

Hitachi Virtual Storage Platform G/F350, G/ F370, G/F700, G/F900

SVOS RF 8.2

SNMP Agent User Guide

This document describes and provides instructions for using the SNMP Agent on Hitachi Virtual Storage Platform F350, F370, F700, and F900 all-flash arrays and Hitachi Virtual Storage Platform G350, G370, G700, and G900 storage systems.

© 2018 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Contents

Preface	5
Intended audience.....	5
Product version.....	5
Release notes.....	5
Changes in this revision.....	6
Referenced documents.....	6
Document conventions.....	6
Conventions for storage capacity values.....	8
Accessing product documentation.....	9
Getting help.....	9
Comments.....	9
Chapter 1: Introduction	10
SNMP Manager overview.....	10
How SNMP works.....	10
Management Information Base overview.....	11
SNMP Agent configuration.....	11
SNMP Agent overview.....	12
SNMP traps.....	12
SNMP Agent operations.....	13
SNMP Agent reported errors.....	13
Component status information from SNMP Manager.....	14
Chapter 2: Using SNMP	16
Accessing the Alert Notifications window.....	16
Managing SNMP trap notification.....	17
Adding trap notification for SNMP v1 and v2c.....	18
Adding trap notification for SNMP v3.....	19
Changing trap notification for SNMP v1 and v2c.....	20
Changing trap notification for SNMP v3.....	21
Deleting SNMP trap notification.....	22
Managing SNMP request authentication.....	23
Adding request authentication for SNMP v1 and v2c.....	23
Adding request authentication for SNMP v3.....	24
Changing request authentication for SNMP v1 and v2c.....	25

Changing request authentication for SNMP v3.....	26
Deleting SNMP request authentication.....	27
Testing SNMP trap reports.....	28
Chapter 3: SNMP supported MIBs.....	29
SNMP Agent failure report trap contents.....	29
SNMP Agent extension trap types.....	30
Standard MIB specifications.....	30
MIBs supported by SNMP Agent.....	30
SNMP Agent MIB access mode.....	31
Example object identifier system.....	31
MIB mounting specifications supported by SNMP Agent.....	32
Extension MIB specifications.....	33
Extension MIB configuration.....	33
raidExMibName.....	35
raidExMibVersion.....	35
raidExMibAgentVersion.....	35
raidExMibDkcCount.....	35
raidExMibRaidListTable.....	36
raidExMibDKCHWTable.....	37
raidExMibDKUHWTable.....	38
raidExMibTrapListTable.....	39
Chapter 4: Troubleshooting.....	41
Solving SNMP problems.....	41
Glossary.....	43
Index.....	44

Preface

This document describes and provides instructions for using the SNMP Agent on VSP Gx00 models and VSP Fx00 models.

Please read this document carefully to understand how to use this product, and maintain a copy for reference purposes.

Intended audience

This document is intended for system administrators, Hitachi Vantara representatives, and authorized service providers who install, configure, and operate VSP Gx00 models and VSP Fx00 models.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- Hitachi Virtual Storage Platform Gx00 or Fx00 models and the *Product Overview*.
- The Hitachi Device Manager - Storage Navigator software and the *System Administrator Guide*.

Product version

This document revision applies to:

- Firmware 88-02-0x or later
- SVOS RF 8.2 or later

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Vantara Support Connect: <https://knowledge.hitachivantara.com/Documents>.

Changes in this revision

- Updated information on raidExMibDKUHWTTable.

Referenced documents

- *Command Control Interface User and Reference Guide*, MK-90RD7010
- *System Administrator Guide*, MK-97HM85028
- *SIM Reference Guide*, MK-97HM85023

Document conventions

This document uses the following storage system terminology conventions:




Convention	Description
VSP Fx00 models	Refers to all of the following models, unless otherwise noted. <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform F350 ▪ Hitachi Virtual Storage Platform F370 ▪ Hitachi Virtual Storage Platform F700 ▪ Hitachi Virtual Storage Platform F900
VSP Gx00 models	Refers to all of the following models, unless otherwise noted. <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform G350 ▪ Hitachi Virtual Storage Platform G370 ▪ Hitachi Virtual Storage Platform G700 ▪ Hitachi Virtual Storage Platform G900


This document uses the following typographic conventions:

Convention	Description
Bold	<ul style="list-style-type: none"> ▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. ▪ Indicates emphasized words in list items.

Convention	Description
<i>Italic</i>	<ul style="list-style-type: none"> Indicates a document title or emphasized words in text. Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <pre>pairdisplay -g group</pre> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p>
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>
< > angle brackets	Indicates variables in the following scenarios: <ul style="list-style-type: none"> Variables are not clearly separated from the surrounding text or from other variables. Example: <pre>Status-<report-name><file-version>.csv</pre> Variables in headings.
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a b } indicates that you must choose either a or b.
vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a b] indicates that you can choose a, b, or nothing. { a b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).

Icon	Label	Description
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes
1 exabyte (EB)	1,000 PB or $1,000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: <ul style="list-style-type: none"> ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes

Logical capacity unit	Value
1 EB	1,024 PB or 1,024 ⁶ bytes

Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: <https://knowledge.hitachivantara.com/Documents>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

[Hitachi Vantara Support Connect](#) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](#) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you!


Chapter 1: Introduction

This chapter provides an overview of the SNMP implementation for monitoring Hitachi Virtual Storage Platform F350, F370, F700, F900 and Hitachi Virtual Storage Platform G350, G370, G700, G900 storage systems, including the agent and management functions.

SNMP Manager overview

SNMP Manager is installed in the network management station. It collects and manages information from SNMP agents installed in the managed devices on the network.

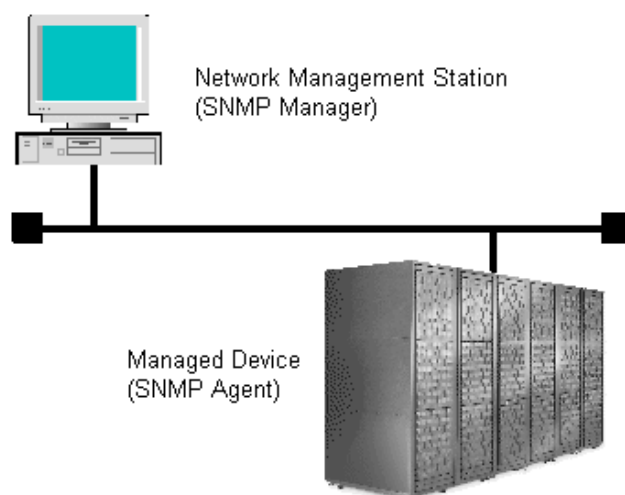
The SNMP Manager graphically displays information collected from two or more SNMP agents, accumulates the information in the database, and analyzes problems discovered while accumulating this information.

