

Chapter 10

Configuring and Starting the SDX SNMP Agent

This chapter describes how to configure and run the SDX Simple Network Management Protocol (SNMP) agent. It also describes how to install and use the Net-SNMP agent in the SDX environment. It contains the following sections:

- Configuring the SNMP Agent on page 123
- Operating the SNMP Agent on page 133
- Starting the SDX SNMP Agent on page 134
- Stopping the SDX SNMP Agent on page 134
- Monitoring the SDX SNMP Agent on page 134
- Installing and Using the Net-SNMP Agent on page 135

Configuring the SNMP Agent

The SNMP agent monitors host resources and the SDX components that use the host resources. The SNMP agent obtains most of its information from the directory. A local configuration file primarily stores bootstrapping information that cannot be stored in the directory.

The SDX SNMP agent cannot act as a master agent, and it can communicate with master agents only by using the Agent Extensibility (AgentX) protocol. The SDX SNMP agent runs as a subagent to an installed AgentX master agent, such as the Net-SNMP agent. This setup means that SNMP requests to the master agent for SDX MIB objects (typically on port 161) are automatically redirected to the SDX SNMP agent (on its configured port).

You can use the local configuration tool to configure the SNMP agent. For information about using the local configuration tool, see *Chapter 15, Configuring Local Properties*.

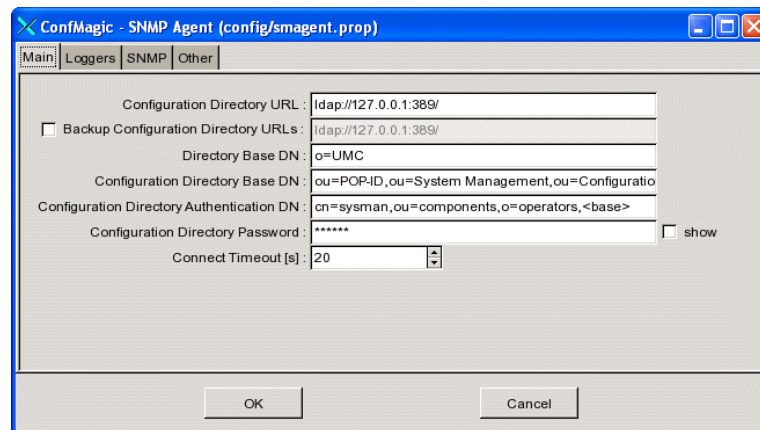
For more information about the SNMP agent, see *SDX Monitoring and Troubleshooting Guide, Chapter 4, Using the SNMP Agent*.

To configure the SNMP agent:

1. On the SAE host, log in as `root` or as an authorized nonroot admin user.
2. Start the local configuration tool from the SNMP agent installation directory.

`/opt/UMC/agent/etc/config -l`

The SNMP Agent screen appears.



3. Configure the SNMP agent by completing the fields in the tabs of the SNMP Agent screen. These sections describe the fields for each tab:
 - *Configuring Directory Connection Parameters on page 124*—Main tab
 - *Configuring SNMP Agent Logging on page 126*—Loggers tab
 - *Configuring Communication with the Master Agent on page 131*—SNMP tab
 - *Configuring Other SDX SNMP Agent Parameters on page 132*—Other tab
4. Click OK when you have completed the configuration, or click Cancel to cancel all changes made since you started the tool.
5. Restart the SNMP agent for the changes to take effect. (See *Starting the SDX SNMP Agent on page 134.*)

Configuring Directory Connection Parameters

Use the Main tab to configure directory connection parameters.

Configuration Directory URL

- URL of the directory server that stores the SNMP agent configuration data.
- Value—URL in the format `ldap:// <URL >`
- Default—`ldap://127.0.0.1/389`

Backup Configuration Directory URLs

- URL of the backup directory server that stores the SNMP agent configuration data.
- Value—URL in the format `ldap:// <URL >`
- Guidelines—Use a semicolon to separate URLs for multiple backup directory servers. Do not insert spaces on either side of the semicolon.
- Default—`ldap://127.0.0.1/389`
- Example—`ldap://127.153.27.1/389;ldap://192.168.0.1/389`

Directory Base DN

- The distinguished name (DN) of the directory used for the SNMP agent configuration data.
- Value— `<DN >`
- Guidelines—You must set this attribute if you use a directory-naming scheme different from the default.
- Default—`o = umc`

