



# Sun StorageTek™ SL3000 Modular Library System

## Simple Network Management Protocol

### Reference Guide

Part Number: 316194501

Revision: B

September 2009





# Sun StorageTek™ SL3000 Modular Library System

---

## Simple Network Management Protocol Reference Guide

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part Number: 316194501  
September 2009  
Revision: B

**Copyright © 2007, 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.  
All rights reserved.**

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, AnswerBook2, docs.sun.com, and Solaris, Storage Technology, and StorageTek are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright 2007, 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis.  
Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, AnswerBook2, docs.sun.com, et Solaris, StorageTek, e Storage Technology sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciées de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

---

Sun is interested in improving its documentation and welcomes your comments and suggestions, you can:

- Use the OpinionLab [+] feedback system on the documentation Web site

Please include the publication name, part number, and edition number in your correspondence if they are available.  
This will expedite our response.



Please  
Recycle



# Summary of Changes

---

EC Number	Date	Revision	Description
000348	April 2008	A	Initial release
	September 2009	B	Updated to include these additional object identifiers (OID's): <ul style="list-style-type: none"><li>• sICap</li><li>• sIDrive</li><li>• sIInventory</li><li>• sILibVersion</li><li>• sIPowerSupply</li><li>• sIRobot</li><li>• sIStorage</li></ul>

Change bars are used in this manual to help identify the updates.



# Contents

---

<b>Preface</b> .....	<b>xi</b>
Organization .....	.xi
Related Publications .....	.xi
Additional Information .....	xii
Sun's External Web Site .....	xii
Documentation and Download Web Sites .....	xii
Partners Site .....	xii
<b>1: Introduction</b> .....	<b>1</b>
Architecture .....	1
SNMP Terms .....	2
Versions .....	3
Protocol .....	4
Management Information Base .....	5
Agents .....	6
Management Stations .....	6
Commands .....	6
What is a Trap or Notification? .....	6
<b>2: Management Information Base</b> .....	<b>7</b>
Access Control .....	7
Management Information Base .....	8
MIB Variables .....	9
Library Type .....	9
Library Location .....	9
Library Date .....	9
Additional MIB Variables .....	10
Cartridge Access Ports .....	11
Inventory .....	12
Power Supply .....	13
Robotics .....	14
Storage .....	15
Tape Drives .....	16
Versions .....	18

<b>3: Configuration</b> .....	<b>19</b>
SNMP Default Settings .....	19
SNMP Configuration Sequence .....	20
Retrieve the Management Information Base .....	21
Command Line Interface Entries .....	22
Add Trap Recipients .....	22
Add Users .....	22
Delete Trap Recipients .....	23
Delete Users .....	23
Disable Port ID .....	23
Enable Port ID .....	24
List Trap Recipients .....	24
List Users .....	24
Configure the SNMP Service Information .....	25
Examples of SNMP Entries .....	26
Adding a Trap Recipient .....	26
Adding a User .....	27
Deleting a Trap Recipient .....	27
Deleting a User .....	28
<b>4: Traps, Events, and Notifications</b> .....	<b>29</b>
SNMP Traps and Notifications .....	29
Organization .....	29
Levels .....	30
Generic Traps .....	31
Error Trap .....	32
Warning Trap .....	32
Information Trap .....	33
Specific Traps .....	34
Agent Boot Date .....	35
Library Status Good .....	35
Library Status Check .....	35
Environmental Hardware Check .....	36
Drive Status Good .....	36
Drive Status Check .....	37
CAP Status Good .....	37
CAP Status Open .....	37
CAP Status Check .....	38
<b>A: Hewlett-Packard OpenView</b> .....	<b>39</b>
SNMP Configuration .....	39
Hewlett-Packard OpenView .....	40



Loading the MIB .....	40
Configuring SNMP Events .....	40
Critical, Error Alarms (Red) .....	41
Major Events (Orange) .....	42
Warning Events (Cyan) .....	43
Normal, Informational Events (Green) .....	43
<b>B: CA Unicenter .....</b>	<b>45</b>
SNMP Configuration .....	45
CA Unicenter .....	46
Installing NSM .....	47
Starting the NSM Enterprise Manager .....	47
Installing the NSM Trap Manger .....	48
Loading the NSM Trap Manager .....	48
<b>Glossary .....</b>	<b>51</b>
<b>Index .....</b>	<b>53</b>



# Tables

---

Table 1. Versions of SNMP	3
Table 2. Protocol Comparisons	4
Table 3. MIB Request for Comment Standards	5
Table 4. Library Type	9
Table 5. Location	9
Table 6. Date and Time of Day	9
Table 7. Cartridge Access Port Data	11
Table 8. Cartridge Inventory	12
Table 9. Power Supply Count and Data	13
Table 10. Robot Data	14
Table 11. Storage Elements	15
Table 12. Tape Drive Data	16
Table 13. Library Firmware Version	18
Table 14. SNMP Default Settings	19
Table 15. Trap Levels	30
Table 16. Generic Traps	31
Table 17. Error Trap	32
Table 18. Warning Trap	32
Table 19. Information Trap	33
Table 20. Specific Traps	34
Table 21. Agent Boot Date	35
Table 22. Library Status Good	35
Table 23. Library Status Check Condition	35
Table 24. Environmental Hardware Check	36
Table 25. Drive Status Good	36
Table 26. Drive Status Check	37
Table 27. CAP Status Good	37
Table 28. CAP Status Open	37
Table 29. CAP Status Check	38



# Preface

---

This reference guide provides information about the Simple Network Management Protocol (SNMP) and the implementation on Sun StorageTek SL3000 modular libraries.

## ■ Organization

The organization of this guide is:

Chapter	Use this chapter to:
<a href="#">Chapter 1, "Introduction"</a>	Get an introduction to SNMP.
<a href="#">Chapter 2, "Management Information Base"</a>	Understand the SL3000 management information base.
<a href="#">Chapter 3, "Configuration"</a>	Configure the SL3000 library to support SNMP.
<a href="#">Chapter 4, "Traps, Events, and Notifications"</a>	See the supported traps for the SL3000 library.
<a href="#">Appendix A, "Hewlett-Packard OpenView"</a>	Implement SNMP for this application.
<a href="#">Appendix B, "CA Unicenter"</a>	Implement SNMP for this application.
<a href="#">Glossary</a>	Learn terms and abbreviations used in this guide.
<a href="#">Index</a>	Locate information in this guide.

## ■ Related Publications

All publications listed below are available in portable document format (PDF).

Description	Part Number
<i>SL3000 System Assurance Guide</i>	316194101
<i>SL3000 User's Guide</i>	316194401
<i>SL3000 Library Installation Manual</i> (Service representatives only.)	316194201

## ■ Additional Information

Sun Microsystems, Inc. (Sun) offers several methods to obtain additional information.

### Sun's External Web Site

Sun's external Web site provides marketing, product, event, corporate, and service information. The external Web site is accessible to anyone with a Web browser and an Internet connection.

Sun Microsystems, Inc. Sunexternal Web site is: <http://www.sun.com>

StorageTek™ brand-specific information is: <http://www.sun.com/storagetek/>

### Documentation and Download Web Sites

Web sites that enable customers, members, and employees to search for technical documentation, downloads, patches, features, and articles include:

- Documentation: <http://docs.sun.com/app/docs> (customers)
- Documentation: <http://docs.sfbay.sun.com/app/docs> (internal)
- Sun Partner Exchange: <https://spe.sun.com/spx/control/Login>

Firmware and graphical user interface download sites:

- Sun Download Center: <http://www.sun.com/download/index.jsp> (customers)
- Uniform Software Repository: <http://dlrequest.sfbay.sun.com:88/usr/login> (internal)

### Partners Site

The Sun StorageTek Partners site is a Web site for partners with a StorageTek Partner Agreement. This site provides information about products, services, customer support, upcoming events, training programs, and sales tools to support StorageTek Partners. Access to this site, beyond the Partners Login page, is restricted. On the Partners Login page, Sun employees and current partners who do not have access can request a login ID and password and prospective partners can apply to become StorageTek resellers.

The URL for partners with a Sun Partner Agreement is:  
<http://www.sun.com/partners/>

# Introduction

# 1

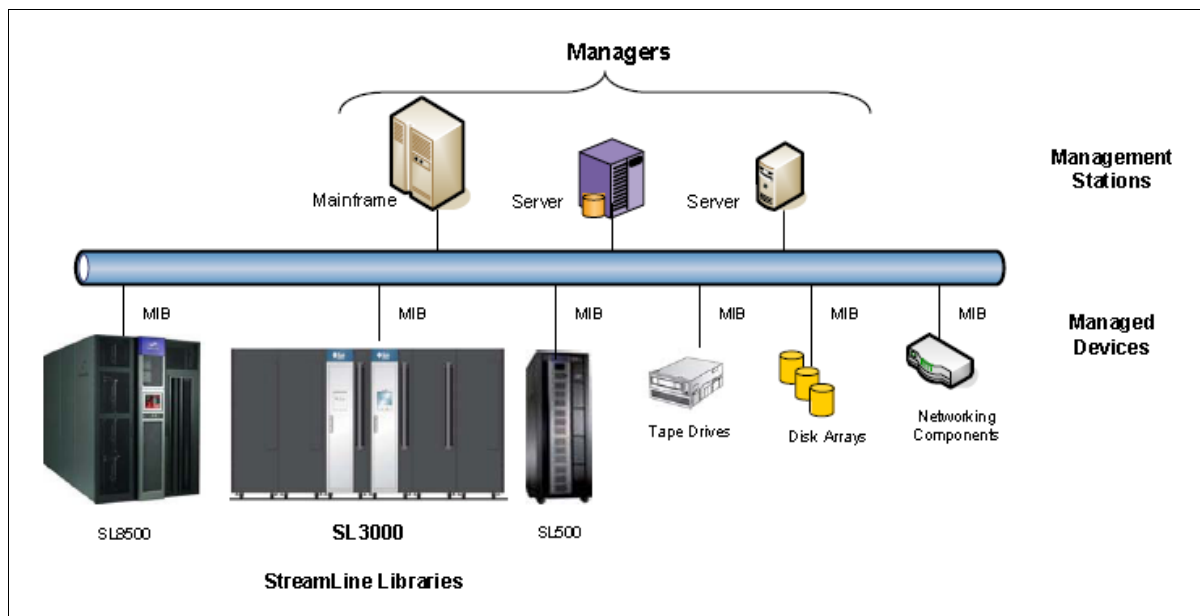
The Simple Network Management Protocol (SNMP) is a network protocol designed to monitor and manage network-attached devices.