 **Note:** SNMP versions v1, v2c, and v3 are supported.

How SNMP works

Simple Network Management Protocol (SNMP) is an industry-standard protocol for managing and monitoring network devices, including disk devices, routers, and hubs. SNMP uses Simple Gateway Management Protocol (SGMP) to manage TCP/IP gateways.

The following figure shows an example SNMP environment.



An SNMP manager monitors the devices, which are referred to as managed nodes. Typically, an SNMP Manager polls the SNMP agents on a periodic basis. The manager receives the reports from the agents and determines whether the devices are operating normally. If an abnormal event occurs, an SNMP Agent can report the condition without a request from the manager, by using a trap message.

When an SNMP manager polls an agent, the following dialogue takes place:

- An SNMP Manager sends a request packet to an SNMP Agent, which requests data regarding the status of the managed node.
- The SNMP Agent sends a response packet back to the SNMP Manager.
- SNMP uses the TCP/IP User Datagram Protocol (UDP). If the SNMP Agent does not respond within a specified time period, the SNMP Manager re-sends the request packet. That time period is set by the system administrator, taking into account the network traffic and operation policy.
- If an SNMP Agent again does not respond to the resent packet, the SNMP Manager assumes that an error has occurred. Depending on the times set for polling and response, this dialogue can take several seconds.

If an SNMP Agent detects an abnormal event, it sends a trap to the SNMP Manager. However, if a trap is dropped in transmission, the SNMP Manager does not know that it was sent. For this reason, you should use both polling and traps to determine whether an abnormal event has occurred.

Management Information Base overview

The standardized configuration and database of network management information is called a Management Information Base (MIB). A standard MIB is common to all SNMP interfaces. An extension MIB is defined by the particular managed device or protocol.

A MIB is a collection of standardized configuration and network management information that is contained in each device on the network. Each MIB contains a set of parameters called managed objects. Each managed object consists of a parameter name, one or more parameters, and a group of operations that can be executed with the object. The MIB defines the type of information that can be obtained from a managed device, and the device settings that can be controlled from a management system.

The MIB definition file, `VSPGx00MIB.txt`, is located in the `program\SNMP` folder of the software media kit.

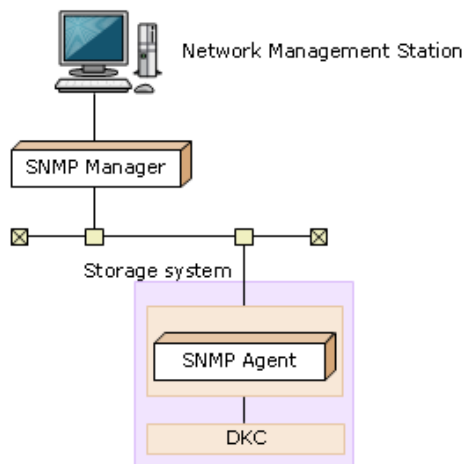
SNMP Agent configuration

The SNMP Agent runs on the storage system.

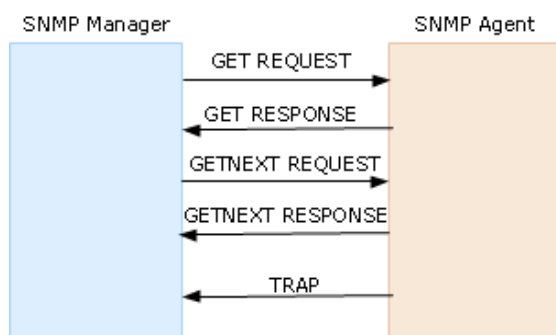
The SNMP Agent communicates with the SNMP manager through the LAN between the storage system and the SNMP manager.

Note: If you cannot use two or more MIB definition files for USP, USP V/VM, VSP, VSP G1x00, VSP F1500, VSP Gx00 models, or VSP Fx00 models because of the specifications of the SNMP manager software, use the MIB definition files for VSP F350, F370, F700, F900 or VSP G350, G370, G700, G900. Error reports include storage system nicknames, which can be used to identify each storage system.

The following figure illustrates the SNMP environment.



The following figure shows an example of SNMP operations using an SNMP manager.



SNMP Agent overview

The SNMP Agent is mounted on a managed device (such as a hard disk) in the network. It collects error information, the usage condition, and other information about the device, and forwards the information to the SNMP Manager.

The SNMP Agent reports disk storage system failures to the manager using the SNMP trap function.

SNMP traps

An SNMP Agent reports storage system errors to the SNMP Manager using the SNMP trap function.

When an error occurs, the SNMP Agent issues an SNMP trap to the SNMP Manager that includes the product number, nickname, reference code, component where the failure occurred, failure date and time, and detailed information about the failure.

For details about SNMP trap reference codes, see the SIM reference guide.

The following table lists the types of events that trigger an SNMP Agent trap.

Events	Description
Acute failure detected.	All operations in a storage system stopped.
Serious failure detected.	Operation in a component where a failure occurred stopped.
Moderate failure detected.	Partial failure.
Service failure detected.	Minor failure.

SNMP Agent operations

Operations that an SNMP Agent can perform fall into the categories GET REQUEST, GETNEXT REQUEST, GETBULK REQUEST, and TRAP.

The following table describes the types of SNMP Agent operations.

Operation	Description
GET REQUEST	Obtains a specific MIB object value. GET REQUEST is the request from an SNMP Manager, and GET RESPONSE is the agent's response to that request.
GETNEXT REQUEST	Continuously finds a MIB object. GETNEXT REQUEST is the request from an SNMP Manager, and GET RESPONSE is the agent's response to that request.
GETBULK REQUEST	Continuously finds specified MIB objects only. GETBULK REQUEST is the request from an SNMP Manager, and GET RESPONSE is the agent's response to that request.
TRAP	Reports an event (failure) to an SNMP Manager. TRAP occurs without a request from the SNMP Manager.

