

Chapter 2

Configuring Logging for SDX Components

This chapter describes how to configure logging for SDX components and applications. It contains the following sections:

- Overview of Logging on page 3
- Accessing the Logging Configuration for All Components Except the NIC on page 4
- Accessing the Logging Configuration for the NIC on page 5
- Saving Event Messages in Text Files on page 5
- Saving Event Messages on a Logging Server on page 7
- Specifying Categories and Severity Levels for Event Messages on page 10
- Overview of Deleting Logs and Process Files for SDX Components on page 12
- Deleting Files for SDX Components on page 13

Overview of Logging

SDX components and applications generate event messages that you can save in logs—either by writing the messages to text files or by using the system log (syslog) facilities. You can use these logs to monitor the SDX components and troubleshoot problems.

For more information about system logging, see:

The syslog Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration)

Each SDX component has its own logging configuration. For example, the license server, NIC hosts and monitors, the SAE, and SNMP each have a logging configuration.

You can use SDX Configuration Editor to configure logging for a component.

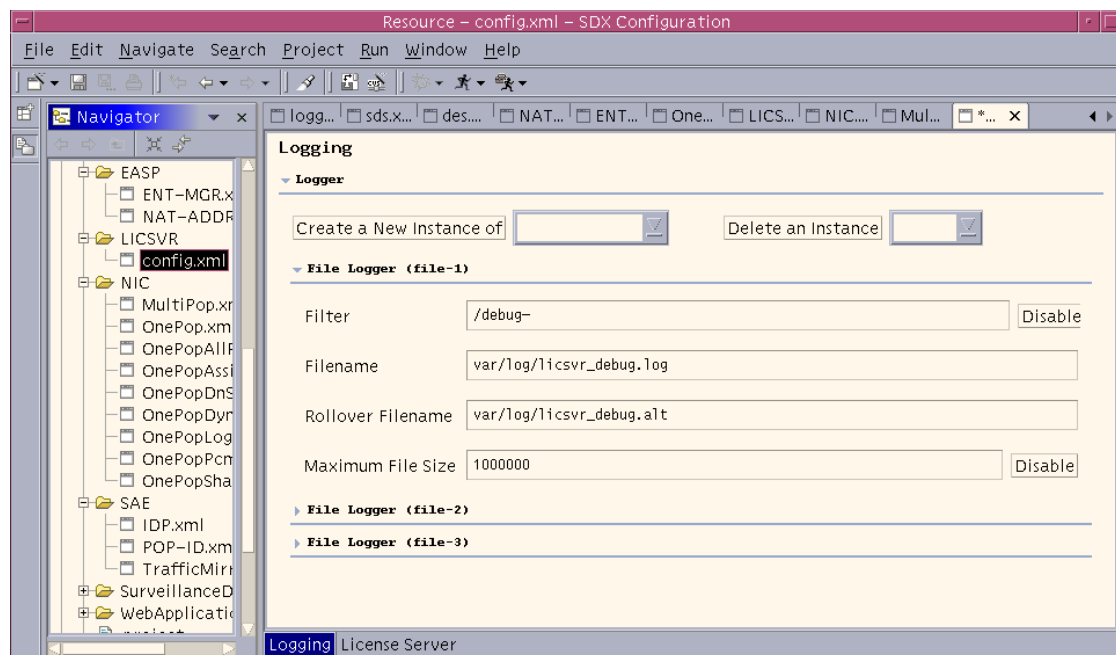
For the SNMP agent, you can also configure logging through the agent's local configuration tool. See *SDX Getting Started Guide, Chapter 10, Configuring and Starting the SDX SNMP Agent*.

Accessing the Logging Configuration for All Components Except the NIC

To access a component's logging configuration in SDX Configuration Editor:

1. In the navigation pane, select the component for which you want to configure logging.
2. Select the Logging tab.

The Logging pane appears. Each SDX component comes with a default logging configuration. This pane changes depending on the component that you select in the navigation pane. The following pane shows the file logging configuration for a license server.



Most components have default logging configurations that you can use as they are or modify.

Accessing the Logging Configuration for the NIC

To access a NIC's logging configuration in SDX Configuration Editor:

1. In the navigation pane, select the NIC for which you want to configure logging.
2. Select the Hosts tab.

The Hosts pane appears. In the Hosts pane, you can configure logging for all NIC hosts on the NIC that you selected, or you can configure logging separately for each NIC host.

