Such alarms have “**Specific SNMP notification**” alarm message and severity level of “**Warning**”. To differentiate among such alarms, one needs to inspect the details of the original SNMP notification included in alarms, which can be viewed in the Event Details sub-window, under the “SNMP notification” section.

In general, whenever applicable, one should create two trap-to-alarm rules for each type of alarm condition, one that triggers the alarm and one that clears it. For example, if a device sends an SNMP Trap when the chassis temperature raises above the normal level and another SNMP Trap when the temperature drops back to normal, you should create two-trap-to alarm rules: one that will raise the alarm (set the alarm severity level to other than “Cleared”) and the other to clear the alarm (i.e., set its severity level to “Cleared”).

Each trap-to-alarm mapping rule consists of two parts, a **trap filter** part and an **alarm mapping** part. A trap filter contains one or more conditions that must be met in order for the SNMP notification to be controlled by the given rule and accordingly mapped to alarm. These conditions are attributes of the SNMP notification, e.g., enterprise specific OID, variable bindings, the version of the SNMP protocol used for conveying the notification, etc. Alarm mapping part, on the other hand, determines the attributes of the resulting alarm, i.e., the severity level, alarm message and source info of the alarm. The **`source info`** property can be configured to contain one or more attributes of the received SNMP notification by using “notification” reserved words. If specified, the source info value serves also as a condition for clearing the alarm, as described below.

Once you create a trap-to-alarm rule, it is automatically applied, meaning that from that moment on Net Inspector will map all newly received SNMP notifications that match the given trap filter to alarms according to the rule.

The Trap-To-Alarm Rules panel includes the following controls:

Rules List

Displays the list of existing trap-to-alarm rules. It contains the following columns:

Rule Name
Displays the names of existing trap-to-alarm rules.

Specific OID
Displays the OID that identifies the SNMP notification(s) to which the rule applies.

Alarm Severity
Displays the configured severity level of the alarm.

Alarm Message
Displays the configured alarm message.

Buttons

Add (button)
Opens the New Trap-To-Alarm dialog box, which lets you create and configure a new trap-to-alarm rule.

Edit (button)
Opens the Edit Trap-To-Alarm dialog box, which lets you modify the selected trap-to-alarm rule.

Duplicate (button)
Creates a copy of the selected trap-to-alarm rule. After creating a copy of an existing rule, you should edit the properties of the new rule. This option lets you quickly create new trap-to-alarm rules that are similar to existing (source) rules.

Remove (button)
Deletes the selected trap-to-alarm rule(s).

8.6.1 New/Edit Trap-To-Alarm Dialog Box

Purpose

The New Trap-To-Alarm dialog box and Edit Trap-To-Alarm dialog box let you create a new and edit an existing trap-to-alarm mapping rule in two steps. In the first step, you specify the condition(s) an SNMP notification has to meet to be controlled by the rule. In the second step, you specify the alarm severity level, alarm text message and, optionally, the source info property of the resulting alarm.

Opening

Click the ***Add*** button in the Trap-To-Alarm Rules panel to open the New Trap-To-Alarm dialog box.

Select an existing trap-to-alarm rule in the Trap-To-Alarm Rules panel and click the ***Edit*** button to open the Edit Trap-To-Alarm dialog box.

Alternatively, you can create a new trap-to-alarm rule by right-clicking an alarm that is based on a received enterprise specific SNMP Trap or Inform message in the Events window (such alarms have “Specific SNMP notification” alarm message and severity level of “Warning”), and selecting the ***Create Trap-To-Alarm Rule*** from the pop-up menu. This opens a New Trap-To-Alarm dialog box (first screen) and automatically inserts filter conditions that match the SNMP notification attributes of the selected alarm. This way, you can quickly create a trap-to-alarm rule from a received specific SNMP notification (i.e., “Specific SNMP notification” alarm). You can also edit the conditions to match your preferences before saving the new trap-to-alarm rule.

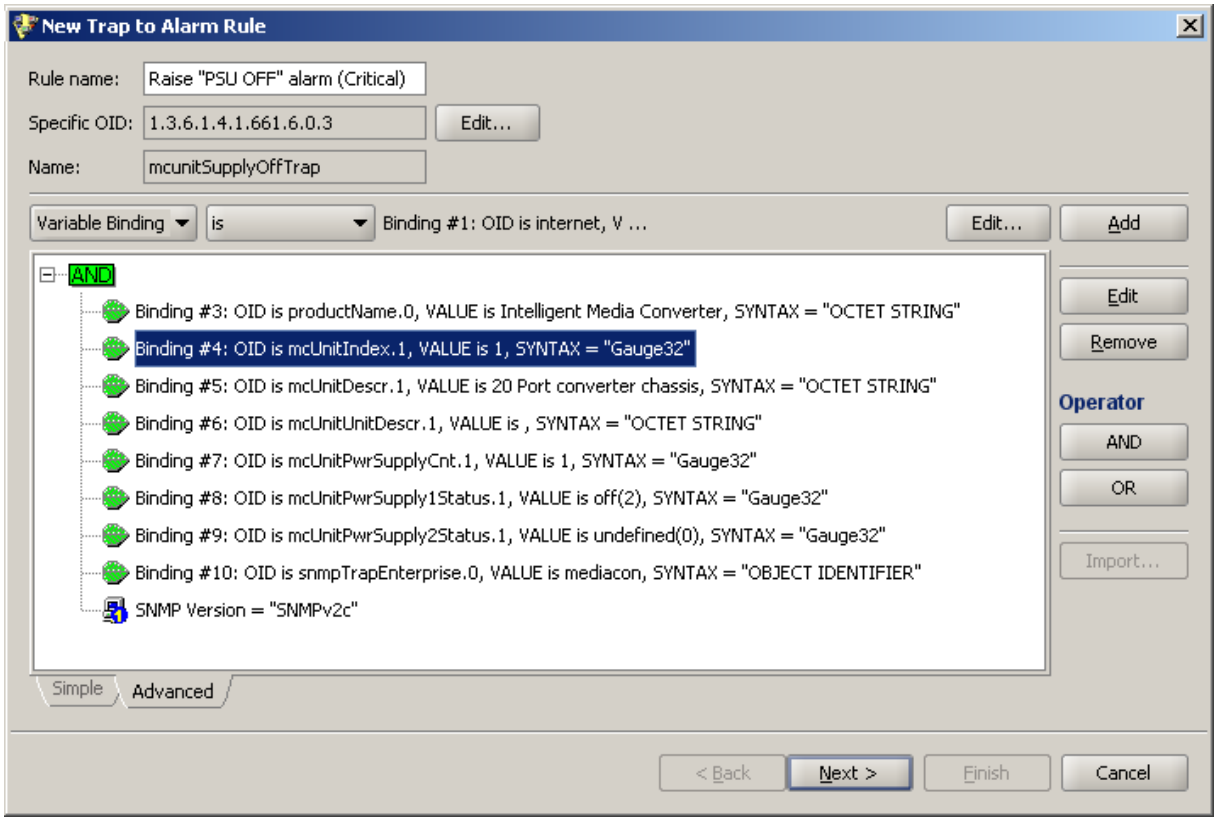
Description

The New Trap-To-Alarm dialog box and Edit Trap-To-Alarm dialog boxes let you create and edit a trap-to-alarm rule in a wizard-like fashion using two screens, as follows:

First Screen (Trap Filter Screen)

This screen is used for configuring a trap filter. A trap filter contains one or more conditions that must be met in order for an SNMP notification to be controlled by the given trap-to-alarm rule and accordingly mapped to alarm. These conditions are attributes of the SNMP notification, like the enterprise specific OID, variable bindings,

and the version of the SNMP protocol used for conveying the notification. The enterprise specific OID (specific OID), which identifies an SNMP notification, is the key condition that is checked first when Net Inspector receives an SNMP notification message. If the specific OID value of a received notification matches the one specified in the trap filter, the remaining conditions of the given trap-to-alarm rule are evaluated (compared to notification attributes). If the remaining conditions that are configured in this screen are satisfied, the notification is controlled by the given rule, meaning that it will either raise or clear an alarm. The latter depends on the alarm mapping properties (alarm severity, message, source info), which are configured in the second screen of the Trap-To-Alarm dialog box.



Example of Trap-To-Alarm dialog box, first screen

Trap filter conditions can be specified by using the following controls in the first screen of the New/Edit Trap-To-Alarm dialog box:

Rule Name (input line)
Specifies the name of the trap-to-alarm rule. It is recommended that you give a meaningful name to each rule (e.g., it should denote which SNMP notification it applies to, whether it triggers or clears alarm, alarm text, etc.).

Specific OID (input line)
Displays the OID that identifies the SNMP notification(s) to which the rule applies. For SNMPv2c and SNMPv3 notifications, this is **value** of the second variable binding (`snmpTrapOID.0`) included in the notification PDU. For SNMPv1 Traps, this OID is constructed as follows: `<enterprise OID>.0.<specific trap number>`, where `<enterprise OID>` and `<specific trap number>` are values of the `enterprise` and `specific-trap` fields in the SNMPv1 Trap PDU.

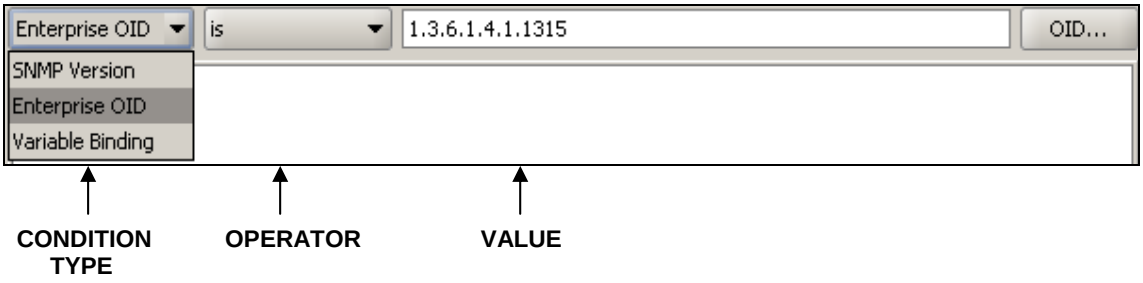
When you create a trap-to-alarm rule from a received specific SNMP notification, the Specific OID value is automatically set to match the SNMP notification specific OID.

> **Note:** Specific OID value is the key condition that is checked first in received SNMP notification message. Only if the specific OID value of a received notification matches the one specified in the trap-to-alarm rule, the remaining conditions of the given rule (trap filter) are evaluated (compared to notification attributes).

Edit (button)
Opens the Specific OID dialog box that lets you edit or select the notification's enterprise specific OID from the MIB tree.

Name
Displays the name of the specific OID as it resolves through loaded MIB modules. For user-friendlier SNMP notification viewing and handling, you should load the private MIB module(s) that define relevant enterprise specific SNMP notifications into Net Inspector.

New condition (toolbar)
The New condition toolbar lets you create conditions and add them to the trap filter one-by-one, while the central section of the dialog box (Conditions panel) displays existing filter conditions and relations between them. The Conditions panel displays a trap filter in form of a hierarchical tree, where individual conditions are connected with logical operators (AND, OR).



This toolbar lets you create a filter condition by selecting the condition type, operator and value from the corresponding drop-down lists. For the "variable Binding" condition type, more than one property can be set, as explained below.

Once the condition is configured, you can add it to the filter by clicking the ***Add*** button in the right section of the dialog box. Added conditions appear in the Conditions panel below the New condition toolbar.

Condition type (drop-down list)
Specifies the type of the condition. You can select among the following types of conditions:

- ***SNMP Version***
  Lets you configure a filter condition that will let through only notifications of particular SNMP protocol version (i.e., SNMPv1 Traps or SNMPv2c Traps and Informs or SNMPv3 Traps and Informs).

- ***Enterprise***
  Lets you configure a filter condition that will let through only SNMP notifications with a particular enterprise OID (specified in the accompanying input line). If the relevant MIB module is loaded, click the ***OID*** button next to this input line to open the **Select OID** dialog box and select the desired object

from the MIB tree. The OID of the selected object will be inserted into the OID input line. This OID will be compared with the value of the “enterprise” field in the SNMPv1 trap messages or with the value of the “snmpTrapEnterprise.0” variable binding included into SNMPv2c and/or SNMPv3 notification messages.

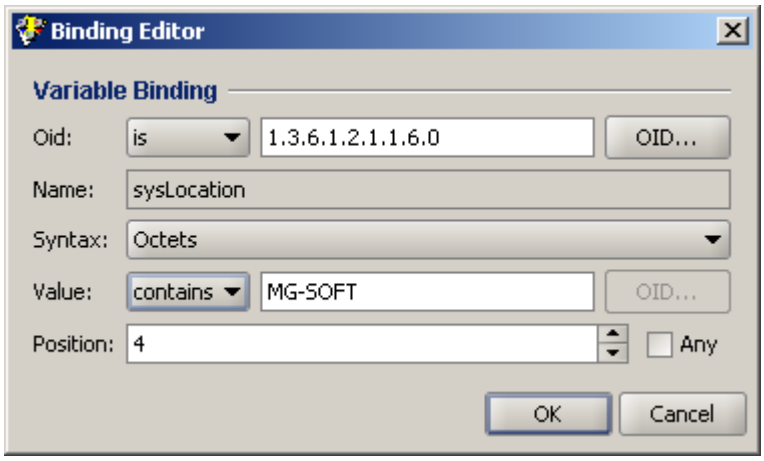
- ***Variable Binding***
  Lets you configure a filter condition that will let through only SNMP notifications containing a particular variable binding. To add a variable binding filter condition, select the “Variable Binding” condition type from the New condition drop-down list. The variable binding configuration preview and the ***Edit*** button are displayed in the New condition toolbar:

You need to configure a variable binding condition before adding it to the filter.

Note: A variable binding has the following properties:

OID/name, syntax, value and position in the variable bindings list. For example: `sysUpTime.0, Timeticks, 2344223, Binding#1`. These settings can be configured in the Binding Editor dialog box.

To configure a variable binding, click the ***Edit*** button in the New Conditions toolbar. The **Binding Editor dialog box** opens, providing the following controls:



OID (operator, **input line** and **button)**
From the operator drop-down list, select the desired operator (e.g., “is”, “is not” or “contains”) and enter the OID of the name portion of the variable binding into the ***OID*** input line. Alternatively, click the ***OID*** button next to this input line to open the **Select OID** dialog box and select the desired object from the MIB tree. The OID of the selected MIB object will be inserted into the ***OID*** input line.

Name
Displays the name of the OID specified above as it resolves through loaded MIB modules. For user-friendlier SNMP notification viewing and handling, you should load the MIB module(s) that define relevant OIDs in the Server Settings dialog box, MIB Modules panel.

Syntax (drop-down list)
Lets you select the syntax of the OID specified above (e.g., Octets, Counter32, IP address, etc.). Depending on the selected syntax, different **Value** operators are available below.

Value (operator, **input line** and **OID button)**
Lets you specify the variable binding value. From the operator drop-down list, select the desired operator (e.g., “is”, “is not”, “contains”, “greater”, etc.). The list of available operators depends on the syntax selected above. Then, enter the desired value of the variable binding into ***Value*** input line. If the “OID” syntax is selected, you can click the ***OID*** button next to the ***Value*** input line to select the relevant object (and thus its OID) from the **Select OID** dialog box.

Position (input line with **spin button)**
Specifies the position of the variable binding in the variable bindings list included in the notification PDU. For example the number “3” means that this variable binding must be the third binding in the variable bindings list. Note that SNMP specification requires that the first and the second variable binding in all SNMPv2c and SNMPv3 Trap and Inform PDUs be “sysUpTime.0” and “snmpTrapOID.0” respectively (this is not required for SNMPv1 Traps). Therefore, consider this requirement when creating trap-to-alarm rules for notifications transmitted via SNMPv2c or SNMPv3.

Any (checkbox)
If checked, all variable bindings in the received notification PDU are checked for the matching binding. This option can useful when the position of bindings in Trap PDUs vary or when creating a trap-to-alarm rule to cover SNMPv1 and SNMPv2c/v3 notifications (note that the first binding in a specific SNMPv1 Trap will be the third binding in equivalent SNMPv2c or SNMPv3 Trap).

Note: this option should be disabled if possible, as it may significantly degrade the Net Inspector Server performance.

OK (button)
Applies the changes and closes the Binding Editor dialog box. A preview of the newly configured variable binding is displayed in the New condition toolbar. Click the ***Add*** button in the New/Edit Trap-to-Alarm Rules dialog box (first screen) to add the configured condition to trap filter.

Cancel (button)
Discards the changes and closes the Binding Editor dialog box.

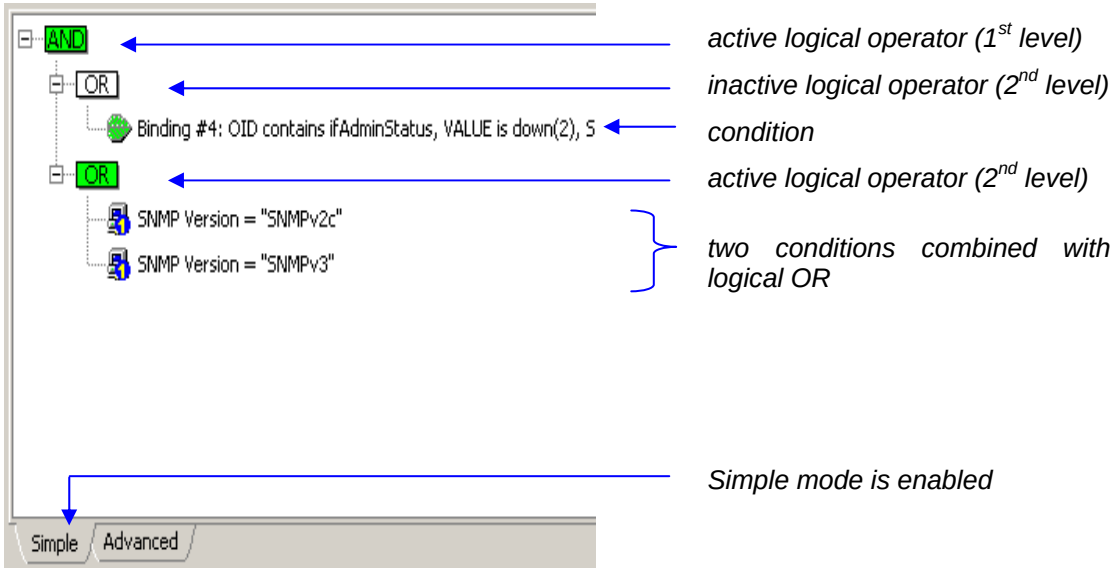
Operator (drop-down list)
Displays the condition operator, e.g., “is”.

Value (drop-down list or **input line)**
Lets you enter or select the condition value. Available (and valid) values depend on the type of the condition selected.

Conditions (panel):

The **Conditions panel** displays and lets you re-configure existing filter conditions, and logical operators connecting them.

Example of the Conditions panel contents:



Expression equivalent to the filter displayed above would be:

(Binding#4: OID contains ifAdminStatus, value is down(2), syntax is integer32) AND (SNMP version=SNMPv2c OR SNMP version=SNMPv3)

Simple and Advanced Mode

Conditions panel contains two tabs providing two modes of operation: Simple and Advanced. For more information about Simple and Advanced modes, please consult the Create Filter dialog box section.

Editing Conditions

For more information about editing existing conditions, please consult the corresponding description of the Create Filter dialog box section. The variable binding condition editing slightly differs from editing other conditions. To edit a variable binding condition, first double-click the relevant condition line in the Conditions panel or click the ***Edit*** button in the right section of the dialog box and then click the ***Edit*** button that appears in the condition line to display the Binding Editor dialog box, where you can edit variable binding condition.

Buttons:

- **Add**
  Adds the condition from the New condition toolbar to the Conditions panel. In Advanced mode the condition is added to the selected branch in the filter tree.
- **Edit**
  Lets you edit the selected condition or operator. Operators can be modified only in Advanced mode.

- **Remove**
  Removes the selected condition or operator (and all its child objects) from the Conditions panel.

- **AND**
  Adds the logical AND operator to the selected filter branch. This button is enabled only in Advanced mode.

- **OR**
  Adds the logical OR operator to the selected filter branch. This button is enabled only in Advanced mode.

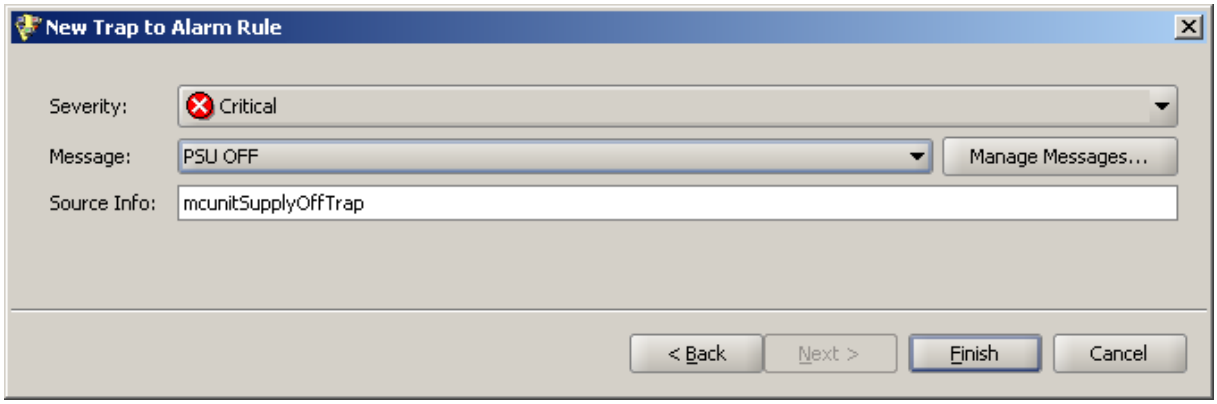
- **Next (button)**
  Lets you proceed to the second screen.

- **Cancel (button)**
  Discards all changes and closes the dialog box.

Second Screen (Alarm Mapping Screen)

The second screen of the New/Edit Trap-To-Alarm dialog box is used for configuring alarm mapping. Alarm mapping controls the resulting alarm attributes, i.e., the alarm severity level, the alarm message and, optionally, alarm source info alarm property.

The alarm mapping screen also determines whether the given trap-to-alarm rule (i.e., matching SNMP notification) will raise or clear the alarm.



Example of Trap-To-Alarm dialog box, second screen

The second screen of the New/Edit Trap-To-Alarm dialog box provides the following controls:

Severity (drop-down list)
Lets you select the severity level for the resulting alarm. If the severity level is set to a value other than “Cleared”, the rule will trigger (raise) alarm. If the severity level is set to “Cleared”, the rule will clear the alarm, provided that other conditions for clearing the alarm (trap filter, alarm message, source info) are also met.

Message (drop-down list)
Lets you specify the message (text) for the resulting alarm. To create a new message or edit an existing user-defined message, click the ***Manage Messages***

button and add/edit a message in the dialog box that appears, then select the new/edited message from the ***Message*** drop-down list. Note that the message value serves as one of the conditions for clearing the alarm.

Manage Messages (button)
Opens the Manage Event Attributes dialog box that lets you view the built-in alarm messages, event types and probable event causes, as well as add and edit user-defined alarm messages, event types and probable event causes.

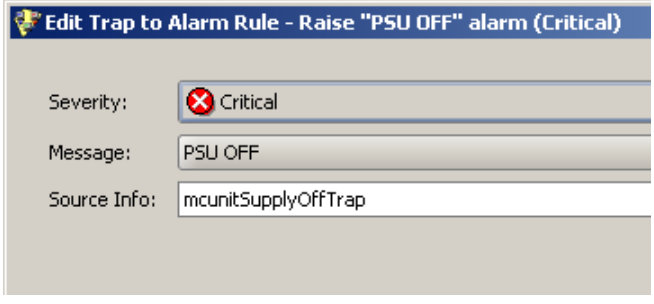
Source Info (input line)
Lets you specify the source info property for the resulting alarm. The source info alarm property is used to provide more information about the alarm condition. It can be configured to display one or more attributes of the received SNMP notification by entering the "notification" reserved words into this input line (you can combine any text with reserved words). The source info value is optional. However, if specified, it serves as one of the conditions for clearing the alarm, as described below.

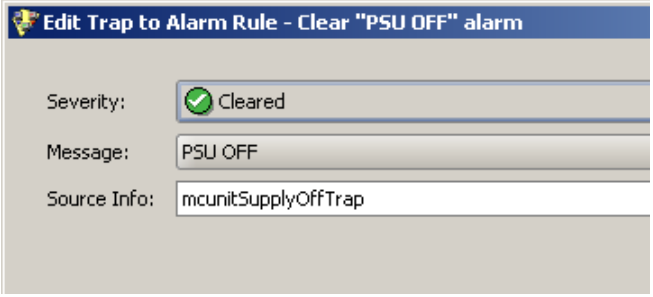
Alarm Clearing Principle

Whenever applicable, one should create two trap-to-alarm rules for each type of alarm condition (e.g., fault), one that triggers the alarm and the other that clears it. For example, if a device sends an SNMP Trap when the chassis temperature raises above the normal level and another SNMP Trap when the temperature drops back to normal, you should create two-trap-to alarm rules: one that will raise the alarm (set the alarm severity level to other than "Cleared") and the other to clear the alarm (i.e., set its severity level to "Cleared").

Alarm clearing is controlled by the severity, message and source info values (besides the trap filter). **More specifically, a trap-to-alarm rule B, which clears the alarm triggered by the trap-to-alarm rule A, must have the same alarm message and source info value as the rule A, and the severity set to "Cleared".** Of course, rule B will have a different trap filter than rule A.

Example of two trap-to-alarm mapping rules (second screen) used for triggering and clearing the "PSU OFF" alarm

	This rule triggers (opens) the user-defined "PSU OFF" alarm

	This rule clears (closes) the user-defined “PSU OFF” alarm

Note that when using reserved words (e.g., $VB_VALUE(4)) for the source info value, the **reserved words are expanded** (replaced with the actual values from a received SNMP notification) and then the expanded source info value is compared to source info values of open alarms (when clearing alarms).