SNMP Agent reported errors

Several different types of errors can be reported when GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST operations are sent to an SNMP Agent.

The following table describes the errors that can be reported and suggests corrective action.

Error	Description	Corrective action
noError (0)	Normal	N/A
noSuchName (2)	<ul style="list-style-type: none"> ▪ There are no MIB objects that are required. (Not supported.) ▪ The GETNEXT REQUEST command that is specified for the following object identifier of the last supported MIB object is received. 	Verify that the name of the requested object is correct.
	SET REQUEST is received.	SET REQUEST operation is not supported.
genErr (5)	Error occurred for other reasons.	Retry the operation.

Component status information from SNMP Manager

You can obtain the status information of certain storage system components from the SNMP Manager.

The following table lists the components for which the status can be obtained.

Area	Component name
Storage System	Processor(s)
	Cache
	Power supplies
	Batteries
	Fans
	Others
DB	Power supplies
	Environments
	Drives

The following table lists the status of storage system components, as well as the trap report functions.

Status	Description
Normal	Normal operation.
Acute failure detected	All operations in a storage system stopped.
Serious failure detected	Operation in a component where a failure occurred stopped.
Moderate failure detected	Partial failure.
Service failure detected	Minor failure.

Chapter 2: Using SNMP

By using the maintenance utility, you can manage alert settings, SNMP trap notification, SNMP request authentication, test SNMP trap reports.

Accessing the Alert Notifications window

Since the other topics (SNMP v1, v2c , and v3) talk about how to configure in details, this high level (useless) topic should either be removed or modified to talk about how to access the config window. The edits below show the latter.

You can configure SNMP traps using the Alert Notifications window in the maintenance utility.

Before you begin

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: Host Report All

Email Syslog **SNMP**

SNMP Agent: Enable Disable

SNMP Version: v3 ▼

Sending Trap Setting:

Registered Sending Trap Settings						
<input type="checkbox"/>	Send Trap to	User Name	Authentication		Encryption	
			Mode	Protocol	Mode	Protocol
Add Change Remove						Selected: 0

Request Authentication Setting:

Registered Request Authentication Settings						
<input type="checkbox"/>	User Name	Authentication		Encryption		
		Mode	Protocol	Mode	Protocol	
Add Change Remove						Selected: 0

System Group Information:

Storage System Name: (Max. 180 characters)

Contact: (Max. 180 characters or blank)

Location: (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074046136306530353061

Apply Cancel

5. For **Notification Alert**, select one of the following:
 - **All** (Sends alerts of all SIMs.)
 - **Host Report** (Sends alerts only of SIMs that report to hosts. Alert destinations are common to Syslog, SNMP, and Email.)
6. Confirm the settings, and then click **Apply**.

Managing SNMP trap notification

Use the procedure for the SNMP version you use to set SNMP trap notification. The items to specify are different depending on the SNMP version.

Adding trap notification for SNMP v1 and v2c

Follow this procedure to add IP addresses and communities to trap notification for SNMP versions v1 and v2c.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v1** or **v2c**.
7. Under **Registered Sending Trap Settings**, click **Add**.
8. In the **Add Sending Trap Setting** window, under **Community**, complete one of the following:
 - If you select an existing community, uncheck the **New** checkbox, and then select from the list of existing community names.
 - If you add a new community, check the **New** check box, and then enter a community name.

You can enter up to 180 letters, numbers, and symbols, except the following:

" \ ; : , * ? < > | / ^ & % ' "

Do not use a space at the beginning or end of the name.

9. Under **Send Trap To**, complete the following:
 - To enter a new IP address, check the **New** check box. Select **IPv4** or **IPv6** for the version of the IP address, and then enter an IP address.
 - To use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.
 - To add more IP addresses, click **Add IP Address** to add input fields.
 - To delete an IP address from **Send Trap to**, click the - button to delete the IP address.



Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF, inclusive. The default form of the IPv6 address can be specified.

10. Click **OK**.
The IP address and community you entered are added to the **Registered Sending Trap Settings** table.
11. Confirm the settings, and then click **Apply**.

Adding trap notification for SNMP v3

Follow this procedure to add IP addresses and users to trap notification for SNMP v3.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Sending Trap Settings**, click **Add**.
8. In the **Add Sending Trap Setting** window, under **Send Trap To**, select **IPv4** or **IPv6** and enter an IP address.



Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF, inclusive. The default form of the IPv6 address can be specified.

9. Under **User Name**, enter a user name.



Note:

If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.

- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

You can enter up to 32 letters, numbers, and symbols, except the following:

" \ ; : , * ? < > | / ^ & %

Do not use a space at the beginning or end of the name.

10. Under **Authentication**, select whether to **Enable** or **Disable** authentication. If you select **Enable**, complete the following steps:
 - a. For **Protocol**, select an authentication type.
 - b. For **Password**, enter a password.

11. Under **Encryption**, select whether to **Enable** or **Disable** encryption.
If you select **Enable**, complete the following steps:
 - a. For **Protocol**, select an encryption type.
 - b. For **Key**, enter a key.
 - c. For **Re-enter Key**, enter the same key for confirmation.
12. Click **OK**.
The IP address and user you entered are added to the **Registered Sending Trap Settings** table.
13. Confirm the settings, and then click **Apply**.

Changing trap notification for SNMP v1 and v2c

Follow this procedure to change the IP addresses and communities for trap notification for SNMP versions v1 and v2c.

Before you begin

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v1** or **v2c**.
7. Under **Registered Sending Trap Settings**, select a trap setting that you want to change, and then click **Change**.
8. In the **Change Sending Trap Setting** window, under **Community**, enter a community name.

You can enter up to 180 letters, numbers, and symbols, except the following:

" \ ; : , * ? < > | / ^ & % '

Do not use a space at the beginning or end of the name.

9. Under **Send Trap To**, complete the following:
 - If you enter a new IP address, click **Add IP Address** to add input fields. Check the **New** check box, and then select **IPv4** or **IPv6** for the version of the IP address. Enter an IP address.
 - If you use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.
 - If you delete an IP address from **Send Trap to**, click the - button to delete the IP address.

10. Click **OK**.
The IP address and community that you entered are changed to the **Registered Sending Trap Settings** table.
11. Confirm the settings, and then click **Apply**.