This chapter describes the architecture, versions, protocols, and commands for the Simple Network Management Protocol.

## ■ Architecture

The framework for SNMP consists of managed devices, agents, an information base, managers and management station software.

Figure 1. SNMP Architecture



- A *managed device*—such as the SL3000 library—is a network node that contains an SNMP *agent*, which is an SNMP-capable software module.
- The *management information base*—called a MIB—is an ASCII text file, organized hierarchically, that describes the elements of a managed device. When a manager requests information, or a managed device generates a trap, the MIB translates the numerical strings into readable text that identifies each data object within the message.
- The *manager* or *management station* provides the managing, monitoring, and receiving roles of an SNMP-capable network.

## ■ SNMP Terms

SNMP uses a manager/agent structure, a database, and a small set of commands to exchange information. SNMP terms include:

- **Advanced Encryption Standard (AES)**—An NIST-standard cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192, or 256 bits.
- **Agent**—A module that resides in a managed device. The agent is responsible for responding to requests from the manager and for sending traps to a recipient that inform the systems administrator of potential problems.
- **Community String**—Applications use community strings for access control. The manager includes the community string in its SNMP messages to an agent. This can be a maximum of 31 alpha-numeric characters.
- **Data Encryption Standard (DES)**—An NIST-standard cryptographic cipher that uses a 56-bit key.
- **EngineID**—An administratively unique identifier of an SNMP v3 engine used for identification, not for addressing.
- **Host keyword**—Currently, the host keyword is limited to the machine's IP address. The maximum keyword length is 31 alpha-numeric characters.
- **Managed device**—A device that hosts the services of an SNMP agent that provides monitored information and controlled operations using SNMP. Sun StorageTek libraries are managed devices.
- **Management Information Base (MIB)**—A collection of information stored in a database that contains configuration and statistical information for a managed device. For Sun StorageTek libraries, a copy of the MIB is loaded with microcode and stored on the library control card.
- **Manager**—Provides the communication link between the systems administrator and the managed devices on the network. A management station or server allows the systems administrator to get information about the device through the MIB and to receive traps from an agent.
- **Message Digest 5 (MD5)**— A popular one-hash function that creates a message digest for digital signatures. MD5 is faster than SHA, but is less secure.
- **National Institute of Standards and Technology (NIST)**—An agency of the Commerce Department's Technology Administration.
- **Recipient**—A location on a manager where the SNMP agent sends traps. This location is defined by the combination of either the IP address or DNS name and the port number. The default recipient port number is 162.
- **Secure Hash Algorithm**—A popular one-hash algorithm that creates a digital signature; it is more secure than MD5.
- **Trap/Notification**—A message that reports a problem, error, or significant event that occurred within the device.
- **Trap Level String**—The list of trap levels. The maximum length is 31 alpha-numeric characters.



## ■ Versions

Within the group of computer network engineers, *Request for Comments* (RFCs) are a series of documents that members use to define research, innovations, and methodologies applicable to the Internet, such as SNMP.

The Internet Engineering Task Force (IETF) adopts and applies this information creating Internet standards.

There are currently three versions of SNMP; [Table 1](#) lists these versions and the RFCs that define them.

**Table 1. Versions of SNMP**

Version	Comments	Defining RFCs
<b>SNMPv1</b> is the initial release.		
	<ul style="list-style-type: none"> <li>The first version of SNMP is described in RFC 1157</li> <li>This version is a widely used and accepted standard</li> <li>Version 1 has been criticized for its poor security</li> </ul>	RFC 1065: Structure RFC 1066: MIB RFC 1067: Protocol
<b>SNMPv2</b> is a revised protocol, not just a new MIB (RFCs 1592 and 1907).		
– SNMPv2p	<ul style="list-style-type: none"> <li>Party-based (now obsolete)</li> <li>Includes improvements in performance, security, and communications</li> </ul>	RFC 1441 through RFC 1452
– SNMPv2c	<ul style="list-style-type: none"> <li>Community-based</li> <li>Includes SNMPv2p <i>without</i> the controversial security</li> <li>Widely considered the “<i>de facto</i>” SNMPv2 standard</li> </ul>	RFC 1901 through RFC 1908
– SNMPv2u	<ul style="list-style-type: none"> <li>User-based</li> <li>Includes USM (user-based security model)</li> <li>Offers greater security, but without the complexity</li> </ul>	RFC 1909 and RFC 1910
<b>SNMPv3</b> is the latest version.		
	<ul style="list-style-type: none"> <li>Described in RFC 1906, RFC 2572, 2573, and 2574</li> <li>IETF recognizes this as the current standard version</li> </ul>	RFC 3411 through RFC 3418
<b>Notes:</b>		
<ul style="list-style-type: none"> <li>In practice, SNMP implementations often support multiple versions: typically SNMPv1, SNMPv2c, and SNMPv3. Refer to RFC 3584, the <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>, for more information.</li> <li>For more listings and information about SNMP and Requests for Comments, go to the Internet Engineering Task Force (IETF) Web site at: <a href="http://www.ietf.org/">http://www.ietf.org/</a></li> <li>For more information about SNMP, go to: <a href="http://www.snmp.com/">http://www.snmp.com/</a></li> </ul>		

## ■ Protocol

The SNMP specification is based on the User Datagram Protocol (UDP)<sup>1</sup>.

Similar to TCP<sup>2</sup>, UDP runs on top of IP<sup>3</sup> networks (called UDP/IP) using familiar client-server models, such as the OSI<sup>4</sup> model, for data transmissions.

**Note:** OSI standards and the IP protocol suite do not conflict with each other because the two protocol stacks were developed concurrently. However, some differences do exist; *for example*, the OSI model contains seven layers where the IP suite only has four layers.

That said, any other differences between the two are only minor.

Table 2 shows a comparison between the IP Suite and the OSI Model.

**Table 2. Protocol Comparisons**

IP Suite	OSI Model
4. Application layer Applications and end-user processes, such as <b>SNMP</b> , DNS, FTP, HTTP, SMTP, and others.	7. Application layer Applications and end-user processes, such as <b>SNMP</b> , DNS, FTP, HTTP, SMTP, and others.
	6. Presentation layer Transforms data into a format that the application layer can accept.
	5. Session layer Connection coordination.
3. Transport layer: TCP and <b>UDP</b> Transfers data between system components.	4. Transport layer: TCP and <b>UDP</b> Transfers data between system components
2. Internet layer: <b>IP</b> (IPv4)	3. Network layer: <b>IP</b>
1. Link layers: Makes use of existing standards rather than defining its own, such as: 10/100 BaseT and IEEE 802.x There are two different layers: <ul style="list-style-type: none"> <li>- Data link layer</li> <li>- Physical link layer</li> </ul>	2. Data Link layer: Physical addressing, media access control (MAC)
	1. Physical layer: Physical aspects for sending and receiving data

1. UDP = User Datagram Protocol, a *connection-less* communications protocol that offers limited service for exchanging messages between networked devices.
2. TCP = Transmission Control Protocol, a *connection-based* protocol that offers reliable, ordered communications between networked devices.
3. IP = Internet Protocol, the connection method over which data is sent from one device to another on a network. UDP like TCP uses the Internet Protocol to actually get a data unit (datagram or packet) from one computer to another.
4. OSI = Open System Interconnection, a model that defines the concept and describes how information flows from one application through the network into another.

SNMP only uses UDP ports for the transfer of information:

- Port 161 for the *agent*
- Port 162 for the *manager*

Each managed host runs a process called an agent. The agent is a server process that maintains the MIB database for the host.

Hosts that are involved in network management run a process called a manager. A manager is a client application that generates requests for MIB information and processes responses.

The protocol for communications between manager and agent is:

- The manager can send requests from any available port to the agent at port 161. The agent then responds to that source port, to the requesting manager.
- The agent generates traps or notifications and sends them from any available port to the manager at port 162.

## Management Information Base

The management information base (MIB) is a collection of *objects* in a database that SNMP uses to manage devices in a network.

This database is hierarchical in structure—tree-like—with entries called *object identifiers* (OIDs).

This structure permits management across all layers of the OSI model, extending into applications, databases, and area-specific information.

As with SNMP, the MIB has defining standards in the Request for Comment (RFC) format shown in [Table 3](#).

**Table 3. MIB Request for Comment Standards**

RFCs	Description
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1156	Management Information Base for Network Management of TCP/IP-based Internets
RFC 1157	A Simple Network Management Protocol (SNMP)
RFC 1213	Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
RFC 1441	Introduction to Version 2 of the Internet-standard Network Management Framework
RFC 3418	Management Information Base for the Simple Network Management Protocol

## Agents

The SNMP agent:

- Responds to requests from an SNMP manager
- Sends SNMP traps to managers

The objects that an SNMP agent can manipulate are defined in the MIB.

## Management Stations

Management stations are systems or servers that have an SNMP application installed. Examples of these applications include:

- Sun Microsystems SunNet Manager
- HP OpenView
- IBM NetView
- CA Unicenter Network and System Management
- Plus several others

## ■ Commands

SNMP offers a limited number of commands (protocol data units or PDUs) that follow a simple request and response exchange to communicate between the manager and the agent.

The manager issues requests such as:

- **Get:** A request for information of a specific variable.
- **GetNext:** A request for information of the next specific variable.
- **Set:** A request to change the value of a specific variable.

The agent responds with:

- **Get-Response:** A response to the manager's Get commands.

Another communication element between the agent and the manager is the **trap**—also called a notification. These are asynchronous messages to a manager or other recipient about an error or event.

## What is a Trap or Notification?

A trap or notification is a message that reports a problem, error, or significant event that occurred within the device. These messages are sent by the agent to a manager.

This chapter describes the management information base (MIB) for the Sun StorageTek SL3000 modular library to support the SNMP feature.



**Important:** SNMP configuration requirements:

- SL3000 library firmware must be version [FRS\\_1.7](#) or higher.
- StorageTek Library Console version [FRS\\_4.00](#) or higher.
- *By default, the SNMP agent is disabled and must be enabled through the Command Line Interface (CLI) for customers requiring this feature.*

Initially, SNMP can be configured only through the command line interface (CLI)—which requires a service representative working together with systems administrators and network managers to properly configure SNMP for their account.