Buttons:

- **Previous (button)**
  Returns to the first screen (while preserving the second screen configuration).
- **Finish (button)**
  Applies the changes and closes the dialog box. If you have configured a new rule, it is added to the Rules list in the Trap-To-Alarm Rules panel. After clicking this button, Net Inspector maps all newly received SNMP notifications (that match the given rule conditions) to alarms according to the rule.
- **Cancel (button)**
  Discards all changes and closes the dialog box.

8.7 Event Attributes Panel

Purpose

This panel is used for viewing and managing certain event/alarm attributes, i.e., event message, probable cause and event type attributes.

Description

Users with administrator access rights can use this panel to view the list of built-in event messages, probable causes and event types, as well as to add, edit and remove user-defined event message, probable cause and event type values. Administrators can also assign probable cause and event type values to user-defined event messages.

User-defined event/alarm messages can be used in trap-to-alarm rules.

The Event Attributes panel contains 3 tabs: Messages, Cause and Event Type. To switch to the desired tab, click its tab symbol in the upper section of the Event Attributes panel.

8.7.1 Messages Tab

This tab lets you view the list of the built-in event messages, their message ID values and associated probable causes and event types. The built-in event messages cannot be edited or deleted. It also lets you add user-defined event messages to the list, as well as edit and delete the existing user-defined messages.

The Messages tab provides the following controls:

Messages List

Displays the existing event/alarm messages. Each message is represented by one line. Lines containing the built-in messages have grey background color, indicating that these messages cannot be edited. Lines containing the user-defined messages have white background color, indicating that they can be edited.

The Messages list contains the following columns:

ID
Displays the unique identification number (ID) of the message. User-defined messages have message ID in range 50000 - 90000.

Message
Displays the message text.

Cause
Displays the probable cause associated with the message.

Event Type
Displays the event type associated with the message.

Buttons

Add (button)
Adds a new line to the Messages list and puts the line in the edit mode so its attributes can be configured by entering the message ID and message text values into corresponding input lines (ID, Message) and selecting the probable cause end event type values from the corresponding drop-down lists (Cause, Event Type). After you have finished configuring the message attributes, click the ***Apply*** button to apply the changes and exit the edit mode.

Edit (button)
Puts the selected user-added line in the edit mode so its attributes can be configured by editing the message text in the Message input line and by selecting different probable cause end event type values from the corresponding drop-down lists (Cause, Event Type). After you have finished editing the message attributes, click the ***Apply*** button to apply the changes and exit the edit mode. This button is disabled if a built-in message is selected.

Remove (button)
Deletes the selected line (message).

Apply (button)
Applies the changes in the edited line and exits the edit mode.

Cancel (button)
Discards all changes in the edited line and exits the edit mode.

8.7.2 Cause Tab

This tab lets you view the list of the built-in probable causes and their ID values. It also lets you add, edit and remove user-defined causes and corresponding IDs.

The Cause tab provides the following controls:

Cause List

Displays the existing event/alarm probable causes. Each cause is represented by one line. Lines containing the built-in cause values have grey background color, indicating that they cannot be edited. Lines containing the user-defined causes have white background color, indicating that they can be edited.

The Cause list contains the following columns:

ID
Displays the unique identification number (ID) of the cause. User-defined causes have cause ID value in range 10000 - 20000.

Cause
Displays the probable cause text.

Buttons

Add (button)
Adds a new line to the Cause list and puts the line in edit mode so it can be configured by entering the ID and cause text values into corresponding input lines (ID, Cause). After configuring the cause attributes, click the ***Apply*** button to apply the changes and exit the edit mode.

Edit (button)
Lets you modify the selected user-defined cause text. After editing the cause text, click the ***Apply*** button to apply the change and exit the edit mode. This button is disabled if a built-in cause is selected.

Remove (button)
Deletes the selected line (cause).

Apply (button)
Applies the changes in the edited line and exits the edit mode.

Cancel (button)
Discards all changes in the edited line and exits the edit mode.

8.7.3 Event Type Tab

This tab lets you view the list of the built-in event types and their ID values, as well as add, edit and remove user-defined event types and corresponding IDs.

The Event type tab provides the following controls:

Event Type List

Displays the existing event/alarm types. Each event type is represented by one line. Lines containing the built-in event type values have grey background color, indicating that they cannot be edited. Lines containing the user-defined event types have white background color, indicating that they can be edited.

The Event Type list contains the following columns:

ID
Displays the unique identification number (ID) of the event type. User-defined event types have the ID value in range 10000 - 20000.

Event Type
Displays the event type text.

Buttons

Add (button)
Adds a new line to the Event Type list and puts the line in the edit mode so it can be configured by entering the ID and event type text values into corresponding input lines (ID, Event Type). After configuring the event type attributes, click the ***Apply*** button to apply the changes and exit the edit mode.

Edit (button)
Puts the selected user-defined event type in edit mode so its event type text can be edited. After editing the event type, click the ***Apply*** button to apply the change and exit the edit mode. This button is disabled if a built-in event type is selected.

Remove (button)
Deletes the selected line (event type).

Apply (button)
Applies the changes in the edited line and exits the edit mode.

Cancel (button)
Discards all changes in the edited line and exits the edit mode.

8.8 Object Types Panel

Purpose

The Object Types panel is used for viewing and managing types of objects used in Net Inspector (managed objects, actions objects and system objects).

Description

The configuration in the Object Types panel determines in which object type and sub-type categories the objects in Net Inspector fall into and what icons are used for displaying them.

Furthermore, this panel lets you define ***new types*** of objects based on the built-in (base) types, and ***sub-types*** that are variations of base types, meaning that they have the same object type name as the base types (e.g., IP), but different vendor, class and/or icon property.

Once you create a new object type or sub-type, you can add an object of this (sub)type to the Net Inspector workspace.

This panel is used also for changing the object type icons.

> **Note:** To use custom icons, copy the custom icon image files to the //Engine/icon folder on computer running Net Inspector Server. The icons dimensions must be 32x32 pixels and they must be stored in PNG file format (.png).

About sub-types and new types

Every object type has four properties, which uniquely identify it: name, class, vendor and icon.

Sub-types

A sub-type is a variation of a base type, meaning that it has the same type name as the base type (e.g., IP), but different vendor, class and/or icon property.

For example, Net Inspector displays different icons for different classes (router, switch, workstation, printer, etc.) of the IP object type. These are actually sub-types of the IP managed object type, as follows:

Type name	Class	Vendor	Icon
IP	Router	blank (=any)	X
IP	Switch	blank (=any)	Y
IP	Printer	blank (=any)	Z

Furthermore, we can define different sub-types within a class, e.g., different icons for different vendors of IP routers:

Type name	Class	Vendor	Icon
IP	Router	Cisco	X1
IP	Router	Juniper	X2
IP	Router	Iskratel	X3

In cases where two or more sub-type definitions apply, a more specific definition takes precedence over less specific definition(s).

Example:

Type name	Class	Vendor	Icon
IP	blank (=any)	blank (=any)	O
IP	Router	blank (=any)	M
IP	Router	MG-SOFT	N

In the example above, three IP sub-types of different scopes are defined. Line 1 defines the least specific IP (sub)type that covers objects of the broader scope (any class and any vendor). If lines 2 and 3 did not exist, the line 1 would cover all classes and vendors of the IP object type. In such case, Net Inspector would display the icon "O" for all IP objects, regardless of their class and vendor properties. However, as the lines 2 and 3, which are more specific, do exist, they take precedence over the line 1 in cases where the "IP" object type is of class "Router" and vendor is "MG-SOFT". For example, if we add a new object to the workspace, whose type is "IP", class is "Router" and vendor is other than "MG-SOFT", then Net Inspector will display the icon "M" for this object (the sub-type defined in the second line applies). On the other hand, if we create a new object of type "IP", class "Router" and vendor "MG-SOFT", then Net Inspector will display the icon "N" for this object (sub-type from the third line).

New Types

A new type (also named a derived type) is an object type that is based on one of the built-in types (e.g., IP), but has its own unique name (e.g., NEWIP). New types inherit all the properties of the base types they are derived from. As the built-in types, new types can also be sub-typed, i.e., users can define sub-types of a new type.

The Object Types panel provides the following controls:

Filter (drop-down list)
Is displayed in the upper left side of the panel, below the title bar. It lets you enter text that functions as a filter, i.e., it displays only those lines in the Object Types panel that contain the entered text in selected columns. To specify which columns will be taken into account, click the filter symbol  and select desired columns (described below) from the drop-down menu that appears. Then, enter the text in to the accompanying input line, which will serve as the filter criterion.

For example, if the ***Type name*** and ***Class*** columns are selected in the filter drop-down list and you enter the string “ip” into the Filter input line, the Object Types panel will display only those lines that include string “ip” in the ***Type Name*** or ***Class*** columns (e.g., **IP** [Type Name column], Multi**ip**lexer [Class column]).

Object Types (list)
Displays the existing object types and sub-types in the following columns:

Type Name
The name of the object type (e.g., “IP”).

Class
The class of the managed object (e.g., “Workstation”). If this field is blank, it covers all possible classes (=any).

Vendor
The vendor of the managed object (e.g., “MG-SOFT”). If this field is blank, it covers all possible vendors (=any).

Icon

The image and filename of the icon assigned to the object (sub-)type (e.g., “  ip”)

Derived From
The name of the base object type (e.g., “IP”) the new type is derived from. This field is blank for the built-in types and sub-types.

Add (button)
Opens the New Object Type dialog box, which lets you create and configure a new object type or sub-type.

Edit (button)
Opens the Edit Object Type dialog box, which lets you view and change the icon for the selected type.

Remove (button)
Deletes the selected object type or sub-type. The built-in object types cannot be deleted.

Note: Types that are currently in use (i.e., assigned to one or more managed objects) cannot be deleted.

New/Edit Object Type dialog box

The New Object Type and the Edit Object Type dialog boxes have the same appearance, with the exception that only the ***Icon*** property can be edited in the Edit Object Type dialog box. These dialog boxes provide the following controls:

New Type (radio button)
If this option is selected, a new type of object can be created from one of the built-in (base) types.

Sub-type (radio button)
If this option is selected, a new sub-type can be created from one of the built-in (base) types.

Based on (drop-down list)
Lets you select the name of the base object type (e.g., “IP”) the new type will be derived from, or sub-type of which you are creating.

Name (input line)
Lets you enter the name of the new type. This input line is read-only when creating sub-types.

Class (drop-down list)
Lets you select the class of the managed object (e.g., “Switch”).

Vendor (input line)
Lets you enter the vendor of the managed object (e.g., “MG-SOFT”). To cover all possible vendors, leave this input line blank.

Icon (drop-down list)
Lets you select the icon of the new type.

> **Note:** To use custom icons, copy the custom icon image files to the //Engine/icon folder on computer running Net Inspector Server. The icons dimensions must be 32x32 pixels and they must be stored in PNG file format (.png).

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

8.9 Chart Panel

Purpose

The Chart Panel is used for creating, opening and deleting charts. Charts display lines that show how the values of variables retrieved from managed object(s) change in time.

Description

Net Inspector lets you monitor the values of some important numerical variables (e.g., CPU load, memory usage, storage usage, interface utilization, etc.) collected from one or more devices in charts. Charts display lines that show how the values of selected variables change in time. Charts are configured in the Chart Panel by the users with administrator access rights. When a chart is configured, Net Inspector Server collects the relevant data from the managed objects and stores the chart values and settings. Network operators can connect to Net Inspector Server, open the pre-configured charts available in the Chart Panel and view the charts in Net Inspector Client.

Note that charts can be viewed only in the user view in which they were created.

The Chart Panel provides the following controls:

Charts (list)
Lists the names of existing charts.

Add (button)
Opens the New Chart dialog box, which lets you create a new chart in two steps.

Open (button)
Opens a new tab in the Maps window and displays the selected chart in it.

Remove (button)
Deletes the selected chart.

8.9.1 New Chart Dialog Box

To open the New Chart dialog box, click the ***Add*** button in the Chart Panel.

The New Chart dialog box lets you create a new chart in two simple steps. In the first step, you need to select the managed object(s) whose values you want to plot on the chart. In the second step, you need to select one of the predefined variables that will be plotted on the chart (e.g., CPU load, memory usage, storage utilization, interface utilization, etc.).
This dialog box lets you create a new chart in a wizard-like fashion and has two screens: the Select source(s) screen and the Select chart variable screen

1. The **Select source(s)** screen provides the following controls:

Chart name (input line)

Lets you enter the name for the new chart. This name will be listed in the Charts Panel.

Selected source(s) (list)
Lists the names of managed objects that you want to include in the chart.

Add (button)
Opens the Select Source dialog box. The Select Source dialog box displays two panels; the left panel contains the expandable map tree, while the panel on the right displays all objects included in the map that is selected in the left panel. The left panel also displays some properties of the listed objects. To select a source object, click the relevant map in the left panel, choose the object on the right panel and click the ***OK*** button. This will add the name of the selected source to the ***Selected source(s)*** list. Repeat this procedure to add another source object to the list.

Remove (button)
Deletes the selected source object from the list.

Next (button)
Lets you proceed to the next step, i.e., the ***Select chart variable*** screen.

Cancel (button)
Discards all changes and closes the dialog box.

2. The **Select chart variable** screen provides the following controls:

Select chart variable (list)

Lists the names of variables that can be included into charts, like CPU usage, memory usage, storage usage, interface inbound/outbound utilization rate and traffic,…). The selected variable will be plotted on the same graph for all managed objects selected in the previous step that return this information.

Finish (button)
Closes the New Chart dialog box and adds new chart name to the Chart Panel dialog box.

Back (button)
Lets you return to the previous screen, i.e., the Select source(s) screen.

Cancel (button)
Discards all changes and closes the dialog box.

8.9.2 Chart Tab Pop-up Menu

By opening a chart from the Chart Panel, a new chart tab in the Maps window is created, displaying the chart. The graph lines show how the values of variables collected from managed object(s) change in time. The chart is automatically updated

when the new values are retrieved. How frequently the chart is updated depends on the polling interval set in the polling profile assigned to the source objects.

By right-clicking inside the chart tab a pop-up menu appears with the following commands:

- ***Properties***
  This command opens the chart Properties dialog box that lets you view and configure properties of the given chart.
- ***Show Points***
  If this toggle command is selected, the individual values retrieved from managed objects are depicted as scatter marks along the graph line.
- ***Fit in Window***
  Automatically adjusts the chart zoom level to show the entire chart in the currently selected chart tab.

8.9.3 Chart Properties Dialog Box

The chart properties dialog box lets you view and configure the properties of the given chart.

To open this dialog box right-click inside the chart tab in the Maps window and select the ***Properties*** command from the pop-up menu that appears.

The chart properties dialog box provides the following controls:

Name (input line)
Displays the name of the chart.

Units (drop-down list)
Displays and lets you select the units for chart values, i.e., absolute values, percent values, bytes, bytes per second, bits per second. Selected units are displayed along the vertical axis of the chart.

Add (button)
Opens the Add Chart Variable dialog box, which lets add additional variables to the chart in two steps. This dialog box has the same appearance and is used in the same way as the New Chart dialog box.

Remove (button)
Removes selected variable from the chart.

Sources (list)
Displays the source objects and variables that are monitored on each source.

OK (button)
Closes the dialog box and applies the changes.

Cancel (button)
Closes the dialog box and discards the changes.

8.10 MIB Modules Panel

Purpose

The MIB Modules panel lists all MIB modules registered with Net Inspector and lets you load and unload them.

Description

The MIB Modules panel contains two lists: the **Loaded Modules** list on the left side of the panel displays the names of currently loaded MIB modules, while the **Available Modules** list on the right side lists the names of MIB modules, which are currently not loaded.

In order for a MIB module to appear on the list of available modules, it must be properly registered on the computer that runs Net Inspector Server. Net Inspector comes with over 200 standard MIB modules that are registered already at the time of installing the software. The package includes also MG-SOFT MIB Compiler application that lets you compile private MIB modules provided by the vendors of the network equipment. You can load MIB modules into Net Inspector in order to enable managing network nodes in a user-friendly way, e.g., to view the relevant MIB objects in the MIB tree shown in the MIB Browser window, to display the names and certain values of retrieved SNMP variables in the MIB Browser window, to identify received SNMP Trap and Inform notifications by their names, etc.

To compile additional MIB modules and load them in Net Inspector, proceed as follows:

1. Use the bundled MG-SOFT MIB Compiler on the PC that runs Net Inspector Server to compile additional MIB module(s).
2. Use MG-SOFT MIB Compiler to save the compiled MIB module(s) to .smidb file format in the default location, which is:

   a) On Windows Vista, Windows Server 2008 and Windows 7:
   `<drive>:\ProgramData\MG-SOFT\SMI Modules\MIB Modules\SMIDB`

   NOTE: "`ProgramData`" is a hidden folder.

   b) On Windows XP, Windows Server 2003:
   `<drive>:\Documents and Settings\All Users\Application Data\MG-SOFT\SMI Modules\MIB Modules\SMIDB`

   NOTE: "Application Data" is a hidden folder.

   `<drive>` is the letter of the drive where operating system is installed (e.g., `C`).

   c) On Linux:
   `/usr/local/mg-soft/common/SmiModules/MibModules/smidb`

3. Click the ***Refresh*** button at the bottom of the MIB Modules panel to refresh the list of available MIB modules.
4. Load the new MIB module(s) in the MIB Modules panel by selecting one or more modules in the list of available modules and clicking the ***Load*** button.

For detailed instruction on compiling and saving MIB modules, kindly refer to the MIB Compiler User Manual that installs with the software.

The MIB Modules panel contains the following controls:

Loaded Modules (list)
Displays the names of currently loaded MIB modules. To unload a MIB module, select in the list and click the ***Unload*** button below.

Unload (button)
Unloads the MIB module(s) selected in the Loaded Modules list. The unloaded MIB module disappears from the Loaded Modules list and appears on the Available Modules list.

Available Modules (list)
Displays the names of available MIB modules, which are currently not loaded. To load a MIB module, select in the list and click the ***Load*** button below.

Load (button)
Loads the MIB module(s) selected in the Available Modules list. The loaded MIB module disappears from the Available Modules list and appears on the Loaded Modules list.

OK (button)
Closes the dialog box and applies the changes; i.e., it loads or unloads (depending on the command you selected) MIB module(s) into Net Inspector Server and Client.

Cancel (button)
Closes the dialog and discards all changes.

8.11 Auto Configuration

Purpose

It is used for controlling the Net Inspector auto configuration feature. Auto configuration automatically adds new managed objects to the system and starts monitoring them if Net Inspector receives an SNMP Trap or SNMP Inform notification message or a NetFlow or sFlow message from unknown devices (i.e., devices that were previously not included in the Net Inspector configuration). Auto configuration is a type of passive device discovery, where devices are discovered by receiving SNMP notifications and NetFlow/sFlow packets from the network. This feature may be used as an alternative to the active network discovery functionality or in combination with it (e.g., to discover some devices through the active discovery operation and other through the passive method - received SNMP notifications and NetFlow packets).

Description

Users with administrator access rights can enable, disable and configure the Auto configuration settings to control adding new devices to the system based on received SNMP notification messages and NetFlow/sFlow streams.

Managed objects representing devices that have been automatically added to the system by the auto configuration feature carry with the "**NEW**" label displayed in the upper-left corner of the managed object icon. This label can be hidden or displayed by selecting the respective managed object(s) and choosing the ***New Device*** toggle command from the pop-up menu.

The Auto Configuration panel includes the following controls:

Add devices on received SNMP notifications from unknown sources to configuration (checkbox and drop-down list)
If this checkbox is checked, the automatic adding of new managed objects (devices) based on received SNMP notifications is enabled. In the accompanying drop-down list, select the configuration, which the new devices will be added to.

> **Add devices to user view X, map Y (checkbox, drop-down list and input line)**
> If this checkbox is checked, new managed objects (devices) are automatically added to the workspace, i.e., to the user view X and map Y specified in the accompanying drop down list and input line, respectively, If no map is specified, the managed object icons are placed to the root of the selected user view.

Add devices on received NetFlow streams from unknown sources to configuration (checkbox and drop-down list)
If this checkbox is checked, the automatic adding of new managed objects (devices) based on received NetFlow and sFlow packets is enabled. In the accompanying drop-down list, select the configuration, which the new devices will be added to.

> **Add devices to user view X, map Y (checkbox, drop-down list and input line)**
> If this checkbox is checked, new managed objects (devices) are automatically added to the workspace, i.e., to the user view X and the map Y specified in the accompanying drop down list and input line, respectively, If no map is specified, the managed object icons are placed to the root of the selected user view.

Apply Changes (button)
Applies the changes without closing the dialog box.

OK (button)
Applies the changes and closes the dialog box.

9 MANAGE POLLING ENGINES DIALOG BOX

9.1.1 Purpose

The Manage Polling Engines dialog box is used for viewing, adding, editing and removing Performance Manager polling engines.

9.1.2 Opening

To open this dialog box, click the ***Manage Polling Engines*** button in the Performance Manager Properties window.

The Performance Manager Properties window can be opened by double-clicking the Performance Manager system object icon in the Maps window or by right-clicking the Performance Manager object and selecting the ***Properties*** pop-up command.

9.1.3 Description

This dialog box has the same appearance and is used in the same way as the Polling Engines Panel.

10 PERFORMANCE STATISTICS WINDOW

Note: This window is not accessible in MG-SOFT Net Inspector LITE Edition.

10.1 Purpose

The Performance Statistics window is a Java-based web browser used for viewing the performance web page for the device selected in Net Inspector. The device performance web page is generated by the Performance Manager polling engine that polls that device (in MG-SOFT Net Inspector WorkGroup, Enterprise and Carrier Edition). The device performance web pages include the following statistics (current data and history): device response time and packet loss rate, and for SNMP devices (depending on type) also network interface statistics, resources utilization statistics, running processes statistics, IP SLA statistics, custom statistics, etc.

10.2 Opening

To open the Performance Statistics window for the specific device, right click the respective managed object in the Maps Window and select ***Show Performance Statistics*** from the pop-up menu that appears. Alternatively, select the managed object (device) you want in the Maps Window and click the ***Show Performance Statistics*** button in the Toolbar.

10.3 Description

The Performance Statistics window lets you view and browse the performance web page for the selected device. It displays the system information, response times (average, min., max.) and packet loss rate for the selected device, as well as the status and utilization rates of all monitored network interfaces on that device. For devices implementing the HOST-RESOURCES-MIB module and for Cisco devices, this page displays also the Memory & Processor Information (memory usage, CPU load), Storage Information and Process information (process name, path, PID, CPU and memory consumption) provided that monitoring of all these metrics is enabled in the polling profile that is assigned to the given device. If any custom statistics are configured and enabled in the associated polling profile and in the device page layout, this page displays also custom statistics polled on the given device.

In addition to displaying the last retrieved device performance values, this report page shows also **history graphs** for the response time, packet loss, memory usage, and CPU load variables (where applicable).

To view more detailed graphs and tables for any metric, click on its graph/chart in the device performance page.

The bottom section of the device performance page displays all device-related alarms (if any).

The Performance Statistics window contains the toolbar, web browser and status bar components, as follows:

10.3.1 Toolbar

The toolbar is displayed directly below the title bar and contains the following buttons:

Back (button)
This button lets you to go to the previously visited web page.

Forward (button)
This button lets you browse to the next web page in the browse history.

Refresh (button)
Re-loads the current web page.

10.3.2 Web Browser

This frame occupies the area between the toolbar and the status bar. It displays the performance web page for the selected device. The device performance web page includes the following components (depending on the device type):

Device Performance Toolbar

It displays the name of the monitored device, links to different sections of device performance page (depending on device type), and the following graph controls:

Time Period (drop-down list)
Lets you select the time window for graphs on the page. By default, graphs display the values of the monitored variables for the last 120 minutes. To use a different time frame, select a corresponding entry from the drop-down list:

Example: Current Date/Time: Tue, 2010/10/05 14:45:00

Time Period	Example Start Date/Time	Example End Date/Time
This hour	2010/10/05 14:00:00	2010/10/05 15:00:00
Last 60 minutes	2010/10/05 13:45:00	2010/10/05 14:45:00
Last hour	2010/10/05 13:00:00	2010/10/05 14:00:00
***Last 120 minutes**	2010/10/05 12:45:00	2010/10/05 14:45:00
Today	2010/10/05 00:00:00	2010/10/06 00:00:00
Yesterday	2010/10/04 00:00:00	2010/10/05 00:00:00
This week	Mon, 2010/10/04 00:00:00	Mon, 2010/10/11 00:00:00
Last 7 days	2010/09/29 00:00:00	2010/10/06 00:00:00
Last week	Mon, 2010/09/27 00:00:00	Mon, 2010/10/04 00:00:00
Last business week	Mon, 2010/09/27 00:00:00	Sat, 2010/10/02 00:00:00
Last 14 days	2010/09/22 00:00:00	2010/10/06 00:00:00
This month	2010/10/01 00:00:00	2010/11/01 00:00:00
Last 30 days	2010/09/06 00:00:00	2010/10/06 00:00:00
Last month	2010/09/01 00:00:00	2010/10/01 00:00:00

The Date/Time format is: YYYY/MM/DD HH:mm:ss
***** Default time period

Sample Interval (drop-down list)
Lets you select the sampling interval for data displayed in graphs and tables on the page. The sampling interval determines the granularity of the data shown, i.e., how many bars in graphs or lines in tables are shown per given time period. For example, if the time period is set to *Last 60 minutes*, and the sample interval is set to *5 minutes*, the graphs will display 12 bars within one hour interval (60/5=12). The graph bars and values in tables display the **average values** within the sampling intervals.