Changing trap notification for SNMP v3

Follow this procedure to change the IP addresses and users for SNMP v3 trap notification.

Before you begin

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Sending Trap Settings**, select a trap setting that you want to change, and then click **Change**.
8. In the **Change Sending Trap Setting** window, under **Send Trap To**, select **IPv4** or **IPv6** and enter an IP address.



Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF, inclusive. The default form of the IPv6 address can be specified.

9. Under **User Name**, enter a user name.



Note:

If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.

- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

You can enter up to 32 letters, numbers, and symbols, except the following:

" \ ; : , * ? < > | / ^ & %

Do not use a space at the beginning or end of the name.

10. Under **Authentication**, select whether to **Enable** or **Disable** authentication.
If you select **Enable**, complete the following steps:
 - a. For **Protocol**, select an authentication type.
 - b. If you change your password, check the **Change Password** checkbox and then enter a password.
11. Under **Encryption**, select whether to **Enable** or **Disable** encryption.
If you select **Enable**, complete the following steps:
 - a. For **Protocol**, select an encryption type.
 - b. If you change a key, check the **Change Key** checkbox and then enter a key.
 - c. For **Re-enter Key**, enter the same key for confirmation.
12. Click **OK**.
The IP address and user you entered are changed to the **Registered Sending Trap Settings** table.
13. Confirm the settings, and then click **Apply**.

Deleting SNMP trap notification

Follow this procedure to delete IP addresses and communities or users from SNMP trap notification.

Before you begin

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select your SNMP version.
7. Under **Registered Sending Trap Settings**, select one or more specific combinations of IP address and community or user, and then click **Delete**.
8. Confirm the settings, and then click **Apply**.

Managing SNMP request authentication

Use the procedure for the SNMP version you use to set SNMP request authentication. The items to specify are different depending on the SNMP version.

Adding request authentication for SNMP v1 and v2c

Follow this procedure to add IP addresses and communities for request authentication for SNMP versions v1 and v2c.

Before you begin

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v1** or **v2c**.
7. Under **Registered Request Authentication Settings**, click **Add**.
8. In the **Add Request Authentication Setting** window, under **Community**, complete one of the following:
 - If you add a new community, check the **New** check box, and then enter a community name.
 - If you select an existing community, uncheck the **New** check box, and then select from the list of existing community names.

You can enter up to 180 letters, numbers, and symbols, except the following:

" \ ; : , * ? < > | / ^ & % ' "

Do not use a space at the beginning or end of the name.

9. Under **Request Permitted**, complete the following:
 - If you want to allow REQUEST operations from all managers, select the **All** check box.
 - If you want to allow REQUEST operations only from specified managers, select **IPv4** or **IPv6** and enter an IP address, or select from the list of existing IP addresses.
 - If you enter a new IP address, check the **New** check box. Select **IPv4** or **IPv6** for the version of the IP address, and then enter an IP address.
 - If you use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.

- If you add more IP addresses, click **Add IP Address** to add input fields.
- If you delete an IP address from **Request Permitted**, click the - button to delete the IP address.



Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF, inclusive. The default form of the IPv6 address can be specified.

10. Click **OK**
The community and IP address that you entered are added to the **Registered Request Authentication Settings** table.
11. Confirm the settings, and then click **Apply**.

Adding request authentication for SNMP v3

Follow this procedure to add IP addresses and users for SNMP v3 request authentication.

Before you begin

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Request Authentication Settings**, click **Add**.
8. In the **Add Request Authentication Setting** window, under **User Name**, enter a user name.



Note:

If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.

- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

9. Under **Request Permitted**, complete the following:
 - If you want to allow REQUEST operations from all managers, select the **All** check box.
 - If you want to allow REQUEST operations only from specified managers, select **IPv4** or **IPv6** and enter an IP address, or select from the list of existing IP addresses.
 - If you enter a new IP address, click **Add IP Address** to add input fields, and then check the **New** check box. Select **IPv4** or **IPv6** for the version of the IP address, and then enter an IP address.
 - If you use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.
 - If you delete an IP address from **Request Permitted**, click the - button to delete the IP address.



Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF, inclusive. The default form of the IPv6 address can be specified.

10. Click **OK**.
The community and IP address that you entered are changed to the **Registered Request Authentication Settings** table.
11. Confirm the settings, and then click **Apply**.

Changing request authentication for SNMP v3

Follow this procedure to change IP addresses and users for SNMP v3 request authentication.

Before you begin

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Request Authentication Settings**, select an authentication setting that you want to change, and then click **Change**.
8. In the **Change Request Authentication Setting** window, under **User Name**, enter a user name.

**Note:**

If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.

- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

You can enter up to 32 letters, numbers, and symbols, except the following:

" \ ; : , * ? < > | / ^ & %

Do not use a space at the beginning or end of the name.

9. Under **Authentication**, select whether to **Enable** or **Disable** authentication.

If you select **Enable**, complete the following steps:

 - a. For **Protocol**, select an authentication type.
 - b. If you change your password, check the **Change Password** checkbox, and then enter a password.
10. Under **Encryption**, select whether to **Enable** or **Disable** encryption.

If you select **Enable**, complete the following steps:

 - a. For **Protocol**, select an encryption type.
 - b. If you change a key, check the **Change Key** checkbox, and then enter a key.
 - c. For **Re-enter Key**, enter the same key for confirmation.
11. Click **OK**.

The user you entered is changed to the **Registered Request Authentication Settings** table.
12. Confirm the settings, and then click **Apply**.

Deleting SNMP request authentication

Follow this procedure to delete IP addresses and communities or users from request authentication.

Before you begin

You must have the Storage Administrator (the Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select your SNMP version.
7. Under **Registered Request Authentication Settings**, select one or more specific combinations of IP address and community or user, and then click **Delete**.
8. Confirm the settings, and then click **Apply**.

Testing SNMP trap reports

Follow this procedure to test SNMP trap reporting by sending a test trap.

Before you begin

An IP address and community have been added in the **Set Up Alert Notifications** window.

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. Select the **SNMP** tab.
4. Click **Send Test SNMP Trap**.
Reports the test SNMP trap to the community or user registered in the storage system. Reports the events registered in the storage system instead of the events that are set on the **SNMP** tab. If you want to test the events set on the **SNMP** tab, click **Finish** and apply to the storage system, and then report the test SNMP trap.
5. Verify whether the SNMP trap report (reference code 7fffff) is received by the SNMP manager that has the IP address specified for **Sending Trap Setting** in the **Alert Notifications** window.

