Chapter 9

# Configuring the SNMP Traps on a Solaris Platform

This chapter describes how to configure and use the Simple Network Management Protocol (SNMP) agent on a Solaris platform using the configuration applications that run only on Solaris platforms.

You can also use the CLI that runs on Solaris platforms and the C-series platforms to configure the SNMP agents. See *Chapter 8, Configuring the SNMP Traps with the SRC CLI*.

Topics in this chapter include:


- Overview of SNMP Traps on page 54
- SNMP Agent Hierarchy and Objects on page 57
- Adding Subfolders in SDX Admin for an SNMP Agent on page 61
- Deleting Subfolders in SDX Admin for an SNMP Agent on page 61
- Adding System Management Configuration for an SNMP Agent on page 61
- Deleting System Management Configuration for an SNMP Agent on page 61
- Adding an SNMP Agent Component on page 62
- Deleting an SNMP Agent Component on page 65
- About Configuring Traps on page 66
- Adding Traps on page 66
- Deleting Traps on page 69

## Overview of SNMP Traps

The SNMP agent provides network management systems with SNMP trap notifications in case of component failure or when critical resources are out of configurable limits. This information is captured in a Management Information Base (MIB).

The SNMP agent can be run on each SRC host. It can monitor any SRC process running on the host and is preconfigured to monitor SRC processes. Additionally, it provides detailed monitoring and configuration of SRC server components.

The SNMP agent automatically discovers SRC components that expose component-specific management information and components that are directory eventing system (DES) clients (that is, have a directory connection managed by DES). When the SNMP agent discovers a component, it adds variables and table entries to its MIB to export the component's management capabilities.

For components that are automatically discovered, the SNMP agent communicates directly with a management server built into the components. For these components, the agent can perform exhaustive tests to determine operability rather than just determining process status. The SNMP agent ensures that the management infrastructure built into the component continues to respond to management requests.

In addition to monitoring components that it automatically discovers, you can also configure the SNMP agent to monitor any process or collection of processes running on its host. The SNMP agent monitors processes by looking at entries in the process table. For many processes that are run only once, such as directory servers, it is sufficient to monitor the single entry in the process table that includes the command used to start the process.

When a component is written in Java or Python, you need to differentiate between the different instances of the Java or Python process because there will be multiple processes in which the executed command is **java** or **python**. The technical name field in the component definition allows you to make this differentiation. The technical name of a component is the command that is used to start the process for the component. In the case of a Java program, the technical name is the name of the main Java class that is specified as an argument to the **java** command. For a Python program, it is the name of the script that is specified as an argument to the **python** command.

### *MIBs*

The SNMP agent monitors MIB variables. Most variables measure the performance of the system. Some variables are counters, such as the saeLogins variable, which counts the total number of subscriber logins since startup. Some variables are gauges, and their numbers go up and down, such as the saeHeapUsed variable, which measures the Java Virtual Machine heap that is currently in use.

A MIB defines a trap type that is associated with many MIB variables. For traps based on counters, the SNMP agent periodically polls each specified variable. It takes the difference between the previous and current values of the variable and compares that difference with the threshold. If the value has moved up across thresholds, the SNMP agent sends a trap raising an alarm (minor, major, or critical) for the highest threshold crossed to all configured receivers. If the value has moved down across thresholds, the agent sends a trap clearing the alarm of the lowest threshold crossed.

You can configure the polling interval between samples. If you change the polling interval, also adjust the thresholds. For instance, if the critical threshold for SAE logins is 1,000 and the interval is 60 seconds, then a critical alarm is raised if there are more than 1,000 logins in 60 seconds. But if you change the interval to 600 seconds, then you would need to change the threshold to 10,000 to have the same meaning.

For traps based on gauges, the previous value is not needed; the current value is compared with the thresholds.

In the trap tables, there is a field named R/AV, where R means rate, and AV means absolute value. Rate is used for variables that are counters, and it measures the rate of change of the counter. Absolute value is used for variables that are gauges.

For a list of all traps, see *Chapter 10, Understanding Traps*.

## *IOR Files*

An SRC component writes its object references to an interoperable object reference (IOR) file, and the SNMP agent discovers components by monitoring IOR files.