Configuration Directory Base DN

- The DN of the system management configuration in the directory server that provides the remaining configuration for the SNMP agent. If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration. See *SDX Monitoring and Troubleshooting Guide, Chapter 4, Using the SNMP Agent*, for details on creating system management configurations for different classes of hosts.
- Value— `<DN >`
- Guidelines—You can use the special value `<base >` to refer to the globally configured base DN.
- Default—`ou = POP-ID, ou = System Management, ou = Configuration, o = Management, < base >`

Configuration Directory Authentication DN

- The DN of the entry in the directory server that authenticates the SNMP agent's directory bind.
- Value— `<DN >`
- Guidelines—You can use the special value `<base >` to refer to the globally configured base DN.
- Default—`cn = sysman, ou = components, o = operators, < base >`

Configuration Directory Password

- The password used for authentication with the directory server.
- Value—String
- Default—`sysman`

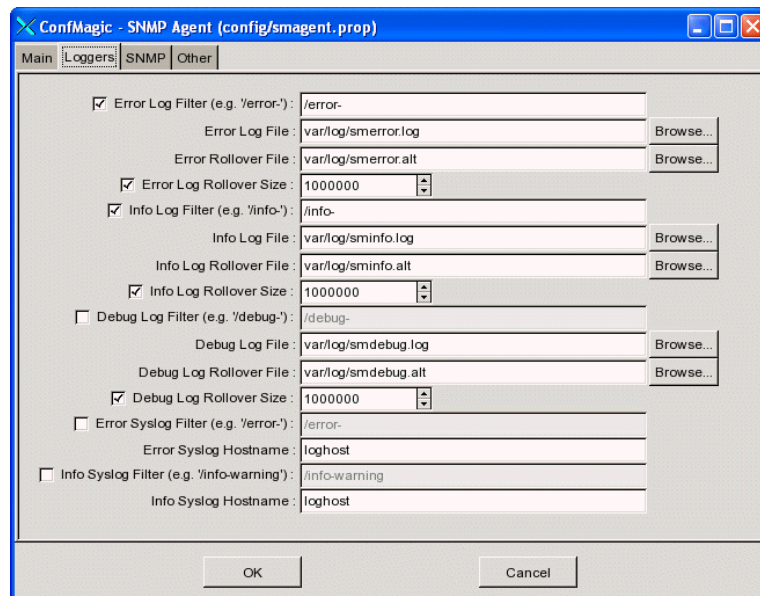
Connect Timeout [s]

- The time limit for establishing a connection to the directory server.
- Value—Number of seconds in the range 1–2147483. If you enter 0 or a negative value, the default configuration of the host's operating system is used.
- Default—20

Configuring SNMP Agent Logging

Use the Loggers tab shown in Figure 21 to configure the SNMP agent logging facility. For more information about the logging attributes and about cleaning the logs, see *SDX Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SDX Components*.

Figure 21: Logging Tab of SNMP Agent Local Configuration Tool

**Severity Levels**

Log filters let you specify the level of severity for the event messages to be saved in log files. 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 17 on page 127.

Enable info-level logging only when you are initially setting up the SDX software or when you are troubleshooting. Do not leave info-level logging on during normal network operation. Do not enable debug logs unless you have been advised to do so by the Juniper Networks Technical Assistance Center. During normal network operations, enable error-level logging.

Table 17: 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

Error Log Filter

- Enable or disable the error log, and specify the minimum severity level of event messages saved to the log file.
- Value—Severity level specified by name or number. See *Severity Levels* on page 126. The format is:
 /severity name-
 or
 /severity number-
- Default—/error-

Error Log File

- Filename and path of the log to which error event messages are saved.
- Value—Path and filename of the log file in the format
 <pathname> / <filename.log>
 - <pathname> —Directory in which the log file is stored
 - <filename.log> —Name of the log file
- Default—*var/log/smerror.log*

Error Rollover File

- Filename of the rollover log file. When the log rollover size is exceeded, the contents of the primary log file are saved to the rollover file.
- Value—Path and filename of the rollover file in the format `< pathname > / < filename.alt >`
 - `< pathname >` —Directory in which the rollover log file is stored
 - `< filename.alt >` —Name of the rollover log file
- Default—`var/log/smerror.alt`

Error Log Rollover Size

- Size of the primary log. If the rollover size is exceeded, the contents of the primary log are saved to the rollover log, overwriting any previous contents. New events are saved to the emptied primary log.
- Value—Number of kilobytes in the range 0–4294967295
- Default—1000000