Chapter 3: SNMP supported MIBs

This chapter describes the standard and extension MIB specifications, and trap configuration.

SNMP Agent failure report trap contents

A standard extension trap protocol data unit (PDU) includes the product number of the device that experienced the failure, the device nickname, and a failure reference code. A failure report trap contains additional information about the failure, such as the area, date, and time of the failure.

If you obtain the information with the `GetRequest` command, access the MIB by using the product number of the device as an index.

The following table shows the failure report trap.

Name	Object identifier	Type	Description
eventTrapSerial Number	.1.3.6.1.4.1.116.5.11.4.2.1	INTEGER	The product number of the device that experienced the failure.
eventTrapNickname	.1.3.6.1.4.1.116.5.11.4.2.2	DisplayString	The device nickname "HM850" is displayed.
eventTrapREFERENCE	.1.3.6.1.4.1.116.5.11.4.2.3	DisplayString	The failure reference code.
eventTrapPartSID	.1.3.6.1.4.1.116.5.11.4.2.4	OBJECT IDENTIFIER	The area where the failure occurred.*
eventTrapDate	.1.3.6.1.4.1.116.5.11.4.2.5	DisplayString	Failure occurrence date.
eventTrapTime	.1.3.6.1.4.1.116.5.11.4.2.6	DisplayString	Failure occurrence time.

Name	Object identifier	Type	Description
eventTrapDescription	.1.3.6.1.4.1.116.5.11.4.2.7	DisplayString	Detailed information of a failure.
*The object identifier for a failure in a storage system processor would be .1.3.6.1.4.1.116.5.11.4.1.1.6.1.2.			

SNMP Agent extension trap types

SNMP Agent extension trap types are set according to the severity. The character strings following "RaidEventUser" indicate their severity.

The following table describes the SNMP Agent extension trap types.

Specific Trap Code	Trap	Description
1	RaidEventUserAcute	All operations in a storage system stopped.
2	RaidEventUserSerious	Operation in a component where a failure occurred stopped.
3	RaidEventUserModerate	Partial failure.
4	RaidEventUserService	Minor failure.

Standard MIB specifications

MIBs supported by SNMP Agent

SNMP Agent supports a limited number of MIBs. If you send a GET request for an object (MIB) that is not supported, you will receive `NoSuchName` as a GET RESPONSE.

The following table lists MIBs and indicates whether they are supported.

MIB	Support	
Standard MIB: MIB-II	system group	Yes
	interface group	No

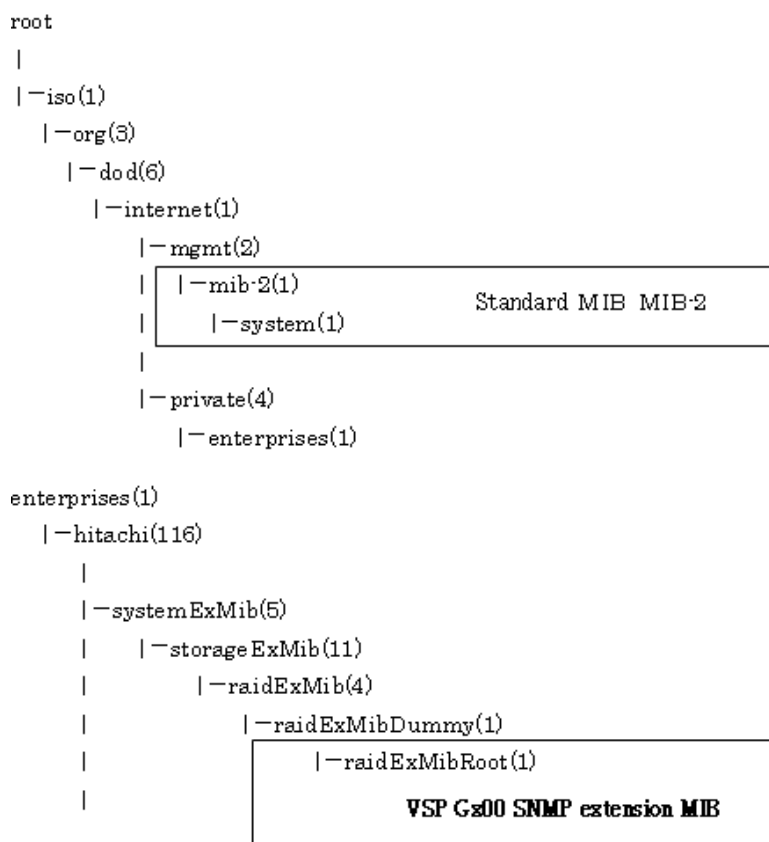
MIB		Support
	at group	
	ip group	
	icmp group	
	tcp group	
	udp group	
	egp group	
	snmp group	
Extension MIB		Yes

SNMP Agent MIB access mode

The access mode for MIB in all communities is read only. If you send a GET request for a SET REQUEST operation, you will receive `NoSuchName` as a RESPONSE.

Example object identifier system

The following figure shows an example object system supported by SNMP Agent.



MIB mounting specifications supported by SNMP Agent

SNMP Agent supports two MIB mounting specifications.

The supported MIB mounting specifications are as follows:

- mgmt OBJECT IDENTIFIER ::= {iso(1) org(3) dod(6) internet(1) 2 }
- mib-2 OBJECT IDENTIFIER ::= {mgmt 1}

An SNMP Agent mounts only system groups in mib-2, as shown in the following table.