The StreamLine libraries support the following versions of SNMP:

- **SNMPv2c:** Read-only support, primarily for machine status queries. Any information transmitted *will not* be secure.
- **SNMPv3:** Both read *and* write support; transmitted information *is* secure.

## ■ Access Control

Community strings are capable of providing a form of access control in SNMP. Because of this, the Sun StorageTek embedded agent will not allow community strings to make changes to the library's configuration.

The MIB can be retrieved with either SNMPv2c or SNMPv3; however, because SNMPv3 provides encryption capabilities and a stronger user identification, library properties can be changed only with the SNMPv3 `set` command.

Using an administrative password also provides access control and authorization for `set` command operations.

Traps, however, can be sent to recipients using either SNMPv2c and SNMPv3 by adding entries to the Trap Recipient List.

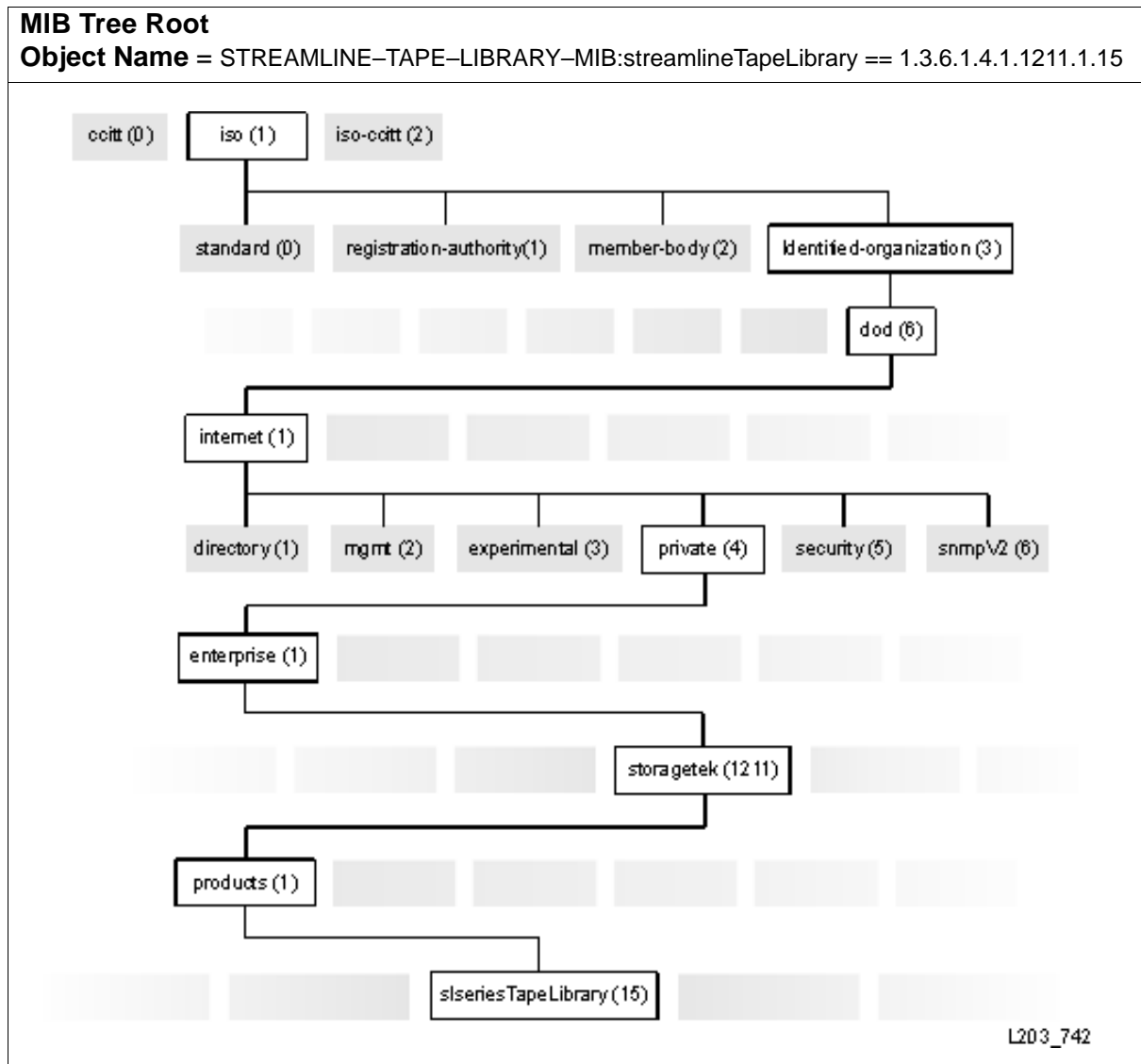
**Note:** Customers can download the MIB through the StreamLine Library Console, but it cannot be directly viewed from the console itself. However, because the MIB is a plain ASCII text file, it can be viewed from any readily available text editor of choice.

## Management Information Base

The management information base (MIB) is a viewable document that contains descriptions about the characteristics for a managed device. These characteristics are the functional elements for that device which can be monitored using SNMP software.

Figure 2 shows the MIB structure for the Sun StorageTek modular libraries. STREAMLINE-TAPE-LIBRARY-MIB

Figure 2. StreamLine MIB Hierarchy



## MIB Variables

MIB variables (or objects) are queried by Get or GetNext commands; for example:

### Library Type

The **sLib** variable provides information about the library; such as type, serial number, and overall operating condition.

**Table 4. Library Type**

Object	Content	Description
1.3.6.1.4.1.1211.1.15.3.1	sLibStkBaseModel	Sun StorageTek Library model number See vendor specific model data
1.3.6.1.4.1.1211.1.15.3.2	sLibSerialNumber	Library frame serial number
1.3.6.1.4.1.1211.1.15.3.3	sLibWWNNumber	Library World Wide Name (WWN). A 64-digit hexadecimal number
1.3.6.1.4.1.1211.1.15.3.4	sLibLibraryTopLevelCondition	Library overall condition (for example: normal, degraded, or not-operational)

### Library Location

The **sLibLocation** variable provides information about the library location.

**Table 5. Location**

Object	Content	Description
1.3.6.1.4.1.1211.1.15.3.10.1	sLibLocatContact	Primary contact for administration
1.3.6.1.4.1.1211.1.15.3.10.2	sLibLocatStreet	Location/site – Street address
1.3.6.1.4.1.1211.1.15.3.10.3	sLibLocatState	Location/site – State/province
1.3.6.1.4.1.1211.1.15.3.10.4	sLibLocatZip	Location/site – ZIP code or other data
1.3.6.1.4.1.1211.1.15.3.10.5	sLibLocatCountry	Location/site – Country
1.3.6.1.4.1.1211.1.15.3.10.6	sLibLocatDescr	Location/site – Description or other data
1.3.6.1.4.1.1211.1.15.3.10.7	sLibLocatCity	Location/site – City

### Library Date

The **sLibDate** variable provides information about the date and time-of-day.

**Table 6. Date and Time of Day**

Object	Content	Description
1.3.6.1.4.1.1211.1.15.3.13.1	sLibDateString	Date and time in the following format: YYYY:MM:DD HH:MM:SS.xxxx

## ■ Additional MIB Variables

Similar to the basic variables, additional variables provide a complete set of variables for full functionality of Sun StorageTek SL3000 libraries and support of SNMP, these include:

[“Cartridge Access Ports” on page 11](#) (sICAP)

[“Inventory” on page 12](#) (sInventory)

[“Power Supply” on page 13](#) (sPowerSupply)

[“Robotics” on page 14](#) (sRobot)

[“Storage” on page 15](#) (sStorage)

[“Tape Drives” on page 16](#) (sIDrive)

[“Versions” on page 18](#) (sLibVersion)



## Cartridge Access Ports

The **sICAP** variable provides information about the cartridge access ports.

**Table 7. Cartridge Access Port Data**

Content	Description
sICapCount	Number of the CAPs in the CAP table
<b>sICapTable</b>	<b>Table of cartridge access ports (CAPs)</b>
sICapEntry	Cartridge access port
sICapIndex	Integer index into the CAP table
sICapAddress	CAP device address
sICapAccessibility	Accessibility of a CAP For example: Open, Allow/Prevent
sICapAccessStateEnum	Access state of the CAP presented as an enumeration Unknown (1), Open (2), Close (3)
sICapState	Physical state of the CAP
sICapStatusEnum	Operational status of the CAP presented as an enumeration OK (0), Error (1), Warning (2), Info (3), Trace (4)
sICapName	CAP name
sICapRotations	CAP rotation count
sICapRotationRetries	Number of rotation retries performed by the CAP
sICapRotationFails	Number of rotation failures performed by the CAP
sICapIPLs	Number of IPL's performed by the CAP

## Inventory

The **sInventory** variable provides information about the contents of the library, such as: number of and types of cartridges and labels in the library.

**Table 8. Cartridge Inventory**

Content	Description
sITapeCount	Number of the cartridges in the inventory table
<b>sITapeTable</b>	<b>Table of data cartridges (tapes) in the library</b>
sITapeEntry	Cartridge
sITapeIndex	Integer index into the inventory table
sITapeLabel	Cartridge label
sITapeType	Cartridge type
sITapeLocationElementID	Cartridge location – Element ID
sITapeHostAccessible	Indication of host accessible status True (1), False (2)

## Power Supply

The **slPowerSupply** variable provides information about the power supplies in the library.

**Table 9. Power Supply Count and Data**

Content	Description
slPowerSupplyCount	Number of power supplies installed in the library
<b>slPowerSupplyTable</b>	<b>Table of the library's power supplies</b>
slPowerSupplyEntry	A power supply
slPowerSupplyIndex	Integer index into the power supply table
slPowerSupplyName	Name of the power supply
slPowerSupplyInstalled	Indicates if the supply is: Not installed (1), installed (2)
slPowerSupplyOperational	Indicates if the supply is OK (2), Meaningless if not-installed: Failed (1), Normal (2)

## Robotics

The **slRobot** variable provides information about the robotics in the library, such as: quantity, firmware, serial numbers, and number of robotic retries.