To use a different sampling interval, select a corresponding entry from the drop-down list:

- 1 Minute
- 5 Minutes
- 30 Minutes
- 1 Hour
- 6 Hours
- 12 Hours
- 1 Day

Note: About data aggregation and values displayed

For all metrics shown in device performance web pages (e.g., response time, CPU load, interface utilization, MOS, etc.) the collected values are being gradually aggregated, meaning that from individual readings, average values are being calculated and displayed in graphs and tables, depending on the time period and the sampling interval set.

By default, the following aggregation model is used for performance data (a different model is used for the NetFlow data):

* The values for the last 7 days are kept unmodified in the database (**raw data** without aggregation).
* For the period between the last 32 days and last 7 days, only the **hourly averages** are kept in the database.
* For the period between the last 366 days and last 32 days, only the **daily averages** are kept in the database.

The graph bars and table values in device performance web pages always display the **average values** of readings within sample intervals, for example, if the polling interval is 1 minute and the sampling interval is 5 minutes, then each graph bar and table value will show the average value of 5 readings (approximately). By setting the sampling interval to equal to or less than polling interval (for any period within the last 7 days for which the raw data is kept by default), one can view the actual raw data (individual readings collected from devices).

In addition to average values, the absolute maximum (**MAX**) and minimum (**MIN**) values are shown in graphs and tables for each sampling interval.

Scale (drop-down list)
Lets you set the scale for the graphs on this page, as follows:

- Linear
- Logarithmic

Statistics (drop-down list)
Lets you select the statistics line(s) to be shown in graphs, as follows:

- None,
- 95-percentile,
- Trend line or
- Both

Note: 95-percentile and trend lines

A percentile is the value of a variable below which a certain percent of observations fall. Therefore, the 95-percentile line is a line under which you will find 95% of observations.

Trend line is a straight line connecting multiple points on a chart. A trend line is used in technical analysis to determine the direction and strength of a trend. An up trend line has a positive slope and connects at least two low points on a chart. A down trend line has a negative slope and connects at least two high points on a chart. The steepness of the slope of a trend line indicates the strength of the trend.

To view more detailed graphs and tables for any metric, click on its graph/chart in the device performance page.

System Information and Responsiveness

The Response Time frame in the Performance Statistics window provides the basic information about the given device, its status (titlebar color and text) and ping statistics. This frame provides the general information about the device, like its IP address/hostname, SysName, SysLocation, SysContact, SysDescription, etc. The Sys* data is obtained by querying the standard MIB-II system group of objects via SNMP. The information displayed will depend upon what information is available for that device in its MIB. The section on the right displays the ping statistics history graphs, i.e. device response times (in milliseconds), and the packet loss rate (in %). The current response time and packet loss rate are presented also in gauge charts.

Memory and Processor Usage Statistics

The **Memory and Processor Info** frame in the Performance Statistics window displays information only for Cisco devices and devices supporting the standard HOST-RESOURCES-MIB module (like servers, workstations, etc.), provided that the host resources monitoring is enabled in the polling profile assigned to those devices.

This frame displays information about device resources and their utilization rates, i.e., physical memory size and consumption, the number of CPUs, processes and users and the CPU usage. The last-retrieved values are presented in gauge charts, while the history graphs are shown in the right section of the page. Click on a graph to view a web page with history data (in form of a graph and table) for the corresponding metric.

Storage Usage Statistics

The **Storage Info** frame in the Performance Statistics window displays the monitored storage volumes (logical disks), their names, sizes and current usage (used and free space).

The last-retrieved values are presented in gauge charts. Click a gauge chart to view a web page displaying the storage volume usage history (in form of a graph and table).

Services Statistics

The **Services** frame in the Performance Statistics window displays the list of monitored services (e.g., HTTP, FTP, DNS, SMTP, etc.), their current status, name and port for every service. Services monitoring must be enabled in the polling profile that is assigned to the given device.

The following icons are used to indicate the current status of services:

-  - Service is responding
-  - Service is not responding

By clicking a service in the list, you can view its detailed statistics in a dedicated web page (Service Availability), including history graphs of service availability in % and service request-response round-trip-time (RTT) in ms.

Processes Statistics

The **Processes** frame in the Performance Statistics window displays the list of monitored processes, their current status, path, process identification number (PID), CPU load and memory load for every process.

The following icons are used to indicate the current status of processes:

-  - Process is running
-  - Process is stopped

By clicking a process in the list, you can view its detailed statistics in a dedicated web page (Process Info). This includes the graphs for CPU load and memory consumption.

Network Interfaces Statistics

The **Interfaces** frame of the Performance Statistics window displays the lists of monitored network interfaces on the device, as well as the current status, address, type, speed and the inbound and outbound utilization rate for every interface.

The following icons are used to indicate the current status of interfaces:

-  Up – Interface is up
-  Down – Interface is down
-  Off – Interface has been administratively disabled

By clicking an interface in the list, you can view its detailed statistics in a dedicated web page (Interface Info). This includes the interface utilization rate, bit rate, packet rate, error rate, queue drops (for Cisco devices only) and discard rate statistics with history.

IP SLA Statistics

The **IP SLA** frame in the device Performance Statistics window displays the lists of IP SLA categories (e.g., HTTP, DNS, Jitter (VoIP), etc.) and operations within categories (source->destination items) as well as the current IP SLA measurements. IP SLA statistics can only be monitored on Cisco devices that are properly configured

(enabled IP SLA operations), provided that the **IP SLA** monitoring is enabled in the polling profile assigned to those devices.

> For more information on configuring IP SLA operations on Cisco devices, please consult the Cisco documentation
> (e.g.: http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.html).

The **IP SLA** frame in the Performance Statistics window displays the lists of IP SLA categories (e.g., HTTP, DNS, Jitter (VoIP), etc.) and operations within categories (source->destination items) configured on the given device. It also displays the current IP SLA measurements, i.e., round trip times (RTT), and for VoIP also jitter from source to destination and vice-versa (Jitter SD/DS), packet loss from source to destination and vice-versa (Packet Loss SD/DS), and latency from source to destination and vice-versa (Latency SD/DS).

By clicking an IP SLA operation in the first column (e.g., VoIP RTTMON), you can view more detailed statistics with history for the given IP SLA operation. For VoIP IP SLA this includes the MOS (mean opinion score), round trip time (RTT), jitter, packet loss, latency, packet out of sequences, packet MIA, and packet late arrivals. For more information about those parameters, please consult the Cisco documentation that came with your equipment.

Custom Statistics

The **Custom Statistics** frame in the device performance web page displays the list of custom (user configured) SNMP parameters and their values. The **Custom Statistics** frame is not displayed by default. To enable displaying it, enable the **Custom Statistics** category in the **Edit Page Layout** drop-down frame.

By clicking an item in the list, you can view its detailed statistics in a dedicated web page. This includes a table of retrieved values and a graph of retrieved numerical values of the user-specified SNMP parameters.

Device Related Alarms

The **Alarms** frame in the Performance Statistics window displays all active alarms that are associated with the given device. If no active alarm for the given device exists, the **Alarms** frame is not displayed.

The following information is displayed for each alarm:

`Time`	Date and time when the alarm occurred
`Description`	Short description of the alarm
`Severity`	Severity of the alarm
`Source Info`	Additional information about the source of alarm
`Value`	Value of the variable (for threshold alarms only)

10.3.3 Status bar

Here, you can see which polling engine you are currently connected to, and the full URL of the Performance Manager site you are currently viewing.

11 PERFORMANCE MANAGER HOME PAGE WINDOW

Note: This window is not accessible in MG-SOFT Net Inspector LITE Edition.

11.1 Purpose

The Performance Manager Home Page window is a Java-based web browser used for viewing the web pages of the MG-SOFT Net Inspector Performance Manager web site. If more than one Performance Manager polling engine is used (e.g., in Net Inspector distributed setup) this web site contains consolidated information from all polling engines.

11.2 Opening

To open the Performance Manager Home Page window select a device in the Maps Window and choose the ***Tools / Show Performance Manager*** command or click the ***Show Performance Manager*** toolbar button.

11.3 Description

The Performance Manager Home Page Window enables you to browse the Net Inspector Performance Manager web pages. In the Performance Manager Home Page window you can monitor devices polled by all Performance Manager polling engines and view associated alarms. You can also create and view reports and perform other actions available in the MG-SOFT Performance Manager module. For details, please refer to the Net Inspector Performance Manager User Manual that installs with the software.

The Performance Manager Home Page window contains the toolbar, web browser and status bar components, as follows:

11.3.1 Toolbar

The toolbar is displayed directly below the title bar and contains the following buttons:

Back (button)
This button lets you to go to the previously visited web page.

Forward (button)
This button lets you browse to the next web page in the browse history.

Refresh (button)
Re-loads the current web page.

Print (button)
Clicking this button opens the standard Print dialog box that lets you print the current web page.

11.3.2 Web Browser

This frame occupies the area between the toolbar and the status bar. It displays the web pages generated by the Performance Manager polling engine(s), where you can monitor devices' status and alarms. Furthermore, you can create and view reports. By default, the user's homepage displays the Welcome frame and a list of all devices in the system (showing their status). PM website has the following components:

Tabs

The following tabs are displayed at the top of the website:

Home (tab)
When you click this tab, the user's homepage is displayed. Every Net Inspector user has its own home page, which is displayed automatically when the user opens the Net Inspector Performance Manager website. Home pages can be customized to contain one or more custom reports (graphs, tables), external web pages (included as HTTP frames), and/or a map on which the user can drag-and-drop icons of devices and monitor their status. User home pages fall into category of custom report pages and are configured in the same manner.

Devices (tab)
When you click this tab, the Performance Manager Devices page is displayed, where you can view all monitored devices included in the currently active Net Inspector user view, the current status of devices, assigned polling engine, and the basic device alarm information (the number of alarms and severity of the most critical alarm associated with the device).

Alarms (tab)
When you click this tab, the Performance Manager Alarms page is displayed. The Alarms page displays all active (open) alarms. New alarms will be automatically added to the Alarms list as they occur (after web page refresh), and the existing alarms will disappear from the list (after web page refresh) when they are cleared.

Services
When you click this tab, the Performance Manager Services page is displayed. The Services page displays a list all monitored services on devices by service category (DNS, HTTP, IMAP, SSH,…) and a list of services with status "Critical". By clicking a service on the list, more detailed statistics for the selected service is displayed (service availability and round trip time (RTT)).

NetFlow (tab)
When you click this tab, the Performance Manager NetFlow page is displayed. The NetFlow page displays a list of all configured NetFlow/sFlow source devices (if any) and the TopN NetFlow traffic reports for all NetFlow sources. By expanding and clicking the individual subentries in the Top N reports, more detailed statistics for the selected item (e.g., device, interface, conversation, application, etc.) is shown.

IP SLA (tab)
When you click this tab, the Performance Manager IP SLA page is displayed. The IP SLA page displays the lists of IP SLA categories (e.g., HTTP, DNS, Jitter (VoIP), etc.) and operations within categories (source->destination items) as well as the current IP SLA measurements (e.g., round trip time (RTT), latency, packet loss, etc.).

Reports (tab)
When you click this tab, the Performance Manager Report page is displayed. In the Reports page, you can view the predefined time reports, configure custom report pages and export predefined and custom report pages to PDF and CSV format. Examples of custom reports are Top10 reports, reports of monitored objects with problems, etc.

Homepage

By default, the user's homepage displays the Welcome page and a list of all devices in the system (showing their status). Each Performance Manager user can customize his/her own homepage to contain one or more custom reports (graphs, tables), external web pages (included as HTTP frames) and/or a map on which a user can drag-and-drop icons of devices and monitor their status. User homepages are configured in the same manner as custom report pages.

Export (button)
Exports the homepage report to a PDF document. It can be accessed in the Report page.

Configure (button)
Lets you configure the homepage. User homepages are configured in the same manner as custom Report pages.

Devices page

The Devices page displays all monitored devices included in the currently active user view, the current status of devices, assigned polling engine, and the basic device alarm information (the number of alarms and severity of the most critical alarm associated with the device).

Alarms page

The Alarms page displays all active (open) alarms. New alarms will be automatically added to the Alarms list as they occur (after web page refresh), and the existing alarms will disappear from the list (after web page refresh) when they are cleared.

> **Note 1:** **Alarms** are messages that indicate faults or conditions that could lead to faults on managed devices. An alarm can be **active** or **cleared**. An alarm is active as long as the condition that triggered it is present (e.g., when a managed device does not respond to queries, the "Device is down" alarm is raised and becomes active; when the device starts responding again, the "Device is down" alarm is cleared).
>
> **Note 2:** Only active alarms are displayed in the Alarms page.

Every line in the Alarms list represents one alarm. Alarms provide the following information:

`Time`	Date and time when the alarm occurred
`Description`	Short description of the alarm
`Severity`	Severity of the alarm
`Device`	Name of the device associated with alarm
`Source Info`	Additional information about the source of alarm
`Value`	Value of the threshold variable (for threshold alarms only)

Alarms are colored according to their severity levels:

- Informational (Cyan)
- Warning (Yellow)
- Minor (Dark yellow)
- Major (Orange)
- Critical (Red)

Services page

The Services page displays a list all monitored services on devices by category (DNS, HTTP, IMAP, SSH,…), and a list of services with the status of “critical”. Critical status means that the service is not available. By clicking a service on the list, more detailed statistics for the selected service is displayed (service availability and round trip time (RTT)).

NetFlow page

The NetFlow page displays a list of all configured NetFlow/sFlow source devices (if any) and the Top N NetFlow traffic reports for a configurable time frame for all NetFlow/sFlow sources. By expanding and clicking the individual subentries in the TopN reports (N is configurable), more detailed statistics for the selected item (e.g., device, interface, conversation, application, etc.) is shown.

> **Note:** To enable NetFlow or sFlow monitoring, the source device(s) must be first configured (using a vendor-specific method) to send NetFlow or sFlow packets to Net Inspector polling engine and the source devices must be set as NetFlow source in Net Inspector.

IP SLA page

Here you can monitor various Cisco IP SLA operations. By clicking an item in the first column (RTTMON), you can view more detailed statistics with history for the given IP SLA operation.

Report page

Here you can view the predefined time reports, configure custom report pages and export predefined and custom report pages to PDF and CSV format.

The Report page contains 3 frames:

Custom Pages
Net Inspector Performance Manager lets you configure custom report pages, containing graphs or tables displaying metrics monitored on one or more devices. Examples of such custom reports are Top10 reports, reports of monitored objects with problems, etc.

Time Reports
The Time Reports frame contains a list of predefined fault and performance management reports (e.g., device availability, number of alarms per severity, network interface utilization,…) that are accessible out-of-the-box.

Exports
This frame contains all Custom pages and Time reports that have been exported to PDF format.

Custom Pages Frame

This frame displays a list of user-configured custom page reports and the following buttons:

Remove (button)
Removes the existing report page.

Edit (button)
Lets you edit the existing report (editing is virtually the same as adding).

Add New (button)
Click on this button at the bottom of the frame to add a new custom report page.

Add/Edit custom report page

Report page name

Set custom page title (input line)
After clicking the ***Add New*** button, enter the name of the new report on this input line.

OK (button)
When you have written the name of your new report, click the ***OK*** button.

Custom report page data

Statistics group (drop-down list)

- **General**
  Select the ***General*** entry to be able to select one of the built-in report types for more than one object (Top 5, alarms lists, device status list, devices with problems list) in the next step.
- **Default Statistics**
  Select the ***Default statistics*** item to be able to choose from one of the built-in report pages for one or more devices in the next drop-down list (here, reports for all parameters collected through SNMP and ICMP ping can be selected, like the interface-related statistics, host resources-related statistics, Cisco-related statistics etc.).
- **Custom Statistics**
  To create a report page for custom-made statistics, select the ***Custom statistics*** entry.
- **External HTTP frame**
  To create a report page containing an existing HTTP page on any web site, select the ***External HTTP frame*** item.

Statistics (drop-down list)

Depending on the entry you have selected in the ***Statistics group*** drop-down list, a different set of options is available in the ***Statistics*** drop-down list. Select the desired statistics from this drop-down list.

If you chose the ***General*** statistics group you have the following statistics available:

- Alarms
- Top5
- Top10
- Top20
- Device Status
- Devices with problems
- Device Map
- Response Time
- Current Response Time
- Current Packet Loss

If you have selected the ***Default Statistics*** group, you can further select among the following statistics:

- Device status, response time and packet loss statistics:
  - Response time
  - Packet loss
- Network interfaces traffic, errors and status statistics:
  - Interface input octets
  - Interface output octets
  - Interface input packets
  - Interface output packets
  - Interface input utilization
  - Interface output utilization
  - Interface input traffic
  - Interface output traffic
  - Interface input average packet size
  - Interface output average packet size
  - Interface input average packet rate
  - Interface output average packet rate
  - Interface admin status
  - Interface operation status
  - Interface input discards
  - Interface output discards
  - Interface input errors
  - Interface output errors
  - Interface input unknown protocols
  - Interface input error rate
  - Interface output error rate
  - Interface input discard rate
  - Interface output discard rate
- Host resources statistics:
  - Number of users

- Number of processes
- Memory used
- CPU Load
- Storage usage

- Cisco statistics:
  - CPU Load
  - Used memory
  - Free memory
  - Largest number of contiguous free bytes
  - Interface in traffic rate
  - Interface in packet rate
  - Interface out traffic rate
  - Interface out packet rate
  - Interface in queue drops
  - Interface out queue drops
  - Round trip time
  - Jitter source-to-destination
  - Jitter destination-to-source
  - Packet loss source-to-destination
  - Packet loss destination-to-source
  - Latency destination-to-source
  - Mean opinion score (MOS)
  - Packets out of sequence
  - Packet loss unknown direction (MIA)
  - Packet arrived after the timeout (late arrival)
  - Echo round trip time
  - Path echo round trip time
  - TCP round trip time
  - DNS round trip time
  - DLSW round trip time
  - DHCP round trip time
  - FTP round trip time
  - HTTP round trip time
  - HTTP round trip time (DNS part)
  - HTTP round trip time (TCP connection part)
  - HTTP round trip time (transaction part)
  - Completion status

- Running processes statistics
  - Process running status
  - Process CPU load
  - Process memory usage

- Service availability
  - Availability of service

If you have selected the ***External HTTP Frame*** option, you can create a report page containing an existing HTTP page on any web site.

Depending on the selected statistics, you need to configure some or all of the following settings:

Data value (drop-down list)
Here you choose the value data to be shown: **Average/Raw**, **Min** or **Max**.

Object Label (input line)
Specify the name (label) for the given custom report page object (note that report pages can contain more than one object).

Time period (drop-down list)
Select the time period for which the data in the report will be included.

Sample interval (drop-down list)
Select the sample interval for which the data in the report will be included.

View type (drop-down list)
Here you can select the ***Data Table*** entry to present the data in form of a table, the ***Graph*** (if applicable) to show values in a graph, the ***Pie Graph*** (if applicable) to present the results in a pie graph or the ***Gauge Graph*** (if applicable) to render the results in a gauge graph.

Width in % (drop-down list)
Select the desired width of the object, as it will appear in the report page.

Graph scale (drop-down list)
This option appears only if you have selected the ***Graph*** option in the ***View type*** drop-down list.
Choose between the **linear** or **logarithmic** scales for graphs.

Graph type (drop-down list)
Here you can decide between ***Line*** or ***Area*** graph types.

This option appears only if you have selected the ***Graph*** option in the ***View type*** drop-down list.

Graph color (input line, color choosing dialog)
Here you can choose a color for the graph line or area. You can choose via a dialog, or you can write the HTML color code in the input line.

This option appears only if you have selected the ***Graph*** option in the ***View type*** drop-down list.

Records per page (input line and checkbox)
Enter the number of records per page, or check the checkbox if you do not want a limit.

This option appears only if you have selected the ***Data table*** option in the ***View type*** drop-down list.

Device (drop-down list or multiple-choices list)
Here you can select for which device(s) you want the data in the report.

Interface (drop-down list)
Pick the interface you want monitored.

MIN Severity (drop-down list)
This drop-down list lets you choose the minimal severity level reported in this report. You can choose between:

- Informational
- Warning
- Minor
- Major
- Critical

TopN group (drop-down list)
Here you can select from which statistics you want to view the top5 report. You have the following choices:

- Cisco statistics
- Host resources statistics
- Network interfaces traffic, errors and status statistics

TopN statistics (drop-down list)
Depending on the entry you have selected in the ***TopN group*** drop-down list, a different set of options is available in the ***TopN statistics*** drop-down list. Select the desired statistics from this drop-down list.

If you selected ***Cisco statistics*** you have the following options:

- Jitter destination-to-source
- Jitter source-to-destination
- Mean opinion score
- Packet loss destination-to-source
- Packet loss source-to-destination
- Round trip time

If you chose ***Host resources statistics*** you can select:

- CPU Load
- Memory used
- Storage usage

If you have selected ***Network interfaces traffic, errors and status statistics*** you can choose between:

- Interface input traffic
- Interface input utilization
- Interface output traffic
- Interface output utilization

Map image filename (drop-down list)
Here you can select an image file for a map report.

Upload map image (input line)
If you want to upload an image the path to it must be entered here. You can enter it manually or find it with the open file dialog by clicking the ***Browse...*** button.

Browse... (button)
If you click this button the standard Open dialog box appears, where you can choose an image, you want to upload.

Upload (button)
When you click this button the image you have written the path to or have selected in the open file dialog will be uploaded.

Add (button)
When you are done choosing what you would like to have in the report click this button to add it.

Custom report finalization

Here you can see all the objects you want in the report. You can delete the objects you don't want, add new ones, edit existing ones, move them up or down with these controls:

Delete object (button)
This button enables you to delete existing objects.

Edit object (button)
This button enables you to edit existing objects.

Delete row (button)
This button lets you delete a whole row (more than one object can be in one row).

Move down (button)
Moves the row down.

Move up (button)
Moves the row up.

View (button)
When you click this button you go to the report page where you see the report you have created/edited.

Exports

This frame contains all Custom pages and Time reports that have been exported by users to PDF format.

Remove (button)
Removes the existing PDF report from the frame.

Time Reports Frame

The Time Reports frame contains a list of predefined fault and performance management reports (e.g., device availability, number of alarms per severity, network interface utilization,…) that are accessible out-of-the-box. The user can select the desired time interval (e.g., day, week, month, quarter, year,…) for any of the

predefined reports and the results are displayed in a tabular format either for all managed devices or only for a subset of devices specified by a filter. Results can be sorted by any column included in reports (e.g., device name, availability, number of alarms, discarded packets, min. and max. values, etc.). Predefined reports can be exported to PDF and CSV (comma-separated values) file formats for external viewing or post-processing.

The **Time reports** frame in the **Reports** page contains a list of predefined reports in different categories (e.g., Interfaces, Host resources, Services, etc.). Click the category name to view all time reports that belong to it. The categories are:

- Status: device availability, response time and packet loss reports
- Fault: fault management reports (number of alarms per severity, alarm duration and frequency, etc.)
- Interfaces: network interface-related reports (input/output utilization, traffic, error rate, etc.)
- Host resources: system resources usage reports (CPU, memory, storage volumes)
- Processes: monitored processes reports (process running status, CPU usage, memory usage)
- Services: service availability, service round trip time (RTT)
- NetFlow: user-selectable NetFlow/sFlow statistics (TopN repots, NetFlow categories (applications, receivers, transmitters, protocols,…), NetFlow sources (all, specific), network interfaces (all, specific)).
- Cisco: Cisco-specific resources usage reports (memory, interfaces) and Cisco IP SLA-specific reports (round trip times for ICMP, HTTP, DNS, VoIP jitter, VoIP MOS, etc.)
- NetFlow: NetFlow/sFlow reports (TopN applications, transceivers, protocols, conversations or countries for the selected router (or all routers) and interface (or all interfaces))

Optionally, use the ***Search*** facility in the right portion of the ***Time Reports*** frame to quickly find the reports that math the entered search phrase. Click the report you want to view in the ***Time Reports*** frame.

The selected report is displayed for the previous day time frame. You can sort the report items by any column (e.g., device name, value, min., max. value) by clicking the sort symbol ( ) in the respective column.

To view the report for a different time frame, select the desired category from the **Time interval** toolbar drop-down list (e.g., day, week, month, quarter, year etc.) and optionally shift the displayed time frame forward or backward by clicking the arrow buttons ( ) in the **Time interval** toolbar. When the desired time interval for the report is selected, click the ***Apply*** button in the right section of the **Time interval** toolbar to update the report to include the data for the new time interval.

11.3.3 Status bar

Status bar displays the name of the managed object whose performance statistics are displayed, and the URL of the Performance Manager web page currently displayed.

12 CREATE FILTER DIALOG BOX

12.1 Purpose

It is used for creating filters for displaying specific active alarms in the Events window. Filtered list of alarm is dynamic (i.e., new alarms appear on the list and cleared alarms disappear from the list (by default) over time), as opposed to the static list of alarms/events displayed by the Find Events operation.

12.2 Opening

To open the Create Filter dialog box, select the ***Event / Create Filter*** command.

12.3 Description

The Create Filter dialog box lets you create a display filter that will show only those active alarms that match the filter conditions. Filtered alarms are displayed in a separate tab in the Events window. The list of filtered alarms dynamically changes over time, i.e., new alarms that match the filter criteria are added to the list when they are triggered, and by default, automatically cleared alarms disappear from the list (while manually cleared alarms stay on the list).

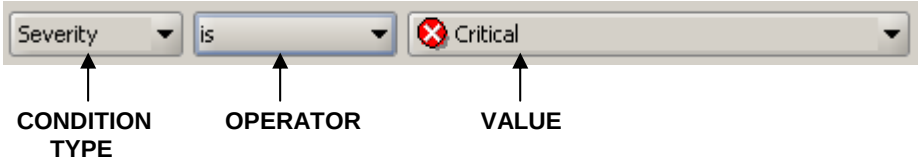
The Create Filter dialog box contains a toolbar that lets you create filter conditions and add them to the filter one-by-one, while the central section of the dialog box (Conditions panel) displays the entire filter consisting of filter conditions and relations between them. The Conditions panel displays a filter in form of a hierarchical tree, where the filter conditions are connected with logical operators (AND, OR) and can be grouped into branches.