Name	Description	Mounted value
sysObjectID {system 2}	This is the product identification number.	Fixed value. See Object identifier system (on page 31) . 1.3.6.1.4.1.116.3.11.4.1.1
sysUpTime {system 3}	An accumulated time from an SNMP agent.	Unit: 100 ms
sysContact {system 4}	A manager who manages an agent or a contact address.	Maximum 180 characters in an ASCII characters string. Input by a user from an SNMP setting window.*

Name	Description	Mounted value
sysName {system 5}	The name of an agent manager	Maximum 180 characters in an ASCII characters string. Input by a user from an SNMP setting window.*
sysLocation {system 6}	An agent setup location.	Maximum 180 characters in an ASCII characters string. Input by a user from an SNMP setting window.*
sysService {system 7}	Value indicating a service.	Fixed value 76 (decimal)
*The following symbols cannot be used: \, / ; * ? " < > & % ^		

Extension MIB specifications

Extension MIB configuration

The following shows the extension MIB object system for the storage system.

```
raidExMibRoot(1)
├-raidExMibName(1)      Maintenance utility product name
├-raidExMibVersion(2)   Maintenance utility firmware version
├-raidExMibAgentVersion(3) Extension MIB internal version
├-raidExMibDkcCount(4)  Number of DKC
├-raidExMibRaidListTable(5) List of DKC
├-raidExMibDKCHWTable(6) Disk control device information
├-raidExMibDKUHWTable(7) Disk device information
├-raidExMibTrapListTable(8) Error information list
```

The following figures show an example extension MIB configuration.

```
├- enterprises(1)
  └- hitachi(116)
    |
    └- systemExMib(5)
      └- storageExMib(11)
        └- raidExMib(4)
          └- raidExMibDummy(1)
            └- raidExMibRoot(1) → ①
```

```

①→  |- raidExMibRoot(1)
      |- raidExMibName(1)
      |- raidExMibVersion(2)
      |- raidExMibAgentVersion(3)
      |- raidExMibDkcCount(4)
      |- raidExMibRaidListTable(5)
      |   |- raidExMibRaidListEntry(1)
      |     |- raidlistSerialNumber(1)
      |     |- raidlistMibNickName(2)
      |     |- raidlistDKCMainVersion(3)
      |     |- raidlistDKCProductName(4)
      |   |- raidExMibDKCHWTable(6)
      |     |- raidExMibDKCHWEntry(1)
      |       |- dkcRaidListIndexSerialNumber(1)
      |       |- dkchWProcessor(2)
      |       |- dkchWCSW(3)
      |       |- dkchWCache(4)
      |       |- dkchWSM(5)
      |       |- dkchWPS(6)
      |       |- dkchWBattery(7)
      |       |- dkchWFan(8)
      |       |- dkchWEnvironment(9)
      |
      |→②

```

```

②→  |- raidExMibDKUHWTable(7)
      |   |- raidExMibDKUHWEEntry(1)
      |     |- dkuRaidListIndexSerialNumber(1)
      |     |- dkuHWPS(2)
      |     |- dkuHWFan(3)
      |     |- dkuHWEEnvironment(4)
      |     |- dkuHWDrive(5)
      |   |- raidExMibTrapListTable(8)
      |     |- raidExMibTrapListEntry(1)
      |       |- eventListIndexSerialNumber(1)
      |       |- eventListNickName(2)
      |       |- eventListIndexRecorderNo(3)
      |       |- eventListREFCODE(4)
      |       |- eventListDate(5)
      |       |- eventListTime(6)
      |       |- eventListDescription(7)

```

raidExMibName

raidExMibName indicates the product name.

```
raidExMibName          OBJECT-TYPE
SYNTAX                 DisplayString
ACCESS                 read-only
STATUS                 mandatory
DESCRIPTION             "product name."
 ::= { raidExMibRoot 1 }
```

raidExMibVersion

raidExMibVersion indicates the maintenance utility firmware version.

```
raidExMibVersion       OBJECT-TYPE
SYNTAX                 DisplayString
ACCESS                 read-only
STATUS                 mandatory
DESCRIPTION             "GUM firmware version."
 ::= { raidExMibRoot 2 }
```

raidExMibAgentVersion

raidExMibAgentVersion indicates the internal version of the extension MIB.

```
raidExMibAgentVersion OBJECT-TYPE
SYNTAX                 DisplayString
ACCESS                 read-only
STATUS                 mandatory
DESCRIPTION             "Extension agent version."
 ::= { raidExMibRoot 3 }
```

raidExMibDkcCount

raidExMibDkcCount suggests the number of a storage system.

```
raidExMibDkcCount      OBJECT TYPE
SYNTAX                 INTEGER
ACCESS                 read-only
STATUS                 mandatory
DESCRIPTION             "Number of DKC"
 ::= { raidExMibRoot 4 }
```

raidExMibRaidListTable

raidExMibRaidListTable indicates the storage system.

```

raidExMibRaidListTable OBJECT TYPE
SYNTAX                  SEQUENCE OF raidExMibRaidListEntry
ACCESS                  not-accessible
STATUS                  mandatory
DESCRIPTION             "List of DKC."
 ::= { raidExMibRoot 5}

raidExMibRaidListEntry OBJECT TYPE
SYNTAX                  RaidExMibRaidListEntry
ACCESS                  not-accessible
STATUS                  mandatory
DESCRIPTION             "Entry of DKC list."
INDEX                   { raidlistSerialNumber }
 ::= { raidExMibRaidListTable 1}

```

The following table lists the information displayed for each storage system

Name	Type	Description	Mounted value	Attribute
raidlistSerialNumber ::=RaidExMibRaidListEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only
raidlistMibNickName ::=RaidExMibRaidListEntry(2)	DisplayString	Storage system nickname.	(Max. 18 characters)	read-only
raidlistDKCMainVersion ::=RaidExMibRaidListEntry(3)	DisplayString	Software version.	Max. 14 characters	read-only
raidlistDKCProductName ::=RaidExMibRaidListEntry(4)	DisplayString	Storage system product type.	7 characters*	read-only
*HM850 will be used as storage system product type raidlistDKCProductName.				

raidExMibDKCHWTable

raidExMibDKCHWTable indicates the status of the storage system components.

```

raidExMibDKCHWTable OBJECT TYPE
SYNTAX                SEQUENCE OF RaidExMibDKCHWEntry
ACCESS                not-accessible
STATUS                mandatory
DESCRIPTION            "Error information of the DKC."
 ::= { raidExMibRoot 6}

raidExMibDKCHWEntry OBJECT TYPE
SYNTAX                RaidExMibDKCHWEntry
ACCESS                not-accessible
STATUS                mandatory
DESCRIPTION            "Entry of DKC information."
INDEX                 {dkcRaidListIndexSerialNumber}
 ::= { raidExMibDKCHWTable 1}

```

The following table lists the information displayed for each storage system component.