**Table 10. Robot Data**

Content	Description
slRobotCount	Number of robot mechanisms
slRobotTable	A table of robots (HandBots)
slRobotEntry	A robot entry
slRobotIndex	A robot index
slRobotElementID	Element ID / Address or address of the robot
slRobotPosition	Physical position of the robot in counts
slRobotHandCartStatus	Robot hand state No cartridge (0), Cartridge (1)
slRobotSerialNum	Robot card serial number
slRobotState	Robot state Such as: Empty, Loaded, or Moving
slRobotFaultLED	Robot card serial number
slRobotStatusEnum	Robot operational status in enumerated form OK (0), Error (1), Warning (2), Info (3), Trace (4)
slRobotCodeVer	Robot code version
slRobotVersion	Robot version
slRobotFirmwareVer	Robot firmware version
slRobotGetRetries	Number of mount retries performed by the robot
slRobotPutRetries	Number of dismount retries performed by the robot
slRobotGetFails	The number of Get fails for the individual robot
slRobotPutFails	The number of Put fails for the individual robot
slRobotGetTotals	The sum of all Get operations of individual robot
slRobotPutTotals	The sum of all Put operations of individual robot

## Storage

The **sIStorage** variable provides information about the storage elements, such as: cells or slots, hands or drives, cartridges and labels within the library.

**Table 11. Storage Elements**

Content	Description
sICellCount	Count of the storage elements in the cell table
sICellStorageFreeCells	Number of available (empty) storage cells in the library
sICellStorageRestrictedFreeCells	Number of available restricted (empty) storage cells in the library
<b>sICellTable</b>	<b>Table of storage elements in the library</b>
sICellEntry	Storage element
sICellIndex	Integer index into the storage cell table
sICellElementID	Physical Element ID / Address of the storage cell
sICellHostAccessible	Indication of host accessible status True (1), False (2)
sICellContentStatus	The status of the cell UNKNOWN (0), EMPTY (1), READABLE (2), NOT_READABLE (3), CAP_MAG_NOT_PRESENT (4), DRIVE_NOT_PRESENT (5), DRIVE_NOT_AVAILABLE (6)
sICellContentLabel	The label of the cartridge in the cell (zero length string if empty, '?????' if unreadable)
sICellContentType	The type of the cartridge in the cell (zero length string if empty)
sICellGetRetryCount	Number of get retries performed from this cell
sICellPutRetryCount	Number of put retries performed to this cell
sICellHostType	The type of cell (system, restricted, data) INVALID (0), STORAGE (1), DRIVE (2), CAP (3), PLAYGROUND (4), INTRANSIT (5), PTP (6), HAND (7), GENERIC (8)

## Tape Drives

The **sIDrive** variable provides information about the tape drives.

**Table 12. Tape Drive Data**

Content	Description
sIDriveCount	Count of the drives in the drive table
<b>sIDriveTable</b>	<b>Table of drives</b>
sIDriveEntry	Tape drive entry
sIDriveIndex	Integer index into the drive table
sIDriveElementID	Element ID/Address of the drive
sIDriveType	Drive type (for example: STK9840, LTO4)
sIDriveVendor	Drive vendor (for example: STK, IBM, HP)
sIDriveSerialNum	Drive electronic serial number
sIDriveInterfaceType	Drive physical data transport type Unknown (1), SCSI (2), Fibre (3)
sIDriveID	Drive SCSI ID or Fibre Port assignment
sIDriveState	Drive state (such as: empty, loaded, needs cleaning)
sIDriveLED	Drive Tray LED state Off (0), On (1)
sIDriveStatusEnum	Drive operational status in enumerated form: Initializing (1), Empty (2), Cartridge Present (3), Loading (4), Loaded (5), Cleaning (6), Rewinding (7), Unloading (8), Inoperative (9), Not Loadable (10), Not Unloadable (11)
sIDriveCodeVer	Drive code version
sIDriveVersion	Drive version
sIDriveFirmwareVer	Drive firmware version
sIDriveGetRetries	Number of mount retries performed to the drive
sIDrivePutRetries	Number of dismount retries performed to the drive
sIDriveCommandClean	Signal to clean or cancel cleaning of the drive Enable (1), Cancel (2)
sIDriveCellStatusEnum	Drive cell presented as an enumeration Unknown (1), Empty (2), Full (3)
sIDriveCellStatusText	Drive cell status
sIDriveCellContentLabel	Label of the cartridge in the drive (zero length string if empty, '??????' if unreadable)
sIDriveCellContentType	Type of cartridge in the drive (zero length string if empty)

**Table 12. Tape Drive Data**

<b>Content</b>	<b>Description</b>
slDriveIdleSeconds	Number of seconds that the drive has been idle (un-mounted)
slDriveNumMounts	Number of mounts to the drive
slDriveFibreNodeName	Drive Fibre node name
slDriveFibrePortCount	Number of active ports in the drive Single (1), Dual (2)
slDriveFibrePortAwwn	Port A – World Wide Name (WWN)
slDriveFibrePortAAddressingMode	Port A – Addressing mode Hard (1), Soft (2)
slDriveFibrePortAPortEnabled	Port A – Port enabled Disabled (1), Enabled (2)
slDriveFibrePortALoopId	Port A – Loop ID
slDriveFibrePortAPortSpeed	Port A – Port speed Unknown (1), One Gbit (2), Two Gbit (3), Four Gbit (4)
slDriveFibrePortBwwn	Port B – World Wide Name
slDriveFibrePortBAddressingMode	Port B – Addressing mode Hard (1), Soft (2)
slDriveFibrePortBPortEnabled	Port B – Port enabled Disabled (1), Enabled (2)
slDriveFibrePortBLoopId	Port B – Loop ID
slDriveFibrePortBPortSpeed	Port B – Port speed Unknown (1), One Gbit (2), Two Gbit (3), Four Gbit (4)
slDriveWWNEnabled	Drive World Wide Name option. This option can only be set using the command line interface (CLI).  Contact a Service Representative.  Disabled (1), Enabled (2)
slDriveAddress	The drive's device generic address (either logical or SCSI element ID) as a string.

## Versions

The **sLibraryVersion** variable provides information about the firmware, code, and versions for the library.

**Table 13. Library Firmware Version**

Content	Description
sLibVersionFirmRev	Library embedded firmware version per engineering change (EC) field releases
sLibVersionFirmDate	Library embedded firmware build date
sLibVersionBootRev	Library boot software/OS version
sLibVersionHardware	Library controller hardware version



Because SNMP can only be enabled through the command line interface (CLI), a Sun StorageTek service representative must work with the customer's system administrator to obtain the information they require, make the necessary entries, and then enable SNMP.

This chapter lists the default settings, describes how to configure trap notifications, and references the command line interface commands.

## ■ SNMP Default Settings

Table 14 lists the default settings for a StreamLine library.

**Table 14. SNMP Default Settings**

Setting	Default	Description
Port ID	Disabled	Agent trap requests are sent and received over the HBC card port: <ul style="list-style-type: none"><li>• 2B = standard, public port</li><li>• 2A = optional dual-port feature</li></ul>
Socket number <sup>1</sup>	161	Agent requests are sent/received on the enabled port.
Socket number <sup>1</sup>	162	Traps are sent to this socket on the host port.
SNMPv2c users string <sup>2</sup>	Public	Community String Public Agent Community. Use this field (setting) to <i>read-only</i> MIB data.
SNMPv3 users string <sup>2</sup>	Empty	Community String Public Agent Community. Use this field (setting) to both <i>read</i> and <i>write</i> MIB data.
Trap Recipients	Empty	This list supports up to 20 recipients with no duplicate entries. Users must add themselves to the recipients list for traps to be sent to them. See <a href="#">page 22</a> for information.
SNMP (agent)	Disabled	Enabled or disabled through CLI command <i>only</i> .
<b>Notes:</b>		
1. Socket numbers, or ports, must be enabled to pass through a firewall.		
2. User Strings. There can be a maximum of 20 SNMP users total. This field can be changed or deleted.		

## ■ SNMP Configuration Sequence

To configure SNMP:

1. Have an administrator [Retrieve the Management Information Base](#) from the library, see [page 21](#).

2. Obtain the trap/notification destinations from the administrator:

IP address of the hosts receiving the traps

---

EngineId of the hosts receiving the traps if using SNMPv3

---

Authentication protocol/authPassPhrase (MD5 or SHA /authPassPhrase string) for users and hosts receiving traps if using SNMPv3.

---

Authentication privacy protocol/Privacy PassPhrase (DES or AES / PrivPassPhrase string) for users and hosts receiving the traps if using SNMPv3

---

User names and hosts receiving the traps if using SNMPv3.

---

3. Have a Sun StorageTek service representative log in and use the [“Command Line Interface Entries” on page 22](#) to:

- a. Add users:

```
prompt> addUser
```

- b. Configure trap recipients:

```
prompt> addTrapRecipient
```

- c. Double check that the information was entered correctly, using:

```
prompt> listTrapRecipients and
```

```
prompt> listUsers
```

- d. Enable the agent:

```
prompt> enable port<portID>
```

SNMP traps should now be enabled and the agent should respond to gets from the clients.