SRC components have a property called sysman.iordirectory that specifies the location of the IOR file for the component. The default value for the location is the *var* folder relative to the SNMP agent folder (*/opt/UMC/agent/var*). If you install the SNMP agent in a folder other than the default, or if you previously changed the sysman.iordirectory property to a folder other than */opt/UMC/agent/var,* you need to change the property so that it points to the folder where the IOR file currently resides.

The following sections provide the location and name of the property file for each component.

### SNMP Agent

Use this information to access the SNMP agent property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/agent/config*
- Name of property file—smagent.prop
- Property name—smagent.sysman.iordirectory
- Default value—*var*

You can change the location of the IOR file for the SNMP agent with the local configuration tool for the SNMP agent. Set this property in the Sysman Agent IOR Directory field.

See *SRC-PE Getting Started Guide, Chapter 31, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*.

### SAE

Use this information to access the SAE property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/sae/etc*
- Name of property file—default.properties
- Property name—sysman.iordirectory
- Default value—*/opt/UMC/agent/var*

You can change the location of the IOR file for the SAE with the local configuration tool for the SAE. Set this property in the Sysman Agent IOR Directory field.

See *SRC-PE Getting Started Guide, Chapter 30, Setting Up an SAE on a Solaris Platform*.

### License Server

Use this information to access the license server property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/licsvr/etc*
- Name of property file—bootstrap.properties
- Property name—sysman.iordirectory
- Default value—*/opt/UMC/agent/var*

You can change the location of the IOR file for the license with the local configuration tool for the license server. Set this property in the Sysman Agent IOR Directory field.

For information about license server, see *SRC-PE Getting Started Guide, Chapter 12, Customizing and Managing the License Server*.

### NIC Host

Use this information to access the network information collector (NIC) property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/nic/etc*
- Name of property file—nic.properties
- Property name—sysman.iordirectory
- Default value—*/opt/UMC/agent/var*

You can also change the location of the IOR file for the NIC host with the local configuration tool for the NIC. Set this property in the Sysman IOR field.

For information about NIC hosts, see *SRC-PE Network Guide, Chapter 11, Configuring NIC on a Solaris Platform*.

### Web Redirector

Use this information to access the Web redirector property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/redir/etc*
- Name of property file—redir.properties
- Property name—agent.path
- Default value—*../agent/var*

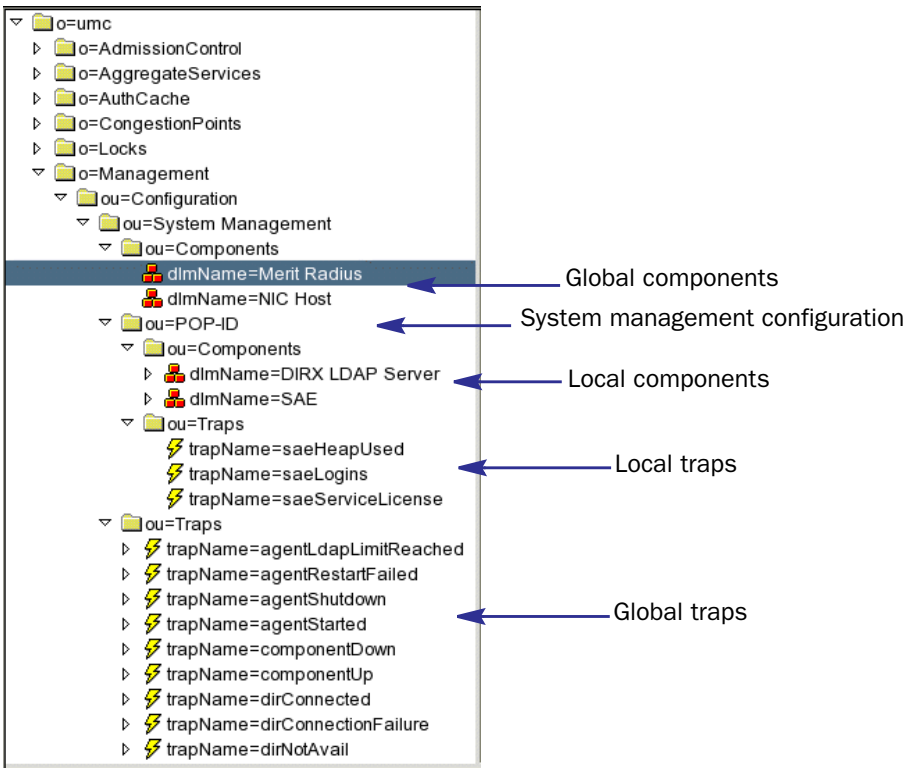
## SNMP Agent Hierarchy and Objects

The SNMP agent configuration consists of:

- System management configuration
- Subfolders
- Components (local and global)
- Traps (local and global)

Figure 1 shows a sample set of system management objects that make up the SNMP agent.

**Figure 1: SNMP Object Hierarchy in SDX Admin**




## *System Management Configurations*

A system management configuration consists of components and traps. The SRC software comes with a default system management configuration that has an *ou = components* object and an *ou = traps* object. The components and traps in the default system management configuration are called global components and global traps.

You can add components to, delete components from, or modify components in the global components object. You can modify the trap configurations in the global traps object, but you cannot add or delete traps in the global traps object.

You can create additional system management configurations with their own components and traps. System management configurations are a convenient way to specify a configuration for multiple SNMP agents installed on multiple hosts that all run the same set of components.

For instance, if you have a host in a point of presence (POP) that runs an SAE and shadow directory, you could set up a POPHost system management configuration for the POP host. You could also have a host in a back office that runs a master directory, a NIC host, and a RADIUS server. For this setup, you could create a BackOfficeHost system management configuration. Typical deployments have a small number of roles for hosts, and the system management configuration can be shared across a potentially large number of hosts with the same role.

For a given system management configuration, both the local and global components and traps are considered part of the configuration. Traps in parent system management configurations or subordinate system management configurations are not considered. If a component or trap occurs in both the global and local folder, then the local version overrides the global one.

### *Subfolders*

SDX Admin lets you create subfolders to organize your system management configurations.

### *Components*

Components are SRC and other network components that you can monitor with the SNMP agent; for example, the SAE, NIC hosts, RADIUS servers, directory servers, and SRC license servers.

The SNMP agent automatically creates local components for each SRC package that is installed on the host where it runs. In this case, most attributes of the component are automatically configured, including the type, start, and stop commands, and the installation date and version.

A global component is a component that is defined for all system management configurations. The global component saves you from defining the local component for each individual system management configuration when the local component definitions would all be the same. If you define a global component and a particular system management configuration requires a different definition, you can define a local component that would override the global component definition.

You can also create a container component and put subcomponents into it. Generally, container components are for monitoring components that require multiple processes, such as DirX. The SNMP agent considers the operational status of a container component as up only when all subcomponents are up, and it considers the container down if any of the subcomponents is down.

The container component start and stop commands are ignored when SNMP is used to set the administrative state of the container component. The start and stop commands of the container component are used to start and stop the whole component and are assumed to manage the starting and stopping of the processes corresponding to the contained components.

### Traps

Traps are individual events that the SNMP agent can monitor, such as the number of timeouts or errors that have occurred or connections that have opened or closed. There are two types of traps:

- Performance traps—Traps that poll MIB variables associated with the trap to determine whether a variable has crossed configured thresholds. If the variable crosses a threshold, an alarm is triggered and a trap is sent to the list of receivers configured in the master agent.

  A global performance trap provides thresholds and polling intervals that are used by default wherever the trap is enabled. To enable a trap for a particular system management configuration, you must create a local version of the trap. Any local definitions of thresholds or polling intervals will override the global definitions.

- Event traps—Traps that are sent when an event occurs; for example, when a connection is established or closed.

  Global event traps do not have any effect on the system management configuration. To enable an event trap for a particular system management configuration, you must create a local version of the trap. To define trap receivers, you must configure the trap receivers in the master agent configuration.

For a list and description of all traps, see *Chapter 10, Understanding Traps*.

### SNMP Traps and Informs

SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. The standard and enterprise-specific traps are compiled into the network management software. For more information on SRC traps, see *Chapter 10, Understanding Traps*. For information on system logging severity levels for SNMP traps, see ***Chapter 2, Configuring Logging for SRC Components***.