The screenshot shows the 'Hosts' configuration pane in the SDX Configuration Editor. It is divided into two main sections. The top section is for configuring logging for all hosts on the NIC, and the bottom section is for configuring logging for a specific host.

Logging configuration for all hosts on the NIC: This section is titled 'Hosts' and contains a 'Logger' section. It has a 'Create a New Instance of' dropdown menu and a 'Delete an Instance' button. Below this is a 'Host' section with another 'Create a New Instance of' dropdown and 'Delete an Instance' button. Underneath, there is a 'Host (DemoHost)' section with fields for 'Hosted Resolvers' (containing '/realms/ip/A1, /realms/ip/B1, /realms/ip/C1') and 'Hosted Agents' (containing '/agents/PoolVr, /agents/VrSaeId'). There is also a 'Redundant Hosts' section.

Logging configuration for a specific NIC host: This section is titled 'Hosts' and contains a 'Logger' section. It has a 'Create a New Instance of' dropdown menu with 'Syslog Logger' selected and a 'Delete an Instance' button. Below this is a 'Syslog Logger (Syslog - DemoHost)' section with fields for 'Filter' (containing '/error-') and 'Syslog Host' (containing 'loghost').

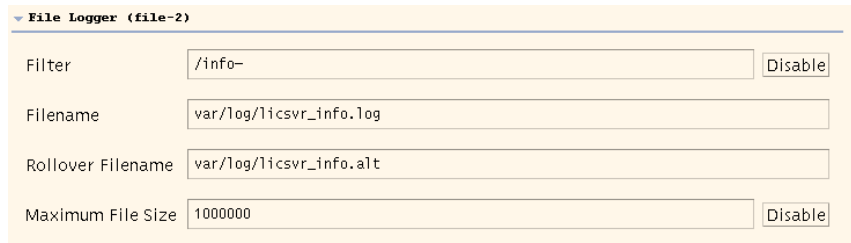
Two blue arrows point from text labels to the configuration fields. The first arrow points to the 'Create a New Instance of' dropdown in the top section, with the label 'Logging configuration for all hosts on the NIC'. The second arrow points to the 'Create a New Instance of' dropdown in the bottom section, with the label 'Logging configuration for a specific NIC host'.

Saving Event Messages in Text Files

To use SDX Configuration Editor to configure the software to save event messages in text files:

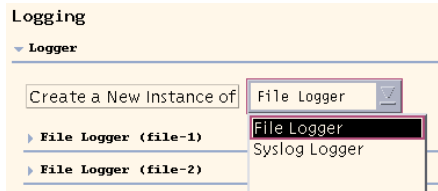
1. In the navigation pane, select the component for which you want to configure logging for text files.
2. Select the Logging tab. (For NIC components, select the Hosts tab.)

The Logging or Hosts pane appears. The following example shows the file logging configuration fields.



Each logging configuration can have multiple instances, with each instance sending different types of logs to different files.

3. (Optional) To create a new logging instance:
 - a. Select File Logger in the Create a New Instance of drop-down list, and click Create a New Instance of.



The Create a New Instance dialog box appears.

- b. Assign a name to the instance, and click OK.

The instance appears in the Logging or Hosts pane.

4. In the section for an individual logger, edit or accept the default values in the fields

See *File Logging Fields* on page 6.

File Logging Fields

In SDX Configuration Editor, you can modify the following fields in a logger section of the Logging pane in a configuration file.

You can also modify the values in this section in a text file that contains logging properties for an SDX component.

Filter

- Disables or enables and specifies a filter that determines the type of messages that this log file contains.
- Value—See *Specifying Categories and Severity Levels for Event Messages* on page 10
- Default—The default value is different for each type of component.