Info Log Filter

- Enable or disable the info log, and specify the minimum severity level of event messages saved to the log file.
- Value—Severity level specified by name or number. See *Severity Levels* on page 126. The format is:
 - `/severity name-`
 - or
 - `/severity number-`
- Default—`/info-`

Info Log File

- Filename and path of the log to which info event messages are saved.
- Value—Path and filename of the log file in the format `< pathname > / < filename.log >`
 - `< pathname >` —Directory in which the log file is stored
 - `< filename.log >` —Name of the log file
- Default—`var/log/sminfo.log`

Info Log Rollover File

- Filename of the rollover log file. When the log rollover size is exceeded, the contents of the primary log file are saved to the rollover file.
- Value—Path and filename of the rollover file in the format `< pathname > / < filename.alt >`
 - `< pathname >` —Directory in which the log file is stored
 - `< filename.alt >` —Name of the log file
- Default—`var/log/sminfo.alt`

Info Log Rollover Size

- Size of the primary info log. When the rollover size is exceeded, the contents of the primary log are saved to the rollover log, overwriting any previous contents. New events are saved to the emptied primary log.
- Value—Number of kilobytes in the range 0–4294967295
- Default—1000000

Debug Log Filter

- Enable or disable the debug log, and specify the minimum severity level of event messages saved to the log file.
- Value—Severity level specified by name or number. See *Severity Levels* on page 126. The format is:
 /severity name-
 or
 /severity number-
- Default—Disabled

Debug Log File

- Filename of the log to which event messages are saved.
- Value—Path and filename of the log file in the format
 < pathname > / < filename.log >
 - < pathname > —Directory in which the log file is stored
 - < filename.log > —Name of the log file
- Default—*var/log/debug.log*

Debug Log Rollover File

- Filename of the rollover log file. When the log rollover size is exceeded, the contents of the primary log file are saved to the rollover file.
- Value—Path and filename of the log file in the format
 < pathname > / < filename.alt >
 - < pathname > —Directory in which the log file is stored
 - < filename.alt > —Name of the log file
- Default—*var/log/debug.alt*

Debug Log Rollover Size

- Size of the primary log. When the rollover size is exceeded, the contents of the primary log are saved to the rollover log, overwriting any previous contents. New events are saved to the emptied primary log.
- Value—Number of kilobytes in the range 0–4294967295
- Default—1000000

Error Syslog Filter

- Enable or disable the error system log, and specify the minimum severity level of event messages saved to the log file.
- Value—Severity level specified by name or number. See *Severity Levels* on page 126. The format is:
/severity name-
or
/severity number-
- Default—/error-

Error Syslog Hostname

- IP address or name of a host that collects error event messages by means of a standard system logging process.
- Value—IP address or hostname
- Default—loghost

Info Syslog Filter

- Enable or disable the information system log, and specify the minimum severity level of event messages saved to the log file.
- Value—Severity level specified by name or number. See *Severity Levels* on page 126. The format is:
/severity name-
or
/severity number-
- Default—Disabled

Info Syslog Hostname

- IP address or name of a host that collects warning event messages by means of a standard system logging process.
- Value—IP address or hostname
- Default—loghost

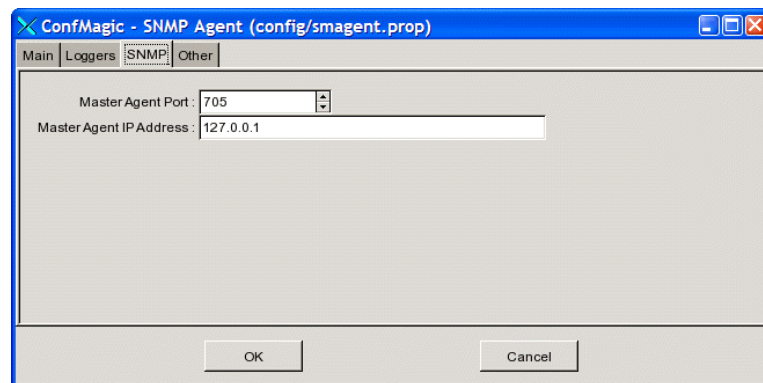
Configuring Communication with the Master Agent

Use the SNMP tab shown in Figure 22 to configure communication with the SNMP master agent.



NOTE: If you change any of the parameters with the local configuration tool, you must restart the SDX SNMP agent.