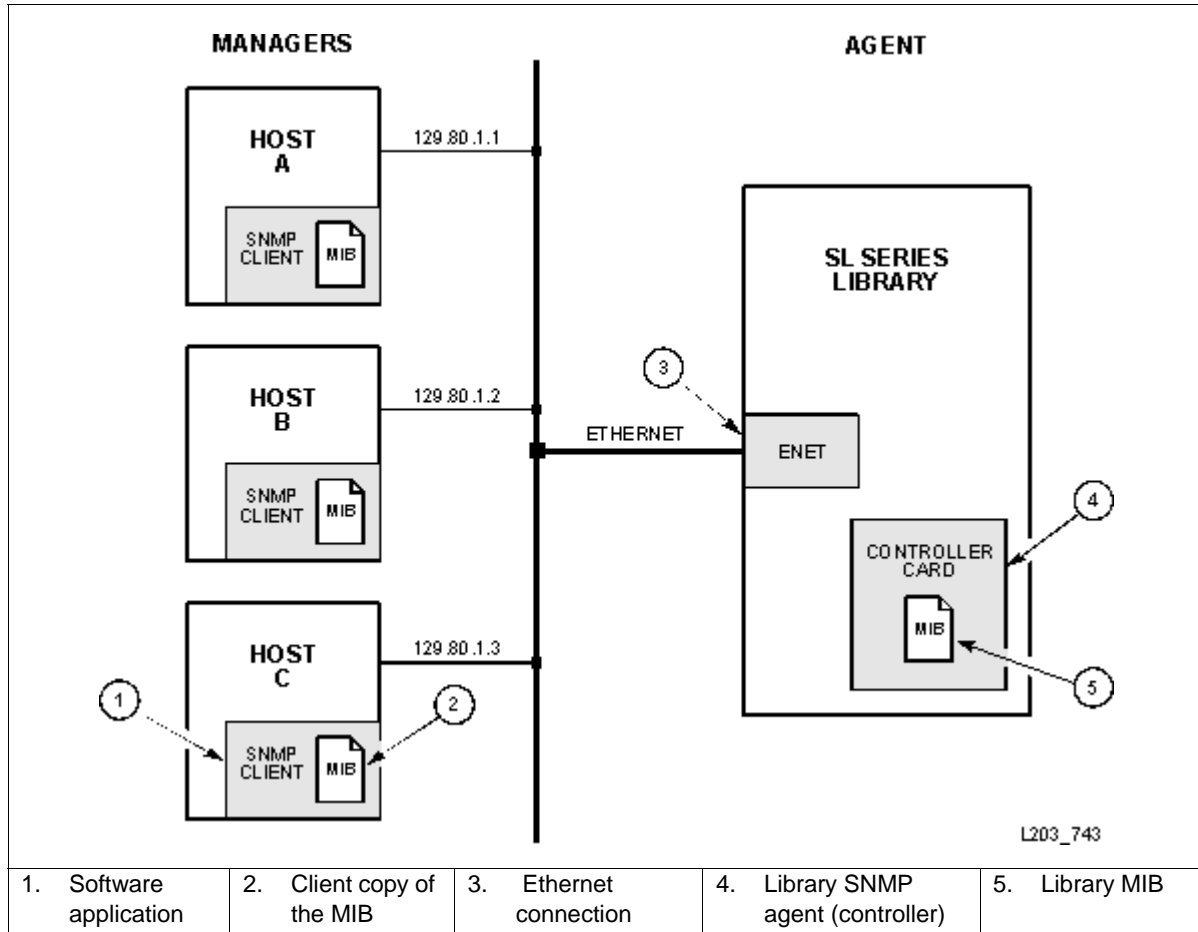
- e. [“Configure the SNMP Service Information” on page 25](#):

```
prompt> config serviceInfo set
```

## ■ Retrieve the Management Information Base

Have a system administrator retrieve the MIB from the library controller card.

**Figure 3. MIB Location**



Using the StreamLine Library Console and the Transfer File Function.

1. Log on to the library using StreamLine Library Console.
2. Select Tools ⇨ Diagnostics.
3. Click the TransferFile tab.
4. Click the Transfer button next to STREAMLINE\_TAPE\_LIBRARY\_MIB\_TEXT.text.
5. In the Save dialog, select a Save in folder, and enter a file name.
6. Click Save.Network Auto-Discovery and Mapping.

**Note:** For auto-discovery to include the library, the SNMP agent provides the [“MIB Variables”](#) on page 9.

## ■ Command Line Interface Entries



**Important:**

Only Sun StorageTek service representatives can use the command line interface (CLI) to enable and configure the SNMP feature.

CLI command syntax for SNMP entries is shown on the following pages.

**Note:** 'community' is a reserved word and can not be used for input strings.

### Add Trap Recipients

```
snmp>> addTrapRecipient
    trapLevel <trapLevelString>
    host <hostName | hostAddr>
    version < v2c community communityString> |
    v3 name <trapUserName>
        auth <MD5 | SHA>
        authPass <authPassPhrase>
        [priv <DES | AES>
        privPass <privPassPhrase>]
        [engineId <engineIdString>]>
```

Where:

<trapLevelString> is a single digit or a comma separated list of digits 1,2,3,4,...

<hostAddr | hostName> need to be fully qualified.

Note: Currently hostName is disabled, the user must use hostAddr.

The engine ID is a string of at most 31 hexadecimal characters, preceded with 0x.

### Add Users

```
snmp>> addUser
    version <v2c community <communityString>
    |
    v3 name set <UserName>
        auth <MD5 | SHA>
        authPass <authPassPhrase>
        [priv <DES |AES>
        privPass <privPassPhrase>]
```

## Delete Trap Recipients

```
snmp>> deleteTrapRecipient
      <id <index>
      |
      host <hostName | hostAddr>
      version <v2c community <communityString>
      |
      v3 name <trapUserName>>>
```

Where: The <hostAddr | hostName> must be fully qualified. Currently hostName is disabled.

## Delete Users

```
snmp>> deleteUser
      <id <index>
      |
      version <
      v2c community <communityString>
      |v3 name <userName>>>
```

## Disable Port ID

```
snmp>> disable port<port ID>
      disables SNMP for <portID>
```

Where: <portID> is 1A | 1B | 2A | 2B

### Notes:

#### SL3000 ports:

- Ports 2A and 2B are public access ports
  - Port 2B is standard;
  - Port 2A requires the Dual TCP/IP feature.
- Ports 1A and 1B are private—reserved—ports and are not used by customers.

## Enable Port ID

```
snmp>> enable port<port ID>  
          enable SNMP for <portID>
```

Where: <portID> is 1A | 1B | 2A | 2B

### Notes:

*SL3000 ports:*

- Ports 2A and 2B are public access ports
  - Port 2B is standard;
  - Port 2A requires the Dual TCP/IP feature.
- Ports 1A and 1B are private—reserved—ports and are not used by customers.

## List Trap Recipients

```
snmp>> listTrapRecipients
```

## List Users

```
snmp>> listUsers
```

## Configure the SNMP Service Information

Like configuring for users and traps/notifications, you must also configure the MIB variables that relate to service information.

Service information is also entered through the CLI port. Command syntax for these entries, an example of entering one field (the sLibLocatCountry variable/description), and verifying this entry are supplied below.

Important notes for these entries are:

- The `config serviceInfo set` entries must be entered as a string.
- Each string will be truncated at 80 characters
- Each string must be delimited by single quotation marks ( ' ' )

```
snmp>> config print
```

```
display configuration of library
```

```
—(config options are displayed, then the following syntax for the config serviceInfo set command is displayed)—
```

### **config serviceInfo set**

```
contact '<contactString>'
```

```
streetAddr '<streetAddrString>'
```

```
city '<cityString>'
```

```
state '<stateString>'
```

```
country '<countryString>'
```

```
zip '<zipString>'
```

```
description '<descriptionString>'
```

```
phone '<phoneString>'
```

```
Sets the service information
```

```
NOTE:
```

```
Users can enter any or all options when performing a serviceInfo set operation.
```

When configuring the service information, you can set one field or multiple fields with the `config serviceInfo set` command.

An example of setting multiple fields with one entry, would be:

```
SL3000> config serviceInfo set city 'Denver' contact 'Joe' country  
'USA' description 'Manager' phone '303-555-1234' state 'CO'  
streetAddr 'One Tape Drive' zip '80028'
```

## ■ Examples of SNMP Entries

An embedded SNMP agent can distinguish and filter trap recipients based on the trap numbers for which they are registered.

Entries must be made *exactly* as displayed in the SNMP help screens—text is case sensitive. For example, an entry of “authpass” instead of “authPass” will result in a parsing error.

Four examples of SNMP entries that you might enter through the CLI are provided in the following sections.

**Note:** The prompt (*SL3000*> ) indicates the library model number, or login (such as MFG, Service, etc.).

### Adding a Trap Recipient

As an example, a CLI entry for SNMPv2c to monitor for all three trap levels—error, warning, and informational—for an SL3000 library would be:

```
SL3000> snmp addTrapRecipient trapLevel 1,2,3 host 128.45.1.162  
version v2c community public
```

As another example, here is this CLI entry for the same error conditions, but using SNMPv3 protocol with additional “secure” parameters:

IP address of 128.45.1.162  
Security name of “stkTrapV3,”  
Mixed security levels  
SHA authentication, and DES encryption would be:

```
SL3000> snmp addTrapRecipient trapLevel 1,2,3 host 128.45.1.162  
version v3 name stkTrapV3 auth SHA authPass SHAPassPhrase priv DES  
privPass privPassPhrase engineId 0X12345678901234567890
```

**Note:** The “engineId” parameter is required on SNMPv3 traps.  
The Engine ID is a string of, *at most*, 31 hexadecimal characters, preceded with 0x.



## Adding a User

Adding an SNMP Version 2c user to a public community string would be:

```
SL3000> snmp addUser version v2c community public
```

Adding a user with a security name of “stkAgentV3,” a mixed level of security, MD5 authentication, and DES encryption, the entry would be:

```
SL3000> snmp addUser version v3 name stkAgentV3 auth MD5 authPass  
MD5PassPhrase priv DES privPass DESPassPhrase
```

## Deleting a Trap Recipient

Deleting an SNMP Version 2c user (uniquely identified by the recipient’s host) from a public community string would be:

```
SL3000> snmp deleteTrapRecipient host 192.168.1.1 version v2c  
community public
```

Deleting an SNMP Version 3 trap recipient of the same type, but with a trap user name, you would enter:

```
SL3000> snmp deleteTrapRecipient host 192.168.1.1 version v3  
name stkAgentV3
```

## Deleting a User

Deleting an SNMP v2c named user would be:

```
SL3000> snmp deleteUser host 192.168.1.1 version v2c  
community public
```

Deleting an SNMP v3 user, the entry would be:

```
SL3000> snmp deleteUser host 192.168.1.1 version v3 name stkUserV3
```

# Traps, Events, and Notifications

# 4

---

This chapter lists the supported SNMP traps—also known as events or notifications—and the supporting data for the SL3000 modular library.

## ■ SNMP Traps and Notifications

To obtain the information provided by a trap or notification, users must be added to the recipients list. Currently, this can be only be done by a service representative, through the CLI port, and using a “service” log in.

See [Chapter 3, Configuration](#) for this information.

## Organization

SNMP traps provide data that are organized using numeric formats or levels:

- 1 through 10 = Generic traps
- 11 through 20 = Agent specific related traps
- 21 through 100 = Device specific related traps
  - 21 through 27 = Library status change
  - 41 through 45 = Drive status change
  - 61 through 65 = Cartridge access port (CAP) status change
  - 81 through 85 = Pass-thru port (PTP) status change
- 101 and above = Media specific related traps

**Note:** Trap numbers 11 and higher are specific; that is, they contain distinct Object IDs (OIDs) within their messages. As such, they are generated from events within the library rather than the log entries.