Filename

- Absolute path of the filename that contains the current logs.
- Value—Text string
- Default—By default, SDX components and applications write log files in the folder where the application is started. However, the user under which the J2EE application server or Web application server runs may not have write access to this folder. For logging to work properly, configure the component or application to write logs in folders to which this user has write access. If you are using the version of JBoss packaged with the SDX software, add the absolute path */opt/UMC/jboss/server/default/log/* to the filenames and rollover filename for each log. For example, for the debug log, use the filename */opt/UMC/jboss/server/default/log/vta_debug.log*.
- Example—*/opt/UMC/jboss/server/default/log/*

Rollover Filename

- Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.
- Value—Text string
- Default—The default value is different for each type of component.
- Example—*/opt/UMC/jboss/server/default/log/*

Maximum File Size

- Disables or enables and sets the maximum size of the log file and the rollover file.
- Value—Number of kilobytes in the range 0–4294967295
- Guidelines—Do not set the maximum file size to a value greater than the available disk space.
- Default—1000000

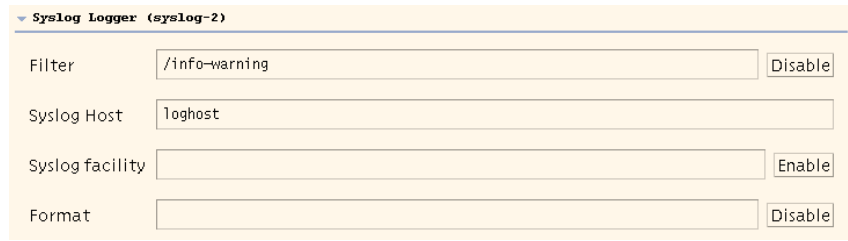
Saving Event Messages on a Logging Server

You can configure the software to save event messages on a host that you have configured as a system logging server. You can also specify the facility for system logging and the format in which the messages will be saved on the host.

To use SDX Configuration Editor to configure the software to save event messages in text files:

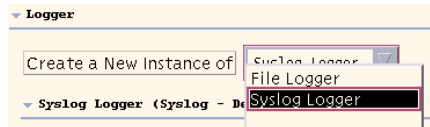
1. In the navigation pane, select the component for which you want to configure logging to a system logging server.
2. Select the Logging tab. (For NIC components, select the Hosts tab.)

The Logging or Hosts pane appears. The following example shows the file logging configuration fields.



Each logging configuration can have multiple instances, with each instance sending different types of logs to different system logging servers.

3. (Optional) To create a new logging instance:
 - a. Select Syslog Logger in the Create a New Instance of drop-down list, and click Create a New Instance of.



The Create a New Instance dialog box appears.

- b. Assign a name to the instance, and click OK.

The instance appears in the Logging or Hosts pane.

4. In the section for an individual logger, edit or accept the default values in the fields

See *System Logging Fields* on page 8.

System Logging Fields

In SDX Configuration Editor, you can modify the following fields in a system logger section of the Logging pane in a configuration file to configure logging to a system log file.

Filter

- Disables or enables and specifies a filter that determines the type of messages that this log file contains.
- Value—See *Specifying Categories and Severity Levels for Event Messages* on page 10
- Default—The default value is different for each type of component.

Syslog Host

- IP address or name of a host that collects event messages by means of a standard system logging daemon.
- Value—IP address or text string
- Default—loghost

Syslog facility

- Type of system log in accordance with the system logging protocol (see *Overview of Logging* on page 3).
- Value—Integer in the range 0–23; each integer corresponds to the standard number for a system logging client
- Default—3

Format

- Specifies how the information in an event message is printed.
- Value—MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event.
- Default—None
- Example for text files—{0,time,HH:mm:ss.SSS z} {0,date,dd.MM.yyyy} [{1}] [{3}] [{4}] {2}

A sample message for the sample setting is:

```
14:13:24.366 EST 19.01.2004 [main] [Start-up module] [20] SAE STARTUP DONE
```

- Example for syslog—SSP[{1}] [{3}] [{4}] {2}

Because the system log system usually timestamps all log messages, no time information is included in the default format. A sample message for the sample setting is:

```
SSP[main] [Start-up module] [20] SAE STARTUP DONE
```

Specifying Categories and Severity Levels for Event Messages

In the filter field of each type of log, you can specify an expression that defines the *categories* and *severity levels* of event messages that the software saves.

Defining Categories

The category of an event message defines the SDX component that generated the event message. If you want to view only event logs in a specific category, you can define a variable `<category>`, which is a text string that matches the name of a category. This variable is not case sensitive. To view the names of categories for event messages, view a log file for one of the default filters (see *Saving Event Messages in Text Files* on page 5).