With traps, the receiver does not send any acknowledgment when it receives a trap and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. With an inform, the receiver acknowledges the message with a response. For information about configuring SNMP notification handling, see the master agent documentation.

## Adding Subfolders in SDX Admin for an SNMP Agent

To use SDX Admin to add a subfolder:

1. In the navigation pane, right-click a system management configuration object or a subfolder object, and select **New > SubFolder**.
2. Enter a folder name in the dialog box, and click **OK**.

   Do not name a subfolder Components or Traps.

## Deleting Subfolders in SDX Admin for an SNMP Agent

To use SDX Admin to delete a subfolder:

1. Delete all objects within the subfolder.
2. Right-click the subfolder, and select **Delete**.

## Adding System Management Configuration for an SNMP Agent

To use SDX Admin to add a system management configuration:

1. In the navigation pane, right-click *ou = System Management* or a subfolder, and select **New > System Management Configuration**.
2. Enter a name in the dialog box, and click **OK**.

   Do not name a system management configuration Components or Traps.

   The software automatically creates a components and traps folder within the system management configuration folder.

You configure the SNMP agent on the desired host(s) to use the system management configuration by setting the Configuration Directory Base DN field in the SNMP agent local configuration tool.

See *SRC-PE Getting Started Guide, Chapter 31, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*.

## Deleting System Management Configuration for an SNMP Agent

To use SDX Admin to delete a system management configuration:

1. In the navigation pane, right-click any component or trap object subordinate to the system management configuration, and select **Delete**; repeat for all such objects.
2. Right-click the subordinate Components object, and select **Delete**; repeat for Traps.
3. Right-click the system management configuration object, and select **Delete**.

## Adding an SNMP Agent Component

To use SDX Admin to add a component:

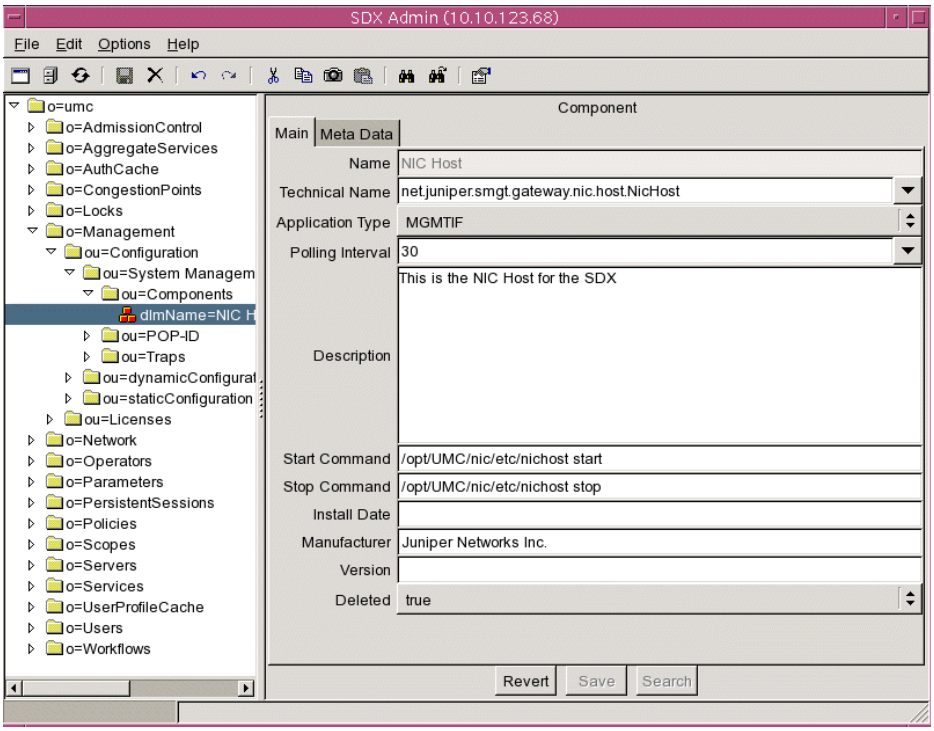
1. In the navigation pane, select a component folder. For example:

   *ou = Components, ou = System Management, ou = Configuration, o = Management, o = umc*

2. Right-click *ou = Components*, and select **New > Component**.

3. In the New Component dialog box, enter a name or select a name from the drop-down list. Names must be no more than 50 characters.