Name	Type	Description	MIB value	Attribute
dkcRaidListIndexSerialNumber ::=raidExMibDKCHWEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only
dkcHWProcessor ::=raidExMibDKCHWEntry(2)	INTEGER	Status of processor.	See Note	read-only
dkcHWCSW ::=raidExMibDKCHWEntry(3)	INTEGER	This value is unused.	See Note	read-only
dkcHWCACHE ::=raidExMibDKCHWEntry(4)	INTEGER	Status of cache.	See Note	read-only
dkcHWSM ::=raidExMibDKCHWEntry(5)	INTEGER	This value is unused.	See Note	read-only
dkcHWPS ::=raidExMibDKCHWEntry(6)	INTEGER	Status of power supply.	See Note	read-only

Name	Type	Description	MIB value	Attribute
dkcHWBattery ::=raidExMibDKCHWEntry(7)	INTEGER	Status of battery.	See Note	read-only
dkcHWFan ::=raidExMibDKCHWEntry(8)	INTEGER	Status of fan.	See Note	read-only
dkcHWEEnvironment ::=raidExMibDKCHWEntry(9)	INTEGER	Information of an operational environment.	See Note	read-only
<p>Note:</p> <p>The status of each component is a single digit which shows the following:</p> <p>1: Normal.</p> <p>2: Acute failure detected.</p> <p>3: Serious failure detected.</p> <p>4: Moderate failure detected.</p> <p>5: Service failure detected.</p>				

raidExMibDKUHWTable

raidExMibDKUHWTable indicates the status of the storage system components.

```

raidExMibDKUHWTable OBJECT TYPE
SYNTAX                SEQUENCE OF RaidExMibDKUHWEntry
ACCESS                not-accessible
STATUS                mandatory
DESCRIPTION           "Error information of the DKU."
 ::= { raidExMibRoot 7 }

raidExMibDKUHWEntry OBJECT TYPE
SYNTAX                RaidExMibDKUHWEntry
ACCESS                not-accessible
STATUS                mandatory
DESCRIPTION           "Entry of DKU information."
INDEX                 { dkuRaidListIndexSerialNumber }
 ::= { raidExMibDKUHWTable 1 }

```

The following table lists the information displayed for each disk device component.

Name	Type	Description	MIB value	Attribute
dkuRaidListIndexSerialNumber ::=raidExMibDKUHWEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only
dkuHWPS ::=raidExMibDKUHWEntry(2)	INTEGER	Status of power supply.	See Note	read-only
dkuHWFan ::=raidExMibDKUHWEntry(3)	INTEGER	This value is unused.	See Note	read-only
dkuHWEEnvironment ::=raidExMibDKUHWEntry(4)	INTEGER	Status of environment monitor.	See Note	read-only
dkuHWDrive ::=raidExMibDKUHWEntry(5)	INTEGER	Status of drive.	See Note	read-only
<p>Note:</p> <p>The status of each component is a single digit which shows the following:</p> <ul style="list-style-type: none"> 1: Normal. 2: Acute failure detected. 3: Serious failure detected. 4: Moderate failure detected. 5: Service failure detected. 				

raidExMibTrapListTable

raidExMibTrapListTable shows the history of the failure traps.

```

raidExMibTrapListTable OBJECT TYPE
SYNTAX                  SEQUENCE OF RaidExMibTrapListEntry
ACCESS                  not-accessible
STATUS                  mandatory
DESCRIPTION              "Trap list table."
 ::= { raidExMibRoot 8 }

raidExMibTrapListEntry OBJECT TYPE

```

```

SYNTAX          RaidExMibTrapListEntry
ACCESS          non-accessible
STATUS         mandatory
DESCRIPTION     "Trap list table index."
INDEX          { eventListIndexSerialNumber ,
                eventListIndexRecordNo }

 ::= { raidExMibTrapListTable 1 }

```

The following table lists the information displayed for each failure.

Name	Type	Description	MIB value	Attribute
eventListIndexSerialNumber ::=raidExMibTrapListEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only
eventListNickname ::=raidExMibTrapListEntry(2)	DisplayString	Storage system nickname.	18 characters maximum	read-only
eventListIndexRecordNo ::=raidExMibTrapListEntry(3)	Counter	Number of records.	1-256	read-only
eventListREFCODE ::=raidExMibTrapListEntry(4)	DisplayString	Reference code (index).	6 characters	read-only
eventListData ::=raidExMibTrapListEntry(5)	DisplayString	Date when the failure occurred.	yyyy/mm/dd (10 characters)	read-only
eventListTime ::=raidExMibTrapListEntry(6)	DisplayString	Time when the failure occurred.	hh:mm:ss (8 characters)	read-only
eventListDescription ::=raidExMibTrapListEntry(7)	DisplayString	Detailed information about the failure.	256 characters maximum	read-only

Chapter 4: Troubleshooting

This chapter provides troubleshooting information for the Hitachi SNMP Agent.

Solving SNMP problems

This topic describes some problems that can occur with SNMP.

Problem	Causes and solutions
Information cannot be received by GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST operations.	<p>Causes:</p> <ul style="list-style-type: none">▪ An SNMP Manager IP address and community or user have not been added.▪ GUM failure occurred.▪ A network environment error occurred. <p>Solutions:</p> <ul style="list-style-type: none">▪ Add an IP address and community or user. (See Adding request authentication for SNMP v1 and v2c (on page 23) or Adding request authentication for SNMP v3 (on page 24).)▪ Restore GUM.▪ Contact your network administrator.
Trap cannot be received.	<p>Causes:</p> <ul style="list-style-type: none">▪ An SNMP Manager IP address and community or user have not been added.▪ GUM failure occurred.▪ A network environment error occurred.

Problem	Causes and solutions
	<p data-bbox="889 254 1019 281">Solutions:</p> <ul data-bbox="889 302 1398 621" style="list-style-type: none"><li data-bbox="889 302 1398 470">▪ Add an IP address and community or user. (See Adding trap notification for SNMP v1 and v2c (on page 18) or Adding trap notification for SNMP v3 (on page 19).)<li data-bbox="889 491 1133 518">▪ Enable a license.<li data-bbox="889 539 1101 567">▪ Restore GUM.<li data-bbox="889 588 1382 615">▪ Contact your network administrator.