Filter conditions can be specified by using the following controls in the Create Filter dialog box:

Name (input line)

Lets you enter the filter name. This is also the name of a tab in the Events window in which the filtered results will be displayed.

New condition (toolbar)



This toolbar lets you create a filter condition by selecting the condition type, operator and value from the corresponding drop-down lists. Once the condition is configured, you can add it to the filter by clicking the ***Add*** button in the right section of the Create Filter dialog box. Added conditions appear in the Conditions panel below the New condition toolbar.

Condition type (drop-down list)
Specifies the type of the condition. You can select among the following types of conditions:

- **Severity**
  Specifies the severity level of the alarm. If this condition type is selected, you can choose the alarm severity level from the ***Value*** drop-down list (e.g. “Critical”, “Major”, etc.).

- **Source**
  Uniquely identifies the object, which has triggered the alarm. This condition type lets you search for objects by their object IDs (note that different objects can have the same name, however, all objects have unique object IDs). If this type of condition is selected, click the (**…**) ***Browse*** button next to the ***Value*** field to open the **Select Source** dialog box. The **Select Source** dialog box displays two panels; the left panel contains the expandable map tree, while the panel on the right displays all objects included in the map that is selected in the left panel. The left panel also displays some properties of the listed objects, including their object IDs. To select a **Source** object (and thus its ID), click the relevant map in the left panel, choose the object on the right panel and click the ***OK*** button. Alternatively, you can select one or more objects in the Maps window and then open the Create Filter dialog box. This will automatically create filter conditions for selected source objects.

- **Source name**
  Specifies the name of the object (as displayed on the workspace), which has triggered the alarm. If this condition type is selected, you can enter the name of the object into the ***Value*** input line. Note, however, that two or more objects can have the same name. Use the **Source** condition type to uniquely specify the source in such case.

- **Source info**
  Specifies additional information about the problem (as displayed in the ***Source Info*** column in the Events window). If this condition type is selected, you can enter additional information about the object into the ***Value*** input line (e.g., “Processor:#1”).

- **Source type**
  Specifies the type of the object, which has triggered the alarm. If this condition type is selected, you can choose the type of the object from the ***Value*** drop-down list (e.g. “IP”, etc.).

- **Message**
  A short description of the alarm. If this condition type and the operator “is” or “is not” is selected, you can choose a message from the list of all messages in the ***Value*** drop-down list (e.g. “Device is down”). If this condition type and the operator “contains” is selected, you can enter a text string (e.g., “Dev”) into the ***Value*** input line to find all alarms whose message field contains the specified character(s).

- **Cause**
  Specifies the cause of the alarm. If this condition type is selected, you can choose a cause from the ***Value*** drop-down list (e.g. “Lan Error”).

- **Type**
  Specifies the type of the alarm. If this condition type is selected, you can choose an alarm type from the ***Value*** drop-down list (e.g. “Communication”).

- **Event state**
  Specifies the state of the alarm or event. If this condition type is selected, you can choose an event or alarm state from the ***Value*** drop-down list (e.g. "ACKNOWLEDGED" or "MANUALLY CLEARED" or "UNCLEARED", etc.).
- **(Un)Acknowledge time**
  Specifies the date and time of acknowledging or unacknowledging the alarm or event. If this condition type is selected, you can enter the desired date and time into the ***Value*** input line, using the date and time formatting as configured in the user preferences (e.g., "Sep 12, 2008 12:45:12 PM").
- **(Un)Clear time**
  Specifies the date and time of clearing or unclearing the alarm or event. If this condition type is selected, you can enter the desired date and time into the ***Value*** input line, using the date and time formatting as configured in the user preferences (e.g., "Sep 12, 2008 12:45:12 PM").
- **Event state info**
  Specifies who has changed the state of the alarm or event as last. This can be either a user that has managed alarm (e.g., acknowledged, unacknowledged, manually cleared, uncleared) or the "Auto" if the alarm has been automatically cleared by the system. When specifying a user, you can also specify the location (IP address) of the user who has managed the alarm in square brackets (e.g., operator [192.168.10.120]). If this condition type is selected, you can enter an event state info into the ***Value*** input line (e.g. "admin [192.168.10.123]" or "Auto", etc.).

Operator

Lets you select the operator, e.g., "is", "is not", "contains", "is greater or equal", "is smaller or equal", etc. Available operators depend on type of the condition selected.

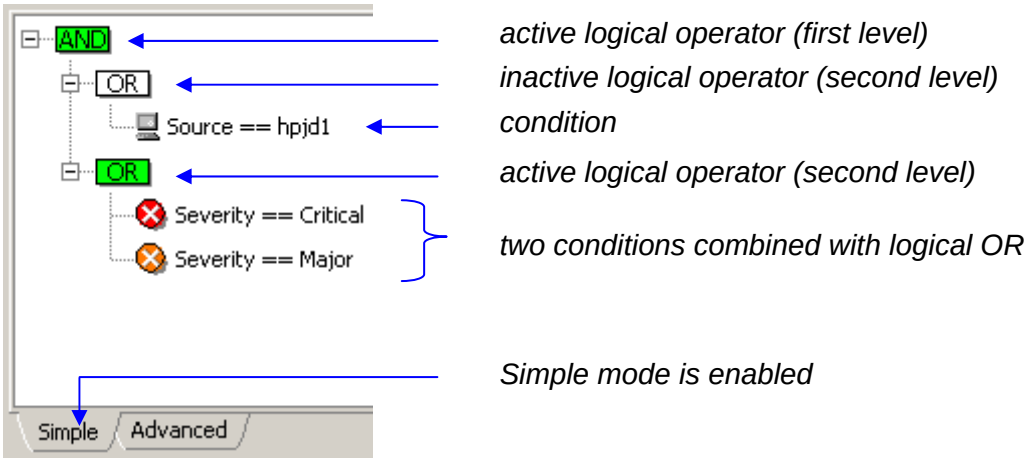
Value

Lets you enter or select the condition value. Available (and valid) values depend on the type of the condition selected.

Conditions (panel):

The **Conditions panel** displays and lets you re-configure existing filter conditions, and logical operators connecting them.

Example of the Conditions panel contents:



Expression equivalent to the filter displayed above would be:

Source=hpjd1 AND (Severity=Critical OR Severity=Major)

Meaning: Show all alarms triggered by ‘hpdj’ object, whose severity levels are either Critical or Major

Simple and Advanced Mode

Conditions panel contains two tabs providing two modes of operation: Simple and Advanced.

The **Simple mode**, which is enabled by default, lets you create filters in a straightforward manner: you only add filter conditions to the Conditions panel and the program automatically groups conditions of the same type and connects them with logical OR operator, while conditions of a different type are connected with logical AND operator. For example, if you add two conditions of the same type (e.g., “severity=critical” and “severity=major”), they will be combined with the logical OR operator, meaning that the filter will let trough alarms that satisfy either one or the other condition (i.e., it will let trough all ‘critical’ alarms and all ‘major’ alarms). If you, on the other hand, add two conditions of different types (e.g., “severity=critical” and “message=device is down”), they are connected with the logical AND operator, meaning that the filter will let trough only those alarms that satisfy both conditions at the same time.

The Simple mode does not let you manipulate logical operators, it only lets you configure and add filter conditions to the filter. This mode also does not allow combining different types of filter conditions with the logical OR operator.

The **Advanced mode**, which can be enabled by clicking the Advanced tab in the Create Filter dialog box, lets you create much more complex filters than the Simple mode, as it imposes no restrictions on combing filter conditions or using logical operators.

In advanced mode, you can double-click any logical operator in the hierarchical filter tree and change it from AND to OR, or vice-versa. Furthermore, you can add new logical operators to the selected filter subtree by clicking the ***AND*** or ***OR*** buttons located in the right hand-side of the dialog box and then add new conditions as child items to those operators. This way, you can create complex filters that comprise more than two hierarchical levels, which the Simple mode of operation is restricted to.

Switching Between Modes

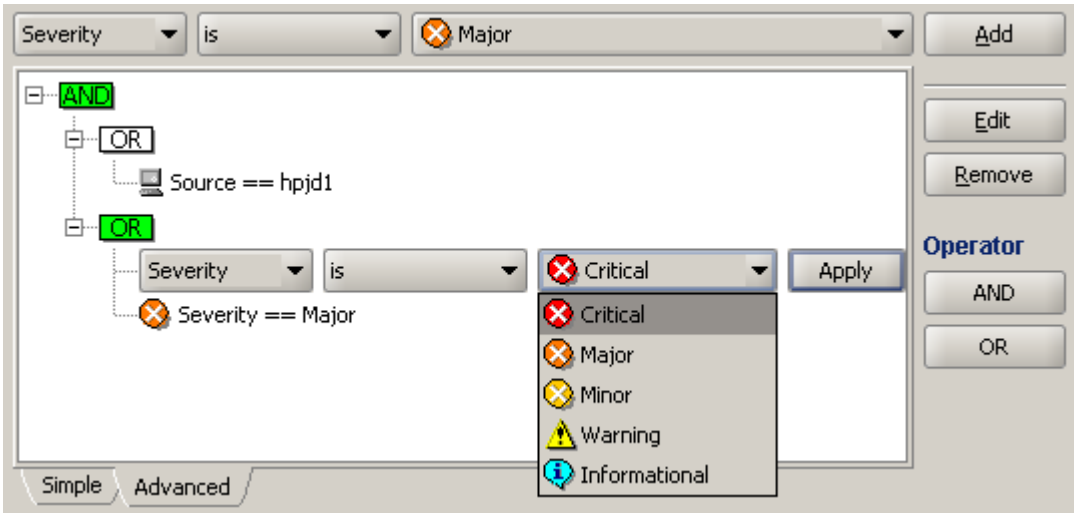
To select desired mode of operation, click the corresponding tab (Simple, Advanced) in the Conditions panel.

You can switch to another mode even while you are already creating a filter, and then continue creating it in another mode; however, with some restrictions. While you can always switch from Simple to Advanced mode, you cannot switch from Advanced to Simple mode if the filter you are currently creating in Advanced mode does not match the simple filter scheme (max. two levels of logical operators: AND operator on the first level, OR operator(s) on the second level, conditions of the same type are grouped together under the same OR operator on the second level). In such case, you need to edit the filter to match the simple filter scheme or delete it.

Editing Conditions

To edit an existing condition, simply double-click it in the Conditions panel or select it and click the ***Edit*** button in the right section of the dialog box.

Example: Editing a filter condition (Advanced mode):



The selected condition will be displayed in editable form, where you can select new entries from the drop-down lists or edit the value in the ***Value*** input line (depending on the condition type). Click the ***Apply*** button in the Conditions panel to apply the changes after you finish editing the condition.

> **Note:** The Simple mode lets you change only the operator and value (not also the condition type) when editing a condition in the Conditions panel.

To edit an existing logical operator (Advanced mode only), simply double-click it in the Conditions panel or select it and click the ***Edit*** button in the right section of the dialog box. This displays the drop-down list from which you can select another logical operator.

> **Note:** In the Conditions panel, green logical operators are active and the white operators are inactive (see the picture above). Only active operators are in effect. A logical operator is active if it has at least two (directly or indirectly) subordinated conditions in the hierarchical filter tree.

Buttons:

- **Add**
  Adds the condition from the New condition toolbar to the Conditions panel. In Advanced mode the condition is added to the selected branch in the filter tree.
- **Edit**
  Lets you edit the selected condition or operator. Operators can be modified only in Advanced mode.
- **Remove**
  Removes the selected condition or operator (and all its child objects) from the Conditions panel.

- **AND**
  Adds the logical AND operator to the selected filter branch. This button is enabled only in Advanced mode.
- **OR**
  Adds the logical OR operator to the selected filter branch. This button is enabled only in Advanced mode.
- **Import**
  Opens the Import dialog box, which lets you select a previously saved filter and import it into Create Filter dialog box (Conditions panel). The Import dialog box lets you select the filter either from the “My filters” repository (which contains all previously saved display and search filters), from the “Action filters” repository (which contains all action filters available in the Manage Action Filters dialog box) or from a file (filters that have been saved to a file in previous versions of Net Inspector).
- **OK**
  Applies the filter and display the filtered alarms in a new tab in the Events window.
- **Cancel**
  Discards all changes and closes the Create Filter dialog box.

13 FIND EVENTS DIALOG BOX

13.1 Purpose

It is used for searching for alarms and events.

13.2 Opening

To open the Find Events dialog box, select the ***Event / Find Events*** command or click the  ***Find*** button in the Events window.

13.3 Description

The Find Events dialog box lets you search for those alarms or events that match the search filter. Search filters are configured in the same manner as display filters in the Create Filter dialog box. The result of a search operation is displayed in a separate tab in the Events window. A search filter can be created by using the following controls in the Find Events dialog box:

Name (input line)
Specifies the name of the Events window tab to display the search results in. If any object is selected in the Maps window before you open the Find Events dialog box, this input line contains the name(s) of the selected object(s).

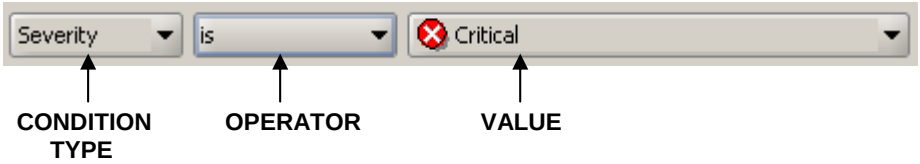
Time frame (drop-down list)
Lets you select a time period for the search operation (i.e., Today, This week, This month, User defined). The search operation will look only for those alarms/events that have been triggered within the specified time frame.

From – To (input lines)
These input lines display the start and end date and time for the search operation, depending on the entry selected in the **Time frame** drop-down list. If the "User defined" option is selected in the **Time frame** drop-down list, you can specify an arbitrary time frame for the search operation by entering the start and end date and time into the **From** and **To** input lines. The search operation will look only for those alarms/events that have been triggered within the specified time frame. The **From** an **To** date and time values are formatted according to the setting of the ***Date/Time format*** parameter in the Client Preferences dialog box.

Search in (radio buttons):

- **Active Alarms**
  Enables searching for active alarms only.
- **All Alarms**
  Enables searching for all alarms (active and cleared).
- **Events**
  Enables searching for events.

New condition (toolbar)



This toolbar lets you create a search condition by selecting the condition type, operator and value from the corresponding drop-down lists. Once the condition is configured, you can add it to the search filter by clicking the ***Add*** button in the right section of the Find Events dialog box. Added conditions appear in the Conditions panel below the New condition toolbar.

Condition type (drop-down list)
Specifies the type of the condition. You can select among the following types of conditions:

- **Severity**
  Specifies the severity level of the alarm or event. If this condition type is selected, you can choose the severity level from the ***Value*** drop-down list (e.g. "Critical", "Major", etc.).
- **Source**
  Uniquely identifies the object, which has triggered the alarm or event. This condition type lets you search for objects by their object IDs (note that different objects can have the same name, however, all objects have unique object IDs). If this type of condition is selected, click the (**…**) ***Browse*** button next to the ***Value*** field to open the **Select Source** dialog box. The **Select Source** dialog box displays two panels; the left panel contains the expandable map tree, while the panel on the right displays all objects included in the map that is selected in the left panel. The left panel also displays some properties of the listed objects, including their object IDs. To select a source object (and thus its ID), click the relevant map in the left panel, choose the object on the right panel and click the ***Select*** button. Alternatively, you can select one or more objects in the Maps window and then open the Find Events dialog box. This will automatically create conditions for finding alarms/events triggered by the selected source objects.
- **Source name**
  Specifies the name of the object (as displayed on the workspace), which has triggered the alarm or event. If this condition type is selected, you can enter the name of the object into the ***Value*** input line. Note, however, that two or more objects can have the same name. Use the **Source** condition type to uniquely specify the source in such case.
- **Source info**
  Specifies additional information about the problem (as displayed in the ***Source Info*** column in the Events window). If this condition type is selected, you can enter additional information about the object into the ***Value*** input line (e.g., "Processor:#1").
- **Source type**
  Specifies the type of the object, which has triggered the alarm or event. If this condition type is selected, you can choose the type of the object from the ***Value*** drop-down list (e.g. "IP", etc.).

- **Message**
  A short description of the alarm or event. If this condition type and the operator “is” or “is not” is selected, you can choose a message from the list of all messages in the ***Value*** drop-down list (e.g. “Device is down”). If this condition type and the operator “contains” is selected, you can enter a character string (e.g., “Dev”) into the ***Value*** input line to find all alarms whose message field contains the specified character(s).
- **Cause**
  Specifies the cause of the alarm or event. If this condition type is selected, you can choose a cause from the ***Value*** drop-down list (e.g. “Lan Error”).
- **Type**
  Specifies the type of the alarm or event. If this condition type is selected, you can choose an event type from the ***Value*** drop-down list (e.g. “Communication”).
- **Event state**
  Specifies the state of the alarm or event. If this condition type is selected, you can choose an event or alarm state from the ***Value*** drop-down list (e.g. “ACKNOWLEDGED” or “MANUALLY CLEARED” or “UNCLEARED”, etc.).
- **(Un)Acknowledge time**
  Specifies the date and time of acknowledging or unacknowledging the alarm or event. If this condition type is selected, you can enter the desired date and time into the ***Value*** input line, using the date and time formatting as configured in the user preferences (e.g., “Sep 12, 2008 12:45:12 PM”).
- **(Un)Clear time**
  Specifies the date and time of clearing or unclearing the alarm or event. If this condition type is selected, you can enter the desired date and time into the ***Value*** input line, using the date and time formatting as configured in the user preferences (e.g., “Sep 12, 2008 12:45:12 PM”).
- **Event state info**
  Specifies who has changed the state of the alarm or event as last. This can be either a user that has managed alarm (e.g., acknowledged, unacknowledged, manually cleared, uncleared) or the “Auto” if the alarm has been automatically cleared by the system. When specifying a user, you can also specify the location (IP address) of the user who has managed the alarm in square brackets (e.g., operator [192.168.10.120]). If this condition type is selected, you can enter an event state info into the ***Value*** input line (e.g. “admin [192.168.10.123]” or “Auto”, etc.).

Operator

Lets you select the operator, e.g., “is”, “is not”, “contains”, “is greater or equal”, “is smaller or equal”, etc. Available operators depend on type of the condition selected.

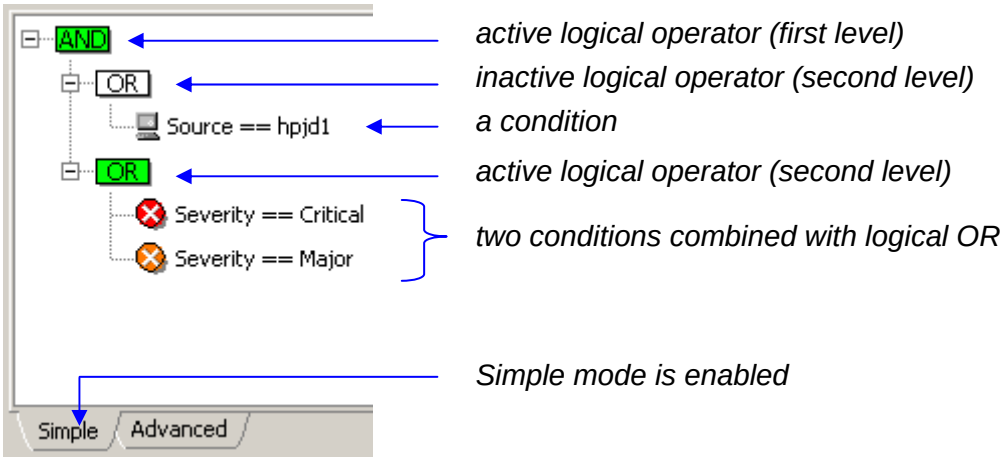
Value

Lets you enter or select the condition value. Available (and valid) values depend on the type of the condition selected.

Conditions (panel):

The **Conditions panel** displays and lets you re-configure existing search conditions, and logical operators connecting them.

Example of the Conditions panel contents:



Expression equivalent to the search criteria (search filter) displayed above would be:
Source=hpjd1 AND (Severity=Critical OR Severity=Major)

Meaning: Find all alarms/events triggered by 'hpdj' object, whose severity levels are either Critical or Major

Simple and Advanced Mode

Conditions panel contains two tabs providing two modes of operation: Simple and Advanced.

The **Simple mode**, which is enabled by default, lets you create a search filter in a straightforward manner: you only add search conditions to the Conditions panel and the program automatically groups conditions of the same type and connects them with logical OR operator, while conditions of a different type are connected with logical AND operator. For example, if you add two conditions of the same type (e.g., "severity=critical" and "severity=major"), they will be connected with logical OR, meaning that the combined criteria will find alarms/events that satisfy either the first or the second condition (i.e., it will find all 'critical' alarms and all 'major' alarms). If you, on the other hand, add two conditions of different types (e.g., "severity=critical" and "message=device is down"), they are connected with logical AND, meaning that only those alarms/events that satisfy both conditions at the same time will be found.

The Simple mode does not let you manipulate logical operators, it only lets you configure and add conditions to the Conditions panel. This mode also does not allow connecting different types of conditions with the logical OR operator.

The **Advanced mode**, which can be enabled by clicking the Advanced tab, lets you create more complex search filters (criteria) than the Simple mode, as it imposes no restrictions on combing search conditions or using logical operators.

In advanced mode, you can double-click any logical operator in the hierarchical filter tree and change it from AND to OR, or vice-versa. Furthermore, you can add new logical operators to the selected filter subtree by clicking the ***AND*** or ***OR*** buttons located in the right hand-side of the dialog box and then add new conditions as child items to those operators. This way, you can create complex search filters that spread over more than two hierarchical levels, which the Simple mode of operation is restricted to.

Switching Between Modes

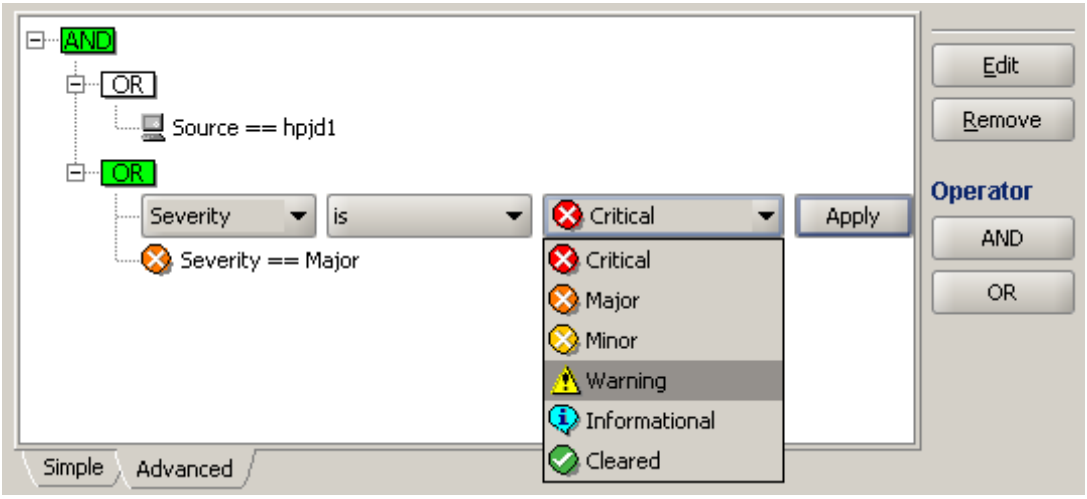
To select desired mode of operation, click the corresponding tab (Simple, Advanced) in the Conditions panel.

You can switch to another mode even while you are already creating a search filter, and then continue creating it in another mode; however, there are some restrictions. While you can always switch from Simple to Advanced mode, you cannot switch from Advanced to Simple mode if the current filter does not match the simple filter scheme (max. two levels of logical operators: AND operator on the first level, OR operator(s) on the second level, conditions of the same type are grouped together under the same OR operator on the second level). In such case, you need to edit the search filter to match the simple filter scheme or delete it.

Editing Conditions

To edit an existing condition, simply double-click it in the Conditions panel or select it and click the ***Edit*** button in the right section of the dialog box.

Example: Editing a condition (Advanced mode):



The selected condition will be displayed in editable form (see the picture above), where you can select new items from the drop-down lists or edit the value in the ***Value*** input line. For description of available condition types, operators and values, kindly refer to the New condition toolbar description. Click the ***Apply*** button in the Conditions panel to apply the changes after you finish editing the condition.

> **Note:** The Simple mode does not lets you change the condition type when editing a condition in the Conditions panel.

To edit an existing logical operator (Advanced mode only), simply double-click it in the Conditions panel or select it and click the ***Edit*** button in the right section of the dialog box. This displays the drop-down list from which you can select another logical operator.

> **Note:** In the Conditions panel, green logical operators are active, while white operators are inactive (see the picture above). Only active operators are in effect. A logical operator is active if it has at least two (directly or indirectly) subordinated conditions in the hierarchical filter tree.

Buttons:

- **Add**
  Adds the condition from the New condition toolbar to the Conditions panel. In Advanced mode the condition is added to the selected branch in the filter tree.
- **Edit**
  Lets you edit the selected condition or operator. Operators can be modified only in Advanced mode.
- **Remove**
  Removes the selected condition or operator (and all its child objects) from the Conditions panel.
- **AND**
  Adds the logical AND operator to the selected filter branch. This button is enabled only in Advanced mode.
- **OR**
  Adds the logical OR operator to the selected filter branch. This button is enabled only in Advanced mode.
- **Import**
  Opens the Import dialog box, which lets you select a previously saved filter and import it into Find Events dialog box (Conditions panel). Note that only the filter conditions can be imported (the search time frame is never saved or imported along with the filter). The Import dialog box lets you select the filter either from the "My filters" repository (which contains all previously saved display and search filters), from the "Action filters" repository (which contains all action filters available in the Manage Action Filters dialog box) or from a file (filters that have been saved to a file in previous versions of Net Inspector).
- **Find**
  Starts the search operation and closes the Find Events dialog box. Search results are displayed in a separate tab in the Events window. The search progress bar at the bottom of this tab moves from left to right and vice-versa, until the search operation is finished. To abort the search operation, click the  button in the Events window.