Figure 22: SNMP Tab of SNMP Agent Local Configuration Tool



Master Agent Port

- TCP port on which the SDX SNMP agent initiates the AgentX connection with the master agent. You must configure your master agent to accept AgentX connections from the SDX SNMP agent host on this port.
- Value—TCP port number
- Default—705

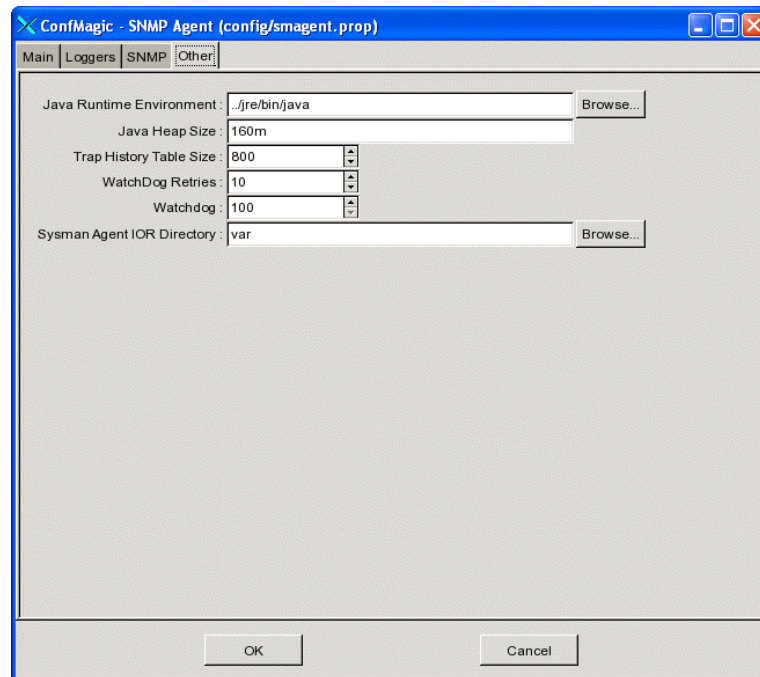
Master Agent IP Address

- IP address of the master agent.
- Value—IP address
- Default—127.0.0.1

Configuring Other SDX SNMP Agent Parameters

Use the Other tab, shown in Figure 23, to configure parameters for the Java Runtime Environment (JRE), trap history, and the watchdog program.

Figure 23: Other Tab of SNMP Agent Local Configuration Tool



Java Runtime Environment

- Path to the JRE.
- Value—Directory in which JRE is stored
- Default—`../jre/bin/java`

Java Heap Size

- Maximum amount of memory available to the JRE.
- Value—Number of megabytes in the format `< integer > m`
- Guidelines—Change this value if you have problems caused by lack of memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping.
- Default—160m

Trap History Table Size

- Maximum number of elements stored in the SNMP trap history table.
- Value—Integer
- Default—800

WatchDog Retries

- Number of times the agent watchdog attempts to restart the agent before sending a trap notification that the agent restart has failed.
- Value—Integer in the range 1–2147483647; 0 or a negative value suppresses the trap
- Default—10

Watchdog

- Polling interval at which the agent watchdog checks whether the agent is running correctly.
- Value—Number of seconds in the range 0–1000000000
- Default—100

Sysman Agent IOR Directory

- Folder that contains the interoperable object reference (IOR) files for SDX components. When the SNMP agent starts, it uses the IOR files in this directory to find SDX components that are already running so that it can connect to them. The SNMP agent also writes its IOR file to this directory so that components that start after the SNMP agent can find and connect to the SNMP agent.
- Value—Path to the folder that contains the IOR files
- Guidelines—By default, the IOR file is in the *var* folder, which is relative to the SNMP agent installation folder (*/opt/UMC/agent*). You need to change this property only if you installed the SNMP agent in a folder other than the default folder, or if you previously changed this property and now need it to point to the folder where the IOR file currently resides.
- Default—*/var*

Operating the SNMP Agent

The SDX SNMP agent can act as a subagent to any AgentX-enabled master agent that is running.

You must configure the SNMP agent and then manually start the agent. If you attempt to manually start the SNMP agent before it is configured, the software displays a message that the agent has not been configured and cannot start.

The SNMP agent automatically restarts in the event of a host reboot or process failure that stops the agent.

Starting the SDX SNMP Agent

Before you start the SDX SNMP agent, you must do the following:

1. Start the installed directory server as described in *Chapter 6, Defining an Initial Configuration*.
2. Configure the SDX SNMP agent as described in *Configuring the SNMP Agent* on page 123.