Glossary

community name

An SNMP entity in which up to 32 names and up to 32 IP addresses can be registered.

extension trap

An error message generated by a third-party node and sent to the SNMP agent.

failure trap

An error message that indicates a problem within a managed node.

IPv4

Internet Protocol, Version 4

IPv6

Internet Protocol, Version 6

managed device

A network node on which the SNMP Agent software is installed. Using the agent, managed devices exchange node-specific information with the SNMP management software.

managed node

See managed device.

management information base (MIB)

A virtual database of objects that can be monitored by a network management system. SNMP uses standardized MIBs that allow any SNMP-based tool to monitor any device defined by a MIB file.

Simple Network Management Protocol (SNMP)

An industry-standard protocol that is used to manage and monitor network-attached devices for conditions that warrant administrative attention. The devices can include disk devices, routers, and hubs. SNMP uses Simple Gateway Management Protocol (SGMP) to manage TCP/IP gateways.

SNMP Agent

Software that is installed on the maintenance utility and responds to queries from SNMP Manager.

SNMP Manager

Software that is installed on the network management station that collects and manages information from SNMP agents installed in the managed devices on the network.

SNMP trap

An event generated by an SNMP agent from the managed resource that communicates an event, such as an error or failure.

user datagram protocol (UDP)

Software that requests data regarding the status of a managed node.

Index

A

- access mode
 - MIB 31
- adding
 - request authentication for SNMP v1 and v2c 23
 - request authentication for SNMP v3 24
 - trap notification for SNMP v1 and v2c 18
 - trap notification for SNMP v3 19
- administration guide 29
- alerts
 - editing settings 16
- architecture
 - SNMP environment 11

C

- changing
 - request authentication for SNMP v1 and v2c 25
 - request authentication for SNMP v3 26
 - trap notification for SNMP v1 and v2c 20
 - trap notification for SNMP v3 21
- cold trap function, troubleshooting 41
- components
 - storage system 14
- configuration
 - extension MIB 33
 - SNMP Agent 11
- configuring
 - alert settings 16

D

- definition files, trouble inputting 41
- deleting
 - SNMP request authentication 27
 - SNMP trap notification 22

E

- editing
 - alert settings 16
- environment

- environment (*continued*)
 - SNMP 11
- errors
 - REQUEST operation 13
 - SNMP Agent, reported by 13
- extension trap
 - supported types 30
- extension traps
 - protocol data unit 29

F

- failure
 - trap report 29

I

- interaction
 - SNMP Manager and SNMP Agent 10
- introduction 10

M

- Management Information Base
 - overview 11
- MIB
 - access mode 31
 - configuration
 - MIB 31
 - extension configuration 33
 - extension specifications 33
 - mounting specifications 32
 - object identifier system 31
 - overview 11
 - raidExMibAgentVersion 35
 - raidExMibDkcCount 35
 - raidExMibDKCHWTable 37
 - raidExMibDKUHWTable 38
 - raidExMibName 35
 - raidExMibRaidListTable 36
 - raidExMibTrapListTable 39
 - raidExMibVersion 35

- MIB (*continued*)
 - supported types 30
- MIB definition files, trouble inputting 41
- mounting
 - MIB specifications 32
 - system groups 32

O

- objects
 - identifier system 31
- operations
 - REQUEST 13
 - SNMP Agent 13
- overview
 - Management Information Base 11
 - MIB 11
 - Simple Network Management Protocol 10
 - SNMP 10
 - SNMP Agent 12
 - SNMP Manager 10

P

- PDU 29
- protocol data unit 29

R

- raidExMibAgentVersion 35
- raidExMibDkcCount 35
- raidExMibDKCHWTable 37
- raidExMibDKUHWTable 38
- raidExMibName 35
- raidExMibRaidListTable 36
- raidExMibTrapListTable 39
- raidExMibVersion 35
- reports
 - testing, for SNMP traps 28
- request authentication
 - deleting 27
- requests
 - adding authentication for SNMP v1 and v2c 23
 - adding authentication for SNMP v3 24
 - changing authentication for SNMP v1 and v2c 25
 - changing authentication for SNMP v3 26

S

- security function, troubleshooting 41
- Simple Network Management Protocol
 - overview 10

- SNMP
 - architecture 11
 - environment 11
 - interaction of manager and agent 10
 - overview 10
 - traps 12
- SNMP agent 29
- SNMP Agent
 - configuration 11
 - environment 11
 - errors reported 13
 - operations, types of 13
 - overview 12
 - traps 12
- SNMP Manager
 - components, status of 14
 - environment 11
 - overview 10
 - status of components 14
- specifications
 - extension MIB 33
 - MIB mounting 32
- status
 - storage system components 14
- system groups
 - mounting 32

T

- testing
 - SNMP trap report 28
- trap notification
 - deleting 22
- traps
 - failure report 29
 - SNMP 12
 - SNMP Agent 12
 - SNMP v1 and v2c, adding notification for 18
 - SNMP v1 and v2c, changing notification for 20
 - SNMP v3, adding notification for 19
 - SNMP v3, changing notification for 21
 - supported types 30
 - testing, of SNMP trap reports 28
 - triggers 12
- troubleshooting
 - abnormal response to SNMP commands 41
 - inputting MIB definition files 41
 - SNMP cold trap function 41
 - SNMP security function 41

V

Virtual Storage Platform F350 [29](#)
Virtual Storage Platform F370 [29](#)
Virtual Storage Platform F700 [29](#)
Virtual Storage Platform F900 [29](#)
Virtual Storage Platform G350 [29](#)
Virtual Storage Platform G370 [29](#)
Virtual Storage Platform G700 [29](#)
Virtual Storage Platform G900 [29](#)
VSP F350 [29](#)
VSP F370 [29](#)
VSP F700 [29](#)
VSP F900 [29](#)
VSP Fx00 models [29](#)
VSP G350 [29](#)
VSP G370 [29](#)
VSP G700 [29](#)
VSP G900 [29](#)
VSP Gx00 models [29](#)

Hitachi Vantara Corporation



Corporate Headquarters

2845 Lafayette Street

Santa Clara, CA 95050-2639 USA

www.HitachiVantara.com | community.HitachiVantara.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

Europe, Middle East, and Africa: +44 (0) 1753 618000 or info@emea@hitachivantara.com

Asia Pacific: + 852 3189 7900 or info.marketing.apac@hitachivantara.com