  Note: To modify the search conditions after the search operation has been started, select the tab in the Events window where the results of this search operation are displayed and use the ***Events / Modify Filter*** command. The Find Events dialog box will reappear listing all the conditions that were used in the initial/previous search operation. After modifying the search conditions, click the ***Find*** button again. The old research results will be deleted and new search results will be displayed in the same tab of the Events window.

- **Cancel**
  Discards all changes and closes the Find Events dialog box without starting the search operation.

14 MANAGE EVENT ATTRIBUTES DIALOG BOX

14.1 Purpose

This dialog box is used for viewing and managing certain event/alarm attributes, i.e., event message, probable cause and event type attributes.

14.2 Opening

To open the Manage Event Attributes dialog box click the ***Manage Messages*** button in the New/Edit Trap-To-Alarm dialog box, second screen.

14.3 Description

This dialog box has the same general appearance and is used in the same way as the Event Attributes Panel.

15 MANAGE ACTION FILTERS DIALOG BOX

15.1 Purpose

It is used for viewing and managing action filters. Action filters can be applied to action objects to restrict their functionality so that only events that match the filter conditions will carry out the given action.

15.2 Opening

To open the Manage Action Filters dialog box, click the ***Manage Action Filters*** button in the Filters view of the action object's Properties window.

15.3 Description

This dialog box has the same general appearance and is used in the same way as the Action Filters Panel.

16 NETWORK DISCOVERY WIZARD

16.1 Purpose

The Network Discovery Wizard lets you configure the settings for and start the network discovery operation in a few guided steps. The network discovery operation can discover the devices and topology of your network and automatically add discovered devices as managed objects to Net Inspector configuration and map(s). Net Inspector starts automatically monitoring the added managed objects.

16.2 Opening

To display the first screen of the Network Discovery Wizard, select the ***Tools / Discovery Wizard*** command or click the  ***Discovery Wizard*** toolbar button.

The Network Discovery wizard is also started automatically when the administrator connects to the Net Inspector Server for the first time after a fresh installation of Net Inspector (when there are no managed objects in the configuration yet).

16.3 Description

Net Inspector incorporates an advanced network discovery feature that can discover devices and topology of your network in an automated fashion, based on your input. The Network Discovery Wizard helps you configure the settings for and start the network discovery operation in a few steps. The wizard contains these controls:

Back (button)
Go to the previous step of the Network Discovery Wizard.

Next (button)
Proceed to the next step of the Network Discovery Wizard.

Start Discovery (button)
Starts the network discovery operation after you have configured all the necessary settings. While the discovery operation is running, the `Discovery is running` message and a progress bar is displayed in the status bar of the Net Inspector Client main window. To view the intermediate results (discovered devices and subnets) of the discovery operation, select the ***Tools / Discovery Panel*** command to display the Discovery Panel dialog box and open the relevant discovery operation in it. When the discovery operation finishes, the newly discovered devices are automatically added to the maps (selected user view).

Cancel (button)
Closes the Network Discovery Wizard without starting the discovery operation.

Welcome Screen (Step 0)

This screen introduces you to the Network Discovery Wizard and describes its steps.

Specify SNMP Profile(s) (Step 1)

In the first step of the Network Discovery wizard you can manage and select the SNMP access profiles that will be used for discovering the network devices. Please note that the SNMP access profile with which a device has been discovered, is automatically assigned to that device, so Net Inspector Server will use it to poll that device.

SNMP profiles (list)

Lists available SNMP access profiles. Note that the order in which the enabled profiles are listed is important. First, the top-listed profile will be used for discovering the network, then the second profile from the top will be used, etc. To move a profile up or down on the list, select it and click the ***Up*** or ***Down*** button next to this list, respectively. The order of the SNMP access profiles also determines which profiles will be assigned to discovered devices and affects the duration of the discovery operation (if a device can be successfully queried using the first profile on the list, this profile will be assigned to the managed object, and the remaining profiles won't be used for discovering that device).

To not use a specific SNMP profile in discovery, uncheck the ***Use*** checkbox in front of its name.

Each SNMP profile is displayed in one row, comprised of the following columns:

Use (checkbox)
If this checkbox is checked, the corresponding SNMP access profile will be used for discovering the network.

Name
The name of the SNMP access profile.

Version
The SNMP version used in the profile.

Description
The description of the SNMP profile.

You can click on any column header (Name, Version and Description) to sort the profiles by that column.

Add (button)
Opens the New SNMP access Profile dialog box, which lets you create and configure a new SNMP access profile.

Edit (button)
Opens the Edit SNMP access Profile dialog box, which lets you edit the selected SNMP access profile.

Delete (button)
Deletes the selected SNMP access profile (if not in use).

Up (button)
Moves the selected SNMP access profile up on the list.

Down (button)
Moves the selected SNMP access profile down on the list.

Exports (button)
Opens the Export Profile where you can save the selected SNMP access profiles to the XML file.

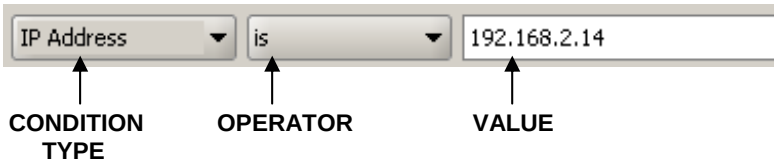
Import (button)
Opens the Import Profile dialog box where you can select the previously exported file containing the SNMP profiles you want to import.

Configure Discovery Filter (Step 2)

In the second step of the Network Discovery Wizard you can optionally select or configure a discovery filter that will narrow down the discovery results by filtering out devices that do not match the filter criteria (e.g., device IP address, type, class, vendor, etc.).

Discovery filter (drop-down list)
Lets you select an existing filter.

New condition (toolbar)



This toolbar lets you create a filter condition by specifying the condition type, operator and value from the corresponding drop-down lists/input lines. Once the condition is configured, you can add it to the filter by clicking the ***Add*** button in the right section of the dialog box. Added conditions appear in the Conditions panel below the New condition toolbar.

Condition type (drop-down list)
Specifies the type of the condition. You can select among the following types of conditions:

- **IP address**
  If this condition type is selected, you can enter the IP address of the managed object into the value input line.
- **IP address range**
  If this condition type is selected, you can enter the IP address range into the accompanying ***From*** and ***To*** input lines.
- **Object type**
  If this condition type is selected, you can choose a type of the managed object from the ***Value*** drop-down list (e.g. “IP”, etc.).
- **Class**
  If this condition type is selected, you can select a class of the managed object from the ***Value*** drop-down list (e.g., “Workstation”).
- **Location**
  If this condition type is selected, you can enter the object location into the ***Value*** input line (e.g., “MG-SOFT Headquarters”).

- **Vendor**
  If this condition type is selected, you can enter the device vendor into the ***Value*** input line (e.g., “MG-SOFT”).
- **Vendor OID**
  If this condition type is selected, you can enter the device vendor OID into the ***Value*** input line (e.g., “1.3.6.1.4.1.1315).

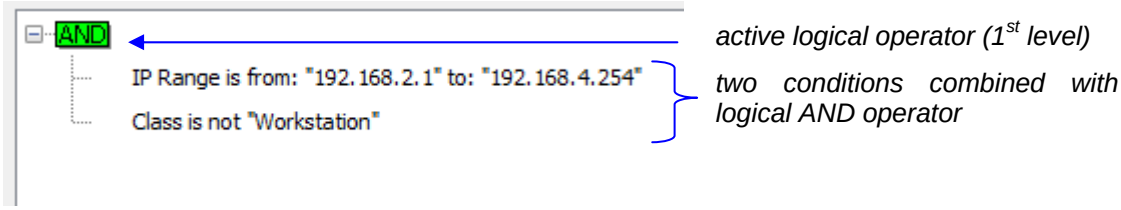
Operator
Lets you select the operator, e.g., “is”, “is not” or “contains”. Available operators depend on the type of condition selected.

Value
Lets you select or enter the condition value. Available (and valid) values depend on the type of condition selected.

Conditions (panel):

The **Conditions panel** displays and lets you re-configure existing filter conditions, and logical operators connecting them.

Example of the Conditions panel contents:



Editing Conditions
For more information about editing existing conditions, please consult the corresponding description of the Create Filter dialog box section.

Buttons:

- **Add**
  Adds the condition from the New condition toolbar to the Conditions panel.
- **Edit**
  Lets you edit the selected condition or operator.
- **Remove**
  Removes the selected condition or operator (and all its child objects) from the Conditions panel.
- **AND**
  Adds the logical AND operator to the selected filter branch.
- **OR**
  Adds the logical OR operator to the selected filter branch.

Select Discovery Strategy (Step 3)

In the third step of the Network Discovery Wizard you need to select the desired strategy for discovering your network, using the following controls:

Scan local subnet (radio button)
Performs the discovery operation within the subnet, which the Net Inspector Server computer is a member of.

Scan IP range(s) (radio button)
Performs the discovery operation within the specified IP range(s). To add the desired IP ranges use the following controls:

Add (button)
Opens the IP range dialog box where you can enter the desired range:

Start address (input line)
Lets you enter the start address of the IP range.

End address (input line)
Lets you enter the end address of the IP range.

Delete (button)
Deletes the selected IP range.

Edit (button)
Opens the IP range dialog box where you can edit the selected range.

Progressive network discovery (radio button)
This type of discovery starts querying a single SNMP device and progressively discovers its neighbors and subnets, etc.

Start SNMP agent address (input line)
The IP address of the SNMP-enabled device that will be scanned first in progressive discovery operation.

Scan entire subnets (checkbox)
If this checkbox is checked and Net Inspector discovers a device that has a network mask that is larger than traditional class C network mask and does not exceed the size of class B mask, it will scan also the entire subnet, which the discovered device is a member of (this can be time consuming). Note that Net Inspector will always scan entire C class subnets it discovers, however, it will not scan entire subnets that are larger than B class.

Advanced (button)
This button opens the Advanced Discovery Settings dialog box:

Name
The name of the discovery operation used by the wizard.

Results (panel)

Create submaps for subnets (checkbox)
If this checkbox is checked, Net Inspector automatically creates and puts the discovered devices into subnet maps when devices are added to the workspace.

Target user view (drop-down list)
Lets you select the user view, which the discovered devices will be added to.

Submap (drop-down list)
Lets you select or enter the name of the target submap, i.e., submap, which the discovered devices and their interconnections will be added to. If the specified submap does not exist yet, it will be created.

Preserve connections (checkbox)
Check this checkbox if you want the Net Inspector to preserve manually added connections between managed objects when adding discovered managed objects and their interconnections to the submap. This option is relevant only if the target submap already contains (some) managed objects and connections between them.

Connection labels (drop-down list)
Lets you select what information will be displayed in connection labels, i.e., labels on the ends of lines connecting managed objects. You can choose to display the IP address or the name or the IP address and name of the endpoint network interface. One can hide the connection labels later by clicking the **Connection labels** checkbox in the Graphics toolbar.

Display tunnel connections (checkbox)
Check this checkbox if you want Net Inspector to display also the discovered tunnel connections between managed objects.

Advanced (panel)

Timeout (input line)
Sets the timeout interval in seconds for ICMP ping and SNMP requests.

Retries (input line)
Sets the retries count, i.e., the number of times the ICMP ping and SNMP requests will be retransmitted after the first timeout occurs.

TTL (input line)
Sets the time-to-live parameter that limits the lifetime of discovery packets to the specified number of hops. This parameter is important for limiting the depth of the progressive discovery operation.

Max queue size (input line)
Specifies the maximum number of concurrent SNMP queries. By using this parameter, you can control the CPU usage and the speed of discovery. By increasing this number, the CPU load and speed will increase and vice-versa.

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

Review Settings and Start Discovery (Step 4)

This is the last step of the Network Discovery Wizard. Here you can review the discovery settings and start or cancel the discovery operation.

Click the ***Start Discovery*** button to starts the network discovery operation or the **Cancel** button to quit the Network Discovery Wizard without starting the discovery operation.

17 DISCOVERY PANEL DIALOG BOX

17.1 Purpose

The Discovery Panel dialog box lists all existing discovery operations within Net Inspector, it lets you view their status and properties, as well as delete existing and add new discovery operations to the dialog box. The subordinated dialog boxes let you add discovered network devices and their interconnections to one or more user views. Discovered devices can also be added to the Device Panel dialog box.

17.2 Opening

To open the Discovery Panel dialog box, select the ***Tools / Discovery Panel*** command.

17.3 Description

The Discovery Panel dialog box lists all existing discovery operations by their names and displays the status of every discovery operation. It also lets you open discovery operations to view their properties and network discovery results, as well as delete existing and add new discovery operations to the dialog box.

Users with administrator access rights are permitted to open this dialog box to view and manage discovery operations as well as add discovered devices and their interconnections to the workspace and to the Device Panel dialog box.

Discovery operation is a procedure that systematically scans the network for network devices and their (inter)connections by means of ICMP ping and/or SNMP queries. The search is performed in accordance with the user-specified discovery parameters. Net Inspector supports three different network discovery methods (strategies):

- local - discovers the network (devices and their connections) within the local subnet
- range - discovers the network within the specified ranges of IP addresses
- progressive - discovers the network by means of the progressive SNMP-based network scan operation that starts scanning a single SNMP device and progressively discovers its neighbors and subnets they belong to. The depth of a progressive discovery operation is limited by the TTL (time-to-live) parameter that limits the lifetime of discovery packets to the configured number of hops.

Discovered devices and their connections within subnets can be added to Net Inspector workspace (i.e., selected user view) either automatically or manually by the user. Furthermore, a network discovery operation can be scheduled to run repeatedly in user-defined intervals and each time automatically add newly discovered devices to the selected user view.

More than one discovery operation can exist and run simultaneously in Net Inspector (e.g., each discovery operation being performed on a different part of the network, storing results to different configuration database and adding devices to different user views).

Adding objects to maps is a part of the procedure of creating and maintaining a user view (for more information see the User Views Panel section).

Discovery Panel dialog box provides the following controls:

Discovery Operations List

Displays the list of existing discovery operations. It contains the following columns:

Discovery
Displays the name of the discovery operation.

Status
Displays the current status of the discovery operation (e.g., Finished, Scanning local subnet, …).

Type
Displays the type of the search, whether it is scanning the local subnet, specified ranges or a SNMP agent.

Buttons

Add
Opens the Add Discovery Preferences dialog box, which lets specify settings for a new discovery operation.

Remove
Deletes the selected discovery operation.

Discovery results
Opens the Discovery Dialog Box with the discovery results.

Configure...
Opens the Configure discovery dialog box, which lets you view and edit the settings of the selected discovery operation.

Start
Starts the selected discovery operation.

Stop
Stop the selected running discovery operation.

17.3.1 Add/Configure Discovery Preferences

The Discovery Preferences dialog box lets you view and edit the settings for the selected discovery operation.

To open this dialog box, select the discovery you wish to edit and = click the ***Configure*** button in the Discovery Panel.

This dialog box provides the following controls:

Name (input line)
Lets you view and edit the name of the discovery operation.

Schedule (frame)

Run discovery every day at X h Y min (checkbox and two input lines)
If this checkbox is checked the discovery operation is run periodically every day at the same time specified in the hour and minutes input lines. If this option is enabled in combination with the ***Automatically add discovered devices*** option, Net Inspector will run the discovery operation on a daily basis, and, each time, it will also automatically add the newly discovered devices to the selected user view and start monitoring them.

Results (frame)
The settings in this frame control where the discovery results will be saved, i.e., to which configuration file and user view.

Create submaps for subnets (checkbox)
If this checkbox is checked, Net Inspector automatically creates and puts the discovered devices into subnet maps when devices are added to the workspace.

Automatically add discovered devices to (checkbox)
If this option is enabled, Net Inspector automatically adds newly discovered devices to the workspace (i.e., selected user view) and Device Panel dialog box (i.e., selected configuration), as follows:

Configuration (drop-down list)
Lets you select the configuration, which the discovered devices will be stored in.

User view (drop-down list)
Lets you select the user view, which the discovered devices will be added to.

Submap (drop-down list)
Lets you select or enter the name of the target submap, i.e., submap, which the discovered devices and their interconnections will be added to. If the specified submap does not exist yet, it will be created.

Preserve connections (checkbox)
Check this checkbox if you want the Net Inspector to preserve manually added connections between managed objects when adding discovered managed objects and their interconnections to the submap. This option is relevant only if the target submap already contains (some) managed objects and connections between them.

Connection labels (drop-down list)
Lets you select what information will be displayed in connection labels, i.e., labels on the ends of lines connecting managed objects. You can choose to display the IP address or the name or the IP address and name of the endpoint network interface. One can hide the connection labels later by clicking the **Connection labels** checkbox in the Graphics toolbar.

Display tunnel connections (checkbox)
Check this checkbox if you want Net Inspector to display also the discovered tunnel connections between managed objects.

Discovery filter (drop-down list)
Lets you select a discovery filter in order to discover only those devices that match the filter conditions.

Manage Discovery Filters (button)
Opens the Manage Discovery Filters dialog box, which lets you configure discovery filters.

Strategy (frame)
This frame lets you specify the preferred discovery strategy, as follows:

ICMP Ping (checkbox)
If this checkbox is checked, the ICMP Ping queries are used for discovering the network devices.

SNMP (checkbox)
If this checkbox is checked, the SNMP queries are used for discovering the network devices and their interconnections.

Scan ENTITY-MIB (checkbox)
If this checkbox is checked, Net Inspector scans the ENTITY-MIB on discovered devices via SNMP protocol and creates a managed object for each discovered entity. If this checkbox is not checked, entities are ignored and a single managed object is created for each discovered device.

Scan local subnet (radio button)
If this option is selected, Net Inspector discovers the network (devices and their connections) within the local subnet, i.e., subnet the PC running Net Inspector Server is a member of.

Scan IP range (radio button)
If this option is selected, Net Inspector discovers the network within the range of IP addresses specified in the input lines below:

IP ranges (list)
Lists the configured IP address ranges.

Add (button)
Opens the IP Range dialog box, which lets you enter the IP range:

Start address (input line)
Lets you enter the start address of the IP range.

End address (input line)
Lets you enter the end address of the IP range.

Delete (button)
Deletes the selected IP range.

Edit (button)
Opens the IP Range dialog box which lets you edit the selected IP range.

Progressive network discovery (radio button)
The Progressive network discovery starts by querying a single SNMP device and progressively discovers its neighbors and subnets by examining the routing tables and other relevant data on scanned objects. You have to enter the IP address of the SNMP device to be scanned first.

SNMP agent address (input line)
The IP address of the SNMP-enabled device that will be scanned first.

Scan entire subnets (not larger than B class) (checkbox)
If this checkbox is checked and Net Inspector discovers a device that has a network mask that is larger than traditional class C network mask and does not exceed the size of class B mask, it will scan also the entire subnet, which the discovered device is a member of (this can be time consuming). Note that Net Inspector will always scan entire C class subnets it discovers, however, it will not scan entire subnets that are larger than B class.

Advanced (button)
This button opens the Advanced Discovery Settings dialog box.

SNMP Profiles (frame)
This frame lets you control what SNMP profiles will be used in the discovery operation and how, as follows:

Use all configured SNMP Profiles (checkbox)
If this checkbox is checked, all existing SNMP profiles will be used in the discovery operation. First, the network will be scanned using the SNMPv3 profile(s), then using the SNMPv2c, and finally by using the SNMPv1 profile(s). Every managed object is automatically assigned that SNMP profile with which is has been discovered.
If this checkbox is **not** checked, you can specify what SNMP profiles will be used in the discovery operation and in which order. This can be configured using the following controls:

Not used in discovery (list)
Displays the names of existing SNMP profiles that will not be used in the discovery operation. To use a specific SNMP profile in discovery, select it in the list and click the right arrow button at the bottom of the list. This moves the selected profile to the ***Used in discovery*** list.

Used in discovery (list)
Displays the names of existing SNMP profiles that will be used in the discovery operation. This list also determines the order in which SNMP profiles will be used for discovering the network devices (first, the top-listed profile will be used, then the second profile from the top will be used, etc.). To move a profile up or down on the list, select it and click the ***Up*** or ***Down*** button next to this list, respectively. The order of the SNMP profiles determines which SNMP profiles will be assigned to discovered devices and affects the duration of the discovery operation (if a device can be successfully queried using the first profile on the list, this profile will be assigned to the managed object, and the remaining profiles won't be used for discovering that device).

To not use a specific SNMP profile in discovery, select it in the list and click the left arrow button at the bottom of the list. This moves the selected profile to the ***Not used in discovery*** list.

Up (button)
Moves the selected SNMP profile up in the **Used in discovery** list.

Down (button)
Moves the selected SNMP profile down in the **Used in discovery** list.

Advanced Discovery Settings Dialog Box

Timeout (input line)
Sets the timeout interval in seconds for ICMP ping and SNMP requests.

Retries (input line)
Sets the retries count, i.e., the number of times the ICMP ping and SNMP requests will be retransmitted after the first timeout occurs.

TTL (input line)
Sets the time-to-live parameter that limits the lifetime of discovery packets to the specified number of hops. This parameter is important for limiting the depth of the SNMP scan discovery operation.

Max queue size (input line)
Specifies the maximum number of concurrent SNMP queries. By using this parameter, you can control the CPU usage and the speed of discovery. By increasing this number, the CPU load and speed will increase and vice-versa.

OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

17.4 Discovery Dialog Box

The Discovery dialog box displays discovered devices grouped into subnet maps. When the discovery operation finishes, you can add either all discovered devices (including the subnet maps), particular groups of devices (maps) or individual devices to the workspace and to the Device Panel dialog box by using the corresponding pop-up commands.

To open this dialog box, select an existing discovery operation in the Discovery Panel dialog box and click the ***Discovery results*** button.

This dialog box provides the following controls:

Discovery results (list)
Displays results of the discovery operation, i.e., discovered subnets, network devices and their interfaces. The list contains the following columns:

Name
Displays the hostname of the discovered device or the IP address of the discovered subnet (e.g., 212.33.224.0 for the subnet 212.33.224.0 - 212.33.224.255).

Address
Displays the IP address of the device's network interface. If a device has two or more interfaces, the IP address for each interface is listed.

MAC
Displays the MAC (Media Access Control) address of the device's network interface.

Info
Displays the information about the device's network interface as reported by the SNMP agent.

17.4.1 Pop-up Menu

To display the pop-up menu, select one or more subnets, devices, or network interfaces in the Discovery results list and right-click it. To select more than one item, hold down the mouse button and drag the mouse pointer over the items you want to select. The pop-up menu contains the following commands:

- ***Add***
  Opens the Add dialog box that lets you specify to which user view and configuration you want to add the selected items. If you use this command to add devices, which are physically connected and located in the same subnet, the command will add also connections between objects to the workspace. Connections (connection lines) can be viewed in the Graphics view of the Maps window. Added managed objects will appear also in the Device Panel dialog box.
- ***Expand***
  Expands the hierarchical structure below the selected subnet or device (if device has more than one interface).
- ***Collapse***
  Collapses the hierarchical structure below the selected subnet or device (if device has more than one interface).

18 MANAGE DISCOVERY FILTERS DIALOG BOX

18.1 Purpose

It is used for viewing and managing discovery filters. A discovery filter can be applied to a discovery operation to restrict its functionality so that it will discover only those network devices that match the filter conditions.

18.2 Opening

To open the Manage Discovery Filters dialog box, select the ***Tools / Manage Discovery Filters*** command. Alternatively, click the ***Manage Discovery Filters*** button in the Configure Discovery dialog box.

18.3 Description

Users with administrator access rights can use Manage Discovery Filters dialog box to create, edit and remove discovery filters.

Once the discovery filter is created, it can be applied to one or more discovery operations by selecting its name from the Discovery filter drop-down list in the relevant Discovery Preferences dialog box.

Discovery filters contain one or more filter conditions.

The Manage Discovery Filters dialog box includes the following controls:

Filter (list)
Lists the names of existing discovery filters.

Add (button)
Opens the New Filter dialog box, which lets you create and configure a new discovery filter.

Edit (button)
Opens the Edit Filter dialog box, which lets you modify the selected discovery filter.

Remove (button)
Deletes the selected discovery filter.

Close (button)
Closes the Manage Discovery Filters dialog box.

18.3.1 New/Edit Filter dialog box

The New Filter dialog box and Edit Filter dialog box contain a toolbar that lets you create filter conditions and add them to the filter one-by-one, while the central section of the dialog box (Conditions panel) displays the entire filter consisting of filter conditions and

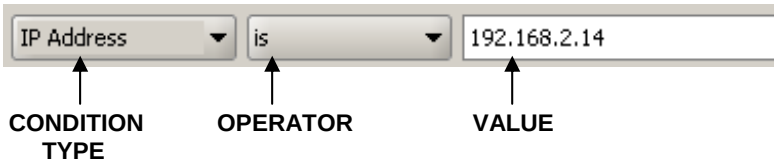
relations between them. The Conditions panel displays a filter in form of a hierarchical tree, where filter conditions are connected with logical operators (AND, OR).

Action filter conditions can be specified by using the following controls in the New/Edit Filter dialog box:

Name (input line)

Specifies the name of the discovery filter.

New condition (toolbar)



This toolbar lets you create a filter condition by specifying the condition type, operator and value from the corresponding drop-down lists/input lines. Once the condition is configured, you can add it to the filter by clicking the ***Add*** button in the right section of the dialog box. Added conditions appear in the Conditions panel below the New condition toolbar.