## Levels

Table 15 lists the traps or notification levels available. These levels are generally filtered to include only those traps that a user wishes to monitor.

**Table 15. Trap Levels**

Trap		Level	Sent When...
<b>Generic</b>	sITrapError	1	Errors are posted in the log
	sITrapWarning	2	Warnings are posted in the log
	sITrapInformation	3	Information is posted in the log
	sITrapConfiguration	4	Changes are made in a system property (such as network ip or fiber mode)
<b>Specific</b>	sITrapAgentStart	11	An SNMP agent has started
	sITrapLibStatusGood	21	Library has changed to normal mode
	sITrapLibStatusCheck	25	Library has changed from normal mode
	sITrapEnvHdwCheck	27	A device in the library has had an environmental check
	sITrapDrvStatusGood	41	Drive has changed to a normal mode
	sITrapDrvStatusCheck	45	Drive has changed from normal mode
	sITrapCapStatusGood	61	CAP has changed to a normal mode
	sITrapCapStatusOpen	63	CAP state has changed to open
	sITrapCapStatusCheck	65	CAP has changed from normal mode

## ■ Generic Traps

Generic traps 1 – 4 are *log-based* and contain:

- Severity for indications such as an error or a warning
- Result codes such as “0000 = success,” or “5010 = robotic position error”
- Activity string such as “HLI move” or “CLI version print”
- A descriptive text string
- Date and time
- Other information, such as:
  - Date/Time
  - Device address associated with the event
  - User name associated with the activity
  - Interface-specific request identifier

The examples in [Table 16](#) reflect traps available with library firmware version **FRS\_3.12** and higher. Always consult the MIB for currently available traps.

**Table 16. Generic Traps**

Level	MIB Name	Sent When...	Object ID Content
1	slTrapError	A device condition that is critical to machine operation occurred.  <i>Device inoperable:</i> Refers to the entire system. Failure of a sub-unit or redundant component is not a Category 1	<a href="#">Table 17 on page 32</a>
2	slTrapWarning	A device condition which may need attention has been encountered.  Device degraded: refers to recoverable failures that may allow the system to remain in use, but only in a degraded mode.	<a href="#">Table 18 on page 32</a>
3	slTrapErrorInformation	Information is presented for activity monitoring.  Device activity: a device has reported activity. This information is used to monitor normal activity and messages.	<a href="#">Table 19 on page 33</a>

## Error Trap

**Table 17. Error Trap**

<b>MIB Name</b>	sITrapError
<b>Level</b>	1
<b>Description</b>	An error trap. A device condition which is critical to library operation was encountered.
<b>Objects</b>	sITrapLibrarySerialNumber sITrapDeviceId sITrapDeviceTime sITrapDeviceAddress sITrapDeviceUserName sITrapDeviceInterfaceName sITrapDeviceActivity sITrapDeviceRequestId sITrapDeviceSeverity sITrapDeviceResultCode sITrapDeviceFreeFormText

## Warning Trap

**Table 18. Warning Trap**

<b>MIB Name</b>	sITrapWarning
<b>Level</b>	2
<b>Description</b>	A warning trap. A device condition which may need attention has been encountered.
<b>Objects</b>	sITrapLibrarySerialNumber sITrapDeviceId sITrapDeviceTime sITrapDeviceAddress sITrapDeviceUserName sITrapDeviceInterfaceName sITrapDeviceActivity sITrapDeviceRequestId sITrapDeviceSeverity sITrapDeviceResultCode sITrapDeviceFreeFormText

## Information Trap

**Table 19. Information Trap**

<b>MIB Name</b>	sITrapInformation
<b>Level</b>	3
<b>Description</b>	An information trap. Information is presented for activity monitoring.
<b>Objects</b>	sITrapLibrarySerialNumber sITrapDeviceId sITrapDeviceTime sITrapDeviceAddress sITrapDeviceUserName sITrapDeviceInterfaceName sITrapDeviceActivity sITrapDeviceRequestId sITrapDeviceSeverity sITrapDeviceResultCode sITrapDeviceFreeFormText

## Specific Traps

Specific traps 11 – 85 are *event-based* and have distinct OIDs within their trap messages depending on the trap level. Consult each trap within the STREAMLINE-TAPE-LIBRARY-MIB for the specific data objects returned.

The examples in [Table 20](#) reflect traps available with library firmware version **FRS\_x.yz** and higher. Always consult the MIB for currently available traps.

**Table 20. Specific Traps**

Level	MIB Name	Sent When The...	Object ID Content
11	slAgentBootDate	SNMP agent starts	<a href="#">Table 21 on page 35</a>
21	slTrapLibStatusGood	Library status changes to Good.	<a href="#">Table 22 on page 35</a>
25	slTrapLibStatusCheck	Library status changes to a check condition (degraded, non-operational).	<a href="#">Table 23 on page 35</a>
27	slTrapEnvHdwCheck	Library environmental or hardware condition changes.	<a href="#">Table 24 on page 36</a>
41	slTrapDrvStatusGood	Drive status changes to Good.	<a href="#">Table 25 on page 36</a>
45	slTrapDrvStatusCheck	Drive status changes to a check condition (error, warning, unknown).	<a href="#">Table 26 on page 37</a>
61	slTrapCapStatusGood	CAP status changes to Good.	<a href="#">Table 27 on page 37</a>
63	slTrapCapStatusOpen	CAP status changes to Open.	<a href="#">Table 28 on page 37</a>
65	slTrapCapStatusCheck	CAP status changes to a check condition (error, warning, unknown).	<a href="#">Table 29 on page 38</a>



## Agent Boot Date

**Table 21. Agent Boot Date**

<b>MIB Name</b>	sIAgentBootDate
<b>Level</b>	11
<b>Description</b>	SNMP agent starts
<b>Objects</b>	sIAgentBootDate

## Library Status Good

**Table 22. Library Status Good**

<b>MIB Name</b>	sITrapLibStatusGood
<b>Level</b>	21
<b>Description</b>	This trap is sent when the library status changes to Good.
<b>Objects</b>	sILibraryTopLevelCondition sLibStkBaseModel sLibSerialNumber

## Library Status Check

**Table 23. Library Status Check Condition**

<b>MIB Name</b>	sITrapLibStatusCheck
<b>Level</b>	25
<b>Description</b>	This trap is sent when the library condition changes to a check condition, such as degraded or not-operative.
<b>Objects</b>	sILibraryTopLevelCondition sLibStkBaseModel sLibSerialNumber

## Environmental Hardware Check

**Table 24. Environmental Hardware Check**

<b>MIB Name</b>	sITrapEnvHdwCheck
<b>Level</b>	27
<b>Description</b>	This trap is sent when the library environmental or hardware condition changes.
<b>Objects</b>	sITrapLibrarySerialNumber sITrapDeviceId sITrapDeviceTime sITrapDeviceAddress sITrapDeviceUserName sITrapDeviceInterfaceName sITrapDeviceActivity sITrapDeviceRequestId sITrapDeviceSeverity sITrapDeviceResultCode sITrapDeviceFreeFormText

## Drive Status Good

**Table 25. Drive Status Good**

<b>MIB Name</b>	sITrapDrvStatusGood
<b>Level</b>	41
<b>Description</b>	This trap sent when a drive status changes to Good.
<b>Objects</b>	sILibSerialNumber sIDriveState sIDriveAddress sIDriveType sIDriveVendor sIDriveSerialNum

## Drive Status Check

**Table 26. Drive Status Check**

<b>MIB Name</b>	sITrapDrvStatusCheck
<b>Level</b>	45
<b>Description</b>	This trap sent when a drive status changes to a check condition, such as an error, warning, or unknown.
<b>Objects</b>	sLibSerialNumber sDriveState sDriveAddress sDriveType sDriveVendor sDriveSerialNum

## CAP Status Good

**Table 27. CAP Status Good**

<b>MIB Name</b>	sITrapCapStatusGood
<b>Level</b>	61
<b>Description</b>	This trap sent when a CAP status changes to Good.
<b>Objects</b>	sLibSerialNumber sCapState sCapAddress

## CAP Status Open

**Table 28. CAP Status Open**

<b>MIB Name</b>	sITrapCapStatusOpen
<b>Level</b>	63
<b>Description</b>	This trap sent when a CAP status changes to Open.
<b>Objects</b>	sLibSerialNumber sCapState sCapAddress

## CAP Status Check

**Table 29. CAP Status Check**

<b>MIB Name</b>	sITrapCapStatusCheck
<b>Level</b>	65
<b>Description</b>	This trap sent when a CAP status changes to a check condition, such as an error, warning, or unknown.
<b>Objects</b>	sLibSerialNumber sICapState sICapAddress



---

This appendix provides steps to use the SL3000 modular library SNMP feature with: [“Hewlett-Packard OpenView”](#)

## ■ SNMP Configuration



**Important:**

Because SNMP can only be enabled through the command line interface (CLI) by a Sun StorageTek service representative, they must work with the customer’s system administrator to obtain the information they require to make the necessary entries and enable SNMP.

See [Chapter 3](#) and the [“SNMP Configuration Sequence” on page 20](#) to configure the SNMP feature.

1. Have an administrator retrieve the Management Information Base (see [“Retrieve the Management Information Base” on page 21](#)).
2. Obtain the trap/notification destinations from the administrator:
  - IP address of the hosts receiving the traps.  
There can be a maximum of 20 SNMP users (trap recipients) total.

---

---

---

If using SNMPv3:

- EngineId of the hosts receiving the traps
- Authentication protocol/authPassPhrase (MD5 or SHA)
- Authentication privacy protocol/Privacy PassPhrase (DES or AES)
- User names and hosts receiving the traps

3. Have the Sun StorageTek service representative log in and use the:
  - [Command Line Interface Entries on page 22](#) and
  - [Configure the SNMP Service Information on page 25](#)

## ■ Hewlett-Packard OpenView

The following command sequence configures Hewlett-Packard (HP) OpenView Network Node Manager (NNM) on a Solaris operating system. Configuration examples and categories are also provided.