For example, the category `Cops` defines event messages generated by the COPS server. Similarly, the category `CopsMsg` defines a particular sort of event message that the COPS server generates.

Juniper Networks Customer Service can also provide names of categories, especially for troubleshooting purposes.

Defining Severity Levels

The event filter provides 128 levels of severity numbered 1–127. A higher number indicates a higher level of severity. Common levels of severity also have a specific name, as shown in Table 4.



CAUTION: Enabling the generation of debug log messages has a negative affect on system performance. Do not enable debug log messages unless you are instructed to do so by Juniper Networks Technical Assistance Center (JTAC).

Table 4: Named Severity Levels

Name	Severity Level
logmin	1
debug	10
info	20
notice	30
warning	40
error	50
crit	60
alert	70
emerg	80
panic	90
logmax	127

You can define a severity level as follows:

- Specify an explicit severity. For example:
 - debug—Defines only debug messages
- Specify a minimum severity and a maximum severity. For example:
 - info-warning—Defines messages of minimum severity level of info and a maximum severity level of warning
 - Accept the default minimum (logmin) or maximum (logmax) severity by omitting the minimum or maximum severity. For example:
 - info—Defines messages of minimum severity level info and maximum severity level logmax
 - -warning—Defines messages of minimum severity level logmin and maximum severity level warning
- Specify no severities to log all event messages.

The syntax for the severity takes the format:

```
[ < severity > ] | [ < minimumSeverity > ]-[ < maximumSeverity > ]
```

Use either the name or the number of a severity level shown in Table 4 for the variables in this syntax.

Defining Filters

You specify a filter by defining an expression with the following format:

```
singlematch [,singlematch]*
```

- singlematch—[!] (< category > | ([< category >]/[< severity >] | [< minimumSeverity >]-[< maximumSeverity >]))
- !—Do not log matching events
- < category > —See *Defining Categories* on page 10
- [< severity >] | [< minimumSeverity >]-[< maximumSeverity >]—See *Defining Severity Levels* on page 10.

The software filters events by evaluating each subexpression in order from left to right. When the software determines that an event message matches a subexpression, the software logs or ignores the message accordingly. You can specify an unlimited number of subexpressions; however, the order in which you specify the subexpressions affects the result.

Table 5 shows some examples of filters.

Table 5: Examples of Filters for Event Messages

Syntax	Event Messages Saved
/	All event messages
/info-	Event messages of level info and above from all categories
Cops/debug	Debug events from COPS category only
!Cops,/debug	All debug events except those from COPS category
CopsMsg/info,!CopsMsg,Cops	All messages from COPS category, except those from CopsMsg category with level less than info

Overview of Deleting Logs and Process Files for SDX Components

For the following SDX components, you can issue a command to clean (delete) certain files that are generated by the process for that component.

- License server
- NIC hosts and monitors
- SAE
- SNMP agent

This command cleans:

- Text files that contain event messages.
- The files to which the machine on which you installed the component redirects the stderr and stdout outputs for that the component.
- Other types of files that the process generates and that are not used to reestablish the state of the SDX component when you restart it. These files vary according to each SDX component.

This command does not delete:

- Configurations in the directory or in local files.
- Information generated by the system logging facilities.
- Files that are required to reestablish the state of the SDX component when you restart it.

We recommend that you clean these files for a component when you stop it. When you restart the component, the SDX software creates new files with the same names as the ones you deleted. Cleaning the files keeps the file size small so that you can find data in the files more easily.

Deleting Files for SDX Components

To delete (clean) the files for an SDX component:

1. On the host on which you installed the SDX component, log in as `root` or as another authorized user.
2. Access the folder in which you installed the component.

```
cd /opt/UMC/<sdxComponent>/etc
```

`<sdxComponent >` is the name of the folder in which the SDX component is installed. For information about these names, see *SDX Getting Started Guide, Chapter 5, Installing the SDX-300 Software*.

3. Stop the component.

```
./<sdxComponent> stop
```

4. Clean the logs.

```
./<sdxComponent> clean
```

The system responds with a status message.

5. Restart the SDX component.

```
./<sdxComponent> start
```

For example, to clean files for the SAE, enter the following commands:

```
cd /opt/UMC/sae/etc  
./sae stop  
./sae clean  
./sae start
```