Condition type (drop-down list)
Specifies the type of the condition. You can select among the following types of conditions:

- **IP address**
  If this condition type is selected, you can enter the IP address of the managed object into the value input line.
- **IP address range**
  If this condition type is selected, you can enter the IP address range into the accompanying ***From*** and ***To*** input lines.
- **Object type**
  If this condition type is selected, you can choose a type of the managed object from the ***Value*** drop-down list (e.g. “IP”, etc.).
- **Class**
  If this condition type is selected, you can select a class of the managed object from the ***Value*** drop-down list (e.g., “Workstation”).
- **Location**
  If this condition type is selected, you can enter the object location into the ***Value*** input line (e.g., “MG-SOFT Headquarters”).
- **Vendor**
  If this condition type is selected, you can enter the device vendor into the ***Value*** input line (e.g., “MG-SOFT”).
- **Vendor OID**
  If this condition type is selected, you can enter the device vendor OID into the ***Value*** input line (e.g., “1.3.6.1.4.1.1315).

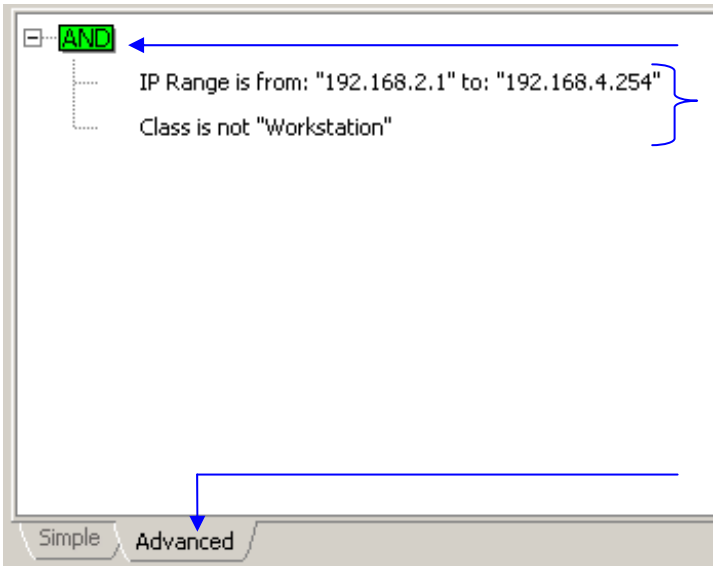
Operator
Lets you select the operator, e.g., “is”, “is not” or “contains”. Available operators depend on the type of condition selected.

Value
Lets you select or enter the condition value. Available (and valid) values depend on the type of condition selected.

Conditions (panel):

The **Conditions panel** displays and lets you re-configure existing filter conditions, and logical operators connecting them.

Example of the Conditions panel contents:



Simple and Advanced Mode
Conditions panel contains two tabs providing two modes of operation: Simple and Advanced. For more information about Simple and Advanced modes, please consult the Create Filter dialog box section.

Editing Conditions
For more information about editing existing conditions, please consult the corresponding description of the Create Filter dialog box section.

Buttons:

- **Add**
  Adds the condition from the New condition toolbar to the Conditions panel. In Advanced mode the condition is added to the selected branch in the filter tree.
- **Edit**
  Lets you edit the selected condition or operator. Operators can be modified only in Advanced mode.

- **Remove**
  Removes the selected condition or operator (and all its child objects) from the Conditions panel.

- **AND**
  Adds the logical AND operator to the selected filter branch. This button is enabled only in Advanced mode.

- **OR**
  Adds the logical OR operator to the selected filter branch. This button is enabled only in Advanced mode.

- **OK (button)**
  Applies all changes and closes the dialog box.

- **Cancel (button)**
  Discards all changes and closes the dialog box.

19 DEVICE PANEL DIALOG BOX

19.1 Purpose

The Device Panel dialog box lists all objects registered with Net Inspector and lets you add those objects to the Net Inspector workspace.

19.2 Opening

To open the Device Panel dialog box, select the ***View / Device Panel*** command or click the  ***Device Panel*** toolbar button.

19.3 Description

The Device Panel dialog box lists all managed objects, action objects, system objects and alarm panel objects registered with Net Inspector and provides information about their current status, active alarms, and other details described below.

Users with administrator access rights are allowed to open this dialog box and add objects from this dialog to the Maps window by using the drag-and-drop technique (use the ***Ctrl*** or ***Shift*** keys to select more than one object or the ***Ctrl+A*** keys to select all objects before dragging them onto maps). Make sure to unlock the map for editing before you try to add the objects onto it.

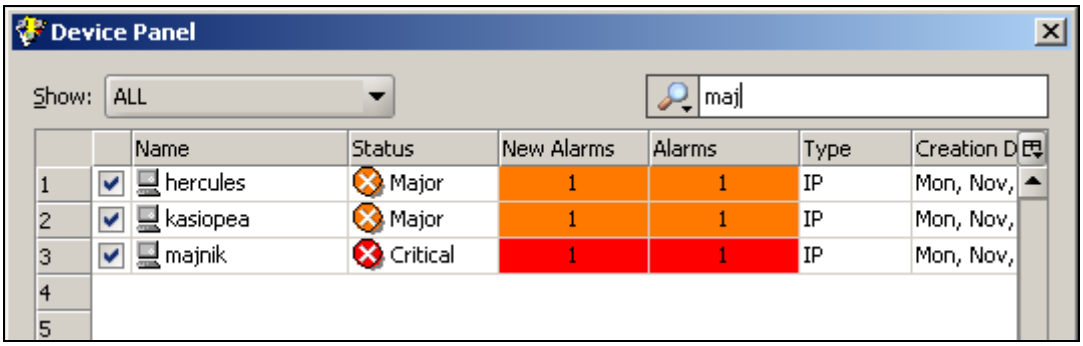
Adding objects onto maps is a part of the procedure of creating a user view (see the User Views Panel section).

The Device Panel dialog box contains the following controls:

Show (drop-down list)
Is displayed directly below the title bar on the left side of the dialog box. It lets you display only objects of the selected type.

Filter Bar (drop-down list)
Is displayed directly below the title bar on the right side of the dialog box. It lets you enter text that functions as a filter, i.e., it displays only those objects in the Device Panel dialog box that contain the entered text in selected columns. To specify which columns will be taken into account, click the filter symbol  and select desired columns from the drop-down menu that appears (columns are described in details below). Then, enter the text in to the accompanying input line, which will serve as the filter criterion.

For example, if the ***Name*** and ***Status*** columns are selected in the Filter Bar drop-down list and you enter the string “maj” into the ***Filter Bar*** input line, the Device Panel dialog box will display only those rows (objects) that include the string “maj” in the ***Name*** and ***Status*** columns (i.e., **Maj**or [Status], **maj**nik [Name] – see the picture below).



The Device Panel dialog box displays a table of all objects in the system. Each row in the table represents one object. By default, rows are colored according to the current status of the object (the row coloring feature can be disabled by unchecking the ***Use Colors*** option in the column selector). The Device Panel dialog box lists details about the objects in the following columns (you can display or hide individual columns by clicking their names in the column selector on top of the vertical scrollbar of the Device Panel dialog box):

Monitoring State (checkbox)
A check mark in this checkbox indicates that the corresponding object is enabled. For a managed object, this means that the device it represents is being monitored by Net Inspector. For an action object, this means that the action functionality it represents (e.g., sending e-mails to particular recipients) is enabled and its operation is being monitored by Net Inspector. For a system object, this means that the Net Inspector subsystem it represents (e.g., event storage subsystem) is enabled and its functioning is being monitored by Net Inspector. This checkbox is always unchecked for maps.

Name
Displays the name of the object.

Status
Displays the current status of the object.

Alarms
Displays the total number of active alarms on the object. This field also reflects the color of the most severe active alarm that currently exists on the object, according to the alarm severity colors configured in the User Preferences dialog box (Colors panel).

New Alarms
Displays the number of new alarms on the object. “New” alarms are active alarms, which are not acknowledged. The New Alarms field also reflects the color of the most severe new alarm that currently exists on the object, according to the alarm severity colors configured in the User Preferences dialog box (Colors panel).

State
Displays a graphic symbol (circle) whose color indicates the current operability state of the SNMP agent on the managed object (this property is shown only for the managed objects). The following operability states and colors are used:

operability state:	color of the graphic symbol:
Disabled	grey
Enabled	green
Unavailable	red
Testing	blue

Type
Displays the type of the object (e.g., “IP”).

Creation Date
Displays the date and time of adding this object into the system.

Node ID
Displays the identification number of the device that has been assigned to the device by the user (according to the user’s classification system).

Object ID
Displays unique identification code of the object within the Net Inspector system. This identification code consists of two integers separated by a dot (e.g., “1.2”). The first integer is the Net Inspector configuration number, while the second integer uniquely identifies the object within the given configuration.

In Active User View
Indicates if the object is included in the currently active user view (i.e., if the check mark is present, the given object is included in the currently active user view).

Description
Displays and lets you edit a short description of the object. For managed objects, Net Inspector discovery operation sets this value to the value of the sysDescription.0 object instance returned by the SNMP agent on the managed object.

Class
Displays the class of the object, which can be one of the following:

- Workstation
- Server
- Printer
- Switch
- Router
- Gateway
- Equipment
- Multiplexer
- Transport
- Database
- Action
- System

Tags
Displays tags (user descriptions) annotated to the managed object. Objects can be searched by the value of their tags.

Location
Displays the physical location of the managed object. Net Inspector discovery operation sets this value to the value of the sysLocation.0 object instance returned by the SNMP agent.

Vendor
Displays the managed object vendor name. Net Inspector discovery operation sets this value to the name of the enterprise responsible for the OID namespace returned by the sysObjectID.0 object instance. The enterprise names displayed are taken from the list of private numbers as registered with IANA and stored on the Net Inspector Server (//Engine/data/nienterprise.txt).

OS
The operating system running on the managed object.

URL
The URL (uniform resource locator) address, e.g., which provides additional information about the managed object (e.g., http://www.iskratel.si/).

Close (button)
Closes the Device Panel dialog box.

19.4 Pop-Up Menu

- ***Locate in Active User View***
  Finds the selected object and displays it in the Maps window.
- ***Show All User View References***
  Shows the References panel in the right section of the Device Panel dialog box, which displays a hierarchical tree structure of user views and (sub)maps that include the selected object(s). The root object in the References panel is the selected object, its child items are the user views that contain this object and the child items of user views are the map branches that contain the selected object (the object is included in the last submap displayed within each branch). To hide the References panel, click the ***X*** button in its title bar.
- ***Enable***
  Enables selected objects (i.e., starts polling managed objects and activates the action objects). This command does not affect the system objects.
- ***Disable***
  Disables selected objects (i.e., stops polling managed objects and deactivates the action objects). This command does not affect the system objects.

- ***Tools (cascading menu)***
  - ***Ping***
    Opens the Ping and Traceroute Console window and starts “pinging” the selected managed object.
- ***Remove Device***
  Removes the selected objects that are marked as deleted (displayed with strikethrough font) from the dialog box.
- ***Export***
  Opens the **Export Device Panel** dialog box, which lets you export the table displayed in the Device Panel dialog box to an HTML or CSV (comma-separated value) file format. The Export Device Panel dialog box closely resembles the operating system’s standard “Save As” dialog box. Note that only information shown in columns that are currently displayed will be exported.
- ***Show Objects Statistics***
  Opens the ***Objects Statistics*** message box, which displays the total number of objects in the system, the number of enabled objects in the system and the number of removed objects (i.e., objects marked for deletion).

19.5 Status bar

The Device Panel status bar displays the total number of objects in the system (T:).

20 PING AND TRACEROUTE CONSOLE WINDOW

20.1 Purpose

The Ping and Traceroute window is used for performing basic Ping and Traceroute operations.

20.2 Opening

The Ping and Traceroute window can be opened in several ways:

- By selecting ***Tools / Ping and Traceroute Console*** command,
- By clicking the  ***Ping and Traceroute Console*** toolbar button,
- By selecting the ***Tools / Ping*** pop-up command in the Maps window or in the Device Panel dialog box.

20.3 Description

The Ping and Traceroute Console window is used for querying managed objects on the network to determine if they respond to Ping (ICMP Echo) requests and to determine the route taken by packets across the network from Net Inspector Server to the specified host.

All queries in the Ping and Traceroute Console window are performed by the Net Inspector Server.

The Ping and Traceroute Console window contains the address drop-down list and toolbar and two vertically divided panels. The **Settings** panel on the left is used for viewing and configuring query parameters. The **Results** panel on the right side displays the results of the Ping and Traceroute operations.

The Ping and Traceroute Console window provides the following controls:

Address (drop-down list)
The IP address or hostname of the host to be queried.

Toolbar

 **Ping (button)**
Starts sending Ping (ICMP Echo) packets to the specified IP host and displays the Ping results (see an example).

 **Traceroute (button)**
Displays the route (hops) taken by packets on the network to reach the specified host.

 **Abort (button)**
Aborts the Ping or Traceroute operation.

Settings Panel

The Settings panel occupies the left section of the Ping and Traceroute window. It is used for viewing and configuring the Ping settings, as follows:

Send X packets (input line)
X is a number that determines how many successive ICMP Echo requests will be sent to the specified host when using the Ping command.

Timeout X seconds (input line)
X is a number that specifies how many seconds the Net Inspector Server will wait for a response to each ICMP Echo request.

TTL (input line)
A time to live number that limits the lifetime of ICMP packets to the specified number of hops.

Results Panel

The Results panel occupies the right portion of the Ping and Traceroute window (below the toolbar). It displays the ICMP Ping and Traceroute results.

Example: Ping results displayed in the Ping and Traceroute Console window

	Resolving www.mg-soft.eu
	Pinging www.mg-soft.eu [161.58.185.177]
3:42:15 PM	Reply from 161.58.185.177: time = 127ms TTL = 245
3:42:20 PM	Reply from 161.58.185.177: time = 128ms TTL = 245
3:42:25 PM	Reply from 161.58.185.177: time = 127ms TTL = 245
3:42:30 PM	Reply from 161.58.185.177: time = 127ms TTL = 245
3:42:35 PM	Reply from 161.58.185.177: time = 129ms TTL = 245
	Ping statistics for 161.58.185.177
	Packets: Sent = 5, Recieved = 5, Lost= 0 (0% loss)
	Approximate round trip times in mili-seconds:
	Minimum = 127ms, Maximum = 129ms, Average = 127ms
	Finished

21 MIB BROWSER WINDOW

21.1 Purpose

The MIB Browser window is used for exploring the graphical MIB tree and querying devices on the network using the SNMP protocol.

21.2 Opening

The MIB Browser window can be opened in several ways:

- By selecting ***Tools / MIB Browser*** command,
- By clicking the  ***MIB Browser*** toolbar button,
- By selecting the ***Tools / MIB Browser*** pop-up command in the Maps window or in the Device Panel dialog box.

21.3 Description

The MIB Browser window is used for navigating the graphical MIB tree and "browsing" SNMP agents on remote managed devices, i.e., retrieving the values of SNMP variables by means of SNMP Get, SNMP GetNext, and Walk operations. It also lets you view the MIB node properties, search for nodes and access the MIB Modules window.

All SNMP queries are performed by the Net Inspector Server.

The MIB Browser window contains the address drop-down list, a toolbar, SNMP settings toolbar, and two vertically divided panels: **MIB tree** and **Results**.

The **MIB tree** panel on the left is used for traversing the expandable MIB tree and selecting the pop-up commands, like Get, GetNext, Walk, etc.

The **Results** panel on the right side displays returned values, i.e., the name or OID, syntax and value of every retrieved object instance, or an error message, e.g., a timeout.

The MIB Browser window provides the following controls:

Address (drop-down list)
The IP address or hostname of the managed object to be queried.

Toolbar

 **Contact (button)**
Queries the SNMP agent on the managed object by means of an SNMP GetNext request and displays query results in the Results panel of the MIB Browser window. If the queried SNMP agent responds, this operation returns the value of the first OID in lexicographical order that is implemented in the SNMP agent (typically: "sysDescr.0" (1.3.6.1.2.1.1.1.0)).

 **Get (button)**
Sends an SNMP Get request to the SNMP agent on the managed object to retrieve the value of the object instance selected in the MIB tree. The result is displayed in the Results panel.

 **Get Next (button)**
Sends an SNMP GetNext request to the SNMP agent on the managed object to retrieve the value of the object instance that lexicographically follows the MIB object selected in the MIB tree. The result is displayed in the Results panel.

 **Walk (button)**
Performs the SNMP Walk operation from the selected node in the MIB tree, i.e., successively queries all object instances within the given OID subtree, to retrieve their values. For example, if you select the `system` MIB tree node (OID 1.3.6.1.2.1.1) and click this button, the software will query the MIB-II system subtree and display returned values (i.e., the name or OID, syntax and value of every retrieved object instance) or an error message, e.g., a timeout.

> **Note:** if the MIB node you are looking for is not displayed in the MIB tree, the MIB module that defines this object is not loaded in Net Inspector. You can load and unload MIB modules in the MIB Modules panel (***Tools*** / ***Server Settings*** / ***MIB Modules***).

 **Cancel (button)**
Cancels the query operation.

SNMP Settings (toolbar)

The SNMP Settings toolbar is displayed in the upper section of the MIB Browser window, directly below the ***Address*** drop-down list. It is used for specifying SNMP parameters for accessing the SNMP agent selected in the ***Address*** drop-down list. The toolbar contains the following controls:

SNMP settings (drop-down list)
Lets you specify SNMP settings for querying managed device via SNMP protocol. This can be done by selecting one of the existing SNMP access profiles (as available in the Manage Profiles dialog box, SNMP tab) from the drop-down list or by selecting the `Custom SNMP settings` entry and specifying custom SNMP access parameters. Users with administrator access rights are allowed to select among all existing SNMP profiles in this drop-down list (including the `Custom SNMP settings` profile), while all other users view only the `Custom SNMP settings` entry. If the `Custom SNMP settings` entry is selected, you can specify SNMP access parameters by using the controls below.

Timeout (input line)
A number that specifies how many seconds Net Inspector Server will wait for a response to each outstanding SNMP requests, before triggering a timeout interrupt signal.

Retries (input line)
A number that determines how many times an SNMP request will be retransmitted after the first timeout occurs.

SNMP Settings (button)
Opens the SNMP Settings dialog box that lets you specify custom SNMP access parameters for querying SNMP agents on managed devices.

SNMP Settings dialog box

Profile (frame)

Name (input line)
The name of the SNMP access profile (`Custom SNMP settings`).

Port (input line)
The UDP port on which SNMP agents on managed objects listen to for incoming SNMP requests.

SNMP version (frame and radio buttons)
The version of SNMP protocol used for querying SNMP agents on managed objects.

Settings (frame)
The SNMPv1 and SNMPv2c community name settings. This frame is disabled if SNMPv3 protocol is selected in the SNMP version frame.

Read community (input line)
The SNMP community name to be used with all SNMPv1 or SNMPv2c queries sent by Net Inspector.

Write community (input line)
This setting has currently no effect.

Trap community (input line)
This setting has currently no effect.

SNMPv3 Settings (frame)
The SNMPv3 security settings. This frame is disabled if SNMPv1 or SNMPv2c protocol is selected in the SNMP version frame.

Security user name (input line)
The name of the SNMPv3 USM user to be used for exchanging all SNMPv3 messages between Net Inspector and managed objects (including SNMPv3 Trap and Inform messages sent by the managed objects).

Context name (input line)
The name of the context in which the management information conveyed in SNMPv3 messages is accessed.

Authentication protocol (drop-down list) and **Change Password/Key (button)**
The drop-down list lets you select the SNMPv3 authentication protocol (HMAC-MD5 or HMAC-SHA) to be used for authenticating SNMPv3 messages sent on behalf of the given SNMPv3 user. The **Change Password/Key** button opens the Authentication Password or Key dialog box that lets you enter the authentication protocol password or key.

Privacy protocol (drop-down list) and **Change Password/Key (button)**
The drop-down list lets you select the SNMPv3 privacy protocol (CBC-DES or CFB-AES-128) to be used for encrypting SNMPv3 messages sent on behalf of the given SNMPv3 user. The **Change Password/Key** button opens the Privacy Password or Key dialog box that lets you enter the privacy protocol password or key.

Do not localize authentication and privacy keys (checkbox)
If this checkbox is checked, the software uses non-localized authentication and privacy keys.

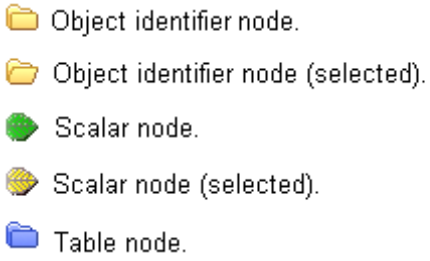
OK (button)
Applies all changes and closes the dialog box.

Cancel (button)
Cancels all changes and closes the dialog box.

MIB Tree Panel

The MIB tree panel occupies the left portion of the MIB Browser window (below the toolbars). It displays the hierarchically structured MIB tree consisting of nodes (MIB objects) defined in the currently loaded MIB modules. In the MIB tree panel, you can explore the MIB tree and select commands from the pop-up menu, for example, to query selected objects on remote SNMP agents, view node properties, load MIB modules, etc.

The following icons are used to represent MIB tree node types:



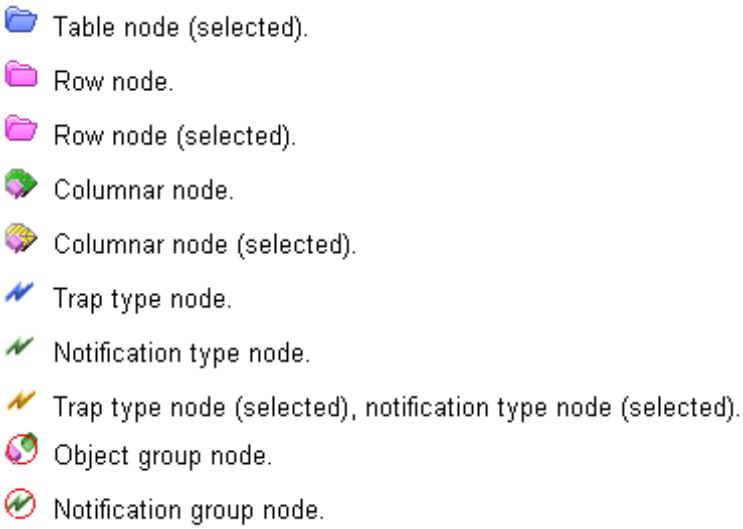


Table node (selected).
Row node.
Row node (selected).
Columnar node.
Columnar node (selected).
Trap type node.
Notification type node.
Trap type node (selected), notification type node (selected).
Object group node.
Notification group node.

MIB Tree panel pop-up menu

To display the pop-up menu, select a node in the MIB tree and right-click it. The pop-up menu contains the following commands:

> **Note:** if the MIB node you are looking for is not displayed in the MIB tree, the MIB module that defines this object is not loaded in Net Inspector. You can load and unload MIB modules in MIB Modules panel (***Tools*** / ***Server Settings*** / ***MIB Modules***).

- ***Contact***
  Queries the SNMP agent on the managed object by means of an SNMP GetNext request and displays result in the Results panel. If the queried SNMP agent responds to the query within a set timeframe, this operation returns the value of the first OID in lexicographical order that is implemented in the SNMP agent (typically: “sysDescr.0” (1.3.6.1.2.1.1.1.0)).
- ***Get***
  Sends an SNMP Get request to the SNMP agent on the managed object to retrieve the value of the object instance selected in the MIB tree. The result is displayed in the Results panel.
- ***Get Next***
  Sends an SNMP GetNext request to the SNMP agent on the managed object to retrieve the value of the object instance that lexicographically follows the MIB object selected in the MIB tree. The result is displayed in the Results panel.
- ***Walk***
  Performs the SNMP Walk operation from the selected node in the MIB tree, i.e., successively queries all object instances within the given OID subtree, to retrieve their values. For example, if you select the `system` MIB tree node (OID 1.3.6.1.2.1.1) and click this button, the software will query the MIB-II `system` subtree and display returned values (i.e., the name or OID, syntax and value of every retrieved object instance) or an error message, e.g., a timeout.

- ***Find***
  Opens the Find dialog box that lets you search for a node by its name (e.g., system) or OID value (e.g., 1.3.6.1.2.1.1). The Find operation searches the MIB tree for the specified input downward or upward from the selected node, depending on whether you click the ***Next*** or the ***Previous*** button in the Find dialog box. To find only the node whose name or OID fully matches the input in the ***Find*** input line, check the ***Whole word only*** checkbox. If this option is disabled, all nodes that contain the specified string in the Name or in the OID value will be found.
- ***Expand***
  Expands the hierarchical MIB tree structure below the selected node.
- ***Collapse***
  Collapses the hierarchical MIB tree structure below the selected node.
- ***MIB Modules***
  Opens the MIB Modules panel used for loading and unloading MIB modules.
- ***Properties***
  Opens the MIB Node Properties dialog box, which displays the SMI properties of the node selected in the MIB tree, like the node name, type, OID, syntax, status, description, etc. Displayed properties are extracted from the MIB module that defines the selected node.

Results Panel

The Results panel occupies the right portion of the MIB Browser window (below the toolbar). It displays the returned values, i.e., the name or OID, syntax and value of every retrieved object instance, or an error message, e.g., a timeout.

Example: Results displayed in the Results panel of the MIB Browser window after performing SNMP Walk operation on the "system" subtree

Walking system on sasor2		
Resolving sasor2		
sysDescr.0	OCTET STRING	Hardware: x86 Family 15 Model 2 Stepping 9 AT/AT COMPAT…
sysObjectID.0	OBJECT IDENTIFIER	mgSoft
sysUpTime.0	TimeTicks	5:58:18.10
sysContact.0	OCTET STRING	sasor@mg-soft.si
sysName.0	OCTET STRING	SasoR
sysLocation.0	OCTET STRING	MG-SOFT HQ, Maribor, Slovenia
sysServices.0	Gauge32	76
Finished		

22 CLIENT PREFERENCES DIALOG BOX

22.1 Purpose

The Client Preferences dialog box is used for setting the client-specific preferences, i.e., the Client look-and-feel and certain aspects of its behavior. These settings are stored on the computer where Net Inspector Client software is installed and are common to all users of the given copy of Net Inspector Client. These settings are independent of the Net Inspector Server the Client connects to.