### Loading the MIB

To load the SL3000 MIB on an OpenView server:

1. Set up the environment using the `./opt/OV/bin/ov.envvars.sh` script:

```
%> ./opt/OV/bin/ov.envvars.sh
```

2. Create a directory for StorageTek MIBs:

```
%> cd $OV_SNMP_MIBS/Vendor
```

```
%> mkdir StorageTek
```

3. Copy the SL3000 MIB from your workstation to the new directory,

```
%>cp /var/opt/OV/share/snmp_mibs/Vendor/StorageTek.
```

4. Launch OpenView.
5. Select Options ⇨ Load/Unload MIBs: SNMP.
6. Press the Load button.
7. Browse to the STREAMLINE MIB file.
8. Press OK to load the trap definitions.
9. If desired, you may use the Tools ⇨ SNMP MIB Browser operation to view the new MIB objects.

### Configuring SNMP Events

When you load a MIB in to the HP OpenView NNM application's database, OpenView automatically adds the SNMP traps that are defined in the MIB to the Event Configuration application. The Event Configuration defines the rules for sending traps to the OpenView NNM alarm browser.

By default, the Event Configuration application creates the SL3000 traps with:

- Category set to Log and
- Severity set to Normal

To change these values:

1. Select Options ⇨ Event Configuration
2. In the Enterprise Identification list, select streamlineTapeLibrary.
3. In the Event Identification list, double-click on an event name (for example: s1TrapError).
4. Configure the desired event categories, severities, and event log messages, following the instructions in:

*Managing Your Network with HP OpenView Network Node Manager:  
Windows, HP-UX, Solaris, and Linux Operating Systems.*

The following listing shows some sample trap configurations; the variable \$\* includes all variables associated with the event in the log message.

## Critical, Error Alarms (Red)

- You could classify all *errors* as SNMP critical (**red**) alarms.
- You could format the message with the alarm severity at the start of each message and all other variables displayed in their native order.

For example:

```
Event name: s1TrapError
Category: error alarms
Severity:
critical (red)
Message: An error trap was received. Severity: $9 Serial Number:
$1 Device ID: $2 Time: $3 Device address: $4 User name:
$5 Interface name: $6 Device activity: $7 Request ID:
$8 Result code: $10 Description: $11
```

- Or you could create a more readable, natural-language message with a leading serial number:

```
Event name: s1TrapError
Category: error alarms
Severity:
critical (red)
Message: SN$1: trapped a $9 error at $3 on device ID $2 at device
address $4: result code $10. Error occurred while user $5 on interfac
$6 was requesting $7 activity (request ID: $8). $11
```

## Major Events (Orange)

You might want to classify *check conditions* as SNMP major (**orange**) events.

For example:

```
Event name: s1TrapLibStatusCheck
Category: status alarms
Severity:
major (orange)
Message: Library status changed to a check condition. Variables: $*
```

```
Event name: s1TrapDrvStatusCheck
Category: status alarms
Severity:
major (orange)
Message: Drive status changed to a check condition. Variables: $*
```

```
Event name: s1TrapCapStatusCheck
Category: status alarms
Severity:
major (orange)
Message: CAP status changed to a check condition. Variables: $*
```



## Warning Events (Cyan)

It makes sense that *warnings* be classified as SNMP warning (**cyan**) events.

For example:

```
Event name: s1TrapWarning
Category: Threshold Alarms
Severity:
warning (cyan)
Message: A warning trap was received. Variables: $*
```

## Normal, Informational Events (Green)

The remainder of the trap types are mostly *informational messages* that can be classified as SNMP normal (**green**) events.

For example:

```
Event name: s1TrapInformation
Category: status alarms
Severity:
normal (green)
Message: Trapped an informational message. Variables: $*
```

```
Event name: s1TrapConfiguration
Category: configuration alarms
Severity:
normal (green)
Message: Trapped a configuration message. Variables: $*
```

```
Event name: s1TrapAgentStart
Category: status alarms
Severity:
normal (green)
Message: The SNMP agent started. Variables: $*
```

**Event name:** s1TrapLibStatusGood  
**Category:** status alarms  
**Severity:**  
normal (green)  
**Message:** Library status changed to Good. Variables: \$\*

**Event name:** s1TrapEnvHdwCheck  
**Category:** status alarms  
**Severity:**  
normal (green)  
**Message:** Library environmental or hardware condition has changed.  
Variables: \$\*

**Event name:** s1TrapDrvStatusGood  
**Category:** status alarms  
**Severity:**  
normal (green)  
**Message:** Drive status changed to Good. Variables: \$\*

**Event name:** s1TrapCapStatusGood  
**Category:** status alarms  
**Severity:**  
normal (green)  
**Message:** CAP status changed to good. Variables: \$\*

---

This appendix provides steps to use the SL3000 modular library SNMP feature with: CA Unicenter Network and System Management application.

## ■ SNMP Configuration



### Important:

Because SNMP can only be enabled through the command line interface (CLI) by a Sun StorageTek service representative, they must work with the customer's system administrator to obtain the information they require to make the necessary entries and enable SNMP.

See [Chapter 3](#) and the [“SNMP Configuration Sequence” on page 20](#) to configure the SNMP feature.

1. Have an administrator retrieve the Management Information Base (see [“Retrieve the Management Information Base” on page 21](#))
2. Obtain the trap/notification destinations from the administrator:
  - IP address of the hosts receiving the traps.  
There can be a maximum of 20 SNMP users (trap recipients) total.

---

---

---

If using SNMPv3:

- EngineId of the hosts receiving the traps
- Authentication protocol/authPassPhrase (MD5 or SHA)
- Authentication privacy protocol/Privacy PassPhrase (DES or AES)
- User names and hosts receiving the traps

3. Have the Sun StorageTek service representative log in and use the:
  - [Command Line Interface Entries on page 22](#) and
  - [Configure the SNMP Service Information on page 25](#)

## ■ CA Unicenter

The following procedure configures CA Unicenter Network and System Management (NSM) application to collect traps on Windows 2000 or 2003 operating systems.

Make sure that the SNMP agents are installed on the system:

1. Right click on My Computer.
2. Select Manage.
3. Under Services and Applications, click on Services.
4. Check for: SNMP Services and SNMP Trap Services
  - If they are **not** there follow the instruction bellow to install the agents.
  - If they are there continue with [“Installing NSM” on page 47](#).

To install SNMP services on Windows 2000 and 2003 platforms:

### Notes:

- You must be logged on as an administrator or a member of the Administrators group to complete this procedure.
  - If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.
1. Click on Start.
  2. Go to and click on Control Panel.
  3. Double-click on Add or Remove Programs.
  4. Click on Add/Remove Windows Components.
  5. In Components, click Management and Monitoring Tools—but do not select or clear the check box—then click Details.
  6. Select the Simple Network Management Protocol check box, and click OK.
  7. Click Next.
  8. Insert the application CD or specify the complete path for the location where the files are stored.

The SNMP application starts automatically after installation.



**CAUTION:** If Unicenter NSM is installed before the Windows SNMP agents, some of the commands on NSM will not work properly and a re-installation of NSM will be required.

## Installing NSM

Components of Unicenter NSM include:

- Enterprise Manager – monitors and displays traps
- Trap Manager – loads the MIBs on the Management system

To install the CA Unicenter Network and System Management application on Windows 2000 and 2003 operating systems:

1. Place the Unicenter NSM Installation DVD/CD in the drive.  
The Unicenter product explorer will start automatically.
2. Under Unicenter for Windows; select Installation Wizard for Unicenter NSM and click Install.
3. Select install any or all Unicenter NSM components and click Next.
4. Accept the License Agreement and click Next.
5. Complete the required information and click Next.  
This launches the component selection window.
6. Under Unicenter NSM components select: Ingres, WorldView, Agent Technologies, and Enterprise Management the click Next.
7. Provide an *nsmadmin password* and click next.  
The installation process starts.
8. After the installation is complete; reboot the system.

## Starting the NSM Enterprise Manager

To start the NSM Enterprise Manager (EM) console:

**Note:** Enterprise Manager console is the window where all the traps (alerts) from devices are displayed.

1. Go to Start ⇨ Programs ⇨ Computer Associates ⇨ Unicenter ⇨ NSM ⇨ Enterprise Management ⇨ EM classics.

The Enterprise Manager for windows starts.

2. Double click on Windows.
3. Double click on Events.
4. Double click on Console Logs.

The Enterprise Manager launches the console.

## Installing the NSM Trap Manger

1. Place the Unicenter NSM Installation DVD/CD in the drive.  
The Unicenter product explorer will start automatically.
2. Under Unicenter For Windows: Post Installation Utilities, select Trap Manager and click Install.
3. Follow the prompts and directions to complete the installation.

## Loading the NSM Trap Manager

To load the Trap Manager with a MIB and traps:

1. Go to Start ⇨ Programs ⇨ CA ⇨ Unicenter.
2. Sign on to the Trap Database.

The Trap Manager connects to the Trap Database and the Unicenter NSM TrapManager window appears.

3. Select MIBs then All MIBs from the View drop-down menu.

The view changes to show All MIBs in the left pane.

**Note:** To add a vendor, MIB, or trap, you must be in the All MIBs view.

4. To add a new trap under a new vendor:
  - a. Select Add, Vendor from the File drop-down menu.
  - b. Right-click the Root node in the Traps tree in the left pane and select Add Vendor.  
  
A node with the name New Vendor is added to the end of the Traps tree in the left pane.
  - c. Enter a name for your new vendor, and press Enter.  
The Vendor name is changed.

**Note:** The new vendor is not saved in the database until you add at least one MIB and one trap under the new vendor.

5. To add your new trap under a new MIB:
  - a. Click the Vendor node under which you want to add a new MIB in the Traps tree in the left pane.
  - b. Select Add, MIB File from the File drop-down menu.  
  
A node with the name New Mibname (New Mibfile) is added to the end of the Traps tree for the Vendor node you selected in the left pane.
  - c. Enter a name for your new MIB, and press Enter.  
The MIB name is changed.

**Note:** The new MIB is not saved in the database until you add at least one trap under the new MIB.

6. Do one of the following:

- Click the MIB node under which you want to add a new trap in the Traps tree in the left pane. Select Add, Trap from the File drop-down menu.
- Right-click the MIB node under which you want to add a new trap in the Traps tree in the left pane, and then select Add Trap.

The Add Trap window appears in the right view pane.