   The Component pane appears. If you selected a name from the drop-down list, the software fills in default values.




4. Edit or accept the default values for the SNMP fields.

   See *SNMP Component Fields* on page 63.

5. Click **Save**.

6. Restart the SNMP agent to update the agent with the changes.

## SNMP Component Fields

In SDX Admin, you can modify the following fields in the content pane for SNMP components.

### Technical Name

- Technical name for the component.
- Value—You can enter a value or select a value from the drop-down list. The value depends on the application type:
  - For a PYTHON application type, use the path to the file that contains the Python program that is executed by the Python process as it appears on the command line of the executed Python command. (Because all Python components run in a process in which the command name is **python**, you must provide the path to distinguish the Python program from other Python components running on the same host.)
  - For a PROCESS application type, use the executed command.
  - For a JAVA application type, use the full package/class name of the class with the "main" function that appears as an argument to the Java command that starts the component. (Because all Java components run in a process in which the command name is **java**, you must provide the name of the main class for a Java component to distinguish it from other Java components running on the same host.)
  - For CONTAINER and MGMTIF application types, the technical name of the component is not necessary and is ignored.
- Default—If you selected a name in the New Component dialog box, the software enters a technical name for you. Otherwise, there is no default.
- Example—net.juniper.smgt.gateway.nic.host.NicHost

### Application Type

- The application type of the component.
- Value
  - JAVA—Java process
  - MGMTIF—Management interface used to monitor SRC-based components, such as subscriber portals or the Workflow application.
  - PROCESS—UNIX process, such as Merit RADIUS
  - PYTHON—Python process
  - CONTAINER—Component that groups related components that need to be monitored as a group. In the MIB, a container component sends a trap if any of its contained components fails. See *Components* on page 59.
- Guidelines—A container component cannot contain another container. It can contain only Python, process, Java, or mgmtif components.
- Default—If you selected a name in the New Component dialog box, the software enters an application type for you. Otherwise, there is no default.

***Polling Interval***

- Length of the interval between checks by the SNMP agent that the component is running.
- Value—Number of seconds in the range 1–3600. You can enter a value or select a value from the drop-down list.
- Default—Depends on the type of component

***Description***

- Text description of the component.
- Value—String
- Guidelines—Optional
- Default—No value

***Start Command***

- Software command that starts the component.
- Value—Path and command
- Guidelines—The software must be configured to start the component with SNMP. When SNMP is used to set the administrative state of a container component, it ignores the start and stop commands of the container component. The start and stop commands of the container component are used to start and stop the whole component and are assumed to manage the starting and stopping of the processes that correspond to the subcomponents.
- Default—For most SRC components, the software enters the correct start command as long as the component is installed in the default location.
- Example—/opt/UMC/sae/etc/sae start

***Stop Command***

- Software command that stops the component.
- Value—Path and command
- Guidelines—The software must be configured to stop the component with SNMP. When SNMP is used to set the administrative state of a container component, it ignores the start and stop commands of the container component. The start and stop commands of the container component are used to start and stop the whole component and are assumed to manage the starting and stopping of the processes that correspond to the subcomponents.
- Default—For most SRC components, the software enters the correct stop command as long as the component is installed in the default location.
- Example—/opt/UMC/sae/etc/sae stop

***Install Date***

- Date component was installed.
- Value—Date in the format YYYYMMDD or YYYYMMDDhhmmssZ
  - YYYYMMDD indicates the year, the month, and the day
  - hhmmss indicates the hour, the minute, and the second
  - Z = Coordinated Universal Time (UTC)
- Guidelines—Optional
- Default—No value

***Manufacturer***

- Component manufacturer.
- Value—Text name of a manufacturer
- Guidelines—Optional
- Default—If you selected a name in the New Component dialog box, the software enters a manufacturer for you. Otherwise, there is no default.

***Version***

- Software version of the component.
- Value—Text or integer
- Guidelines—Optional
- Default—No value

***Deleted***

- Specifies the availability of this entry to other SRC components connected to the directory.
- Value
  - Blank—Other SRC components can access this entry in the directory.
  - True—Other SRC components cannot use this entry in the directory, although the object still exists.
  - False—Other SRC components can access this entry in the directory.
- Default—Blank

## Deleting an SNMP Agent Component

To use SDX Admin to delete a component:

1. In the navigation pane, right-click an object and select **Delete**.
2. Restart the SNMP agent to update the agent with the changes.