You must manually start the SDX SNMP agent the first time it runs. Thereafter, the agent automatically restarts.

To start the SNMP agent:

1. On the SNMP agent host, log in as `root` or as an authorized nonroot admin user.
2. Start the SNMP agent from its installation directory.

```
/opt/UMC/agent/etc/smagent start
```

The system responds with a start message. If the SNMP agent is already running, the system responds with a warning message indicating that fact.

Stopping the SDX SNMP Agent

To stop the SNMP agent:

1. On the SNMP agent host, log in as `root` or as an authorized nonroot admin user.
2. Stop the SNMP agent from its installation directory.

```
/opt/UMC/agent/etc/smagent stop
```

The system responds with a stop message. If the SNMP agent is not running when you issue the command, the software responds with a warning message indicating that fact.

Monitoring the SDX SNMP Agent

To display the SDX SNMP agent status:

1. On the SNMP agent host, log in as `root` or as an authorized nonroot admin user.
2. Display the status from the SNMP agent installation directory.

```
/opt/UMC/agent/etc/smagent status
```

The system responds with a status message.

Cleaning SNMP Agent Logs and Process Files

By using the **stdout** and **stderr** options, you can clean the log files for the SNMP agent and delete the persistent data that the agent writes to files or devices. See *SDX Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SDX Components* for more information.

Commands for the Master Agent

Control of the master agent can vary depending on how you have set it up. See the master agent documentation for more information.

Reading the SNMP Agent MIBs

The master agent may support only certain SNMP versions, such as SNMPv2. For example, if you attempt to read the SNMP agent MIBs in a MIB browser and with SNMPv3 settings, then the reading fails. See the master agent documentation for more information.

Installing and Using the Net-SNMP Agent

The SDX software distribution includes a prepackaged integration for the Net-SNMP agent. For information about using the Net-SNMP master agent in an SDX environment, see:

- *Installing the Net-SNMP Agent on page 135*
- *Configuring the Net-SNMP Agent on page 136*
- *Starting the Net-SNMP Agent on page 136*
- *Stopping the Net-SNMP Agent on page 136*
- *Monitoring the Net-SNMP Agent on page 136*
- *Locating the Log File on page 136*

Installing the Net-SNMP Agent

Before you install the Net-SNMP agent, you must install the Python Runtime Environment (SMCpython and UMCpyadd packages) and disable all other SNMP master agents. For more information about installing the SDX software packages, see *Chapter 5, Installing the SDX-300 Software*.

To install the Net-SNMP agent:

1. On the UNIX host where you will install the Net-SNMP agent, log in as **root**.
2. Load SDX software disk 1 in the CD drive.
3. Install the UMCnetsnmp package using the UNIX **pkgadd** tool.

```
pkgadd -d /cdrom/cdrom0/solaris UMCnetsnmp
```

The UMCnetsnmp package is installed in the `/opt/UMC/net-snmp` folder. Once installed, the Net-SNMP agent starts up automatically. The Net-SNMP agent also automatically restarts in the event of a host reboot.

Configuring the Net-SNMP Agent

The configuration file for the Net-SNMP agent is located in the installation directory (by default, `/opt/UMC/net-snmp/etc/snmpd.conf`). For more information about configuring the Net-SNMP agent, see the Net-SNMP documentation at:

<http://net-snmp.sourceforge.net/>

Starting the Net-SNMP Agent

To manually start the Net-SNMP agent:

1. On the Net-SNMP agent host, log in as `root` or as an authorized nonroot admin user.
2. Start the Net-SNMP agent from its installation directory.

```
/opt/UMC/net-snmp/etc/snmpd start
```

Stopping the Net-SNMP Agent

To stop the Net-SNMP agent:

1. On the Net-SNMP agent host, log in as `root` or as an authorized nonroot admin user.
2. Stop the Net-SNMP agent from its installation directory.

```
/opt/UMC/net-snmp/etc/snmpd stop
```

Monitoring the Net-SNMP Agent

To display the Net-SNMP agent status:

1. On the Net-SNMP agent host, log in as `root` or as an authorized nonroot admin user.
2. Display the status from the Net-SNMP agent installation directory.

```
/opt/UMC/net-snmp/etc/snmpd status
```

Locating the Log File

The log file for the Net-SNMP agent is located in the installation directory (by default, `/opt/UMC/net-snmp/log/snmpd.log`).