**Note:** The Vendor, MIB File, and MIB Name fields are automatically updated.

7. Complete the fields on the Add Trap window, and then click Save.

The new trap is saved and appears under the MIB you selected in the Traps tree in the left pane. The new trap is color-coded to show the trap severity as follows:

- Green icon - trap severity is informational.
- Yellow icon - trap severity is warning.
- Red icon - trap severity is critical.





# Glossary

---

This glossary defines terms and abbreviations used in this publication.

## A

**Advanced Encryption Standard (AES)** An NIST-standard cryptographic cipher that uses a block length of 128 bits and multiple key lengths of 128, 192, or 256 bits to encrypt data.

**agent** A module that resides in a managed device. The agent is responsible for responding to requests from the manager and for sending *traps* to a recipient that inform the systems administrator of potential problems.

## C

**community string** Applications use community strings for access control. The manager includes the community string in its SNMP messages to an agent.

## D

**Data Encryption Standard (DES)** An NIST cryptographic cipher that uses a 56-bit key.

**Dynamic Host Configuration Protocol (DHCP)** A set of rules to allow a network attached device to request and obtain an IP address from a server which has a list of addresses available for assignment.

**Domain Name System (DNS)** A system that translates IP addresses into human readable computer names. Similar to a phone book matching names and numbers.

## E

**EngineID** An administratively unique identifier of an SNMPv3 engine used for identification, not for addressing.

## F

**firewall** In computing, a firewall is a piece of hardware and/or software which controls connectivity between different zones of trust.

**File Transfer Protocol (FTP)** An internet protocol for transferring files between two hosts over a TCP/IP network.

## G

**gateway** A device on a network that serves as an entrance to another network.

## H

**host keyword** Currently, the host keyword is limited to the machine's IP address. The maximum keyword length is 31 alphanumeric characters.

**HyperText Transfer Protocol (HTTP)** The protocol most often used to transfer information from World Wide Web servers to browsers.

## I

**Internet Engineering Task Force (IETF)** Develops and promotes internet standards.

**Internet Protocol (IP)** A data-oriented protocol used for communicating data across a network. IP is a network layer protocol in the internet protocol suite and is encapsulated in a data link layer protocol such as Ethernet.

## M

**managed device** A device that hosts the services of an SNMP agent that provides monitored information and controlled operations using SNMP.

StreamLine libraries are managed devices.

**management information base (MIB)**

A collection of information stored in a database that contains configuration and statistical information for a managed device.

For StreamLine libraries, a copy of the MIB is loaded with firmware and stored on the processor card.

**manager** Provides the communication link between the systems administrator and the managed devices on the network. A manager station or server allows the systems administrator to get information about the device through the MIB and to receive traps from an agent.

**Message Digest 5 (MD5)** A popular one-hash function that is used to create a message digest for digital signatures. MD5 is faster than SHA, but is considered less secure.

**N**

**National Institute of Standards and Technology (NIST)** An agency of the Commerce Department's Technology Administration.

**notification** A message that reports a problem, error, or significant event that occurred within a device—a trap.

**netmask** A hierarchical partitioning of the network address space.

**O**

**Open Source Initiative (OSI)** An organization dedicated to promoting open-source software. The OSI model divides the functions of a protocol into a series of layers

**R**

**recipient** A location on a manager where the SNMP agent sends traps. This location is defined by the combination of either the IP address or DNS name and the port number. The default recipient port number is 162.

**Request for Comments (RFC)** A series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies. The Internet Engineering

Task Force (IETF) adopts some of the applied information theory published in RFCs as Internet standards.

**S****Secure Hash Algorithm (SHA-1/SHA)**

A popular one-hash algorithm used to create digital signatures; it is more secure, but slightly slower than MD5.

**Simple Mail Transfer Protocol (SMTP)** A protocol for sending e-mail messages between servers.

**T**

**Transmission Control Protocol (TCP)** One of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange data. The protocol guarantees reliable and in-order delivery of sender to receiver data (see also User Datagram Protocol).

**trap** A message that reports a problem, error, or significant event that occurred within a device—a notification.

**U**

**User Datagram Protocol (UDP)** is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagrams to one another.

UDP does not provide the reliability and ordering guarantees that TCP does. Datagrams may arrive out of order or go missing without notice. Without the overhead of checking if every packet actually arrived, UDP is faster and more efficient for many lightweight or time-sensitive purposes.

**W**

**World Wide Name (WWN)** A unique identifier in a Fibre Channel or Serial Attached SCSI storage network. Each WWN is an 8-byte number derived from IEEE and vendor-supplied information.

# Index

---

## A

- access control, 7
- add trap recipient, 22
- add users, 22
- additional variables, 10
- address, street location, 9
- administrative password, 7
- architecture, SNMP, 1
- ASCII text file, 1
- authentication protocol, 20, 39, 45

## C

- cartridges, 15
- cell table, 15
- cells, 15
- city, 9
- CLI
  - command syntax, 22
  - service information settings, 25
  - SNMP commands, 19
- commands, list, 6
- communications protocol, 5
- config print, 25
- config serviceInfo set, 25
- config serviceInfo set entries, 25
- configurations
  - service information, 25
- configurations, default settings, 19
- country, 9
- Customer Resource Center (CRC), xii

## D

- date, 9
- default settings, 19
- delete trap recipients, 23
- disable port ID, 23

- drives, 16

## E

- enable port ID, 24
- encryption, capabilities in SNMP, 7

## F

- Fibre ports, 17
- firmware versions, 7
- framework for SNMP, 1

## H

- HandBots, 14

## I

- IETF, 3
- Internet Engineering Task Force, 3
- inventory, 12

## L

- labels, 12, 15
- library
  - contents, 12
  - inventory, 12
  - location, 9
  - model number, 9
  - storage elements, 15
- library default settings, 19
- list trap recipients, 24
- list users, 24
- location, 9

## M

- managed device, 1
- management information base, 1, 5
- Management Information Base. See MIB
- management station, description, 1
- manager, description, 1
- MIB
  - additional variables, 10
  - description, 8
  - hierarchy, 8
  - variables, 9

## N

- notification levels, 30
- notifications
  - description, 6
  - destinations, 20, 39, 45

## O

- object identifiers, 5
- overview of SNMP, 1

## P

- Partner Agreement, xii
- Partners Web site, xii
- PDU, 6
- ports, 17
- ports, UDP, 5
- protocol comparisons, TCP/IP and OSI, 4
- protocol data units, 6

## R

- Request for Comments, 3
- resellers, xii
- RFCs, 3
- robotic data, 14

## S

- service information settings, 25
- Simple Network Management Protocol, 1
- slots, 15

## SNMP

- access control, 7
- agent, 6
- architecture, 1
- configuration, 19
- default settings, 19
- definition, 1
- MIB diagram, 8
- settings, 19
- terms, 51
- versions, 3
- storage elements, 15
- StorageTek
  - Customer Resource Center (CRC), xii
  - Partners site, xii
  - Web site, xii
- StreamLine library settings, 19
- street address, 9
- Sun
  - Customer Resource Center (CRC), xii
  - Partners Web site, xii
  - Web site, xii
- Sun Microsystems, Inc, ii

## T

- TallBots, 14
- tape drives, 16
- time-of-day, 9
- TOD, 9
- transports, 16
- trap
  - description, 6
  - destinations, 20, 39, 45
- trap levels, 30
- traps
  - date, 9
  - library data, 9
  - library location, 9
  - location, 9
  - robotic data, 14
  - storage, 15
  - time-of-day, 9
  - versions, 18

## U

- UDP, 4

UDP ports, 5  
user datagram protocol, 4

## **V**

variables, 10  
versions, 3, 18

## **W**

Web sites, xii

## **Z**

ZIP code, 9





Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web [sun.com](http://sun.com)



ARGENTINA: 5411-4317-5636 • AUSTRALIA: 1-800-550-786 • AUSTRIA: 43-1-601-26-0 • BALKANS: 301-6188-111 • BELGIUM: 32-2-704 89 83 • BRAZIL: 55-11-51872100 • BRUNEI: 65-216-8333 • CANADA: 1-800-422-8020 (GENERAL); 416-964-2001 (LEARNING MANAGEMENT SYSTEM SALES, TORONTO) • CHILE: 562-372-4500 • COLOMBIA: 571-629-2323  
CZECH REPUBLIC: 420 2 33009311 • DENMARK: 45 4556 5040 • EGYPT: 00 202 570 9442 • FINLAND: 358-9-525-551 • FRANCE: 33-1-41-33-17-17 • GERMANY: 49-89-460-08-2788 • GREECE: 30-01-6188101 • HONG KONG: 852-2877-7077 • HUNGARY: 361-202-4415 • INDIA: 91-80-229-8989 • INDONESIA: 65-216-8333 • IRELAND: 353-1-668-4377  
ISRAEL: 972-9-9710500 • ITALY: 39-02-9259511 • JAPAN: 81-3-5779-1820 • KOREA: 82-2-3453-6602 • MALAYSIA: 603-2116-1887 • MIDDLE EAST: 00 9714 3366333 • MEXICO: 525-261-0344 • NETHERLANDS: 31-33-4515200 • NEW ZEALAND: 0800-786-338 • NORTH WEST AFRICA: 00 9714 3366333 • NORWAY: FROM NORWAY: 47-22023950, TO NORWAY: 47-23369650 • PAKISTAN: 00-9714-3366333 • PEOPLE'S REPUBLIC OF CHINA: 8610-6803-5588 • PHILIPPINES: 632-885-7867 • POLAND: 48-22-8747848 • PORTUGAL: 351-21-413-4000 • RUSSIA: 7-095-935-8411 • SAUDI ARABIA: 00 9714 3366333 • SINGAPORE: 65-216-8300 • SOUTH AFRICA: 27-11-256-6300 • SPAIN: 34-902-210-412 • SRI LANKA: 65-2168333 • SWEDEN: 46-8-631 22 00 • SWITZERLAND: 41-1-908-90-50 (GERMAN) 41-22-999-0444 (FRENCH) • TAIWAN: 886-2-25185735 • THAILAND: 662-344-6855 • TURKEY: 90 212 335 22 00 • UNITED KINGDOM: 44-1276-416-520 • UNITED STATES: 1-800-422-8020 • VENEZUELA: 582-905-3800 • VIETNAM: 65-216-8333 • WORLDWIDE HEADQUARTERS: 1-650-960-1300

**SUN™** THE NETWORK IS THE COMPUTER ©2006 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.