## About Configuring Traps

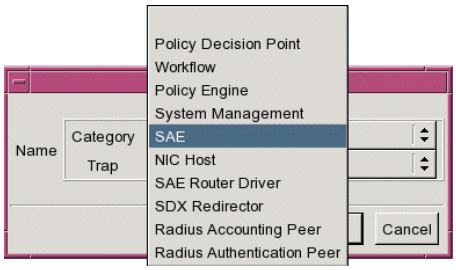
You can modify the trap configurations in the global traps folder, but you cannot add or delete traps in the global traps folder. You can add or delete traps in system management configurations that you create.

*Chapter 10, Understanding Traps* lists all the traps.

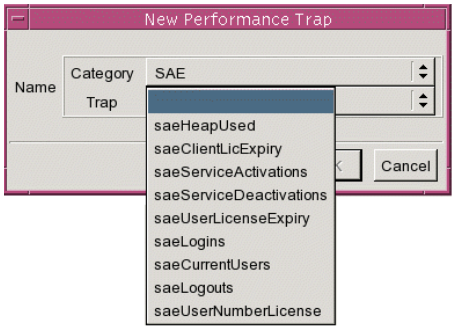
## Adding Traps

To use SDX Admin to add a trap:

1. In the navigation pane, select a system management configuration.
2. Right-click *ou = Traps*, and select **New > Event Trap** or **New > Performance Trap**.
3. In the New Performance Trap or New Event Trap dialog box, select a category from the Category drop-down list. The categories displayed in the list depend on the type of trap that you are creating.




4. Select an item from the Trap drop-down list. The traps displayed in the list depend on the category you selected in the previous step.




5. Click **OK**.

   The Trap pane appears, showing default values for the trap you selected. Figure 2 shows a performance trap. Figure 3 shows an event trap.

6. Edit or accept default values for the SNMP Trap fields to configure the trap.

   See *SNMP Trap Fields* on page 68.