For example, if you enable the option to automatically re-establish a broken connection with the Server, this setting will apply irrespective of the user that currently uses that copy of Net Inspector Client software and regardless of the Net Inspector Server the Client is connected to.

22.2 Opening

To open the Client Preferences dialog box, use the ***Tools / Client Preferences*** command.

22.3 Description

The left section of the Client Preferences dialog box contains a navigation tree with several entries. Depending on the entry selected in the navigation tree, different panel is displayed in the right section of the Client Preferences dialog box.

In addition, the following buttons are displayed at the bottom of the Client Preferences dialog box:

OK (button)
Applies all changes and closes the dialog box.

Apply (button)
Applies all changes and leaves the dialog box open.

Cancel (button)
Discards all changes and closes the dialog box.

General Panel

Look&Fell (Select button)
Opens a dialog box, which lets you select the visual appearance (look&feel) of the Net Inspector Client GUI .

Language (drop-down list)
Displays and lets you select the language for displaying the GUI texts.

Show memory usage in status bar (checkbox)
If this checkbox is checked, the main window status bar displays the amount of memory used and the total amount of memory available to the Net Inspector Client.

Show only one object properties window (checkbox)
If this checkbox is checked, only one object Properties window can be open at a time. Otherwise, more than one Properties window can be displayed at the same time, each showing properties of a different object.

Show server localization (code page) in status bar (checkbox)
If this checkbox is checked, the main window status bar indicates the code page the Net Inspector Server which the Client is connected to is using, i.e., “EN” for English (US), or “SL” for Slovenian. Note that this determines the set of characters that can be used in Net Inspector Client and in the file system on which Net Inspector runs (characters used for naming folders and files). Characters from the English code page can be used regardless of the Net Inspector Server localization (code page used), while international characters can be used only if the server uses the corresponding code page. For example, if localization is “SL”, only characters from the Slovenian and English code page may be used.

Show warning when input characters do not match server code page (checkbox)
If this checkbox is checked, a warning message box is displayed if you attempt to input characters not found in the English (US) code page or the code page used by Net Inspector Server (if different from English (US)).

Show warning when disabling objects (checkbox)
If this checkbox is checked, a warning message box is displayed when you disable (stop monitoring) managed objects. The warning message notifies you that by disabling objects, their alarm information may be lost.

Show link traffic (checkbox)
If this checkbox is checked, the thickness and color of lines connecting managed objects automatically change, visualizing the current connection status (up or down) and traffic (data throughput and interface in/out utilization). The width of a connection line automatically increases with increasing connection data throughput (bitrate) and its color automatically changes from black to pale red with increasing link utilization. If a link is down, the color of the connection line is pure red.

The status and traffic is shown only for connections between those objects that support SNMP MIB-II Interfaces table and for which the endpoint interfaces are known. Displaying the status and traffic can also be enabled or disabled by enabling or disabling the ***Interface nodes*** option available in the Graphics toolbar.

> **Maximum value for connection traffic: X Mbps (input line)**
> Integer value that defines the maximum link speed in the monitored network (e.g., 100 Mbps or 1000 Mbps, …). For example, if this value is set to 100 Mbps, the thickest connection line will be displayed when the corresponding traffic (either inbound or outbound data throughput) reaches 80 Mbps.

Max. number of events/alarm per page in Search tab (input line)
Integer value that defines the maximum number of events or alarms per page shown in the Search tab in the Events window.

Reconnect (frame)
Lets you configure the Net Inspector Client reconnecting behavior:

At startup:

- ***Prompt (radio button)***
  If this option is selected, the Client will prompt you with a dialog box asking whether to re-establish the last used connection or not.
- ***Never (radio button)***
  If this option is selected, the Client will not offer you the option to re-establish the last used connection.

Broken connection after X seconds (checkbox and input line)
If this checkbox is checked, Net Inspector Client will automatically reestablish a broken connection after X seconds.

Graphics Panel

Fill object name background with (checkbox and color selector)
If this checkbox is checked, you can select the color for the object name background (displayed in the Maps window) from the color selector. If this checkbox is unchecked, the object name background color is transparent.

Optimize drawing for:
Lets you choose the screen redraw option (a trade-off between quality and speed):

Quality (radio button)
If this option is selected, the text and graphics is anti-aliased (better quality).

Speed (radio button)
If this option is selected, anti-aliasing is disabled (faster screen redraw).

Sounds Panel

This panel lets you control the audible notifications (sounds), which are emitted when alarms are triggered:

Play sound for alarms (frame with checkboxes)
Lets you select the severity levels of alarms for which sounds are played (i.e., Critical, Major, Minor and Warning alarm severity level).

Play mode (frame)

Play once (radio button)
If this option is selected, the sound is played only once for each alarm (when the alarm is triggered). Note that the sound will be played only once if new alarms are triggered while the sound for the first alarm is still playing.

Repeat until acknowledged or cleared (radio button)
If this option is selected, the sound is played repeatedly for each alarm until the alarm is acknowledged or cleared.

Sound type (frame)

System beep (radio button)
If this option is selected, the default system beep is played.

Sound file (input line)
Lets you choose the sound file (.wav, .au) to be played on alarms.

Tools Panel

This panel lets you configure user-defined commands (actions) that start external programs and optionally pass managed object details (like the IP address, etc.) as command line parameters to external programs. User-defied commands are added to the ***Tools*** section of the pop-up menu for managed objects in the Maps window. To execute a user-defined command, right-click a managed object in the Maps window and choose the ***Tools/[name of user-defined command]*** command from the pop-up menu that appears.

The Tools panel provides the following controls:

Tools (list)
Lists the names of existing user-defined commands (actions).

Add (button)
Opens the Custom Action dialog box, which lets you create and configure a new user-defined command (action).

Edit (button)
Opens the Custom Action dialog box, which lets you modify the selected user-defined command (action).

Remove (button)
Deletes the selected user-defined command (action). By removing a command, it disappears from the Tools section of the Maps window pop-up menu.

22.3.1 Custom Action dialog box

The Custom Action dialog box lets you create and edit a user-defined command (action) that starts an external program on the PC that runs Net Inspector Client and optionally pass the relevant managed object details (like the IP address, etc.) as command line parameters to the given external program. User-defied commands are added to the **Tools** section of the pop-up menu for managed objects in the Maps window.

To open the Custom Action dialog box, click the ***Add*** button in the Tools panel of the Client Preferences dialog box or select an existing user-defined command and click the ***Edit*** button in the same dialog box.

This dialog box contains the following controls:

Name (input line)
Specifies the name of the user-defined command, as it will appear in the Tools section (cascaded menu) of the Maps window pop-up menu.

Application (input line with the Browse button)
Provides the full path to the application to be executed when this command is selected from the pop-up menu. Click the ***Browse*** button next to this input line to navigate to the desired application and select it from disk.

Capture output (checkbox)
If this checkbox is checked a new tab opens in the Events window when the command is selected from the pop-up menu. This tab displays the command line that has invoked the external application and the output printed by that application.

Arguments (frame and input filed)
Lets you specify program switches and parameters to be appended to the command line that invokes the application specified above. To enable passing desired details about managed objects to the invoked program, use the reserved words. All reserved words start with the "$" character. The reserved words are replaced with the managed object attributes when the command is executed, e.g., the "$IP_ADDRESS" reserved word is replaced with the actual IP address (e.g., 192.168.20.15) of the managed object on which the pop-up command was executed. To view all available reserved words, enter the "$" character into the ***Arguments*** input field, which open the drop-down menu of available reserved words. To add a reserved word to the ***Arguments*** input field, select it in the drop-down menu. You can also combine regular text with the reserved words (e.g., "-a $IP_ADDRESS"). Currently, the following reserved words are available:

$ADDRESS – hostname or fully qualified domain name of the managed object

$IP_ADDRESS – the IP address of the managed object

$NAME – the name of the managed object as specified in the ***Name*** input line in the General view of the managed object Properties dialog box.

$URL – the URL of the managed object as specified in the ***URL*** input line in the System view of the managed object Properties dialog box.

Preview (frame)
This frame provides controls that lets you preview and test the user-defined command:

Object (input line) and **Select (button)**
Specifies the managed object on which the command will be executed during the test. Click the ***Select*** button to open the **Select Source** dialog box and select a managed object from it. The Select Source dialog box displays two panels; the left panel contains the expandable map tree, while the panel on the right displays all objects included in the map that is selected in the left panel. The left panel also displays some properties of the listed objects. To select an object, click the relevant map in the left panel, choose the object on the right panel and click the ***OK*** button.

Preview (button)
Displays a message box with fully expanded command line for a preview (without actually executing the command)

Test (button)
Executes the command on the selected object for test purposes.

23 USER PREFERENCES DIALOG BOX

23.1 Purpose

The User Preferences dialog box is used for setting user-specific preferences, like the colors for displaying alarms, format for displaying the date and time, etc. These settings apply only to the user (identified by the username) that has configured them. The user preferences settings are stored on the computer where Net Inspector Server software is installed. When a user logs on to a Net Inspector Server, the Client fetches the user preferences settings from the Server and initializes itself accordingly. Due to this mechanism, the user preferences are independent of Net Inspector Clients and thus independent of the user physical location.

For example, if you set the user preferences option on a particular Net Inspector Server to display critical alarms in blue color, critical alarms will be displayed in blue, no matter from which computer (Net Inspector Client) you log on to that Net Inspector Server (provided that you always log on using the same user account).

23.2 Opening

To open the User Preferences dialog box, use the ***Tools / User Preferences*** command.

23.3 Description

The left section of the User Preferences dialog box contains a navigation tree with two entries. Depending on the entry selected in the navigation tree, different panel is displayed in the right section of the User Preferences dialog box.

The following buttons are displayed at the bottom of the User Preferences dialog box:

OK (button)
Applies all changes and closes the dialog box.

Apply (button)
Applies all changes and leaves the dialog box open.

Cancel (button)
Discards all changes and closes the dialog box.

Colors Panel

The Colors panel lets you configure the colors and font styles used for displaying event/alarm severity levels and states (and thus also colors displayed in alarms balloons and rectangles), and the colors that indicate the status of objects.

The Colors panel provides the following controls:

Show settings for (drop-down list)
The Colors panel provides three views, each containing a different set of color settings. Select one of the following entries from this drop-down list to display the corresponding view:

- ***Event severity***
  Shows and lets you modify the colors and font styles used for displaying severity levels of alarms and events.
- ***Event state***
  Shows and lets you modify the colors and font style used for displaying different states of alarms (new, acknowledged, manually cleared, cleared).
- ***Object status***
  Displays and lets you modify the colors and font styles used for displaying different statuses of objects.

Load defaults (button)
Loads the default values for the selected view (event severity, event state or object status).

Event Severity View

To display this view, select the "Event severity" entry from the ***Show settings for*** drop-down list in the User Preferences dialog box, Colors panel. The Event Severity View provides the following controls:

Event severity levels (list)

This list is located in the left section of the Colors panel and displays the event/alarm severity levels. Select a severity level in the list (e.g., "Major") to view or modify the text color, background color, icon color and/or font style (bold, italic, etc.) assigned to it using the controls described below.

Colors (frame)

Text color (drop-down list) and **Custom (button)**
The ***Text color*** drop-down list displays the text color assigned to the selected severity level. To change the color, select another color from the ***Text color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears. If you select the "Automatic" entry from the ***Text color*** drop-down list, the default system font color will be used.

These colors are used for displaying texts in tables that show events and/or alarms (e.g., Events window (if Use Colors option is enabled), Maps window – Details view (Alarms and New Alarms columns), Device Panel dialog box (Alarms and New Alarms columns), Properties window (General view – Active alarms list), etc.), as well as in alarm balloons and rectangles shown in the Maps window – Graphics view.

Background color (drop-down list) and **Custom (button)**
The ***Background color*** drop-down list displays the background color assigned to the selected severity level. To change the color, select another color from the ***Background color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears. If you select the "Automatic" entry from the ***Background color*** drop-down list, the system background color will be used.

These settings are used for displaying the background colors of cells in tables listing events and/or alarms (e.g., Events window (if Use Colors option is enabled), Maps window – Details view (Alarms and New Alarms columns), Device Panel dialog box (Alarms and New Alarms columns), etc.) as well as for displaying the background color of alarm balloons and rectangles shown in the Maps window – Graphics view.

Icon color (drop-down list) and **Custom (button)**
The ***Icon color*** drop-down list displays the color assigned to the graphic symbol of the selected severity level. To change the color, select another color from the ***Icon color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears.

These settings are used for displaying the colors of graphic symbols associated with event/alarm severity levels in tables that list events and/or alarms (e.g., Events window (Severity column), Event Details window, object Properties windows (General view), etc.).

Effects (frame)

Bold (checkbox)
Enables or disables displaying the texts for the selected severity level in tables that show events and/or alarms in **bold** typeface.

Italic (checkbox)
Enables or disables displaying the texts for the selected severity level in tables that show events and/or alarms in *italic* typeface.

Strikethrough (checkbox)
Enables or disables displaying the texts for the selected severity level in tables that show events and/or alarms in ~~strikethrough~~ typeface.

Preview (field)
This field is displayed at the bottom of the Colors panel and shows the preview of the settings in the selected view. Here, you can observe the results of your changes before applying them.

Event State View

To display this view, select the “Event state” entry from the ***Show settings for*** drop-down list in the User Preferences dialog box, Colors panel. The Event State View provides the following controls:

Event states (list)

This list is located in the left section of the Colors panel and displays different states of alarms and events (new, acknowledged, manually cleared, cleared). Select a state in the list (e.g., “New”) to view or modify the text color, background color and/or font style (bold, italic, etc.) assigned to it using the controls described below.

Colors (frame)

Text color (drop-down list) and **Custom (button)**
The ***Text color*** drop-down list displays the text color assigned to the selected alarm state. By default, this is “Severity color”, which means that the text color assigned to the corresponding severity level is used. If you change this setting, it overrides the severity level color setting (for example, if the “Critical” severity level is assigned red text color and you assign blue text color to the “New” alarm state, all new critical alarms will be displayed in blue text). To change the color, select another color from the ***Text color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears.

These settings are used for displaying the text color in tables that show these states of events and/or alarms (e.g., Events window (if Use Colors option is enabled), object Properties windows - General view (if Use Colors option is enabled)).

Background color (drop-down list) and **Custom (button)**
The ***Background color*** drop-down list displays the background color assigned to the selected alarm state. If the “Severity color” setting is selected, it means that the background color assigned to the corresponding severity level is used. If you change this settings, it overrides the severity level background color settings. To change the color, select another color from the ***Background color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears.

These settings are used for displaying the background colors of cells in tables that show these states of events and/or alarms (e.g., Events window (if Use Colors option is enabled), object Properties windows - General view (if Use Colors option is enabled)).

Effects (frame)

Bold (checkbox)
Enables or disables displaying the texts for the selected state in tables that show events and/or alarms in **bold** typeface.

Italic (checkbox)
Enables or disables displaying the texts for the selected state in tables that show events and/or alarms in *italic* typeface.

Strikethrough (checkbox)
Enables or disables displaying the texts for the selected state in tables that show events and/or alarms in ~~strikethrough~~ typeface.

Note: These effect settings are merged with the effect settings for the corresponding event/alarm severity levels (for example, if the “New” alarm state is assigned the bold effect, and you assign the italic effect to the “Critical” alarm, then all new critical alarms will be displayed in bold and italic typeface).

Preview (field)

This field is displayed at the bottom of the Colors panel and shows the preview of the settings in the selected view. Here, you can observe the results of your changes before applying them.

Object Status View

To display this view, select the “Object status” entry from the ***Show settings for*** drop-down list in the User Preferences dialog box, Colors panel. The Object Status View provides the following controls:

Object status (list)

This list is located in the left section of the Colors panel and displays the object statuses. Select a status in the list (e.g., “Critical”) to view or modify the text color, background color and/or font style (bold, italic, etc.) assigned to it using the controls described below.

Colors (frame)

Text color (drop-down list) and **Custom (button)**
The ***Text color*** drop-down list displays the text color assigned to the selected object status. To change the color, select another color from the ***Text color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears. If you select the “Automatic” entry from the ***Text color*** drop-down list, the default system font color will be used.

These colors are used for displaying texts in tables that show the status of objects (e.g., Device Panel dialog box, if the Use Colors option is enabled).

Background color (drop-down list) and **Custom (button)**
The ***Background color*** drop-down list displays the background color assigned to the selected object status. To change the color, select another color from the ***Background color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears. If you select the “Automatic” entry from the ***Background color*** drop-down list, the system background color will be used.

These settings are used for displaying the background colors of cells in tables that show the status of objects (e.g., Device Panel dialog box, if the Use Colors option is enabled) as well as for displaying the object icon background colors in the Maps window – Graphics view.

Icon color (drop-down list) and **Custom (button)**
The ***Icon color*** drop-down list displays the color assigned to the graphic symbol of the selected status. To change the color, select another color from the ***Icon color*** drop-down list or click the ***Custom*** button and select a custom color from the Select Color dialog box that appears.

These settings are used for displaying the colors of graphic symbols associated with object statuses in tables that list them (e.g., Device Panel dialog box (Status column), Maps window - Details view (Status column), Explorer window (map icon color)).

Effects (frame)

Bold (checkbox)
Enables or disables displaying the texts for the selected status in tables that show object statuses in **bold** typeface.

Italic (checkbox)
Enables or disables displaying the texts for the selected status in tables that show object statuses in *italic* typeface.

Strikethrough (checkbox)
Enables or disables displaying the texts for the selected status in tables that show object statuses in ~~strikethrough~~ typeface.

Preview (field)
This field is displayed at the bottom of the Colors panel and shows the preview of the settings in the selected view. Here, you can observe the results of your changes before applying them.

Formatting Panel

Date/Time format (drop-down list)
Lets you select the date and time format.

24 PRINT DIALOG BOX

24.1 Purpose

The Print dialog box is used for setting the printing options and for sending the selected content from Net Inspector Client to a printer.

24.2 Opening

To open the Print dialog box, use the ***File / Print*** command.

24.3 Description

Depending on what is selected before you open it, the Print dialog box lets you print the contents of the:

- Explorer window, or
- Maps window (selected tab), or
- Events window (selected tab), or
- Event Details sub-window.

This dialog box lets you configure the printing options, like printer setting, page settings, etc., and send the output to the selected printer (which is accessible from the computer that runs Net Inspector Client).

The Print dialog box provides the following controls:

Printer (frame)

Name (field)
Displays the name of the printer to which the print job will be sent. This is the default printer on the system where Net Inspector Client runs. To change the printer, click the ***Print Settings*** button and select another printer from the dialog that appears.

Print Settings (button)
Opens the system standard Print dialog box, which lets you select among available printers, set printer specific options, configure the printing range and the number of copies, etc.

Page (frame)

Size (field)
Displays the size of the paper or other print media. To change it, click the ***Page Setup*** button and select a different paper size from the dialog that appears.

Orientation (field)
Displays the orientation (portrait or landscape) of the paper or other print media. To change it, click the ***Page Setup*** button and select a different orientation from the dialog that appears.

Page Setup (button)
Opens the system standard Page Setup dialog box, which lets you select among available print media, set print orientation, margins, etc..

Fit to page (checkbox)
Scales the output to fit the page size.

OK (button)
Applies all changes, sends the print job to the printer and closes the dialog box.

Cancel (button)
Discards all changes and closes the dialog box.

25 WINDOWS DIALOG BOX

25.1 Purpose

The Windows dialog box lets you view a list of all open Properties and (Sub)map Properties windows, bring listed windows to the foreground and close listed windows.

25.2 Opening

To open the Windows dialog box, use the ***Window / Windows*** command.

25.3 Description

The Windows dialog box lets you view a list of all Properties and (Sub)map Properties windows currently open in Net Inspector Client, bring listed windows to the foreground and close listed windows.

The Windows dialog box provides the following controls:

Open Windows (list)
Displays a list of all Properties and (Sub)map Properties windows currently open in Net Inspector Client.

Activate (button)
Activates (brings to the foreground) the window selected in the list of open windows.

Close Windows(s) (button)
Closes the window(s) selected in the list of open windows.

Close (button)
Closes the Windows dialog box.

26 MENUS

The menu bar, displayed directly below the Net Inspector Client title bar, contains the following program menus:

- **File**
- **Edit**
- **View**
- **Event**
- **Map**
- **Tools**
- **Window**
- **Help**

26.1 File Menu

Connect (Ctrl+Shift+N)
Opens the Connect to Net Inspector Server dialog box, enabling you to configure parameters for a connecting and logging on to Net Inspector Server.

Disconnect
Disconnects Net Inspector Client from the Server and closes all windows in the Client main window. If the workspace has been modified and not saved yet, the Save Maps dialog box appears, which lets you save modified user views or reject the modifications.

Reconnect (Ctrl+Shift+R)
Re-establishes the last used connection between Net Inspector Client and Server.

Switch to Design Mode
Switches Net Inspector Client into the Design mode of operation.

Switch to Alarm Mode
Switches Net Inspector Client into the normal mode. This menu option is available if you are connected to the Net Inspector Server in the Design mode.

Close (Ctrl+F4)
Closes the currently active tab displayed in the Maps window.

Close All (Ctrl+Shift+F4)
Closes all tabs displayed in the Maps window.

Close Other Tabs
Closes all inactive tabs (all but currently active/selected).

Save (Ctrl+S)
Saves the layout of the currently active map (tab) displayed in the Maps window.

Save All (Ctrl+Shift+S)
Saves the layout of all maps (tabs) in the currently active user view.

Revert to Saved
Reverts the layout of the currently active map (tab) displayed in the Maps window to its last saved state.

Print (Ctrl+P)
Lets you print the contents of the Explorer window or the contents of the currently active tab of the Maps window (depending on what is selected before you open the Print dialog box).

Export
Opens the **Export** dialog box, which lets you export the table displayed in the currently active tab of the Maps window (Details view) or in the currently active tab in the Events window to an HTML or CSV (comma-separated value) file format. The Export dialog box closely resembles the operating system's standard "Save As" dialog box. Note that only information in the columns that are displayed will be exported.

Properties
Opens the Properties window of the selected object or submap.

Exit (Ctrl+Shift+X)
Closes the Net Inspector Client application.

26.2 Edit Menu

Cut (Ctrl+X)
Removes selection and puts it on the clipboard.

Copy (Ctrl+C)
Copies selection to the clipboard.

Paste (Ctrl+V)
Places the clipboard contents onto the Maps or Explorer window.

Duplicate
Duplicates the currently selected object(s) in the Maps window.

Delete (Del)
Deletes selection from the Maps or Explorer window.

Remove from Configuration
Removes selected object(s) from the configuration.

Find Objects (Ctrl+Shift+F)
Opens the Find Objects dialog box.

Select All (Ctrl+A)
Selects all items in the currently active window.

26.3 View Menu

Graphics Toolbar
Shows or hides the Graphics toolbar.

Events
Shows or hides the Events Window.

Explorer
Shows or hides the Explorer Window.

Device Panel
Shows or hides the Device Panel Dialog Box.

Map Overview
Shows or hides the Map Overview window.

26.4 Event Menu

Go To Source
Finds and selects the object in the Maps window, which has triggered the selected alarm or event.

Add Comment
Opens the Add Comment dialog box that lets you enter a comment for the selected alarms. User comments are displayed in the Comment column in the Events window.

Acknowledge
Acknowledges the selected alarms. By acknowledging alarms, users declare that they are aware of the alarms. Acknowledged alarms are not shown in the alarm balloons. Events cannot be acknowledged/unacknowledged.

Unacknowledge
Unacknowledges the selected alarms (reverses the Acknowledge operation).

Manually Clear
Manually clears the selected alarms. Note that Net Inspector system alarms (i.e., alarms that have the Message ID value in the range of 10000-15000) cannot be manually cleared. Events cannot be manually cleared/uncleared.

Manually Unclear
Unclears the selected alarms (reverses the Manually Clear operation).

Remove Cleared Alarms
Removes all cleared alarms from the currently active tab of the Events window.

Create Filter
Opens the Create Filter dialog box and lets you create filters for displaying active alarms in the Events window.

Find Events
Opens the Find Events dialog box, which lets you search for alarms and events.

Modify Filter
This command is used for modifying (e.g., refining) conditions of an existing filter, i.e. either display filter or search filter. This command is enabled only if a find or filter tab is selected in the Events window. It opens the Find Events dialog box or Create Filter dialog box (depending on which dialog box has been used initially) and lets you modify the existing filter.

Save Filter
Lets you save the search or display filter applied in the currently active tab of the Events window for later use. The filter will be saved to the “My filters” repository, which is stored on the Net Inspector Server computer. This way, any user can later load and use this filter. This button is disabled if no filter of find tab is selected in the Events window. Note that when saving search filters, the time frame (From – To) is not saved along with the filter conditions.

Load Filter
Opens the Load Filter dialog box, which lets you select a previously saved filter and apply it. The Load Filter dialog box lets you select the filter either from the “My filters” repository (which contains all previously saved filters), from the “Action filters” repository (which contains all action filters available in the Manage Action Filters dialog box) or from a file (filters that have been saved to a file in previous versions of Net Inspector).

Remove Filter
Opens the Remove Filter dialog box, which lists all filters from the “My filters” repository and lets you delete them. If a deleted filter is currently used in a tab in the Events window, it remains in use until the Net Inspector Client is disconnected from the server (or until the tab is manually removed from the Events window).

Save Filters Layout
Lets you save all currently displayed display and action filter tabs in the Events window. This command ensures that the existing display and action filter tabs are automatically restored next time the user opens the same user view. This command is available only if a filter of find tab is selected in the Events window.