7. Click **Save**.

8. Restart the SNMP agent to update the agent with the changes.

**Figure 2: Performance Trap Pane**

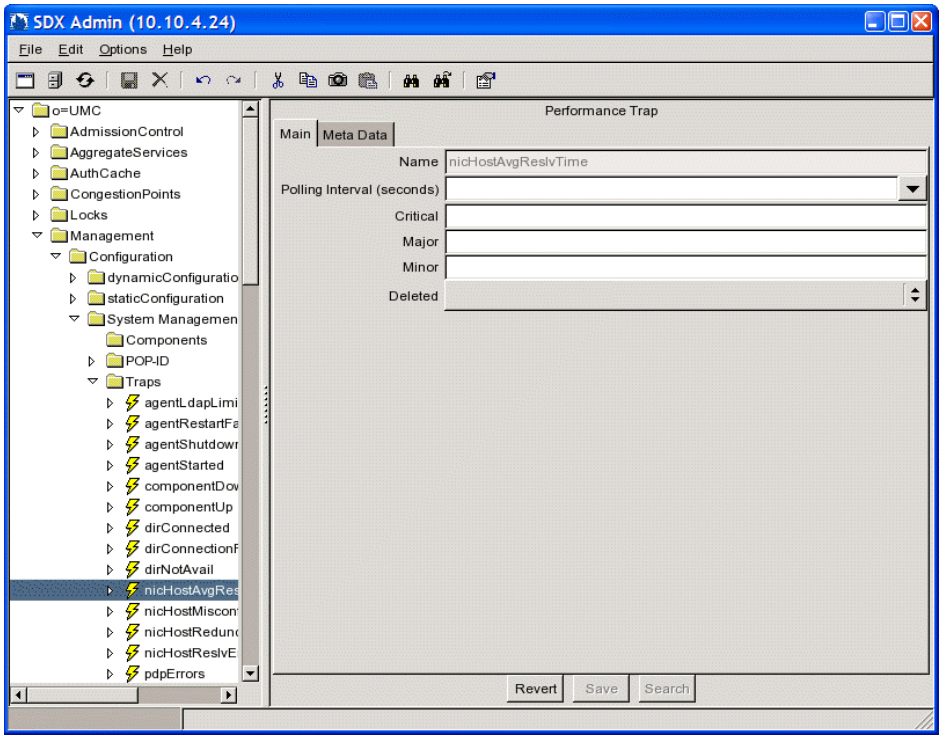
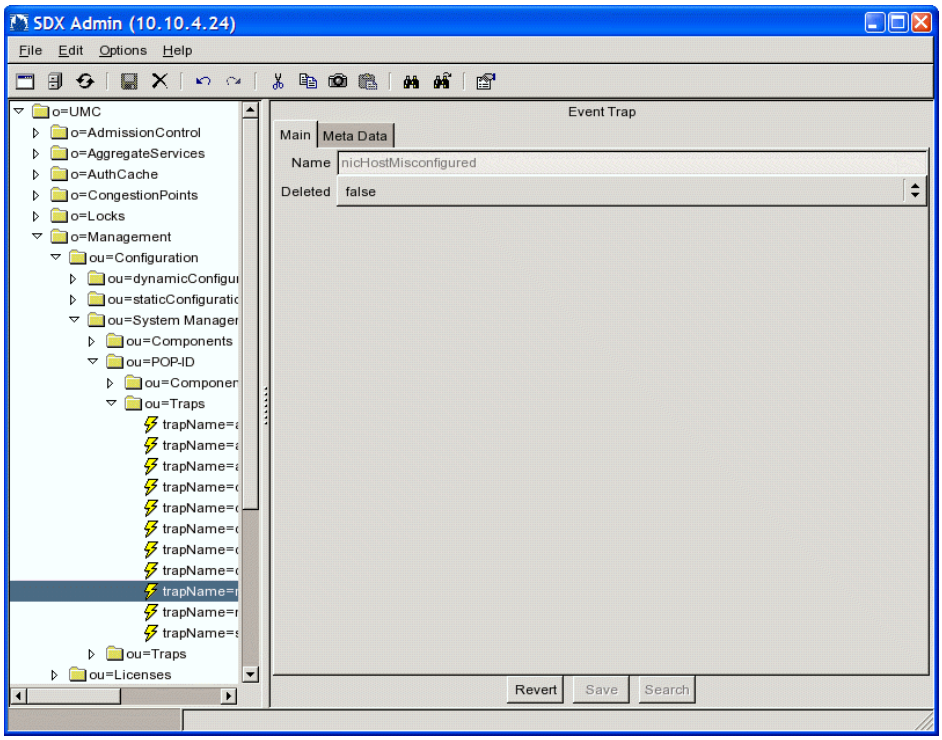


**Figure 3: Event Trap Pane**




## *SNMP Trap Fields*

In SDX Admin, you can modify the following fields in the content pane for an SNMP trap.

### *Polling Interval*

- Interval at which the variable associated with the trap is polled.
- Value —Number of seconds in the range 0–3600. You can enter a specific value or select a value from the drop-down list. If you leave this field blank, the counter is disabled.
- Default—Depends on the type of trap.

### *Critical*

- Threshold above which a critical alarm is generated.
- Value—Integer. The valid range depends on the type of trap. See the tool tip help for the valid range for a trap.
- Default—Depends on the type of trap.

***Major***

- Threshold above which a major alarm is generated.
- Value—Integer. The valid range depends on the type of trap. See the tool tip help for the valid range for a trap.
- Default—Depends on the type of trap.

***Minor***

- Threshold above which a minor alarm is generated.
- Value—Integer. The valid range depends on the type of trap. See the tool tip help for the valid range for a trap.
- Default—Depends on the type of trap.

***Deleted***

- Specifies the availability of this entry to other SRC components connected to the directory.
- Value
  - Blank—Other SRC components can access this entry in the directory.
  - True—Other SRC components cannot use this entry in the directory, although the object still exists.
  - False—Other SRC components can access this entry in the directory.
- Default—Blank

## Deleting Traps

To use SDX Admin to delete a trap:

1. In the navigation pane, right-click the trap object, and select **Delete**.
2. Restart the SNMP agent to update the agent with the changes.