Export Filter to File
Lets you save the filter that is applied in the currently selected tab of the Events window to a file stored on Net Inspector Client computer. This command is disabled if no filter tab is selected in the Events window.

Import Filter from File
Opens the Import Filter dialog box (which closely resembles the standard Open dialog box), which lets you select a previously saved filter file from disk and import it. This creates a new tab in the Events window and applies the imported filter to it.

26.5 Map Menu

Edit Mode (Ctrl+Shift+E)
Enables or disables the Edit mode for the map (tab) currently selected in the Maps window (Graphics view). If the Edit mode is disabled, the map cannot be edited. All commands described below (except the ***Grid*** command) are enabled only if the Edit mode is enabled.

Relayout
Opens the Relayout dialog box, which lets you automatically re-arrange the icons in the currently active tab of the Maps window into the **star** or **mesh** network topology layout (if the icons are connected with connection lines) or arrange the icons onto a gridline (if the icons are not connected). The Relayout dialog box also lets you arrange the icons into **alphabetically sorted** layout.
If the **Only selected** checkbox is checked in the Relayout dialog box, only the selected icons will be repositioned. If the **Ignore unconnected** checkbox is checked in the Relayout dialog box, the unconnected icons will not be repositioned, i.e., aligned to a grid.

Insert Line
Lets you draw a line in the Maps window by clicking and holding down the mouse button while dragging the mouse pointer across the Maps window. Release the mouse button at the point where you want the line to end.

Insert Rectangle
Lets you draw a rectangle to the Maps window by clicking and holding down the mouse button while dragging the mouse pointer across the Maps window. Release the mouse button when the size of the rectangle matches your preferences.

Insert Ellipse
Lets you draw an ellipse to the Maps window by clicking and holding down the mouse button while dragging the mouse pointer across the Maps window. Release the mouse button when the size of the ellipse (circle) matches your preferences.

Insert Text
Lets you add text to the Maps window. To add text, click within the Maps window at the point where the text should start. This opens the Text Editor dialog box. Enter the text into the Text Editor dialog box, adjust the font type and size to meet your preferences, and click the ***OK*** button to close the dialog and display the entered text in the Maps window. To edit existing text, select this command and then click the text to be edited in the Maps window to open the text in the Text Editor dialog box, where you can edit it.

Insert Image
Lets you add a bitmap image to the Maps window by clicking within the Maps window and choosing an image file (JPG, BMP or PNG format) from the Select Image dialog box that appears.

> **Note:** The image file must be stored on the computer running Net Inspector Server (in the "Engine" folder or its subfolders).

26.6 Tools Menu

Change Password
Opens the Change Password dialog box that lets you change the password for the selected user account.

Ping and Traceroute Console
Opens the Ping and Traceroute Console window and lets you query remote managed objects on the network by means of Ping (ICMP Echo) requests.

Discovery Panel
Opens the Discovery Panel dialog box, which lets you view and manage discovery operations.

Manage Discovery Filters
Opens the Manage Discovery Filters dialog box, which lets you view and configure discovery filters.

Show Performance Manager
Displays the Performance Manager Home Page window.

User Preferences
Opens the User Preferences dialog box, which lets you view and configure user-specific preferences.

Client Preferences
Opens the Client Preferences Dialog Box, which lets you view and adjust certain aspects of Net Inspector Client behavior and look-and-feel to your preferences.

Server Settings
Opens the Server Settings Dialog Box, which lets you view and configure the server-specific settings.

MIB Browser
Opens the MIB Browser window, which lets you explore the graphical MIB tree and query devices on the network via the SNMP protocol.

26.7 Window Menu

Close All
Closes all open windows listed in the Windows dialog box.

Windows
Displays the Windows dialog box, which lets you view, activate and close Properties and (Sub)map Properties or Performance Statistics windows that are currently open in Net Inspector Client.

The menu section below the separation line displays the names of up to 10 open Properties, (Sub)map Properties or Performance Statistics windows. You can quickly activate (bring to the foreground) any listed window by selecting its name from the menu.

26.8 Help Menu

MG-SOFT on the WEB
Contains sub-menus with links to the MG-SOFT web site:

MG-SOFT Home Page
Opens the MG-SOFT home web page.

Net Inspector Home Page
Opens the Net Inspector home web page.

Products Page
Opens the MG-SOFT Products web page.

Secure Online Orders
Opens the MG-SOFT ordering web page.

Subscribe to Mailing List
Opens the Mailing List Subscription form web page.

Download Software Details
Opens the MG-SOFT download web page.

Evaluation License Key Request
Opens the 30-day Evaluation License Key Request web page.

Other Products
Displays a cascading menu containing links to web pages related to other MG-SOFT products:

Getting Started Guide
Opens the Getting Started Guide in the system default PDF viewer application.

Reference Manual
Opens the Reference Manual in the system default PDF viewer application.

Performance Manager User Manual
Opens the Performance Manager User Manual in the system default PDF viewer.

Installation and Configuration Guide
Opens the Installation and Configuration Guide in the system default PDF viewer.

Support
Automatically collects the relevant support information and displays it in the Support Information window that lets you copy or save the information to a text file to be attached to your support request. Please include this information into your support request e-mail and provide a detailed description of the problem you are having before sending a support request e-mail to <support@mg-soft.si>.

This command is enabled only when Net Inspector Client is connected to Net Inspector Server.

Check for Updates
Tries to contact the MG-SOFT's update servers on the Internet to check if a newer version of Net Inspector is available for download.

If the newer version is available, the MG-SOFT's Updates download page automatically opens in your default Web browser providing one or more download links. The Updates download page offers download links for the updates that are

available to you free of charge and those that require renewing your license (additional payment). Click appropriate link to download the desired software update with your Web browser. After downloading the software, please consult the Net Inspector Installation and Configuration Guide document or the bundled README.TXT file for the detailed instructions on installing/upgrading the software.

This command is enabled only when Net Inspector Client is connected to Net Inspector Server.

About

Displays the About Net Inspector Java Client dialog box, which provides information about the Net Inspector Client version and build number and the copyright notice.

If the Net Inspector Client is connected to Net Inspector Server, this dialog box provides also information about the version and build of the Net Inspector Server the client is connected to. In this case, the About dialog box displays the product licensing information, like the license serial number and supported edition of the software.

Furthermore, this dialog box also displays the maximal and current number of concurrent client connections, the maximal and current number of devices managed by the Net Inspector Server, as well as the list of all connected Performance Manager polling engines and the number of the objects monitored by each polling engine.

27 TOOLBAR

The toolbar, which is displayed below the menu bar in the Net Inspector Client main window, contains a group of buttons that provide quick access to a series of most common menu commands. You can get a brief description of the operation behind each toolbar button in a tooltip by placing the mouse pointer on the toolbar button (without clicking). The toolbar buttons are:

 **New connection** – shortcut for the *File / Connect* command.

 **Disconnect** - shortcut for the *File / Disconnect* command.

 **Reconnect** - shortcut for the *File / Reconnect* command.

 **Events** - shortcut for the *View / Events* command.

 **Explorer** - shortcut for the *View / Explorer* command.

 **Map Overview** - shortcut for the *View / Map Overview* command.

 **Device Panel** - shortcut for the *View / Device Panel* command.

 **Ping and SNMP Console** - shortcut for the *Tools / Ping and SNMP Console* command.

 **MIB Browser** - shortcut for the *Tools / MIB Browser* command.

 **Manage Profiles**- shortcut for the *Tools / Server Settings, Profiles Panel* command.

 **Graphics Toolbar** - shortcut for the *View / Graphics Toolbar* command.

 **Show Performance Manager** – shortcut for the Tools / Show Performance Manager command.

 **Show Performance Statistics** – shortcut for the Show Performance Statistics pop-up command.

 **Show NetFlow Statistics** – shortcut for the Show NetFlow Statistics pop-up command.

 **Network Discovery Wizard** – shortcut for the Network Discovery Wizard.

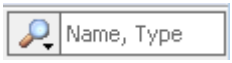
 **Zoom-out** – reduces the magnification of the currently active tab in the Maps window (Graphics view).

Zoom – lets you set the zoom level (magnification in percent) of the currently active tab in the Maps window (Graphics view).

 **Zoom-in** – increases the magnification of the currently active tab in the Maps window (Graphics view) by 20%.

View (drop-down menu) - lets you choose the view in the Maps window:

- **Graphics** – displays managed objects and submaps as icons,
- **Details** – displays managed objects and submaps in a table view.



Filter Bar (drop-down menu) - lets you filter objects in the currently active tab of the Maps window (Details view).

28 STATUS BAR

The status bar is displayed at the bottom of the Net Inspector Client main window. The right part of the status bar provides the following information (from left to right):

- The server localization code (i.e., code page used by Net Inspector Server), which is one of the following:
  - EN – English (US)
  - SL – Slovenian

  This information is displayed only if the Show server localization option is enabled in the Client Preferences.
- Mem: - the Net Inspector Client used memory and the total available memory size (e.g., 73MB/254MB). This information is displayed only if the Show memory usage option is enabled in the Client Preferences.
- - the username of the user connected to Net Inspector Server.
- -the name or address of the Net Inspector Server, which the Client is connected to.
- The Net Inspector Server TCP port number that is used for communication with the Client.

29 NET INSPECTOR CLIENT DESIGN MODE

29.1 Purpose

The design mode is a special Net Inspector Client mode of operation that facilitates the process of designing user views by allowing authorized users to have more than one user view active (open) at the same time and to copy objects between active user views. The design mode cannot be used for monitoring and managing alarms and events.

29.2 Opening

To open Net Inspector Client in design mode, you need to check the ***Design mode*** checkbox in the logon dialog box when logging on to Net Inspector Server. Only users with administrator access rights are authorized to use the design mode.

29.3 Description

Besides the normal mode of operation, which is described in preceding sections, Net Inspector Client offers also a special mode of operation called **design mode**. The design mode facilitates the process of creating user views by allowing authorized users to have more than one user view open (active) at the same time and to copy objects between active user views (in normal mode, only one user view can be open at any given time). Only users with administrator access rights are authorized to use the design mode.

The design mode offers the same features as the normal mode, except the event and alarm management features (i.e., the Events window, Create Filter and Find Events dialog boxes are disabled, as well as the commands related to alarm management).

The main advantage of the design mode is that it allows authorized users to have more than one user view active (open) at the same time and to copy objects between active user views. This can significantly speed-up the process of creating user views.

29.3.1 Working With Two or More Active User Views at the Same Time

To open two or more user views

In design mode, you can open an inactive user view by selecting its icon in the Explorer window and choosing the ***Open*** pop-up command (or by simply double-clicking such icon). This will activate the selected user view without deactivating other active user views. Alternatively, you can use the Server Settings dialog box, User Views panel, select the desired user view and click the ***Open*** button to activate it.

To close an active user view, select it in the Explorer window and choose the ***Close*** pop-up command.

To create a new user view

To create a new user view, select the root node (Net Inspector Server) in the Explorer window and choose the ***New User View*** pop-up command or use the Server Settings dialog box, User Views panel.

To copy or move maps and objects between user views

To copy a part of the user view from one active user view to another, select the desired map icon in the Explorer window and use the ***Copy*** pop-up command, then select the destination map in another user view and choose the ***Paste*** pop-up command. This will copy the entire map structure and all containing objects to the destination user view. To move a part of the user view from one active user view to another, use the ***Cut*** and ***Paste*** pop-up commands in the procedure above.

To copy (move) individual map objects from one user view to another or from one map to another, select those objects in the source map in the Maps window and use the ***Copy*** (***Cut***) pop-up command, then double-click the destination map and choose the ***Paste*** pop-up command.

For more information on other commands, windows and dialog boxes available in the design mode, please refer to the corresponding sections of this document.

APPENDIX 1: EVENT TYPE LIST

In accordance with the ITU X.733 recommendation, Net Inspector reports the following types of events (and alarms):

Event Type ID	Event Type
0	Indeterminate
1	Other
2	Communication
3	Quality Of Service
4	Processing Error
5	Equipment
6	Enviromental
7	Integrity Violation
8	Operational Violation
9	Physical Violation
10	Security Violation
11	Time Domain Violation

APPENDIX 2: CAUSE LIST

In accordance with the ITU X.733 recommendation, Net Inspector reports the following causes of events (and alarms):

Cause ID	Cause
1	AIS
2	Call Setup Failure
3	Degraded Signal
4	Far End Receiver Failure
5	Framing Error
6	Loss Of Frame
7	Loss Of Pointer
8	Loss Of Signal
9	Payload Type Mismatch
10	Transmission Error
11	Remote Alarm Interface
12	Excessive BER
13	Path Trace Mismatch
14	Unavailable
15	Signal Label Mismatch
16	Loss Of Multi Frame
17	Receive Failure
18	Transmit Failure
19	Modulation Failure
20	Demodulation Failure
21	Broadcast Channel Failure
22	Connection Establishment Error
23	Invalid Message Received
24	Local Node Transmission Error
25	Remote Node Transmission Error
26	Routing Failure
51	Backplane Failure
52	Data Set Problem
53	Equipment Identifier Duplication
54	External IF Device Problem
55	Line Card Problem
56	Multiplexer Problem
57	nE Identifier Duplication
58	Power Problem
59	Processor Problem
60	Protection Path Failure
61	Receiver Failure
62	Replaceable Unit Missing
63	Replaceable Unit Type Mismatch
64	Synchronization Source Mismatch
65	Terminal Problem
66	Timing Problem
67	Transmitter Failure
68	Trunk Card Problem

69	Replaceable Unit Problem
70	Real Time Clock Failure
71	Antenna Failure
72	Battery Charging Failure
73	Disk Failure
74	Frequency Hopping Failure
75	I/O Device Error
76	Loss Of Synchronization
77	Loss Of Redundancy
78	Power Supply Failure
79	Signal Quality Evaluation Failure
80	Transceiver Failure
81	Protection Mechanism Failure
82	Protecting Resource Failure
101	Air Compressor Failure
102	Air Conditioning Failure
103	Air Dryer Failure
104	Battery Discharging
105	Battery Failure
106	Commercial Power Failure
107	Cooling Fan Failure
108	Engine Failure
109	Fire Detector Failure
110	Fuse Failure
111	Generator Failure
112	Low Battery Threshold
113	Pump Failure
114	Rectifier Failure
115	Rectifier High Voltage
116	Rectifier Low FVoltage
117	Ventilations System Failure
118	Enclosure Door Open
119	Explosive Gas
120	Fire
121	Flood
122	High Humidity
123	High Temperature
124	High Wind
125	Ice Build Up
126	Intrusion Detection
127	Low Fuel
128	Low Humidity
129	Low Cable Pressure
130	Low Temperature
131	Low Water
132	Smoke
133	Toxic Gas
134	Cooling System Failure
135	External Equipment Failure
136	External Point Failure
151	Storage Capacity Problem
152	Memory Mismatch
153	Corrupt Data

154	Out Of CPU Cycles
155	Software Environment Problem
156	Software Download Failure
157	Loss Of Real Time
158	Application Subsystem Failure
159	Configuration Or Customization Error
160	Database Inconsistency
161	File Error
162	Out Of Memory
163	Software Error
164	Timeout Expired
165	Underlying Resource Unavailable
166	Version Mismatch
201	Bandwidth Reduced
202	Congestion
203	Excessive Error Rate
204	Excessive Response Time
205	Excessive Retransmission Rate
206	Reduced Logging Capability
207	System Resources Overload
500	Adapter Error
503	Call Establishment Error
504	Communications Protocol Error
505	Communications Subsystem Failure
510	Data Set Or Modem Error
512	Dte/Dce Interface Error
514	Equipment Malfunction
515	Excessive Vibration
521	I/O Device Error
522	Input Device Error
523	Lan Error
524	Leak Detected
528	Material Supply Exhausted
531	Output Device Error
532	Performance Degraded
534	Pressure Unacceptable
536	Pump Failure
537	Queue Size Exceeded
541	Resource At Or Nearing Capacity
542	Response Time Excessive
543	Retransmission Rate Excessive
545	Software Program Abnormally Terminated
546	Software Program Error
549	Threshold Crossed
600	Authentication Failure
601	Breach Of Confidentiality
602	Cable Tamper
603	Delayed Information
604	Denial Of Service
605	Duplicate Information
606	Information Missing
607	Information Modification Detected
608	Information Out Of Sequence

609	Key Expired
610	Non Repudiation Failure
611	Out Of Hours Activity
612	Out Of Service
613	Procedural Error
614	Unauthorized Access Attempt
615	Unexpected Information
1024	Other

APPENDIX 3: EVENT MESSAGE LIST AND DESCRIPTION OF EVENTS

The following event (and alarm) messages are built into Net Inspector:

Message ID	Message	Description
10001	Device is down	Device does not respond to ICMP Ping queries, to SNMP queries (if SNMP polling is enabled) and to none of the services queries (if services polling is enabled) within the specified time frame set in the polling profile.
10002	SNMP agent not responding	Device does not respond to SNMP queries within the specified time frame (set in the polling profile).
10003	Resynchronization failed	The resynchronization of events between Net Inspector Server and the given managed object has failed. Possible reasons: invalid SNMP agent version or incorrect SNMP Set community string used.
10004	Invalid address or DNS error	Specified name of the object cannot be resolved through the DNS. Possible reasons: invalid DNS name entered, DNS server not reachable.
10040	Invalid filter name	No filter is assigned to the action object.
10041	Extension process is not running	The Net Inspector extension process associated with the object (e.g., mgmail process for Mail objects) is not running. The corresponding actions cannot be executed. Net Inspector will automatically attempt to restart the extension process, and if successful, this event will be cleared.
10042	Invalid settings	Settings for the action object are invalid or missing.
10043	Modem timeout	Modem connection has timed out (SMS object). Possible reasons: incorrect settings, destination not reachable…
10044	Sending messages is temporarily disabled due to full buffer	The message queue buffer for an action object is full and all new outgoing messages are being discarded.
10045	Failed to run process	The process to be started by the Command object is not running. Possible reasons: insufficient user-rights…
10050	Invalid command line	The file to be run by the Command object does not exist. Possible reasons: invalid command line…
10101	Alarm panel client is down	Remote alarm panel client is not connected to Net Inspector Server. Possible reasons: alarm panel client is not running, a firewall is blocking connections to Net Inspector Server,…

10102	Alarm panel identification is used or invalid	The alarm panel “IP address:ID” combination is already used or invalid.
10103	Alarm panel user view name is invalid	The alarm panel user view name setting is invalid.
10201	Failed to load configuration database	Cannot load the given configuration. Possible reasons: configuration file does not exists, configuration database instance (or catalog) does not exist…
10202	Failed to connect to configuration database	Cannot connect to the configuration database. Possible reasons: incorrect settings, database not reachable…
10203	Failed to read from configuration database	Cannot read from the configuration database. Possible reasons: insufficient user rights…
10204	Failed to initialize OpenMN subsystem	Cannot initialize the OpenMN subsystem. Possible reasons: multicast port for receiving OpenMN notifications cannot be registered.
10210	Failed to connect to event storage database	Cannot connect to the event storage database. Possible reasons: incorrect settings, database not reachable…
10211	Failed to initialize event storage database	Cannot create or retrieve tables from the event storage database.
10212	Failed to access event storage database	Cannot access the event storage database. Possible reasons: Error while disconnecting from the database.
10215	Failed to connect to event storage database for event queries	Cannot connect to the event storage database for event queries. Possible reasons: incorrect settings, database not reachable…
10216	Failed to initialize event storage database for event queries	Cannot create or retrieve tables from the event storage database for event queries.
10217	Failed to access event storage database for event queries	Cannot access the event storage database for event queries. Possible reasons: Error while disconnecting from the database.
10220	Failed to connect to event storage database for event maintenance	Cannot connect to the event storage database for event maintenance. Possible reasons: incorrect settings, database not reachable…
10221	Failed to initialize event storage database for event maintenance	Cannot create or retrieve tables from the event storage database for event maintenance.
10222	Failed to access event storage database for event maintenance	Cannot access the event storage database for event maintenance. Possible reasons: Error while disconnecting from the database.
10230	Failed to initialize SNMP sub-system to register SNMP notifications	Cannot connect to MG-SOFT SNMP Trap service (mgtrapd). Possible reasons: MG-SOFT SNMP Trap service is not running…
10231	Failed to register port for SNMP notifications	Cannot register a new port for receiving SNMP notifications. Possible reasons: port is already used by another application.
10232	Receiving SNMP notifications is temporarily disabled due to full buffer	The SNMP notification reception buffer is full and all new incoming SNMP notifications are being discarded.

10233	Receiving SNMP notifications is temporarily disabled due to SNMP sub-system failure	All new incoming SNMP notifications are being discarded. Possible reasons: MG-SOFT SNMP Trap service is not running…
11000	Threshold value for interface inbound utilization exceeded	The threshold value that is set in the polling profile for inbound interface utilization is exceeded.
11001	Threshold value for interface outbound utilization exceeded	The threshold value that is set in the polling profile for outbound interface utilization is exceeded.
11002	Threshold value for interface inbound error rate exceeded	The threshold value that is set in the polling profile for inbound error rate is exceeded.
11003	Threshold value for interface outbound error rate exceeded	The threshold value that is set in the polling profile for outbound error rate is exceeded.
11004	Threshold value for interface status exceeded	The interface status has changed to “down”.
11005	Threshold value for memory usage exceeded	The threshold value that is set in the polling profile for memory usage is exceeded.
11006	Threshold value for processor load exceeded	The threshold value that is set in the polling profile for processor load is exceeded.
11007	Threshold value for storage usage exceeded	The threshold value that is set in the polling profile for storage usage is exceeded.
11200	Maximal number of objects is exceeded	The maximal number of objects supported by the license is exceeded. No new objects can be added to the system and some of the existing objects may be disabled.
11500	Failed to compute interface traffic due to too long polling interval	Cannot compute the interface traffic values because the currently applied polling interval is too long compared to the interface nominal speed (interface counters may roll over twice in one polling interval, which makes computing traffic values unreliable).
11501	Failed to compute interface traffic due to non-positive ifSpeed value	Cannot compute the interface traffic values because the interface nominal speed (ifSpeed) reported by the SNMP agent is zero or negative.
12000	Link down	Net Inspector Server has received a “linkDown” SNMP Trap or Inform notification message. The SNMP agent on the given managed object reports that the status (ifOperStatus) of the interface (identified by the ifIndex variable binding) has changed to “down”. This event is automatically cleared when the “linkUp” Trap or Inform message for the same interface is received.
12001	Cold start	Net Inspector Server has received a “coldStart” SNMP Trap or Inform notification message. This signifies that the SNMP agent on the given managed object has reinitialized itself in a way that its configuration may have been altered.

12002	Warm start	Net Inspector Server has received a “warmStart” SNMP Trap or Inform notification message. This signifies that the SNMP agent on the given managed object has reinitialized itself such that its configuration is unaltered.
12003	Auth failure	Net Inspector Server has received an “authenticationFailure” SNMP Trap or Inform notification message. This signifies that the SNMP agent on the given managed object has received a SNMP message that is not properly authenticated (e.g., contains a wrong community name).
12004	Neighbor loss	Net Inspector Server has received an “egpNeighborLoss” SNMP Trap or Inform notification message. An egpNeighborLoss Trap signifies that an EGP neighbor for whom the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer obtains.
12005	Specific SNMP notification	Net Inspector Server has received an enterprise specific SNMP Trap or Inform notification message. Its details (including variable bindings) are displayed under the Event Details sub-window (SNMP Notification tree).
12006	Unknown SNMP notification	Net Inspector Server has received an SNMP Trap or Inform notification message that has an invalid format.
14000	Action test	Reserved for future use.
14001	Failed to send message	Send e-mail or SMS message action could not be performed. Possible reasons: E-mail server rejected the message…
15000	HTTP service failed	HTTP service is not responding to queries within the given time frame or a different response than expected has been received (e.g., an error message).
15001	SMTP service failed	SMTP service is not responding to queries within the given time frame or a different response than expected has been received.
15002	FTP service failed	FTP service is not responding to queries within the given time frame or a different response than expected has been received.
15003	DNS service failed	DNS service is not responding to queries within the given time frame or a different response than expected has been received.
15004	POP3 service failed	POP3 service is not responding to queries within the given time frame or a different response than expected has been received.
15005	IMAP service failed	IMAP service is not responding to queries within the given time frame or a different response than expected has been received.

15006	HTTPS service failed	HTTPS service is not responding to queries within the given time frame or a different response than expected has been received.
15007	NNTP service failed	NNTP service is not responding to queries within the given time frame or a different response than expected has been received.
15008	MySQL service failed	MySQL service is not responding to queries within the given time frame or a different response than expected has been received.
15009	Telnet service failed	Telnet service is not responding to queries within the given time frame or a different response than expected has been received.
15010	LDAP service failed	LDAP service is not responding to queries within the given time frame or a different response than expected has been received.
15011	MsSQL service failed	MsSQL service is not responding to queries within the given time frame or a different response than expected has been received.
15012	SSH service failed	SSH service is not responding to queries within the given time frame or a different response than expected has been received.
15013	LPD service failed	LPD service is not responding to queries within the given time frame or a different response than expected has been received.
15014	NNTPS service failed	NNTPS service is not responding to queries within the given time frame or a different response than expected has been received.
15015	LDAPS service failed	LDAPS service is not responding to queries within the given time frame or a different response than expected has been received.
15016	IPP service failed	IPP service is not responding to queries within the given time frame or a different response than expected has been received.
15017	IMAPS service failed	IMAPS service is not responding to queries within the given time frame or a different response than expected has been received.
15018	Oracle service failed	Oracle service is not responding to queries within the given time frame or a different response than expected has been received.
15019	Custom service failed	Custom (user-defined) service is not responding to queries within the given time frame or a different response than expected has been received.
15020	SIP service failed	SIP service (used for VoIP signaling) is not responding to queries within the given time frame or a different response than expected has been received.
15021	H.323 service failed	H.323 service (used for VoIP signaling) is not responding to queries within the given time frame or a different response than expected has been received.